Б.П. Русин , Я.Ю. Варецький

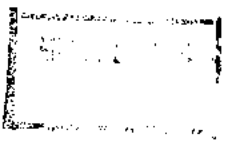
БІОМЕТРИЧНА АУТЕНТИФІКАЦІЯ ТА КРИПТОГРАФІЧНИЙ ЗАХИСТ

КОЛО

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
ФІЗИКО-МЕХАНІЧНИЙ ІНСТИТУТ ІМ. Г.В. КАРПЕНКА

Б. П. РУСИН, Я. Ю. ВАРЕЦЬКИЙ

БІОМЕТРИЧНА АУТЕНТИФІКАЦІЯ ТА КРИПТОГРАФІЧНИЙ ЗАХИСТ



ЛЬВІВ
2007

УДК 004.932.72'1 + 519.711.3

Русин Б. П., Варецький Я. Ю. **Біометрична аутентифікація та криптографічний захист.** – Львів: Коло, 2007. – 287 с.

Монографія присвячена розробці нових підходів до побудови біометричних систем аутентифікації та криптографічного захисту. Проведено порівняльний аналіз існуючих підходів до вирішення проблем біометричної ідентифікації та захисту криптографічних ключів. Запропоновано новий метод розпізнавання мовних сигналів. Приділено увагу оптимальному вибору методів компресії мовних сигналів для задач розпізнавання. Проведено дослідження алгоритмів компресії стосовно можливості оптимального вибору і використання їх в задачах розпізнавання мови.

Розроблено нові системи інформативних ознак зображень відбитків папілярного узору та методи їх ідентифікації. Математично описано спотворення, наведено параметри ідеального неспотвореного зображення папілярного узору, що дало змогу розробити нові та удосконалити існуючі методи обробки. Розроблено нову багатоетапну процедуру ідентифікації, етапи якої комбінуються адаптивними до якості вхідного зображення ітераційними та лінійними порогами, що дозволило компенсувати недоліки й зберегти переваги розроблених систем інформативних ознак.

Запропоновано математичну модель процесу захисту криптографічних ключів, який використовує біометричні ознаки людини. Створено математичну модель біометричного екстрактора випадкових величин, що дало змогу виділити важливі для процесу захисту параметри (втрата ентропії криптографічного ключа, стійкість методу захисту, імовірнісні характеристики ідентифікації). Створено метод та алгоритми блокування та розблокування криптографічних ключів, нечутливі до визначеного рівня змін у біометричних даних. Розроблено нову структурну схему клієнт-серверної системи з криптографічним захистом інформації.

Монографія призначена для наукових співробітників та інженерно-технічних працівників, що займаються розробкою методів та побудовою систем біометричної аутентифікації та криптографічного захисту. Вона може бути також корисна аспірантам та студентам вузів, які займаються проблемами обробки та розпізнавання зображень, систем захисту інформації та криміналістики.

Іл. 122. Табл. 10. Список бібліогр.: 266 назв.

Рецензенти: д.т.н., проф. Дідковський В.С.
д.т.н., проф. Рибальський О.В.

ISBN 978-966-7996-52-9

ЗМІСТ

ПЕРЕЛІК ОСНОВНИХ СКОРОЧЕНЬ 6

ВСТУП 8

РОЗДІЛ 1. ОСНОВИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ 13

1.1. Основні поняття 13
1.2. Системи біометричної аутентифікації 15
1.3. Методологія розпізнавання людини по голосу 21
1.4. Методологія розпізнавання людини за відбитками пальців 52
1.4.1. Особливості попередньої обробки в системах ідентифікації 60
1.4.2. Способи формування зображення 60
1.4.3. Алгоритми попередньої обробки 64
1.4.4. Методи попередньої обробки 68
1.4.5. Інформативні ознаки й методи розпізнавання 73
1.4.6. Кореляційні методи 84
1.4.7. Комбіновані методи 86
1.5. Огляд криптографічних засобів 86
1.5.1. Стійкість класичних криптографічних алгоритмів 96
1.5.2. Біометричні системи 100

РОЗДІЛ 2. ГОЛОСОВА АУТЕНТИФІКАЦІЯ 109

2.1. Визначення інформативних ознак розпізнавання мовних сигналів 109
2.2. Алгоритм визначення ознак розпізнавання мовних сигналів у біометричних системах 115
2.3.Оцінка вірогідності роботи системи розпізнавання людини по голосу на основі диференціальних імовірностей правильного (неправильного) розпізнавання 121
2.4. Методи компресії мовних сигналів 123
2.4.1. Базиси ортогональних функцій 125
2.4.2. Ортогональні перетворення на основі теореми Карунена - Лоєва 130
2.4.3. Компресія з виключенням сукупності мінімальних коефіцієнтів розкладу 138
2.4.4. Критерії оцінки якості компресії 141

РОЗДІЛ 3. ДАКТИЛОСКОПІЧНА АУТЕНТИФІКАЦІЯ 147

3.1. Спотворення, характеристики й особливості дактилоскопічних зображень 147
3.2. Методи попередньої обробки 154
3.2.1. Сегментація дактилоскопічних зображень 154
3.2.2. Квазіоптимальна фільтрація 155
3.2.3. Оцінка зображення локальної орієнтації 160
3.2.4. Локальна нормалізація яскравості 163
3.2.5. Оцінка зображення локального періоду 164
3.2.6. Обробка спрямованим фільтром Габора 165
3.2.7. Перетворення гістограми 169
3.3. Критерії застосування двоетапного методу розпізнавання 169
3.4. Вибір зони опису зображення 173
3.5. Система інформативних ознак зображення локальної орієнтації 174
3.6. Система спектральних інформативних ознак 176
3.7. Порівняння відбитків на основі системи інформативних ознак зображення локальної орієнтації 178
3.8. Порівняння відбитків на основі системи спектральних ознак і кореляційного методу 185
3.9. Особливості реалізації попередньої обробки дактилоскопічних зображень 191
3.9.1. Застосування спектральних ознак і кореляційного методу порівняння у БІС та АДІС 195
3.9.2. Етап запису векторів ознак у базу даних 199
3.9.3. Етап ідентифікації 201
3.9.4. Експериментальне визначення параметрів адаптивних порогів ідентифікації 214
3.9.5. Результати тестування 218

РОЗДІЛ 4. БІОМЕТРИЧНИЙ ЗАХИСТ КЛЮЧІВ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ 221

4.1. Біометричний екстрактор 221
4.1.1. Екстрактор випадкових величин 222
4.1.2. Біометричний екстрактор та біометричний ідентифікатор 224
4.1.3. Біометричний екстрактор з біометричного ідентифікатора та чіткого екстрактора 226
4.2. Конструкції біометричного екстрактора 226
4.2.1. Конструкція для віддалі Хемінга 227
4.2.2. Конструкція для різниці множин 228
4.2.3. Оцінка верхньої межі втрати ентропії біометричного ідентифікатора та біометричного екстрактора 236

4.3. ДАКТИЛОСКОПІЧНИЙ ЗАХИСТ КРИПТОГРАФІЧНИХ КЛЮЧІВ **238**
4.3.1. АНАЛІЗ КРИПТОГРАФІЧНОЇ СТІЙКОСТІ 240
4.3.2. АНАЛІЗ ІМОВІРНІСНИХ ХАРАКТЕРИСТИК 250
4.4. ОСОБЛИВОСТІ РЕАЛІЗАЦІЇ ЗВ'ЯЗУВАННЯ КРИПТОГРАФІЧНИХ КЛЮЧІВ З ДАКТИЛОСКОПІЧНИМИ ДАНИМИ **254**
4.4.1. ГЕНЕРАЦІЯ КЛЮЧА 254
4.4.2. СТВОРЕННЯ МНОЖИНИ БЛОКУВАННЯ 258
4.4.3. БЛОКУВАННЯ КРИПТОГРАФІЧНОГО КЛЮЧА 260
4.4.4. РОЗБЛОКУВАННЯ КРИПТОГРАФІЧНОГО КЛЮЧА ТА ОЦІНКА ЕФЕКТИВНОСТІ 264

ЛІТЕРАТУРА **269**

ПЕРЕЛІК ОСНОВНИХ СКОРОЧЕНЬ

АДІС – автоматизована дактилоскопічна ідентифікаційна система
АЦП – аналого-цифровий перетворювач
АЧХ – амплітудно-частотна характеристика
БД – база даних
БІС – біометрична ідентифікаційна система
БОФ – базис ортогональних функцій
БР – багатозначні розв'язки
БЧХ – коди Боуза-Чоудхурі-Хоквінгема
ВЧ – високочастотний
ГВЧ – генератор випадкових чисел
ДБС – дактилоскопічні та біометричні системи
ДП – динамічне програмування
ДСК – декартова система координат
І – ієрархія
ІБР – ієрархія багатозначних розв'язків
ІВС – інформаційно-вимірювальні системи
ІКДП – ієрархія композиції динамічного програмування
ІНІ – імовірність неправильної ідентифікації
ІНН – імовірність неправильної неідентифікації
ІС – інформаційна система
ІХ – імпульсна характеристика
К – композиція
КДП – композиції динамічного програмування
ККП – код корекції помилок
НЧ – низькочастотний

ОШПФ – обернене швидке перетворення Фур'є

ПММ – приховані марковські моделі

ПОЗ – попередня обробка зображень

РСК – код Ріда-Соломона

С/СП – відношення сигнал/спотворення

СКВ – середньоквадратичне відхилення

СРКР – середньостатистичний рівень коефіцієнтів розкладу

СЧ – середньочастотний

ЦСК – циліндрична система координат

ШВП – швидке вейвлет-перетворення

ШНМ – штучні нейронні мережі

ШПФ – швидке перетворення Фур'є

ВСТУП

Стрімкий розвиток інформаційних технологій, широке застосування інформаційних систем для вирішення прикладних задач у будь-якій галузі, необхідність використання локальних та глобальних мереж зв'язку спричинили зростання уваги до проблем захисту інформації. Основні підстави зацікавлення питаннями безпеки інформації – розповсюдження інформаційних технологій у бізнесі, розширення глобальної мережі Internet, активне використання паралельних та розподілених обчислень. У 2004 році фінансові втрати 255 компаній та корпорацій через правопорушення з використанням інформаційних систем збільшилися на 40% та склали $ 192 022 000. Зокрема, за даними Computer Security Institute (США), 72 компанії втратили за рік тільки внаслідок саботажу даних та комп'ютерних мереж $ 42 022 000. Із року в рік фіксується лише ріст втрат з аналогічних підстав. Витрати на захист інформації складають часом до половини вартості комп'ютерної системи.

Використання науково обгрунтованих методів захисту конфіденційної інформації, забезпечення її цілісності та достовірності уможливлює надійне функціонування складних інформаційних систем (ІС) та сервісів. Подібні системи повинні бути, з однієї сторони, доведено надійними, а з іншої – якомога простішими у користуванні. Тобто складність у користуванні системою легітимним користувачем повинна бути мінімальною, нелегітимним – максимальною. На сьогоднішній день провідним напрямком розвитку таких засобів є застосування систем захисту з ланками біометричної аутентифікації.

Аутентифікація особи, загалом, означає зіставлення невідомого індивідуума з наявною про нього інформацією. Аутентифікація особи в сучасному суспільстві відбувається декілька разів на день. До неї вже так звикли, що й не помічаємо. Її проводять за документом, що посвідчує особу, підписом у касі або банку, візуально під час зустрічі, за голосом по телефону і т.д. У ІС практично до кінця 90-х років основним способом персоніфікації користувача було надання мережевого імені та пароля. Справедливості заради потрібно відзначити, що подібного підходу, як і раніше, дотримуються досі в багатьох установах і організаціях. Слабкі місця подібних систем добре відомі: паролі забувають, зберігають у невідповідному місці, нарешті, їх можна просто вкрасти [167]. Деякі користувачі записують пароль на папері й тримають ці записи поруч зі своїми робочими станціями. Як повідомляють групи інформаційних технологій багатьох компаній,

більша частина дзвінків у службу підтримки пов'язана із забутими паролями або паролями, які втратили силу. Адже відомо, що систему можна обдурити, використавши чуже ім'я. Для цього необхідно лише знати ідентифікуючу інформацію, якою, з погляду системи безпеки, володіє одна - єдина людина. Зловмисник, видавши себе за співробітника компанії, одержує у своє розпорядження всі ресурси, доступні даному користувачеві відповідно до його повноважень і посадових обов'язків. Результатом можуть стати різні протиправні дії, починаючи від крадіжки інформації й закінчуючи виводом із ладу всієї ІС.

Розробники традиційних пристроїв аутентифікації вже зіштовхнулися з тим, що стандартні методи багато в чому застаріли. Проблема, зокрема, полягає у тому, що загальноприйнятий поділ на методи контролю фізичного доступу й методи контролю доступу до інформації є таким, що не відповідає дійсності. Адже для одержання доступу до сервера зовсім не обов'язково входити в приміщення, де він розташований. Причиною є всеосяжна концепція розподілених обчислень, яка поєднує й технологію клієнт-сервер, й Інтернет. Для вирішення цієї проблеми потрібні радикально нові методи, засновані на новій ідеології.

Чи є вихід із цієї ситуації? Виявляється, є, і вже давно. Просто для доступу до системи потрібно застосовувати такі методи аутентифікації, які не працюють у відриві від їхнього носія. Цій вимозі відповідають біометричні характеристики людського організму. Сучасні біометричні технології дозволяють ідентифікувати особистість за фізіологічними і психологічними ознаками. Системи на базі подібних технологій мають кращі ідентифікаційні можливості, ніж сукупність широковживаних засобів ідентифікації: секретний код, ключ, підпис, документ тощо.

Яка ж мета розробників таких систем? Вона одна – спростити системи захисту з одночасним покращанням їх ідентифікаційних можливостей. Це можна зробити, замінивши всі існуючі ідентифікатори: картку з магнітною стрічкою або мікросхемою, коди, паролі, ключі, підпис та інші, - одним універсальним, який не можна забути, загубити, віддати, вкрасти і який завжди є при собі.

Системи біометричної аутентифікації в ширшому трактуванні є радіотехнічними системами розпізнавання, які, в свою чергу, діляться за способом і об'єктами спостереження. Якщо ж розглянути аутентифікацію як частковий випадок розпізнавання об'єктів, то її прямий еквівалент – розпізнавання образів шляхом порівняння з еталоном.

Основні питання, які виникають під час проектування систем аутентифікації, пов'язані з вибором системи інформативних ознак, формуванням векторів ознак і методом їх порівняння. Використання ж нестійких у просторі і часі об'єктів, якими і є біометричні зображення, породжує необхідність аналізу процесу формування образу і проведення попередньої обробки.

Найбільш перспективними на даний момент є дактилоскопічні та голосові системи біометричної аутентифікації. Саме тому основну увагу у монографії приділено аналізу та розробці методів аутентифікації, які ґрунтуються на застосуванні цих видів біометрії.

У розділі 1 проведено порівняльний аналіз і класифікацію відомих алгоритмів розпізнавання мовних сигналів. Установлено, що існуючі методи визначення ознак розпізнавання базуються на використанні "жорстких" алгоритмів, які погано адаптуються до характерних рис мовних сигналів, тим самим погіршуючи ефективність роботи всієї системи розпізнавання.

Здійснено огляд особливостей дактилоскопічних зображень, систем ідентифікації, існуючих алгоритмів і методів попередньої обробки, систем інформативних ознак та методів їх порівняння. Зроблено їх аналіз і перераховано недоліки.

Проведено огляд існуючих криптографічних алгоритмів захисту конфіденційної інформації, принципів роботи систем на базі подібних алгоритмів, проаналізовано їхню стійкість захисту до відомих видів криптографічних атак. Здійснено огляд існуючих систем захисту криптографічних ключів та принципів їх роботи. Розглянуто існуючі способи та підходи до вирішення проблеми блокування криптографічних ключів за допомогою біометричних даних. Виділено недоліки та переваги кожного методу.

У розділі 2 розроблено алгоритм визначення ознак розпізнавання мовних сигналів, який базується на використанні пакетного вейвлет аналізу, основною перевагою якого порівняно з іншими відомими методами є адаптивність до характерних рис мовних сигналів, що поліпшує інформативність отриманих ознак і підвищує ефективність розпізнавання всієї системи. Сформульовано рекомендації практичного застосування розроблених систем формування інформативних ознак і методів їхнього порівняння, що дало можливість побудувати блок-схеми систем розпізнавання й компресії мовних сигналів і поліпшити ефективність їхньої роботи. Отримано залежність імовірності помилки виявлення від відстані Махаланобіса (розділ підготовлений за активної участі аспіранта Лисака Ю.В.).

Розділ 3 присвячено методам попередньої обробки дактилоскопічних зображень (ПОЗ) та створенню системи дактилоскопічної ідентифікації. Для вибору методів ПОЗ проведено аналіз і моделювання спотворень дактилоскопічних зображень. З цією ж метою описано характеристики ідеального дактилоскопічного зображення. Розроблено нові системи інформативних ознак і методи їх порівняння. Велику увагу приділено сумісному застосуванню запропонованих інформативних ознак із метою взаємокомпенсації їх недоліків і збереження переваг. Для комбінування багатоетапної ідентифікації розроблено критерії доцільності й налаштування першого етапу у двоетапному методі ідентифікації. Розглянуто практичне застосування розроблених систем інформативних ознак і методів їх порівняння. Розроблено алгоритми ПОЗ та ідентифікації для автоматизованої дактилоскопічної ідентифікаційної системи (АДІС) та біометричної ідентифікаційної системи (БІС). Проведено подальше збільшення етапів ідентифікації й пришвидшення роботи систем. Приділено увагу практичним аспектам і налаштуванню етапів ідентифікації. Наведено імовірнісні характеристики систем, побудованих за створеними алгоритмами (розділ підготовлений завдяки дослідженням к.т.н., Остапа В.П.).

У розділі 4 опрацьовано математичну модель процесу біометричного захисту криптографічних ключів. Користуючись поняттям екстрактора випадкових величин, який описує процес отримання із випадкових величин нерівномірного розподілу випадкових двійкових послідовностей із розподілом, близьким у певному сенсі до рівномірного, створено нову математичну модель біометричного екстрактора, з допомогою якої здійснено моделювання процесів, пов'язаних із біометричним блокуванням криптографічних ключів. Запропоновано методику відновлення випадкових величин із рівномірним розподілом з нечітких та нерівномірно розподілених біометричних даних. Проаналізовано місце біометричного екстрактора у ланках аутентифікації клієнта мережевої клієнт - серверної системи. Розроблено нову структурну схему клієнт - серверної системи з криптографічним захистом інформації. Визначено шляхи проведення атак на систему та оцінено її стійкість із блоком дактилоскопічного захисту ключів. Розглянуто практичну реалізацію запропонованої конструкції біометричного екстрактора на базі алгоритмів блокування та розблокування таємних криптографічних ключів. Створено новий недетермінований алгоритм генерації випадкових ключових послідовностей. Реалізовано алгоритм відбору особистих ознак для

створення множини блокування. Оцінено ефективність та розроблено рекомендації практичного використання запропонованого методу.

Загалом у монографії значну увагу приділено розробці нових підходів до біометричної аутентифікації та криптографічного захисту. Основний наголос робиться на необхідності застосування особистих ознак людини у ланках управління криптографічними ключами ІС захисту інформації.

Висловлюємо щиру подяку рецензентам монографії: доктору технічних наук, професору Дідковському В.С., доктору технічних наук, професору Рибальському О.В. за поради та цінні вказівки, які сприяли покращанню цього видання, а також голові правління ВАТ "Кредобанк", кандидату економічних наук, Кубіву С.І.

Автори будуть вдячні всім читачам, які надішлють свої зауваження, побажання та конструктивні пропозиції за адресою:

79601, Львів, вул. Наукова, 5, Фізико-механічний інститут ім. Г.В. Карпенка НАН України.

РОЗДІЛ 1. ОСНОВИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ

1.1. Основні поняття

Аутентифікація – це перший крок до гарантування безпеки ресурсів ІС. Аутентифікація – це здатність системи перевірити (підтвердити) особистість суб'єкта аутентифікації, яким у принципі може бути не лише людина, але й програмний процес. Аутентифікація забезпечує основу для ефективного функціонування інших заходів та засобів захисту, задіяних у ІС. Наприклад, механізм реєстрації дозволяє одержати інформацію про використання користувачами ресурсів ІС. Механізм керування доступом надає доступ до ресурсів ІС. Такі механізми ефективні тільки за умови, що користувач, що працює з ІС – це легітимний користувач, який володіє деяким унікальним ідентифікатором, так чи інакше відомим у ІС. Однак ІС не може довіряти заявленому ідентифікатору без підтвердження його дійсності. Установлення дійсності можливе при наявності в користувача чогось унікального, що тільки користувач:

- знає (пароль, особистий ідентифікаційний номер, криптографічний ключ);
- має (особисту картку, ідентифікаційний токен);
- або що є частиною його самого (голос, відбитки пальців, тобто біометричну інформацію).

Надалі, якщо не зазначено протилежне, такий унікальний матеріал для доведення дійсності ідентифікаторів називатимемо підписом суб'єкта аутентифікації, або просто підписом. Чим більшою є кількість таких підписів, наданих користувачем ІС, тим меншим є ризик, що хтось підмінить легітимного користувача.

Такі принципи аутентифікації існують у більшості політик безпеки існуючих ІС. Вони дотримуються неявно в політиках концептуального рівня, що підкреслює необхідність ефективного керування доступом до інформації й ресурсів ІС, або можуть бути явно прописані в політиці безпеки ІС у вигляді заяви, що всі користувачі повинні бути унікально ідентифіковані, а також визначено вид та сукупність використовуваних підписів.

Існує два види систем аутентифікації: ідентифікаційні ("один до багатьох") й верифікаційні ("один до одного").

В ідентифікаційних системах для аналізу надається підпис невідомого суб'єкта аутентифікації. Система порівнює новий підпис із інформацією, що зберігається в базі даних ідентифікаторів із

відповідними відомими підписами. Після порівняння система повідомляє (або оцінює) особистість невідомого суб'єкта на основі інформації зі своєї бази даних. До систем, які використовують ідентифікацію, належать системи, які застосовуються поліцією для ідентифікації людей по відбитках пальців і фотографіях. У цивільних цілях подібні системи можуть застосовуватися при видачі прав водія, при одержанні конкретною людиною соціальної допомоги чи оплати страхової медицини тощо.

У верифікаційних системах суб'єкт аутентифікації надає і підпис, і ідентифікатор, стверджуючи, що цей підпис належить конкретній особі. Алгоритм або приймає, або спростовує це твердження. З іншого боку, алгоритм може повертати індекс упевненості в правильності ототожнення. До верифікаційних систем належать системи, які перевіряють дійсність особи під час транзакцій, або для керованого доступу до комп'ютерів, а також для керування захистом приміщень. Цей спосіб, порівняно з попереднім, відрізняється високою швидкодією й висуває мінімальні вимоги до обчислювальної потужності.

У більшості відомих ІС використовується механізм верифікації на основі схеми ідентифікатор користувача/пароль. Дійсно, парольні системи можуть бути ефективними, якщо повністю відповідають стандартам безпеки, зокрема FIPS112, але це буває дуже рідко. Аутентифікація, що покладається винятково на паролі, часто не може забезпечити адекватний захист для ІС із ряду причин. Користувачі мають тенденцію створювати паролі, які є простими для запам'ятовування й, отже, простими для вгадування. З іншого боку, довгі та випадкові паролі спонукають користувачів записувати їх у "потаємних" місцях поблизу робочого місця. Наступним недоліком подібних механізмів є відсутність будь-якого зв'язку між паролем доступу до ІС і власником цього пароля. Іншими словами, будь-кого, хто знає пароль користувача, система ідентифікує саме як цього користувача.

Наведені фактори вказують на необхідність створення таких технологій аутентифікації, підписи яких володіли б наступними властивостями:

- індивідуальність або неповторність;
- стабільність упродовж тривалого періоду;
- неможливість фальсифікації;
- неможливість розподілу серед декількох користувачів;
- неможливість забути, загубити чи вкрасти.

Саме такими властивостями володіють біометричні системи аутентифікації.

1.2. Системи біометричної аутентифікації

Головною метою біометричної аутентифікації є створення такої системи реєстрації, що украй рідко відмовляла б у доступі легітимним користувачам і в той же час повністю виключала несанкціонований вхід у комп'ютерні сховища інформації. Порівняно з паролями й картками така система забезпечує значно надійніший захист: адже власне тіло неможливо забути чи загубити. Біометричне розпізнавання об'єкта засноване на порівнянні фізіологічних або психологічних особливостей цього об'єкта з його характеристиками, що зберігаються в базі даних системи. Подібний процес постійно відбувається в мозку людини, дозволяючи пізнавати, наприклад, своїх близьких і відрізняти їх від незнайомих людей.

Біометричні технології поділяються на дві категорії – фізіологічні й психологічні (поведінкові). У першому випадку розглядаються фізіологічні (статичні) характеристики людини, тобто унікальні характеристики, дані їй від народження й невід'ємні від неї, а саме:

- Відбиток пальця. В основі цього методу лежить унікальність малюнка папілярних візерунків пальців кожної людини. Відбиток, отриманий за допомогою спеціального сканера, перетворюється в цифровий код (згортку) і порівнюється з раніше уведеним еталоном. Дана технологія є найрозповсюдженішою порівняно з іншими методами біометричної аутентифікації [82,115,118,119,143,151,155,157, 159,171,191,217,244,255].
- Форма долоні. Метод, ґрунтується на геометрії кисті руки. На спеціальному пристрої, що складається з камери й декількох підсвічуючих діодів (включаючись по черзі, вони дають різні проекції долоні), будується тривимірний образ кисті руки, на підставі чого формується згортка й розпізнається людина [84,128,201].
- Розташування вен на лицьовій стороні долоні. За допомогою інфрачервоної камери зчитується малюнок вен на лицьовій стороні долоні або кисті руки, отримана картинка обробляється й за схемою розташування вен формується цифрова згортка [151,201].
- Сітківка ока. Вірніше, це спосіб ідентифікації по малюнку кровоносних судин очного дна. Для візуалізації цього малюнка людині потрібно подивитися на точкове джерело світла, після чого підсвічене очне дно сканується спеціальною камерою [151,201].

- Райдужна оболонка ока. Малюнок райдужної оболонки ока також є унікальною характеристикою людини, причому для її сканування досить портативної камери зі спеціалізованим програмним забезпеченням, що дозволяє захоплювати зображення частини обличчя, з якого виокремлюється зображення ока, з якого, у свою чергу, виділяється малюнок райдужної оболонки, по якому й будується цифровий код для ідентифікації людини [201,231,249,257,263].

- Форма обличчя. У даному методі ідентифікації будується тривимірний образ обличчя людини. На обличчі виділяються контури брів, ока, носа, губ і т.д., обчислюється відстань між ними й будується не просто образ, а ще безліч його варіантів для випадків повороту обличчя, нахилу, зміни виразу. Кількість образів варіюється залежно від цілей використання способу (аутентифікації, верифікації, віддаленого пошуку на великих територіях і т.д.) [150,201,250,251,262].

- Термограма обличчя. В основі даного способу аутентифікації лежить унікальність розподілу на обличчі артерій, які, постачаючи кров у шкіру, виділяють тепло. Для одержання термограми використовуються спеціальні камери інфрачервоного діапазону. На відміну від попереднього цей метод дозволяє розрізняти близнюків [151].

- ДНК. Переваги способу очевидні, однак сучасні методи одержання й обробки ДНК, нажаль, настільки тривалі, що такі системи застосовуються лише для спеціалізованих експертиз.

- Інші методи: ідентифікація по підніґтьовому шару шкіри, по кількості пальців для сканування, формі вуха, запаху тіла й т.д.

Психологічні методи біометричної аутентифікації ґрунтуються на поведінковій (динамічній) характеристиці людини, тобто побудовані на особливостях, типових для підсвідомих рухів у процесі відтворення якої-небудь дії.

Розглянемо методи аутентифікації даної групи:

1. По рукописному почерку. Як правило, для цього виду ідентифікації людини використовується його підпис (іноді написання кодового слова). Цифровий код ідентифікації формується, залежно від необхідного рівня захисту й наявності устаткування (графічний планшет, екран кишенькового комп'ютера Palm і т.д.), двох типів:

- по самому підпису, тобто для ідентифікації достатньо просто збігу двох картинок;

- по підпису й динамічних характеристиках написання, тобто для ідентифікації будується згортка, у яку входить інформація

безпосередньо з підпису, часових характеристик нанесення підпису й статистичних характеристик динаміки натиску на поверхню.

2. По клавіатурному почерку. Метод у цілому аналогічний вищеописаному, але замість розпису береться якесь кодове слово (якщо для цього використовується особистий пароль користувача, таку аутентифікацію називають двохфакторною). Тому немає потреби у спеціальному устаткуванні, крім стандартної клавіатури. Основною ознакою, за якою будується згортка для ідентифікації, є динаміка набору кодового слова.

3. По голосу. Одна з найстаріших технологій, що надзвичайно швидко сьогодні розвивається у зв'язку з її широким застосуванням при побудові "інтелектуальних будинків". Існує досить багато способів побудови коду ідентифікації по голосу, як правило це різні сполучення частотних і статистичних характеристик голосу [111,165,242].

4. Інші методи. Для даної групи методів описані тільки найпоширеніші, але існують ще й такі унікальні способи, як ідентифікація за рухом губ при відтворенні кодового слова, по динаміці повороту ключа у дверному замку й т.д.

На рис 1.1 зображено найпопулярніші об'єкти дослідження біометрії.

У таблиці 1.1 приведена відома з літератури порівняльна характеристика застосування об'єктів біометрії (ідентифікаторів) за наступними параметрами:

- універсальність – чи кожна людина володіє даною ознакою?
- унікальність – чи можна відрізнити людину одну від одної за допомогою цього об'єкта?
- постійність – чи залишатиметься об'єкт постійним (незмінним) протягом тривалого періоду?
- доступність – наскільки якісно можливо отримати та виміряти особливості об'єкта?
- ефективність – наскільки швидко та якісно працюють біометричні системи використовуючи об'єкт?
- зручність – наскільки зручні у практиці системи, що оперують саме цим об'єктом?
- захищеність – наскільки стійкими до атак є біометричні системи, що використовують об'єкт?

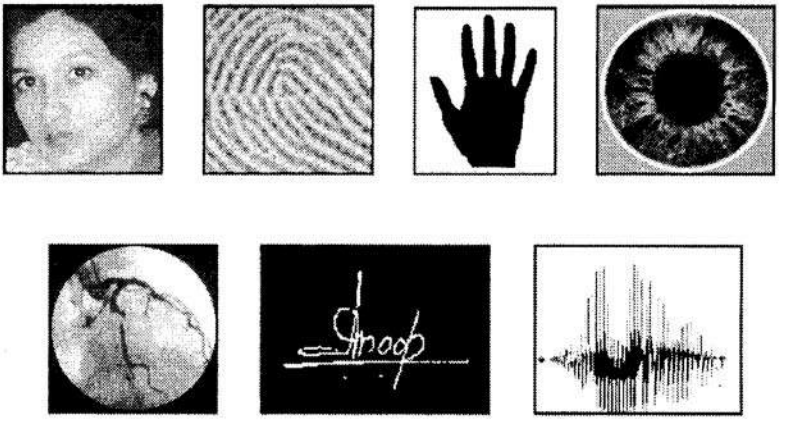


Рис. 1.1. Об'єкти біометрії.

Таблиця 1.1. Порівняння об'єктів біометрії

Ідентифікатор	універсальність	унікальність	постійність	доступність	ефективність	зручність	захищеність
Обличчя	В	Н	С	В	Н	В	Н
Відбитки пальців	С	В	В	С	В	С	В
Геометрія руки	С	С	С	В	С	С	С
Малюнок вен	С	С	С	С	С	С	В
Рогівка ока	В	В	В	С	В	Н	В
Малюнок судин ока	В	В	С	Н	В	Н	В
Динаміка підпису	Н	Н	Н	В	Н	В	Н
Аналіз особливостей голосу	С	Н	Н	С	Н	В	Н
Термограма обличчя	В	В	Н	В	С	В	В
Аналіз роботи з клавіатурою	Н	Н	Н	С	Н	С	С

Параметри оцінювалися у відносних величинах: В – високий рівень, С – середній рівень, Н – низький рівень.

Важливо підкреслити, що всі біометричні засоби аутентифікації в тій чи іншій формі використовують статистичні властивості деяких якостей індивідуума. Це означає, що результати їхньої роботи носять

імовірнісний характер і будуть постійно змінюватися. У системах розпізнавання оперують такими імовірнісними параметрами методів: $P_{пр}$ – імовірність правильного розпізнавання, $P_{нр}$ – імовірність неправильного розпізнавання, $P_{пн}$ – імовірність правильного нерозпізнавання, $P_{нн}$ – імовірність неправильного нерозпізнавання. У системах аутентифікації вони мають свої аналоги: $P_{пі}$ – імовірність правильної ідентифікації, $P_{ні}$ – імовірність неправильної ідентифікації, $P_{пн}$ – імовірність правильної неідентифікації, $P_{нн}$ – імовірність неправильної неідентифікації. Їх аналогія така:

$$P_{пр} \Leftrightarrow P_{пі}, P_{нр} \Leftrightarrow P_{ні}, P_{пн} \Leftrightarrow P_{пн}, P_{нн} \Leftrightarrow P_{нн}.$$

Оскільки імовірності $P_{пі}$ і $P_{пн}$ взаємодоповнюються імовірностями $P_{ні}$ і $P_{нн}$, то системи ідентифікації характеризуються двома з них. Найчастіше вживають $P_{ні}$ і $P_{нн}$. Імовірність неправильної неідентифікації (False Refusal Rate, FRR, помилка 1 роду) $P_{нн}$ характеризує кількість спроб санкціонованого доступу користувача під час ідентифікації системою (не визнали свого). Імовірність неправильної ідентифікації (False Accept Rate, FAR, помилка 2 роду) $P_{ні}$ характеризує імовірність проникнення сторонньої людини в область захисту засобів аутентифікації (пропустили чужого).

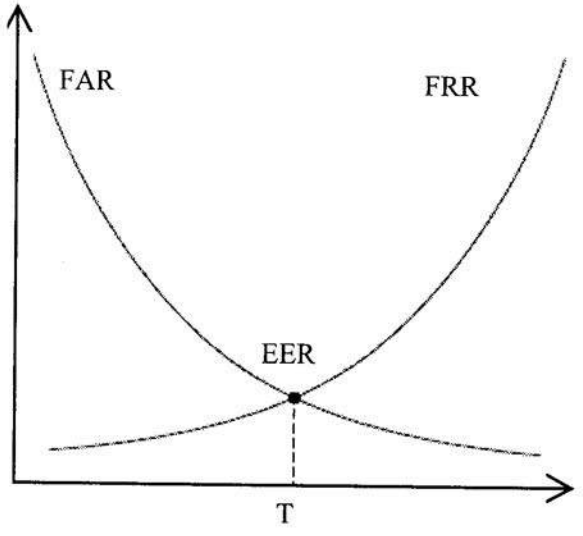


Рис.1.2. Характеристики біометричних систем.

Зауважимо, що ця тема в теорії ймовірностей добре вивчена ще із часів розвитку радіолокації. Як показує практика, ці дві ймовірності зв'язані зворотною залежністю, тобто при спробі посилити контроль підвищується ймовірність не пустити в систему свого, і навпаки. Для опису характеристик

систем і методів ідентифікації застосовують декілька графічних залежностей. Усі вони параметричні. Найбільш загальною є залежність $P_{ні}(P_{нн})$, яка будується за двома параметричними залежностями $P_{ні}(T)$ і $P_{нн}(T)$, де T – деяка порогова величина, яка визначає межу ідентифікації та неідентифікації. Цій величині ставиться у відповідність значення EER (Equal Error Rate або Crossover Rate, рис.1.2), кількісна міра усередненої помилки розпізнавання для рівних значень FAR і FRR. EER дозволяє порівняти різні алгоритми біометричної аутентифікації.

Залежності $P_{ні}(T)$ і $P_{нн}(T)$ також використовуються як окремі характеристики методів біометричних систем.

У системах біометричної ідентифікації вибирають деяке оптимальне значення T, виходячи з умов експлуатації та вимог щодо стійкості. Для забезпечення високого рівня захисту (наприклад, військові системи) значення FAR мусить бути якомога меншим для отримання високих значень FRR, і, навпаки, для створення більш дружнього для користувача інтерфейсу вибирають якомога менші значення FRR, що, відповідно, збільшуватиме FAR.

Наведені вище фактори впливу вказують на те, що звичайне порівняння підпису, записаного на сервері, з підписом, зробленим у процесі аутентифікації, як у випадку парольних систем, втрачає свій сенс. Для прийняття рішення про аутентифікацію у біометричних системах використовують різноманітні методи розпізнавання образів, які враховують відмінності у підписах, оцінюють міру близькості за допомогою системи інформативних ознак, притаманної конкретному об'єкту біометрії [31].

Логічно біометричну систему можна розділити на два модулі: модуль реєстрації й модуль аутентифікації. Перший відповідає за те, щоб навчити систему ідентифікувати конкретну людину. На етапі реєстрації біометричні датчики сканують необхідні фізіологічні або поведінкові характеристики людини й створюють їхнє цифрове відображення. Спеціальний модуль обробляє це відображення для того, щоб виділити характерні риси й згенерувати більш компактний та інформативніший підпис (у біометричних системах використовують ще термін "шаблон"). Підпис для кожного користувача зберігається в базі даних біометричної системи.

Модуль аутентифікації відповідає за розпізнавання людини. На етапі ідентифікації біометричний датчик сканує характеристики людини, яку необхідно ідентифікувати, і перетворює ці характеристики

в той же цифровий формат, у якому зберігається підпис. Отримана інформація порівнюється зі збереженим, щоб визначити, чи відповідають ці підписи один одному.

Очевидно, що жоден із об'єктів біометрії не є оптимальним, кожен має свої переваги та недоліки. На вибір методу, найбільш придатного в тій або іншій ситуації, впливає цілий ряд факторів. Пропоновані технології відрізняються ефективністю, причому їхня вартість у більшості випадків прямо пропорційна рівню надійності. До того ж системи біометричної ідентифікації, на відміну від парольних систем, вимагають складних алгоритмів розпізнавання зображень, що збільшує вартість систем захисту. Так, застосування спеціалізованої апаратури часто суттєво підвищує вартість кожного робочого місця.

Вибираючи спосіб аутентифікації, є сенс ураховувати кілька основних факторів:

- цінність інформації;
- вартість програмно-апаратного забезпечення аутентифікації;
- продуктивність системи;
- відношення користувачів до застосовуваних методів аутентифікації;
- специфіку (призначення) ІС.

1.3. Методологія розпізнавання людини по голосу

За останні кілька десятиліть надзвичайно зріс інтерес до проблеми аутентифікації по голосу. На сьогоднішній день створені десятки систем, що мають різні параметри й вимоги до процесу аутентифікації залежно від конкретних завдань. На жаль, розроблені програми не відрізняються простотою навчання, зручністю роботи або низькою вартістю. Частіше вони застосовуються як додаткові засоби перевірки особистості там, де необхідно забезпечити високий ступінь надійності систем аутентифікації. Тому й тривають роботи по вдосконалюванню алгоритмів обробки мовних сигналів з метою створення механізмів автоматичного розпізнавання людини по голосу, більш адекватних процесу сприйняття мови людиною.

Що ж дозволяє нам відрізняти голос однієї людини від іншої? Це питання приводило перших дослідників до чисто умоглядних теорій. В основному це пояснюється недооцінкою складності мови як багатофункціонального акту комунікації між людьми, який містить у собі інформацію не тільки про індивідуальність голосу мовця, але й про фонетичну якість. Тому дуже важливо забезпечити правильний

вибір і обґрунтування системи особистих ознак, які потім визначать принцип побудови системи аутентифікації. Питання полягає в наступному: які ж об'єктивні передумови аутентифікації людини по голосу? Які фізичні явища лежать в основі процесу розпізнавання дикторів? Які акустичні характеристики можуть бути використані для побудови системи аутентифікації?

Мовний сигнал є засобом передачі різноманітної інформації як вербальної (словесної), так і невербальної (емоційної). Для швидкої передачі інформації в процесі еволюції був відібраний особливим чином закодований і структурований акустичний сигнал. Для створення такого спеціалізованого акустичного сигналу використовується "голосовий апарат", сполучений з фізіологічним апаратом, призначеним для дихання й жування (оскільки мова виникла на пізніх стадіях еволюції, то до мовотворення довелося пристосувати вже наявні органи).

Процес утворення й сприйняття мовних сигналів [6], схематично показаний на рис. 1.3, передбачає наступні основні етапи: формулювання повідомлення, кодування в мовні елементи, нейромускульні дії, рухи елементів голосового тракту, випромінювання акустичного сигналу, спектральний аналіз і виділення

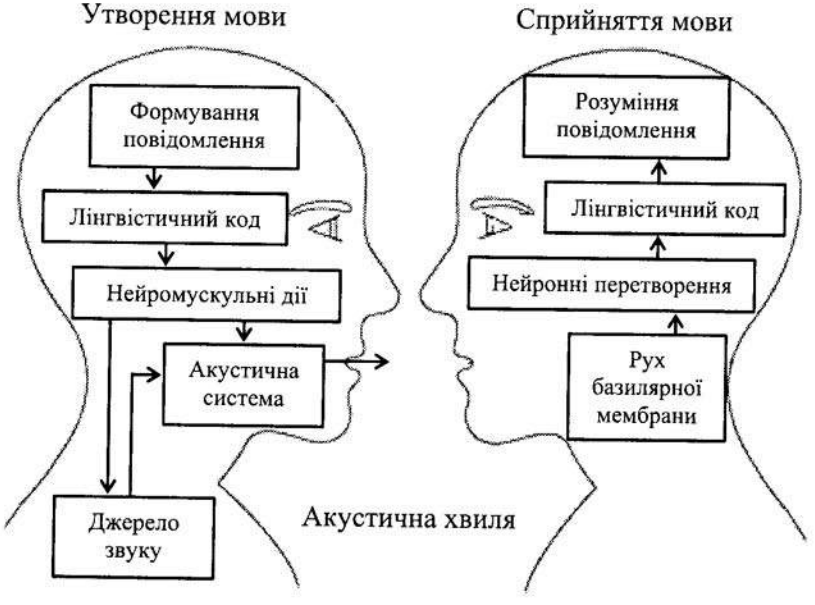


Рис. 1.3. Основні процеси утворення й сприйняття мови.

акустичних ознак периферичною слуховою системою, передача виділених ознак по нейронних мережах, розпізнавання мовного коду (лінгвістичний аналіз), розуміння змісту повідомлення.

Основними складовими частинами апарату мовотворення (рис. 1.4) є:

- **генератор** – дихальна система, яка складається з повітряного резервуара (легенів), де нагромаджується енергія надлишкового тиску, мускульної системи та вивідного каналу (трахеї) зі спеціальним апаратом (гортанню), де модулюється повітряний потік;
- **вібратор** – голосові зв'язки;

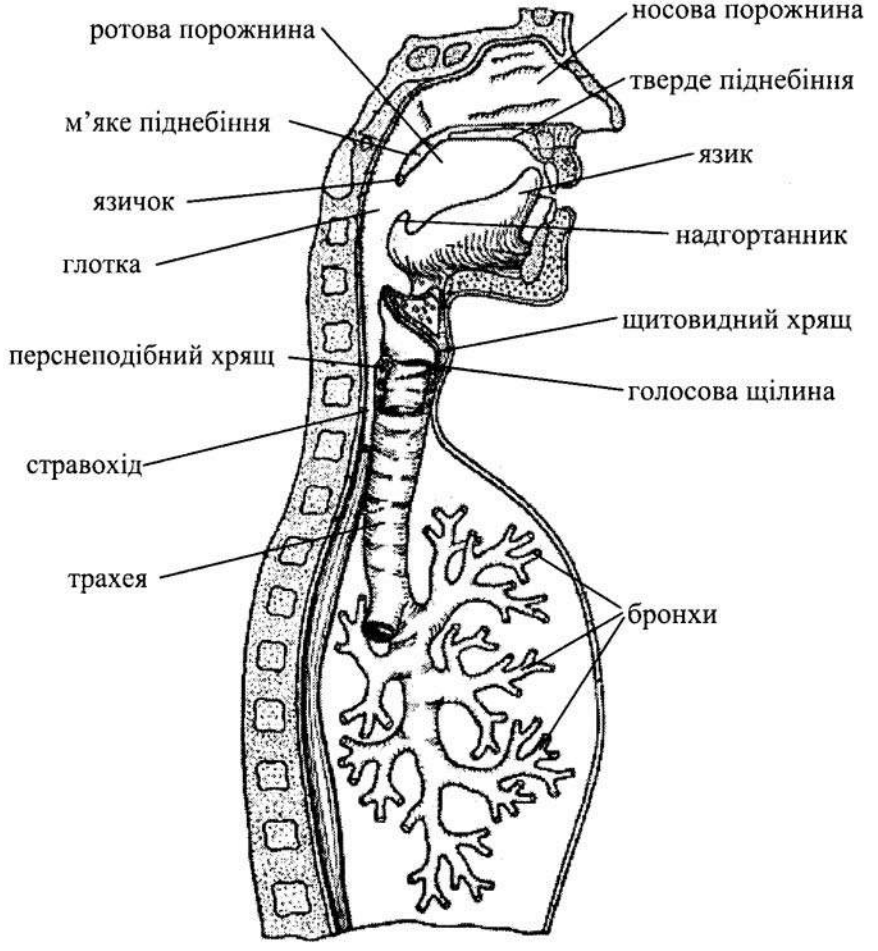


Рис. 1.4. Структура апарату мовотворення.

- **резонатор** – розгалужена система резонансних порожнин складної геометричної форми (глотка, ротова і носова порожнини) – артикуляційна система.

Генерація енергії повітряного стовпа відбувається в легенях, які створюють потік повітря при вдиху й видиху завдяки різниці атмосферного й легеневого тиску. Процеси вдиху й видиху реалізуються за рахунок стиску й розширення грудної клітки, які здійснюються звичайно за допомогою двох груп м'язів: міжреберних і діафрагми, при глибокому посиленому диханні скорочуються також м'язи черевного преса, грудей та шиї. При вдиху діафрагма опускається вниз, скорочення зовнішніх міжреберних м'язів піднімає ребра й відводить їх у сторони, а грудну клітку – вперед. Збільшення грудної клітки розтягує легені, що приводить до падіння внутрішньолегеневого тиску по відношенню до атмосферного та наповнення повітрям цього "вакууму". При видиху мускули розслаблюються, грудна клітка під власною вагою повертається у вихідний стан, діафрагма піднімається, об'єм легенів зменшується, внутрішньолегеневий тиск росте, повітря спрямовується у зворотному напрямку. Таким чином, вдих – процес активний, який потребує витрат енергії, видих – процес пасивний. При звичайному диханні цей процес повторюється приблизно 17 разів у хвилину, керування цим процесом як при звичайному диханні, так і при мові відбувається несвідомо.

Кількість енергії, яка може бути витрачена на створення мовних акустичних сигналів, залежить від об'єму нагромадженого повітря і, відповідно, від величини додаткового тиску в легенях. З огляду на те, що максимально можливий рівень звукового тиску становить 100...112 дБ, очевидно, що голосовий апарат не є ефективним перетворювачем акустичної енергії. Його ККД становить порядку 0,2%.

Модуляція повітряного потоку (внаслідок вібрацій голосових зв'язок) і створення підглоточного надлишкового тиску відбувається в гортані. Гортань (рис. 1.5) – це дихальна трубка-клапан. Гортань розташована на рівні 4-6 шийних хребців і сполучається зв'язками з під'язиковою кісткою. Зверху гортань сполучається з порожниною глотки, знизу – з трахеєю. Скелет гортані утворений кількома рухливо сполученими між собою гіаліновими хрящами. Саме цей апарат і використовується як джерело голосу при мовленні. Гортань утворена з набору хрящів і м'язів. Спереду її охоплює щитоподібний хрящ, позаду – перснеподібний хрящ, позаду також розташовуються дрібніші парні хрящі: черпакуваті, ріжкоподібні та клиноподібні.

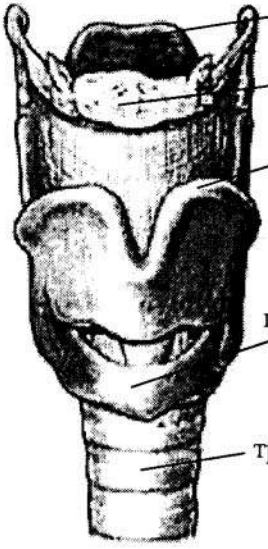


Рис. 1.5. Будова гортані.

Найбільший із них – щитоподібний (непарний), у якого розрізняють дві сполучені між собою під майже прямим (у чоловіків) або тупим (120°, у жінок) кутом чотирикутні пластинки. Від задніх країв пластинок відходять дві пари ріжків (верхні і нижні). Основу гортані складає перснеподібний хрящ (гіаліновий), його дуга звернена вперед, а пластинка – назад. Перснетрахеальна зв'язка сполучає нижній край хряща з першим хрящем трахеї. Перснеподібний хрящ сполучається з щитоподібним і черпакуватими хрящами двома парами суглобів.

Найважливішими (функціонально) у гортані є черпакуваті хрящі, від основи яких вперед відходить голосовий відросток, назад – м'язовий. До останнього прикріплюється м'яз, який змінює положення голосових відростків, що натягують голосові зв'язки. Ріжкоподібний хрящ маленький, конічної форми, своєю основою ніби сидить на верхівці черпакуватого. Клиноподібний хрящ більший, видовжений, непостійної форми і величини, часто рудиментарний. Обидва хрящі еластичні. Зверху гортань вкрита надгортанним хрящем, який прикріплений до щитоподібного хряща і під'язикової кістки за допомогою щитонадгортанної і під'язиково-надгортанної зв'язок. Надгортанний хрящ також побудований за принципом клапана. Він опускається при ковтанні й закриває гортань. Усі ці хрящі поєднані м'язами, від рухливості яких залежить швидкість повороту хрящів. З віком рухливість м'язів зменшується, хрящі також стають менш еластичними, тому можливості володіння голосом зменшуються.

Найбільш складно побудована середня частина гортані (рис. 1.6), у якій розташовані парна м'язова перегородка (еластичний конус) і дві пари складок. Верхні називаються переддверними, або "хибними голосовими", а нижні – голосовими. У тілі останніх лежать голосові

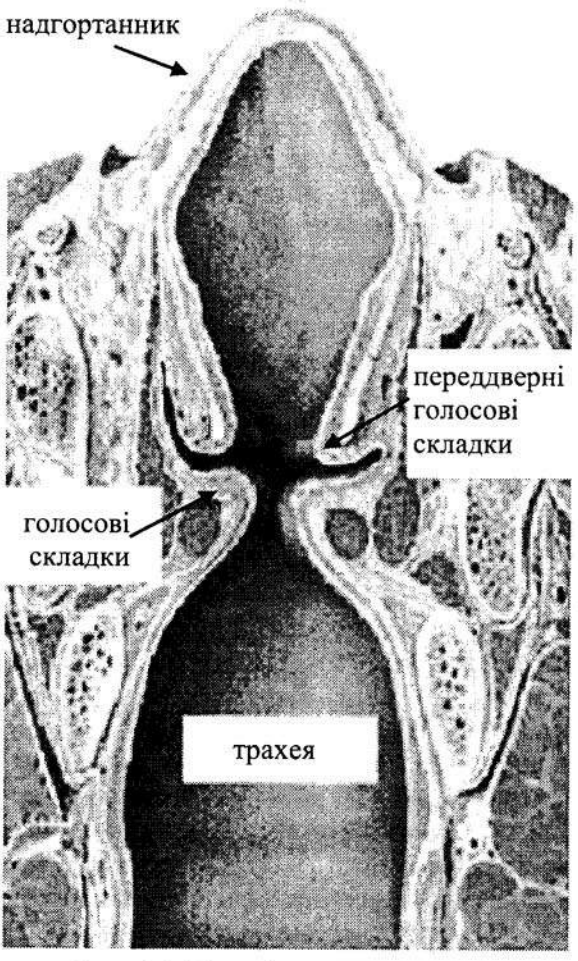


Рис. 1.6. Переріз трахеї и гортані.

зв'язки, утворені еластичними волокнами, і м'язи (рис. 1.7). Проміжок між правою й лівою голосовими складками називається голосовою щілиною. Голосові зв'язки натягнуті між щитоподібним і черпакуватим хрящами. Розміри голосової щілини у відкритому стані 2 см у довжину і 1 см завширшки.

Саме **голосові складки** і є основним (але не єдиним) джерелом мовотворення (вібратором). Переддверні голосові складки виділяють спеціальну слизову секрецію, яка допомагає змазувати голосові складки й охороняє їх від ушкодження при терті під час звукоутворення. Звичайно вони не беруть участі у процесі звукоутворення, однак при деяких патологіях "справжніх" зв'язок вони можуть бути задіяні в утворенні звуку.

Між двома парами складок розміщенні невеликі порожнини (шлуночки гортані), які відіграють роль акустичних фільтрів, зменшуючи рівень високих гармонік (скрипучість голосу), вони ж служать резонаторами для тихих тонів. При русі черпакуватих хрящів голосові складки можуть зрушуватися й розсовуватися,

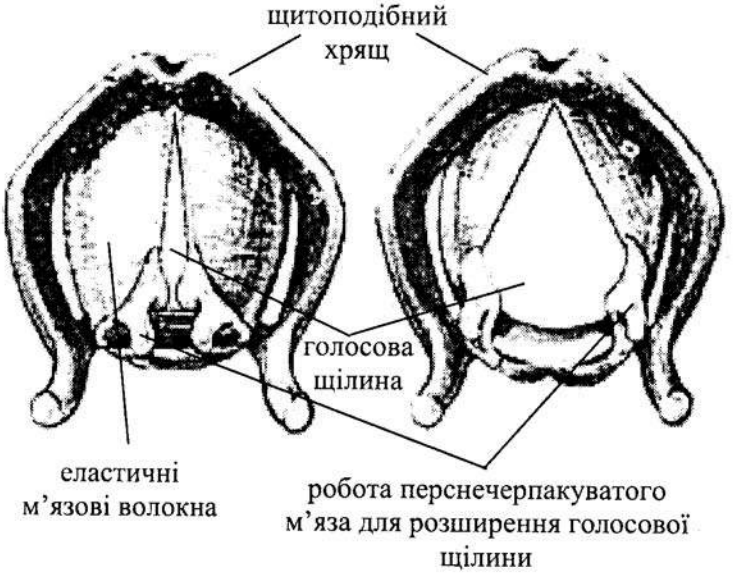


Рис. 1.7. Голосова щілина та складки в динаміці.

відкриваючи прохід повітря. При поворотах щитоподібного й перснеподібного хрящів вони можуть розтягуватися й стискатися, при активації вокальних м'язів вони можуть розслаблюватися і напружуватися. Процес утворення звуків мови визначається рухом (коливаннями) зв'язок, що приводить до модуляції потоку повітря видихуваного з легенів. Такий процес називається фонацією.

Процес фонації. Перед початком мови голосові складки зводяться черпакуватими хрящами, що спричиняє запирання потоку повітря й виникнення надлишкового підглоточного тиску (так зване "передфонаційне настроювання"). Повітря, яке виштовхується легенями із трахеї, нагромаджується у підскладочному просторі і починає тиснути на них. Коли надлишковий тиск підвищується до певної величини, складки розмикаються і повітря спрямовується в голосову щілину. У момент максимального відкриття щілини швидкість потоку повітря стає максимальною, тиск усередині щілини падає (за законом Бернуллі), причому швидкість протікання повітря неоднакова – у найвужчій частині голосової щілини вона максимальна. Усередині голосової щілини утвориться зона пониженого тиску. Навколишній більш високий тиск, а також власна пружність зв'язок змушують складки стулитися. Таким чином, чергування надлишкового тиску в підскладочному просторі й від'ємного тиску завдяки ефекту

Бернуллі змушує складки змикатися-розмикатися, що забезпечує нормальний режим їхніх коливань (рис. 1.8). При цьому відбувається модуляція потоку повітря, яке порціями попадає в резонансні

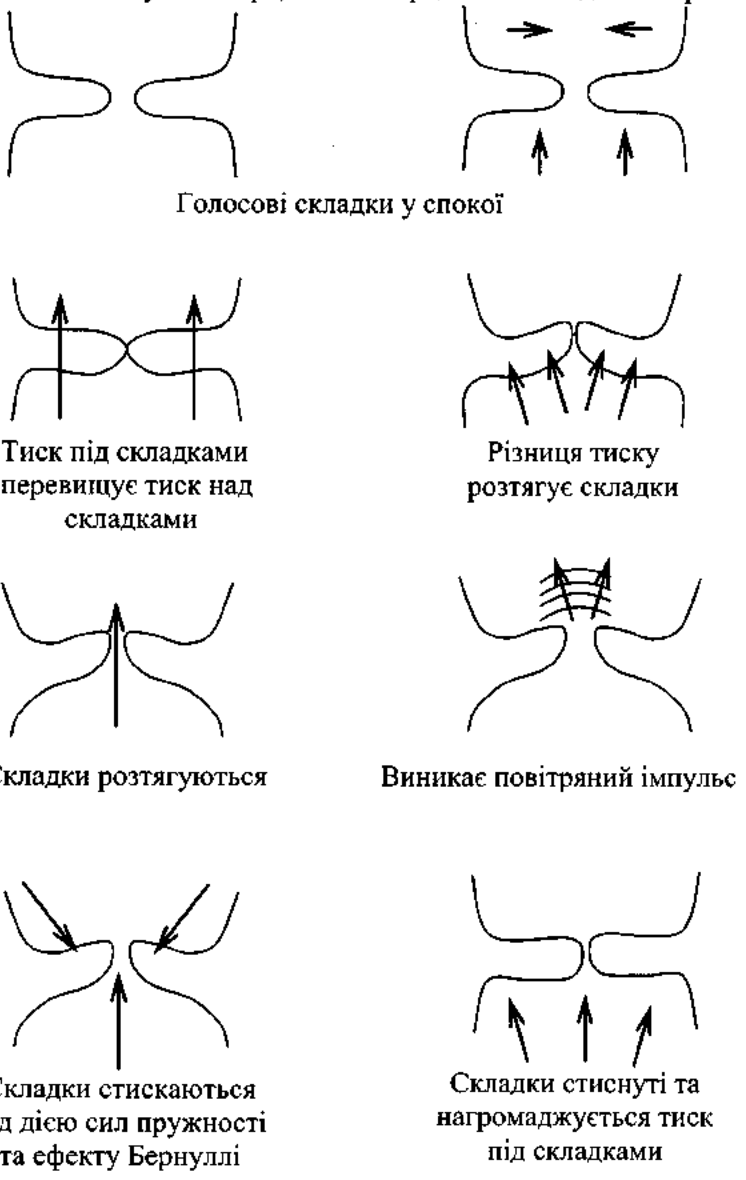


Рис. 1.8. Процес коливань голосових складок.

порожнини. Послідовність повітряних поштовхів, що виникають у результаті коливань голосових зв'язок, називається ковтальною хвилею, звичайно вона представляється у вигляді залежності об'ємної швидкості повітря від часу (рис. 1.9). Як видно із графіків, такий сигнал являє собою послідовність імпульсів, форма яких залежить від співвідношення часу відкриття складок (швидкість потоку поступово

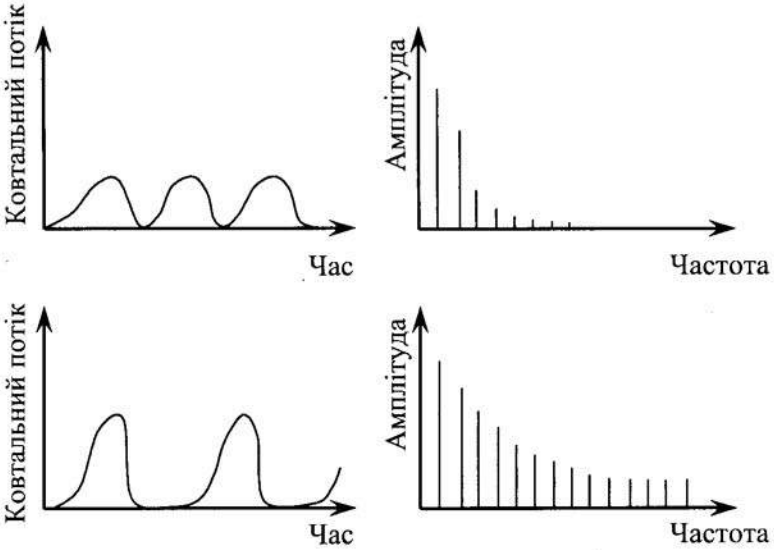


Рис. 1.9. Форма голосових імпульсів та їхній спектр.

наростає) і часу їхнього закриття (швидкість раптово зменшується). Період такої хвилі визначається тривалістю загального циклу коливань зв'язок, тобто основною частотою коливання. Амплітуда зумовлюється максимальною швидкістю потоку повітря, що, у свою чергу, залежить від величини підскладочного надлишкового тиску.

Частота коливань складок визначає висоту голосу (чоловічий голос – в середньому 110 Гц, жіночий – 220 Гц), а амплітуда – його гучність [75].

Якщо записати мікрофоном такий звук біля самих голосових складок, то він нагадує гудіння або дзижчання. Це вихідний матеріал для одержання звуків мови, далі він обробляється в артикуляційному тракті. Спектр такого звуку показаний на рис 1.9. Оскільки коливання голосових складок створюють періодичний сигнал (реальний сигнал не є строго періодичним), то його спектр при нормальній фонації є гармонійним із крутизною заднього фронту 12 дБ/окт. Для збільшення гучності мови необхідно підвищити підскладочний тиск (затратити

більше енергії), при цьому фронти голосових імпульсів стають крутішими (складки швидше відкриваються). Час, коли щілина закрита, збільшується від 40...50% при нормальній фонації, і до 65...70%. Також змінюється спектр, у ньому з'являється більше гармонік, що, відповідно, змінює тембр голосу (робить його яскравішим).

Способи змикання складок при фонації можуть бути різними. Наприклад, якщо складки замикаються не повністю, і між ними є щілина, то форма імпульсів стає майже симетричною, швидкість не падає до нуля, у голосі чутний шум (придиховий голос, шепіт). Навпаки, якщо складки занадто сильно замикаються (голос стає затиснутим), це також міняє форму імпульсів і, відповідно, спектр і тембр голосу.

Усі перераховані характеристики – основна частота коливань голосових зв'язок, форма голосових імпульсів, їхня амплітуда, спектральний склад і форма огинаючої спектра – відіграють істотну роль при розпізнаванні мови. Особливу роль відіграє частота основного тону: у мовному потоці вона визначає висоту голосу, і її зміна використовується також для зміни інтонації, логічних наголосів, а іноді й змісту слів (наприклад, у тональних мовах, таких, як китайська). У вокальній мові (співі) частота основного тону може змінюватися в широких межах, звичайно одна-дві октави (хоча були унікальні співаки з можливістю зміни висоти основного тону до чотирьох октав - Іма Сумак, Мадо Робен та ін.).

Частота основного тону, тобто число коливань голосових зв'язок у секунду, залежить від їхньої довжини, маси й натягу. Приблизно цей зв'язок можна представити таким чином (вираз для струни, хоча зв'язки більше схожі на гумові шнури):

$$f = \frac{1}{2l}\sqrt{\frac{T}{m}},$$

де T – натяг (пружність, Н); l – довжина (м); m – погонна маса (кг/м). Отже, чим довші й важчі складки (це вроджені властивості), тим нижчим є голос, а чим коротші й тонші – тим голос вищий. Маса залежить від довжини, товщини й щільності складок. У процесі мовлення товщина й щільність складок може значно змінюватися за рахунок натягу.

Натяг забезпечує підвищення висоти голосу, і може здійснюватися під час напруження внутрішніх вокальних мускулів і повороту щитоподібного й перснеподібного хрящів один відносно одного.

Оскільки при збільшенні гучності голосу росте підскладочний тиск, який також має вплив на натяг складок (мускули рефлекторно напружуються), то, звичайно, при підвищенні гучності мови росте й висота тону (крик).

Таким чином, при утворенні звуків мови шляхом фонації (тобто коливання голосових зв'язок) формується звуковий сигнал, який трансформується у вокальному тракті з "сирого" матеріалу в послідовність мовних акустичних сигналів.

Отже, вокальний тракт виконує функцію резонатора, тобто підсилює й фільтрує вхідний сигнал. Модель вокального тракту показана на рис. 1.10. Як видно з рисунка, тракт складається із трьох основних резонансних порожнин: глотки, ротової порожнини, носової порожнини. Особливості такої системи резонаторів наступні:

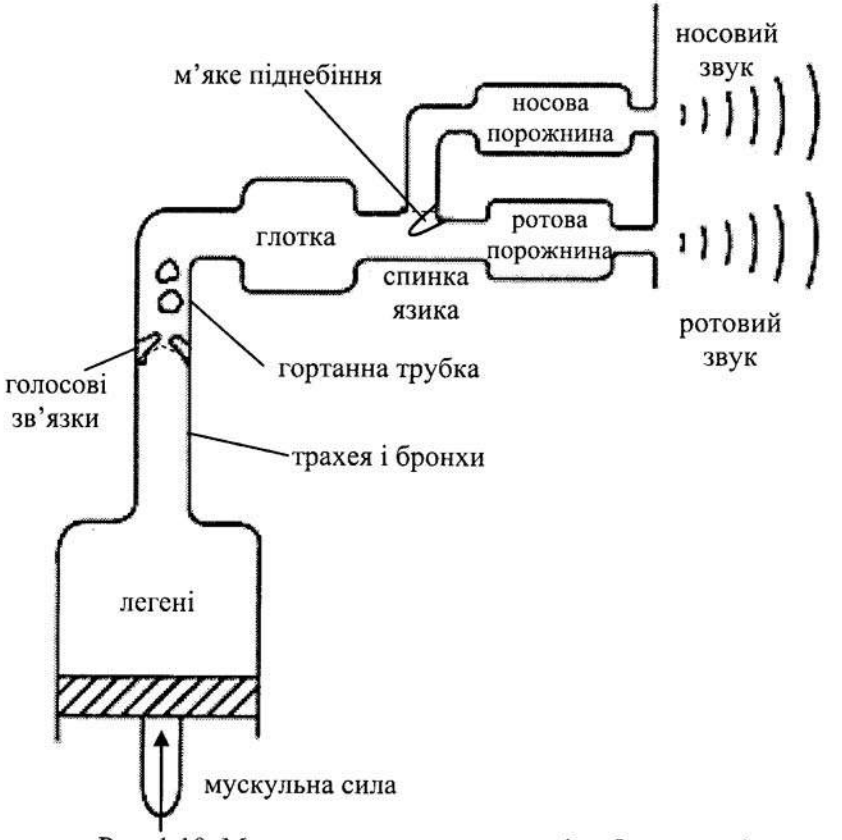


Рис. 1.10. Модель вокального тракту (по Фланагану).

- складна геометрична форма, тобто вокальний тракт можна розглядати як трубу змінного перетину з підключенням паралельної труби (носової порожнини, що може підключатися при опусканні заднього м'якого язичка);
- можливість швидкої перебудови форми труб, площі їхнього поперечного перерізу, щільності й твердості стінок зміною положення язика, м'якого язичка, губ, щелеп, розширення глотки, опускання гортані та ін.

Можливості перебудови параметрів вокального тракту величезні, та властиві лише людині. Такий процес називається артикуляцією. Кожному звуку мови відповідає або якесь статичне положення, або певна динаміка зміни положення язика, щелеп, губ, піднебіння, тобто особлива артикуляція.

Загальна довжина мовного тракту дорослої людини (від голосових складок до губ) близько 17 см, довжина носової порожнини 12,5 см, площа поперечного перетину тракту змінюється у межах 0...20 см^2.

Найпростішою моделлю вокального тракту можна вважати циліндричну трубу довжиною 17 см, закриту на одному кінці. Власні моди (форми) коливань такої труби показані на рис. 1.11, частоти визначаються зі співвідношень:

$$f_n = (2n - 1)\, c / 4\, l,$$

де $l = \lambda/4$; $l = 3\,\lambda / 4$; $l = 5\,\lambda / 4$ і т.д.; n – ціле число; l – довжина труби; c – швидкість звуку. У спектрі такої труби присутні тільки непарні гармоніки 1:3:5 Для довжини $l = 17$ см власні частоти рівні 500, 1500, 2500 Гц. Якщо в різних точках труби змінювати площу поперечного перерізу, то положення її власних частот буде зміщуватися. Аналогічні процеси відбуваються у вокальному тракті: у ньому також є свій набір власних частот з відповідними модами коливань, тобто певним розподілом вузлів і пучностей уздовж його довжини. Зі зміною площі поперечного перерізу у вокальному тракті, змінюється положення власних частот.

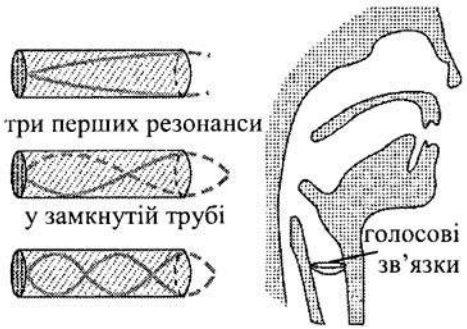


Рис. 1.11. Форми коливань для циліндричної труби і голосового тракту.

Якщо на вхід такої труби (системи труб) подати сигнал, сформований коливаннями голосових зв'язок (рис. 1.9), то на

виході можна записати сигнал, форму якого показано на рис. 1.12, тобто гармоніки, які збігаються із власними частотами тракту, будуть посилені за рахунок резонансів.

Області спектральних максимумів, що відповідають резонансним частотам вокального тракту, називаються **формантами** (іноді просто резонансами вокального тракту). Кожному звуку мови (найпростіший звук мови називається фонемою) відповідає своя форма вокального тракту, яка варіюється зміною положення язика, губ, щелеп і т.д., і своє положення формант (*F*-Картина). Приклади показані на рис. 1.12.

Існують деякі загальні закономірності в керуванні розташуванням власних частот резонаторів. Якщо поперечний переріз труби зменшується в області, де форма коливань (мода), яка відповідає даній резонансній частоті (форманті), має максимум тиску, то частота збільшується, а якщо в точці, де є мінімум тиску, то частота зменшується. Вивчення руху артикуляційних органів під час мови за допомогою рентгенографічних зйомок показало, що аналогічні закономірності типові й для вокального тракту: при підйомі язика вперед і нагору звужується передня частина ротової порожнини, при цьому знижується перша форманта *F1* і підвищується друга *F2*. При перенесені язика назад звужується поперечний переріз тракту в області глотки, при цьому підвищується *F1* і знижується *F2* і т.д. Зсув формант по певних закономірностях викликає зміни в співвідношенні їхніх амплітуд, що приводить до зміни форми огинаючої. Усі ці ознаки (розташування формант і співвідношення їхніх амплітуд) є унікальними акустичними ознаками голосних звуків мови.

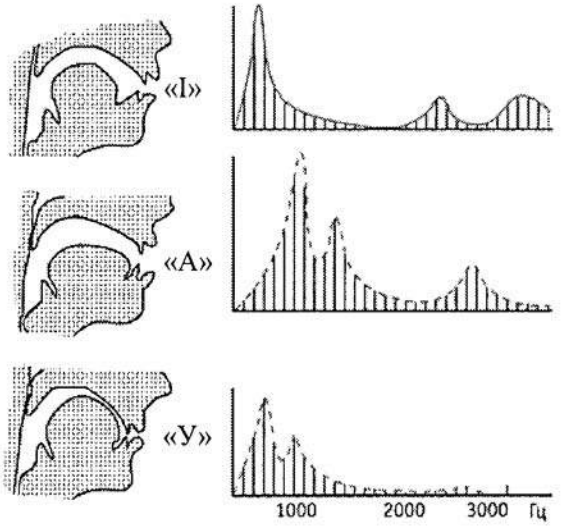


Рис. 1.12. Положення тракту для різних звуків мови і вигляд звукового сигналу з формантами.

Однак під час розмови настільки швидко перебудовуються позиції артикуляційних органів (язика, губ та

ін.), що часто має місце накладення позиції, яка відповідає одному звуку, на позицію іншого (звичайно голосного на сусідній приголосний), таке явище називається коартикуляцією, і воно суттєво ускладнює сприйняття і розпізнавання мови.

Таким чином, вокальний тракт діє на звуковий сигнал джерела як параметричний еквалайзер, при цьому істотне значення мають частоти резонансів, співвідношення їхніх амплітуд і ширина резонансних піків (добротність). Приклади областей розташування перших трьох формант для голосних української мови подано нижче.

Частотний діапазон формант (Гц)			**Ширина формант (Гц)**
Тип голосу	Чоловічий	Жіночий	
F1	200...800	250...1000	40...70
F2	600...2800	700...3300	50...90
F3	1300...3400	1500...4000	60...180

Розпізнавання кожної фонеми відбувається переважно по положенню перших двох формант *F1* і *F2*, більш високі форманти визначають тембральні особливості.

Припущення про незалежність джерела збудження голосу і характеристик голосового тракту є основним для усіх систем обробки мови. Саме ця незалежність джерела та тракту і дозволяє вводити передавальну функцію голосового тракту. Загальновизнаною є цифрова модель мовотворення (Рабінер і Шафер [73]), зображена на рис. 1.13. Якщо підходити до процесу утворення звуків мови за допомогою фонації в термінах передавальних функцій, то його можна описати наступним чином:

$$P(z)=S(z)\ T(z)\ R(z).$$

Джерелами збудження є:

- генератор послідовності імпульсів: відповідає за вокалізовані звуки, вводиться зовнішня синхронізація з періодом основного тону, імпульси проходять через фільтр з передавальною характеристикою $S(z)$;
- генератор шуму: відповідає за невокалізовані звуки, шум імітує квазівипадковий турбулентний потік і спад тиску при утворенні глухих звуків.

Кожне з джерел (або обидва разом) може бути з'єднане з входом лінійного цифрового фільтра зі змінними параметрами, який моделює голосовий тракт, із передавальною функцією $T(z)$. При цьому коефіцієнти фільтра відображають властивості голосового тракту залежно від часу при безперервному мовленні. У середньому кожних

$T_C = 10...20$ мс (інтервал стаціонарності) коефіцієнти фільтра змінюються, відображаючи зміни у мовному тракті. Поведінка потоку повітря біля губ описується цифровим фільтром із передавальною

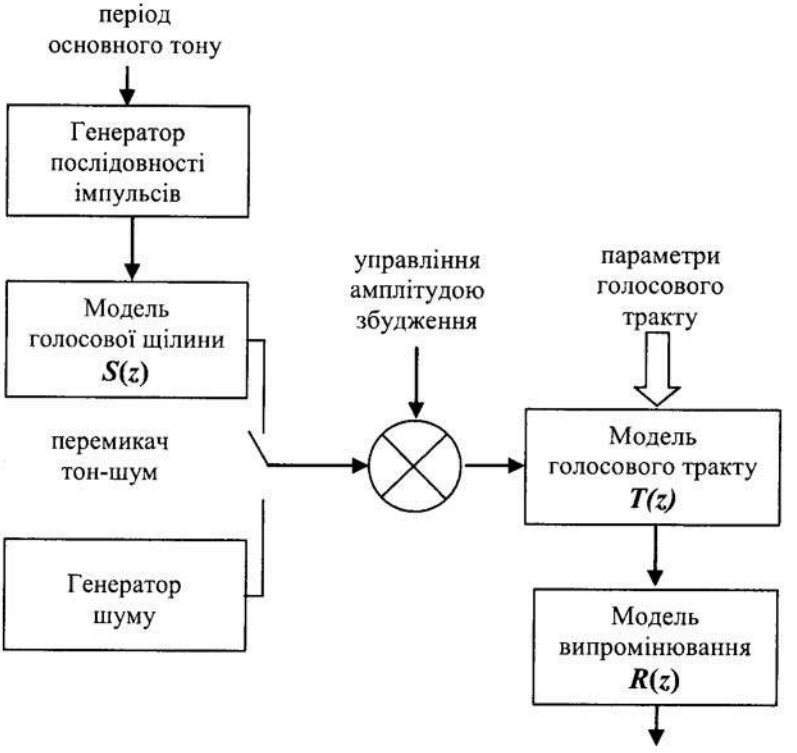


Рис. 1.13. Цифрова модель мовотворення.

функцією $R(z)$. У реальному голосовому тракті передатна функція має дещо складніший характер, але на резонансних частотах тракту, тобто на формантах, вона також має максимуми – полюси. Таким чином, форманти ще можна визначити як полюси передавальної функції.

Як уже було сказано, при утворенні звуків мови задіяні три основні механізми генерації звуку (і їхні різні сполучення): процес фонації, турбулентний шум, імпульсні джерела.

Процес фонації, тобто модуляція повітряного потоку за рахунок коливань голосових зв'язок, використовується при утворенні голосних звуків і дзвінких приголосних. При цьому формується послідовність імпульсів, які фільтруються у голосовому тракті. У результаті виникає мовний акустичний сигнал.

Турбулентний шум проявляється при проходженні потоку повітря через вузький отвір з досить великою швидкістю. У певному місці тракт звужується, і при проходженні повітря через нього утвориться шум, який трансформується в резонансних порожнинах тракту. Спектр турбулентного шуму має **плоску** ділянку в діапазоні 500...3000 Гц, вище й нижче якого він спадає зі швидкістю – 6 дБ / окт. Приклади спектрального розподілу шуму для звуків "ф", "с", "ш", "х" показані на рис. 1.14.

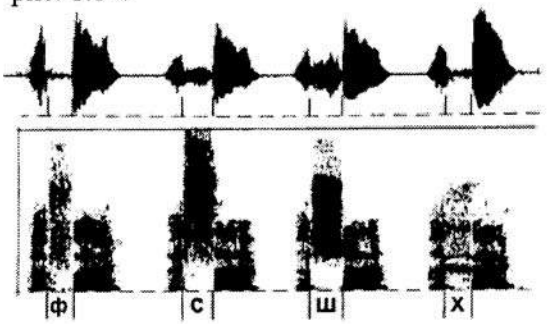


Рис 1.14 Осцилограми и спектрограми шуму при утворенні глухих приголосних

Імпульсне джерело звуку з'являється при стрибкоподібній зміні тиску повітря. Для виникнення звукового імпульсу необхідно створити в мовному тракті значний надлишковий тиск, повністю перекривши вихід повітря на деякий інтервал часу (приблизно 30 мс). Амплітуда імпульсу залежить від величини тиску, тому в мові більш гучними будуть ті приголосні, для яких місце стрибка тиску перебуває ближче до гортані – там тиск накопичується швидше, і його рівень вище. Імпульсний звук такого типу має суцільний спектр.

Кожний із трьох перерахованих вище способів (фонація, турбулентний шум, імпульс) може виступати як самостійне джерело при утворенні звуків мови, а може використовуватися в різних сполученнях.

На відміну від голосних звуків приголосні відрізняються більшою кількістю способів звукоутворення, що ускладнює їхній аналіз і розпізнавання. Однак саме приголосні вимагають особливої уваги при звуковій обробці, оскільки в мові вони несуть основне значеннєве навантаження.

По-перше, при утворенні приголосних можуть використовуватися усі джерела звуку та їхні сполучення: фонація, турбулентний шум, імпульс.

По-друге, варіюється місце розташування джерел звуку: якщо при утворенні голосних резонатори завжди знаходяться перед джерелом звуку (положення голосових зв'язок у гортані незмінне), то при

утворенні приголосних джерело звуку може перебувати в будь-якому місці тракту (наприклад, біля зубів для звуку "з"; біля піднебіння – для звуків "г", "к" та ін.).

По-третє, при утворенні приголосних додатково може використовуватися носова порожнина ("м", "н").

Крім того, приголосні відрізняються коротшими періодами стаціонарності (служать переходом від однієї голосної до іншої) і значно більшою розмаїтістю спектрів. Середня тривалість голосних звуків 0,15 с, середня тривалість приголосних 0,08 с.

У випадку приголосних звуків процес утворення формантних областей значно ускладнюється.

Резонанси, які виникають у порожнині перед джерелом звуку, створюють піки у вихідному сигналі, такі резонанси називаються "полюсами" (формантами); резонанси задніх порожнин називаються "нулями" передавальної функції і проявляються у вигляді провалів. Модель тракту для приголосних "к", "п", "т" і відповідна передавальна функція тракту показані на рис. 1.15. На графіку чітко простежуються піки (полюси) і провали (нулі).

Коли нуль і полюс накладаються, відбувається їхня нейтралізація, і на вихідній характеристиці не видно жодного. У такому разі вони називаються "зв'язаними".

Для опису процесів утворення приголосних звуків уводиться поняття локусної формантної картини. При утворенні голосних звуків передавальна функція тракту, як згадано вище, повністю залежить від структури її формант (F - картини), які під час швидкої мови безупинно змінюються, оскільки постійно перебудовуються артикуляційні органи. Ця плавність зміни конфігурації мовного тракту і його резонансних частот має місце й при вимові приголосних звуків, тільки ці резонанси не завжди помітні у передавальній функції.

Під локусною F - картиною розуміється сукупність резонансів (формант) ротової порожнини тракту, яка відповідає положенню артикуляційних органів при вимові даного приголосного звуку. Таким чином, локуси – це ті форманти, які повинні бути при даній конфігурації тракту, незалежно від того, чутні вони чи ні. Їхнє положення можна відновити зі спектрограм сигналу, і воно має істотне значення для процесів сприйняття приголосних.

Артикуляційні можливості мовного тракту при утворенні звуків надзвичайно різноманітні, і можуть бути використані для створення величезного спектра звуків. Однак для мови використовується

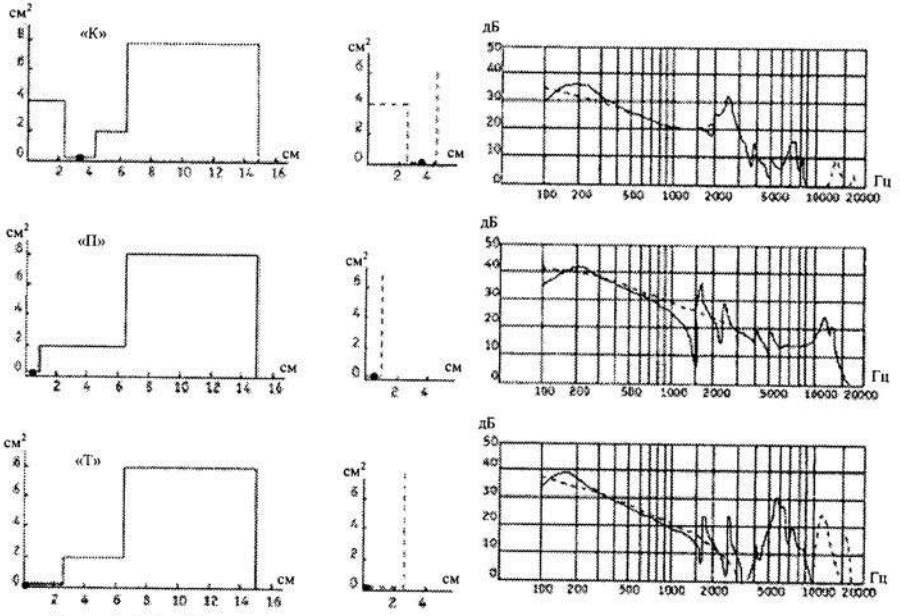


Рис. 1.15. Форма голосового тракту і спектри звуків "к", "п", "т" (точкою помічено місце розташування джерела шуму).

обмежений набір звуків (кількість фонем у різних мовах світу в основному не перевищує 50...70). Такий розрив між можливостями голосового апарату і його застосуванням пояснюється у рамках квантальної теорії, згідно з якою із усіх звуків мови використовуються лише ті, які створюють чіткі слухові контрасти та легко розпізнаються слуховою системою (тобто мова була пристосована до слуху). Наприклад, голосні "і", "у, "а" різко контрастують на слух, тож вони використовуються майже в усіх мовах світу. Тому для різних звуків мови були відібрані ті види артикуляції, які створюють істотні акустичні та слухові відмінності.

Розглянуті вище механізми звукоутворення з урахуванням квантальних артикуляційно-акустичних та слухових залежностей і лежать в основі класифікації звуків мови, коротке ознайомлення з якою є необхідним для аналізу акустичних характеристик мови та їхніх зв'язків з фонетичними ознаками в процесі розпізнавання.

Класифікація звуків мови. В основі класифікації усіх звуків мови, які беруть участь у розрізненні слів, лежить класифікація Міжнародної фонетичної асоціації (МФА) за артикуляційними ознаками. Однак оскільки, з одного боку, всі звуки – це семіотичні

знаки, створювані органами мови, а з іншого – акустичні сигнали, сприйняття яких породжує складні слухові образи, існують класифікації на підставі акустичних ознак. Ознаки, використовувані в класифікації МФА, діляться на групи, залежно від того, який з нижчеперелічених процесів вони застосовують:

- - формування повітряного потоку – генерації (ініціації);
- - участь голосових зв'язок в утворенні звуку – фонації;
- - формування структури вокального тракту – артикуляції.

Усі звуки мови можна розділити на дві більші групи: голосні і приголосні, які істотно відрізняються за цими ознаками.

Оскільки приголосні звуки несуть переважно значеннєве навантаження мови, а голосні - основне емоційне навантаження, то різне кількісне сполучення цих звуків у різних мовах визначає різницю в надлишковості мови і різні вимоги до їхньої цифрової обробки.

Класифікація голосних. При утворенні голосних звуків завжди використовується один спосіб формування повітряного потоку (генерації або ініціації): модуляція потоку повітря внаслідок коливань голосових зв'язок (фонація), тому ця ознака не може служити для їхньої класифікації.

В основі класифікації голосних лежать інші ознаки.

Додаткове темброве забарвлення голосних вимагає складної вокальної артикуляції з додатковими рухами, які модифікують властивості вокального тракту. Нарешті, при створенні голосних можуть використовуватися такі властивості, як:

- - тривалість (довгий/короткий) – не характерно для української мови, а, наприклад, для англійської – це істотна розпізнавальна властивість;
- - напруженість (напружений/ненапружений) – ця розпізнавальна властивість також притаманна ряду мов, ненапружені голосні відрізняються меншою тривалістю й інтенсивністю та зміненою артикуляцією.

Крім чистих голосних у багатьох мовах використовуються складні голосні, які описують плавний перехід від одного типу артикуляції до іншого. Зокрема, сполучення двох голосних називається дифтонгом. Прикладом є "я" [йа], "ю" [йу] в українській мові. Існують сполучення трьох звуків (трифтонги).

Класифікація приголосних. Артикуляція приголосних звуків пов'язана зі створенням перешкоди на шляху повітряного потоку в різних частинах голосового тракту. Крім того, при утворенні приголосних реалізуються всі три типи генерації (ініціації) звуку:

фонація, турбулентний шум і звуковий імпульс (вибух) та сполучення. Тому класифікація приголосних здійснюється за всіма трьома перерахованими тут критеріями.

Способи генерації. Основний спосіб створення повітряного потоку для приголосних – легеневий видихальний механізм.

Способи артикуляції. Головне в них – спосіб утворення перешкоди і місце її виникнення.

Вимовляння приголосних може супроводжуватися додатковими складними артикуляційними рухами. Наприклад, можна виділити приголосні, які долають подвійні перешкоди (їх називають іноді двофокусними) – "ш", "ж"; якщо друга перешкода утворюється шляхом зближення губ, то такі приголосні називаються лабіальними, наприклад, англійське "w".

Крім того, є приголосні з додатковою артикуляцією, зокрема, широко розповсюджені в українській мові м'які приголосні "л", "м", які утворюються за допомогою додаткової язикової артикуляції [И] - подібного типу; цей процес називається палаталізацією.

Також приголосні розрізняються тривалістю (довгий/короткий) і ступенем напруженості артикуляції (сильний/слабкий), але вони не є характерними для української мови. Крім того, всі приголосні, при утворенні яких є додатковий прохід для потоку повітря і, відповідно, відсутній сильний турбулентний шум, поєднуються назвою "сонорні". Це, насамперед, носові приголосні ("м", "н"), апроксимати ("л", "р") і напівголосні "й".

У процесі артикуляції будь-якого звуку є три фази:

- підготовча (екскурс) – органи мови займають вихідну позицію;
- стаціонарна – органи мови (язик, губи та ін.) перебувають у точній позиції, яка відповідає даному звуку;
- рекурсія – органи мови починають перебудову для наступного звуку.

При дотриманні для кожного звуку усіх фаз, мова точилася б у занадто повільному темпі. При швидкій мові (14...18 звуків у секунду) відбувається перебудова послідовностей фаз між сусідніми звуками (коартикуляція). При цьому на артикуляційне положення органів мови для даного звуку накладаються положення (рухи) органів мови, що відповідають наступному звуку. Коартикуляція у швидкій мові істотно впливає на акустичні характеристики мови й процеси її розпізнавання [44].

Частотний діапазон мовного сигналу лежить у межах 70...7000 Гц. При оцінці рівня гучності звуку за еталон звукового тиску P_0

вибирається його мінімальне значення на частоті 1 кГц, при якому звук стає вже чутним, тобто $P_0=2 \times 10^{-5}$Н/м^2. Рівень звукового тиску обчислюється наступним чином:

$$L = 20\lg\frac{P}{P_0} \text{ (дБ)},$$

де P – значення звукового тиску.

Під динамічним діапазоном розуміють різницю між максимальним і мінімальним рівнями сигналів. Динамічний діапазон мови становить 35...45 дБ.

Усі цифрові системи обробки мовних сигналів вимагають представлення аналогового мовного сигналу в цифровому вигляді. При оцифровці мовного сигналу $s(t)$ мають місце дві операції – дискретизація й квантування. Дискретизація – це заміна сигналу $s(t)$ з безперервним часом t на дискретизований сигнал – послідовність чисел $s(t_i)$ для дискретного набору моментів часу $t_1, t_2, \ldots, t_i, \ldots, t_k$ (найчастіше інтервали між моментами часу $\Delta t = t_i - t_{i-1}$ вважають однаковими). При дискретизації, звичайно, частина інформації про сигнал губиться. Втрачаються частотні складові сигналу з частотами порядку $f > 1 / \Delta t$ і вище. Кількість відліків у секунду називається частотою дискретизації. Частота дискретизації $\nu_д$, відповідно до теореми Котельникова, повинна бути принаймні у два рази вищою від максимальної частоти аналогового сигналу [3].

Сигнал після АЦП має крім низькочастотної частини спектра, яка відображає аналоговий сигнал, ще й високочастотні компоненти. Низькочастотний спектр сигналу повторюється у вигляді бічних смуг із центрами в точках, кратних частоті дискретизації ($\nu_д, 2\nu_д$ і т.д.). При зменшенні частоти дискретизації відбувається накладення низькочастотної частини спектра й бічної смуги із центром у точці $\nu_д$. Накладення спектрів приводить до появи нових спектральних складових у сигналі, що спричиняє його спотворення. Проблема вирішується використанням перед АЦП фільтра низьких частот, який придушує частоти, що лежать вище половини частоти дискретизації. Але на практиці неможливо створити фільтр із крутим спадом частотної характеристики, тому значення частоти дискретизації вибирається дещо більшим подвоєного значення верхньої частоти спектра мовного сигналу, наприклад, $\nu_д$=22,05 кГц.

Квантування сигналу – процедура, подібна до дискретизації, але усі дії виконуються над кожним окремим відліком сигналу s. При

цьому вибирається набір можливих рівнів сигналу і кожному $s(t_i)$ ставиться у відповідність найближче s_i з цього набору.

Задаючись необхідним динамічним діапазоном цифрової системи обробки мовних сигналів, необхідне число розрядів квантування можна визначити з виразу

$$D = 6n + 1{,}8 \ ,$$

де D – динамічний діапазон (у дБ); n – число двійкових розрядів. Звідси одержуємо, що для запису мови необхідно відводити не менше восьми біт на кожний відлік.

На підставі проведених досліджень з'ясовано, що прояви індивідуальності мови людини варто шукати у двох основних групах ознак. Вони пов'язані з фізіологічними (анатомічними) особливостями механізму мовотворення людини й унікальним характером приведення його в дію (артикуляційною діяльністю), обумовленим роботою центральної нервової системи.

Перша група ознак ґрунтується на добре відомій моделі мовного тракту [73], що складається з передавальної функції резонансної системи й генератора імпульсів сигналу збудження. Передавальна функція повністю характеризує індивідуальну геометричну форму порожнин мовного апарату: задню глоткову порожнину, звуження між язиком і піднебінням, передню порожнину рота, звуження між губами й т.д. Основними параметрами тут виступають характеристики чотирьох формантних областей (середня частота, частотний діапазон, енергія), огинаюча спектра та похідні від цих параметрів. Частота імпульсів збудження перебуває в прямій залежності від коливань голосових зв'язок. Коливання, у свою чергу, залежать від довжини, товщини й натягу зв'язок. Головними параметрами тут є частота основного тону, параметр тон/шум, дзвінкість, підйом основного тону й похідні від цих параметрів.

Для розрахунку параметрів, пов'язаних із фізіологічними особливостями мовного тракту, найчастіше використовуються методи спектрально-часового аналізу. Такі методи аналізу мовного сигналу адекватні природному механізму сприйняття мови [5], що робить зрозумілою тенденцію багатьох дослідників шукати індивідуальні особливості в миттєвих спектральних розподілах окремих фонем і в розподілах поточного спектра. В основі таких методів лежить класичний Фур'є-аналіз [73] або параметричний авторегресійний аналіз (як окремий випадок лінійне передбачення) [55,56].

Тісно пов'язаний зі спектральним представленням мовного сигналу гомоморфний метод [55]. Цей метод представляє мовний

сигнал у вигляді послідовності векторів кепстральних коефіцієнтів, які вимагають значно меншого об'єму пам'яті для зберігання еталонних образів. Невеликою кількістю кепстральних коефіцієнтів (звичайно 8 або 16) можна апроксимувати формантний розріз, що має високу спектральну густину. Це забезпечує більш компактне подання мовних відрізків без істотної втрати основних інформативних ознак (формантної структури, огинаючої, параметра тон/шум).

Що стосується параметрів сигналу збудження, то вони можуть бути розраховані методом виділення частоти основного тону (наприклад, кореляційний метод, кепстральний метод, метод Голда-Рабінера [55,73]).

Якщо перша група ознак відображає статичні властивості мовотвірного тракту, то друга група покликана повністю описати його зміни в часі, тобто артикуляційну динаміку мови. Припускається, що вихідним і основним етапом в організації процесу мови є керована центральною нервовою системою людини програма комплексу артикуляційних рухів, яка відповідає тому повідомленню, передача якого планується в цей момент часу [5,74].

Не викликає сумніву той факт, що індивідуальний характер результату мовної активності визначений уже на рівні центральної нервової системи, тобто на рівні синтезу артикуляційних програм. Вирішальними факторами цього процесу є такі моменти, як соціально обумовлені мовні навички мовця, його індивідуальний досвід, психологічний склад (зокрема, темперамент), характерологічні особливості й навіть інтелект. Керування мовним процесом не може здійснюватися без цих основних компонентів. Необхідно відзначити, що під артикуляційною програмою мається на увазі така програма, яка містить правила вимови певних структур. Ці правила відносяться до керування інтонацією мови, її ритмікою, наголосом, гучністю, тобто до керування просодичними характеристиками мови. При цьому артикуляційна програма поширюється на синтагми.

Під синтагмою розуміється ритміко-мелодійна, граматично оформлена одиниця мови, що виражає відносно закінчену думку. У рамках однієї синтагми виділяються супрасегментні характеристики або інтонаційні характеристики мовного потоку. Основними параметрами тут виступають інтенсивність, мелодія або рух основного тону, система наголосів, часові характеристики (тривалість сегментів, пауз, темпу), ритмічна картина мовної фрази.

Згідно поділу систем аутентифікації (розділ 1) розглядають системи верифікації та ідентифікації. При цьому під верифікацією

мається на увазі наступна ситуація. Мовець повідомляє, хто він такий (називає прізвище, PIN-код або у будь-який інший спосіб заявляє про свою індивідуальність). Система автоматичного розпізнавання індивідуальних характеристик голосу й мови (або експерт) повинна підтвердити або відкинути індивідуальність мовця. Процес може бути ініційований як легітимним носієм даної індивідуальності, так і зловмисником. Типова схема верифікації представлена на рис. 1.16.

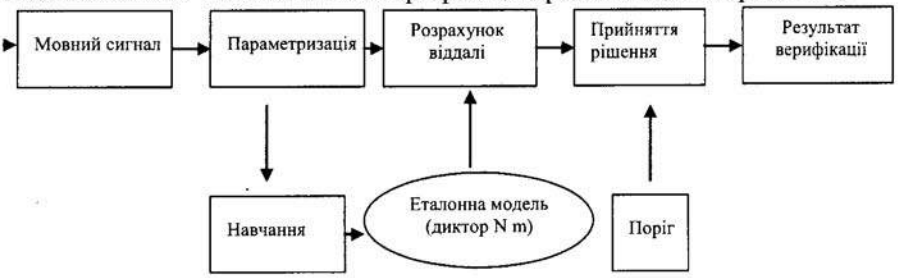


Рис.1.16. Схема верифікації.

Чиста ідентифікація має на увазі наступну ситуацію. Існує обмежена й строго контрольована група користувачів системи. При надходженні мовного сигналу система повинна прийняти рішення, хто з користувачів у даний момент вступає в мовний контакт із системою керування доступом.

Типова схема ідентифікації представлена на рис.1.17.

На жаль, серед можливих застосувань ситуація чистої ідентифікації виникає досить рідко. Прикладами можуть бути аналіз і протоколювання переговорів екіпажів, виявлення каналів витоку інформації при контролі телефонних розмов і т.д.

У більшості додатків (особливо комерційних) виникає ситуація так званої відкритої ідентифікації ("open set identification"). Користувач не надає жодного додаткового ідентифікатора (прізвище, PIN-код або інший індекс індивідуальності), а система повинна звірити мовний сигнал, що надійшов, з усіма мовними еталонами зареєстрованих користувачів. Таким чином, завдання відкритої ідентифікації збігається із завданням багаторазової верифікації.

Аналіз отриманих в Україні та закордоном результатів досліджень дозволяє стверджувати, що у галузі автоматичного розпізнавання та інтерпретації мови актуальними є такі наукові завдання:

- розпізнавання окремих слів;
- розпізнавання висловлювань, які складаються зі слів обраного словника;

- розпізнавання та інтерпретація мови для усного діалогу людини й ЕОМ на формалізованих і природних мовах предметних областей.

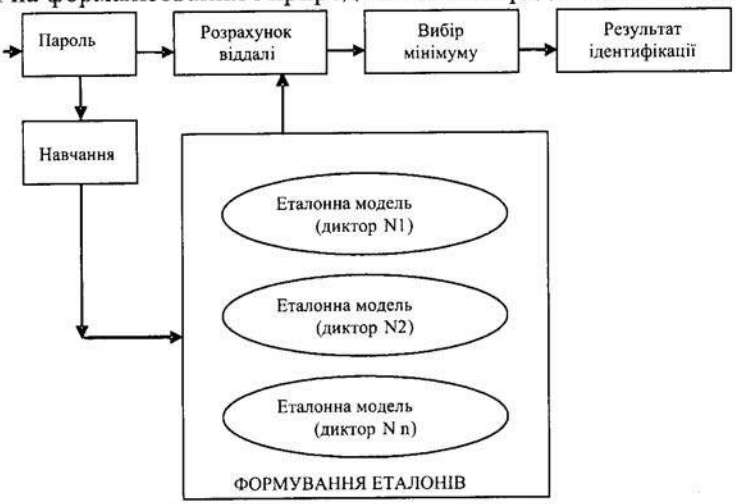


Рис.1.17. Схема ідентифікації.

Один з підходів до вирішення задачі розпізнавання мовних сигналів базується на використанні ієрархічного (І) принципу обробки інформації й введення багатозначних рішень (БР) на всіх рівнях обробки. Скорочено його можна назвати ІБР - підхід. На першому етапі вводиться багатозначна сегментація частин мовного сигналу, які відповідають фонемам або їхнім фазам. На другому рівні виконується багатозначне розпізнавання сегментів як фонем або фаз фонем. На третьому рівні здійснюється перехід від багатозначних фонемних рішень до багатозначних словесних рішень. На четвертому рівні виробляються багатозначні рішення про послідовність слів, які передаються мовним сигналом. Нарешті, на останньому, п'ятому рівні з використанням синтаксису, семантики й прагматики мови діалогу приймається кінцеве рішення про послідовність слів і зміст, які були передані мовним сигналом.

Недоліком ІБР - підходу є недостатня обробка нижніх акустичних рівнів, пов'язаних із сегментацією мовного сигналу й фонемним розпізнаванням, а також надмірна обробка верхніх лексико-семантичних рівнів. Іншим недоліком такого підходу є значна трудомісткість вирішення задачі, у результаті чого розпізнавання не може виконуватися у реальному масштабі часу.

Серед інших підходів вирішення задач розпізнавання та інтерпретації заслуговує на увагу біонічний підхід [28]. Він ґрунтується

на моделях сприйняття людиною мови й на спробах моделювання деяких функцій людини [65]. Допускається, що сприйняття мовного сигналу це – активне висування гіпотез інтелектом системи розпізнавання за законами граматики й семантики предметної області, наступної перевірки, відкидання та визначення вірогідності, тобто біонічний підхід заснований на формулюванні принципів обробки інформації, які, імовірно, використовуються людиною. У цілому цей підхід неконструктивний. Він не виходить за рамки розпізнавання окремо вимовлених слів.

Найбільш ефективним виявилося розпізнавання мови за допомогою динамічного програмування. Загальне визнання здобув так званий КДП - метод, який базується на композиції (К) еталонних мовних сигналів за допомогою автоматних відтворюючих граматик та застосування динамічного програмування (ДП) для спрямованого пошуку еталонного сигналу мови, найбільш подібного до мовного сигналу, який розпізнається. Будучи, по своїй суті, конструктивним втіленням ідеї аналізу сигналів шляхом їхнього синтезу в ланках зворотного зв'язку, КДП - метод дозволяє вирішувати завдання аналізу, розпізнавання та інтерпретації мовних сигналів на підставі єдиних позицій, а також указувати конструктивні шляхи вирішення цих завдань.

Розроблений метод розпізнавання мовних сигналів [16] дозволяє вирішувати основні проблеми їхньої обробки: розпізнавання окремо вимовлених слів; розпізнавання злитої мови, складеної зі слів обраного словника; інтерпретації злитої мови усного діалогу людини з ЕОМ на нормалізованих або природних мовах; пофонемного розпізнавання мови; навчання й самонавчання розпізнавання мови; оптимальної сегментації мовних сигналів; настроювання системи розпізнавання мови на голос диктора; багатомірного квантування мовних сигналів.

У цілому виявилося, що КДП - метод є найбільш придатним до реалізації в системах розпізнавання слів і злитої мови, а також у системах інтерпретації. Це пояснюється відносною простотою переходу від розпізнавання елементів мови до розпізнавання слів, а потім і злитої мови.

Узагальненням КДП - методу є ІКДП - метод [17]. Метод передбачає кілька рівнів ієрархії (І). Перший рівень відповідає мікрофонемам (частинам фонем). Мікрофонема задається одним або декількома еталонними елементами, які найчастіше мають природу, подібну до елементів мови, які розпізнаються. Другий рівень ієрархії – це слова, які задаються своїми звуковими транскрипціями-

послідовностями, складеними з образів першого рівня. При цьому, те ж саме слово може представлятися однією або декількома транскрипціями. Якщо обмежитися тільки двома названими рівнями ієрархії, то будемо мати систему розпізнавання слів, які вимовляються роздільно. На третьому рівні розглядаються довільні послідовності слів, які складені з обраного словника. Одержуємо, таким чином, систему розпізнавання злитої мови. На четвертому рівні ієрархії задаються тільки припустимі речення предметної області й описуються економним способом множини речень мови діалогу, які виражають той самий зміст. У результаті створюється система інтерпретації злитої мови. Образами четвертого рівня виступає переданий зміст повідомлення, який представлено у певній канонічній формі, зручній для наступного використання в автоматичних системах, і відповідей системи на запити людини.

Оскільки мовний сигнал відтворюється динамічною системою – мовним трактом людини, параметри якого під дією керування змінюються, то бажано якомога точніше відтворити ці зміни в математичній моделі сигналу. Методом, який відображає динамічні властивості сигналів і реалізує принцип фонемності в їхньому розпізнаванні, є використання дифонної моделі відтворення еталонних сигналів мови. Кожний дифон має подвійне ім'я: вхідне й вихідне, яке визначається ім'ям відповідної вхідної й вихідної фонеми. Дифони, поєднуючись у послідовність таким чином, що для двох сусідніх дифонів вихідне ім'я першого дифона збігається із вхідним ім'ям другого, створюють дифонні транскрипції слів. Перехід від фонемної транскрипції слова до його дифонної транскрипції не викликає трудностей.

Якщо залишити незмінним перший рівень ієрархії (рівень мікрофонем), а другий рівень замінити дифонним, тоді образи другого рівня ієрархії – дифони – задаються транскрипціями в алфавіті мікрофонем, а образи третього рівня – слова – задаються дифонними транскрипціями, причому, як дифони, так і слова мають не обов'язково тільки одну транскрипцію.

У роботах [19,20] проведено порівняння можливостей двох методів розпізнавання мови: ІКДП - методу й методу, побудованого на прихованих марковських моделях (ПММ - метод). Обидва методи використовують ієрархію мовних образів, конструктивні композиційні способи економного представлення різноманітних мовних сигналів за допомогою статистичних автоматних відтворюючих граматик. Методи базуються на теорії оптимальних рішень – динамічному програмуванні.

На відміну від ПММ - методу ІКДП - метод дозволяє легко задавати обмеження на допустимі тривалості мікрофонем, фонем, дифонів і слів. При цьому модель сигналів мовних образів найнижчого рівня ієрархії задається значно складнішим способом. ПММ - метод ґрунтується на припущенні про "марковість" мовного сигналу, у той час як у ІКДП - методі рекомендується будувати моделі, виходячи з апріорної інформації про словотворення, детермінованих закономірностей перетворень, сприйняття та обробки мовного сигналу.

Процедура прискорення прийняття рішень при розпізнаванні окремо вимовлених слів [18] базується на використанні дерева узагальнених транскрипцій слів. У корені (стовбурі) дерева закладено узагальнені транскрипції слів із найвищим рівнем узагальнення (об'єднання) слів. Ці узагальнення реалізуються в стовбурі наступним чином. Усі фонеми з алфавіту фонем об'єднуються в декілька узагальнених (без взаємного перетину) фонем. Відповідно до того, як об'єднуються фонеми в узагальнені фонеми, фонетична транскрипція кожного слова перетворюється в узагальнену фонетичну транскрипцію слова на рівні стовбура. В результаті весь словник слів буде розбитий на суттєво меншу кількість підсловників, що складаються із слів з однією й тією ж узагальненою фонетичною транскрипцією. У загальному випадку має бути побудоване таке дерево і, відповідно, так вибрані алфавіт узагальнених фонем та узагальнені транскрипції підсловників, щоб гарантувати потрібну швидкодію розпізнавання, а надійність розпізнавання слів була несуттєво меншою від тої, що досягається при повному переборі слів цього словника.

У роботах [97,98] розроблено моделі сигналів фонем з різною кількістю станів. Ці моделі представляють собою стохастичні автоматні породжуючі граматики і призначені для використання в ієрархічній системі розпізнавання сигналів мови. Досліджено ефективність різних моделей фонем і наведено експериментальні дані. Задача навчання розпізнаванню сигналів мови полягає у виборі моделі кожної фонеми та обчисленні ймовірнісних параметрів цих моделей [54].

Роботи [24,25] вирішують проблему узагальненого автоматичного транскрибування усномовного сигналу, яка виникає при створенні дворівневої системи розуміння мови. Вона полягає у знаходженні множини найкращих послідовностей фонем, котрі складають відповідь розпізнавання. Метод ґрунтується на конструктивному заданні всього розмаїття мовних сигналів. Для цього використовуються стохастичні автоматні породжуючі граматики, які синтезують еталонні сигнали

злитої мови, що відрізняються нелінійно змінюваними в часі темпом та інтенсивністю вимовляння, враховують коартикуляцію та редукцію звуків, індивідуальні особливості голосу. Щоб адекватніше врахувати змінюваність мовних сигналів, введено поняття фонем – трифонів та їх еталонних сигналів, а також індивідуального усномовного файла (паспорта). Правило об'єднання еталонних сигналів фонем - трифонів у послідовності полягає в тому, щоб вихідне ім'я та вхідне ім'я двох сусідніх фонем – трифонів співпадали.

Поставлена проблема розв'язується за допомогою ефективної процедури динамічного програмування. З метою значного скорочення обсягів обчислень та пам'яті використані поняття потенційно-оптимальних індексів та потенційно-оптимальних фонемних відповідей розпізнавання.

Ряд робіт [76,77,96] присвячено питанням часової трансформації мовних сигналів. Зазначається, що відповідно до фонетичної теорії мовотворення основна інформація в мовному сигналі зосереджена в межах транзитних ділянок, у той час як довгі стаціонарні фрагменти мовного сигналу є інформаційно набагато біднішими. Разом з цим прискорення або сповільнення мови досягається переважно шляхом зміни тривалості стаціонарних ділянок. Тому якість часового масштабування мовного сигналу можна підвищити, використовуючи адаптивний підхід: суттєво змінюючи тривалість стаціонарних сегментів сигналу та пауз, диференційно підходячи до перетворення тривалості коротких перехідних ділянок. Досліджено вплив на розбірливість та натуральність мови зміни тривалості окремих ділянок мовного сигналу [78], на основі чого запропоновано алгоритм високоякісного регулювання темпу мови при невисоких коефіцієнтах зміни темпу, характерних для логопедії, навчання іноземних мов, телебачення та радіомовлення. У роботі [79] наведено результати використання штучних нейронних мереж (ШНМ) для задач перетворення часового масштабу мовних сигналів, описано структуру мережі та представлено дані прогнозування зміни тривалості мовних одиниць при сповільненні темпу відтворення мовної інформації. З метою істотного підвищення прогностичних властивостей ШНМ введено поняття класу звуку і показано, що подальше покращання результатів може бути досягнуте шляхом введення в структуру мережі нелінійних синаптичних зв'язків. Розглянуто задачу керування темпом надходження голосової інформації, важливу для підвищення ефективності усномовної комунікації в людино-машинних системах [51]. Встановлено, що реалізацію зміни швидкості відтворення мовних

записів за умови натуральності звучання голосового повідомлення необхідно здійснювати через диференційовану зміну тривалості мовних елементів відповідно до властивих їм значень відносної зміни тривалості, зберігаючи загальну структуру звукових сигналів, передусім – тональних.

Усебічному висвітленню питань, пов'язаних з перетворенням часового масштабу мовних сигналів, присвячена робота [79]. У ній проаналізовано особливості зміни структури мовного сигналу в процесі зміни диктором темпу мовлення. Описано цифрову модель мовотворення та приведено моделі мовного сигналу, що використовуються в задачах перетворення часового та частотного масштабів. Запропоновано структуру системи для регулювання темпу мови в реальному часі. В роботі розглянуто лінійні методи перетворення часової структури мови, які використовують як трансформацію сигналу в часовій області, так і перетворення часового та частотного масштабів мовних сигналів за допомогою побудови систем аналізу - синтезу з модифікацією проміжного параметричного представлення сигналу. Значну увагу приділено адаптивним методам перетворення часового масштабу мовних сигналів. Запропоновано ефективну темпоральну модель мовного сигналу і на її основі розроблено алгоритм регулювання темпу мови, особливістю якого є максимальна відповідність виконуваних перетворень структури сигналу реальним процесам, які відбуваються при зміні темпу мовлення. Розглянуто питання побудови функцій темпоральних перетворень та розроблено алгоритм автоматичної сегментації мовного сигналу.

У роботі [30] представлено нові робастні алгоритми обробки мовних сигналів, спрямовані на підвищення якості процедури автоматичної верифікації особи за голосом в умовах сильних частотних спотворень сигналу та потужних завад. Програмно-апаратні комплекси, здатні в автоматичних чи автоматизованих режимах виконувати всі види акустичних та просодичні й фонетичні лінгвістичні дослідження, а також за результатами запису голосів видавати не лише рішення про їх ідентичність, але й оцінку ймовірності помилки прийнятого рішення, описано в праці [54].

Робота [33] присвячена питанням підвищення якості кепстрального аналізу мовних сигналів. У ній зазначається, що хоча в результаті гомоморфного оброблення мовних сигналів усувається вплив на огинаючу спектра мови генераторної функції мови, проте отримана огинаюча непридатна для автоматичної оцінки формантних

частот, оскільки має значно більше максимумів, ніж дійсно є формант. Тому доцільніше звуження вагового вікна (найчастіше - вікна Хемінга) для оброблення кепстру до 1,7...2 мс. Оброблений таким вікном кепстр дає більш згладжений спектр, кількість максимумів котрого дорівнює кількості формант. На цій підставі констатовано, що спектр мовного сигналу, отриманий обробленням кепстру звуженим ваговим вікном, є придатним для оцінки формантних частот і взагалі полюсів та нулів спектра первинного сигналу. Звуження вагового вікна до деякої межі (1...1,4 мс) суттєво не змінює вигляд спектра, але подальше його звуження значно спотворює спектр.

Синтезовано алгоритми автоматичного розпізнавання окремих слів і фонем мови з використанням алгоритмів оцінювання формантних ознак [66]. Спочатку для формування формантно-смугових ознак обчислюються спектрально-смугові сигнали, що відповідають імовірному розміщенню формант, а відтак знаходяться оцінки формантних частот як середніх у виділених смугах. Проведені експериментальні дослідження алгоритмів розпізнавання підтверджують можливість отримання прийнятної якості розпізнавання мовних сигналів за формантними ознаками в умовах дії адитивних гаусівського білого шуму та гаусівської вузькосмугової завади.

У роботі [67] розглянуто алгоритми розпізнавання фонем мови на основі результату "вибілювання" решіткових фільтрів, коефіцієнтів відбивання та логарифмів відношення площ перерізів голосового тракту з використанням як усереднених мір, так і процедур динамічного програмування, які виконують нелінійну часову нормалізацію. Синтезовано алгоритми розпізнавання за допомогою різних алгоритмів оцінки ознак та вирішуючих правил. Показано, що для розпізнавання фонем необхідно використовувати різноманітну інформацію: вокалізованість, тривалість тощо.

Запропоновано алгоритм багатозначної смислової інтерпретації усної мови для машини усного перекладу та диктування [16,21,22]. Цей алгоритм не гарантує глобального розв'язку проблеми розпізнавання, однак за певного вибору кількості смислів у реальному комп'ютерному середовищі знаходиться прийнятний прагматичний результат. Робота [24] містить опис програмного комплексу, в який входять програми розпізнавання усної мови, перекладу її на іншу та озвучування відповіді. Сервісні функції дозволяють вводити нову мову для перекладу, словник і настроюватися на голос диктора.

У роботі [23] розглядається озвучувач українських текстів, заснований на фонемно-трифонній моделі розпізнавання та синтезу

мовних сигналів. Синтез сигналів відбувається в часовому просторі і при цьому використовується акустичний матеріал з усномовного файла диктора. Це дозволяє максимально зменшити внесення спотворень у згенерований сигнал та значно розвантажити обчислювальний модуль. Запропонований метод синтезу дає змогу озвучувати українські тексти з доволі прийнятною розбірливістю, натуральністю синтезованого сигналу та збереженням індивідуальності мовця.

Робота [51] присвячена розробці комп'ютерних технологій моделювання та керування візуальними образами людського обличчя при синтезі мовлення. Опрацьовано два методи візуалізації процесу промовляння: 1) як послідовність змін кадрів зображення конкретного людського обличчя, яке промовляє фонетично розмічений текст; 2) як анімацію, тобто плавний перехід від однієї моделі до іншої, послідовностей об'ємних моделей людського обличчя, яке промовляє фонетично розмічений текст. Для обох методів розроблені й проілюстровані алгоритми їхньої реалізації.

1.4. Методологія розпізнавання людини за відбитками пальців

Як і в багатьох інших галузях, швидкий розвиток інформаційних технологій вніс свої корективи і в цьому напрямку розробок. Сотні висококваліфікованих (високооплачуваних) спеціалістів замінено автоматизованими дактилоскопічними ідентифікаційними системами (АДІС), наступним розвитком яких стали біометричні системи ідентифікації (БІС). Далі відбувся значний прорив у галузі біометричної ідентифікації [62]: на зміну громіздким обчислювальним блокам прийшли мікропроцесори, громіздким сканерам – сенсорні пластини товщиною декілька міліметрів. Ціна ж таких систем знизилася до такого рівня, що вони конкурують з високоякісними професійними і побутовими системами захисту, область застосування яких обмежується лише фантазією розробника.

Апаратно АДІС і БІС можуть кардинально відрізнятися, але алгоритмічне наповнення їх однакове або адаптоване до конкретних цілей, на які розрахована система. Якісні показники систем ідентифікації визначають алгоритми і методи, закладені в них. Хоча на даний час існує велика кількість алгоритмів, розробка нових не припиняється й досі. Нові алгоритми розробляються як для автономного застосування, так і для комбінування з існуючими. Як приклад, констатуємо той факт, що ще донедавна розпізнавання відбитків пальців було суто прерогативою криміналістів, а сьогодні ці

методи знаходять застосування в різноманітних сферах діяльності людини. З'явилися нові системи розпізнавання об'єктів, такі як БІС, а в криміналістиці - АДІС. На жаль, поки що в Україні немає загальнонаціональної АДІС, а використовуються російські системи "Сонда", "Папілон" і "DEX" або білоруська "ДАКТО-2000" [27]. З українських систем існують: "УкрДекс" (експлуатується в Державному науково-дослідному експертно-криміналістичному центрі (ДНДЕКЦ) м.Києва)[1,27], яка вичерпала свої можливості, тому роботи над її удосконаленням припинені, "Матриця"(у вигляді наукової розробки) та "Калина" (встановлена в Науково-дослідному експертно-криміналістичному центрі (НДЕКЦ) м.Львова) – розробка Фізико-механічного інституту ім. Г.В.Карпенка НАН України (в основу роботи якої покладені матеріали, викладені у третьому розділі). У галузі біометричних систем ситуація ще гірша, оскільки лише одна українська фірма "ЧЕЗАР" (Чернігів) випускає одиничними екземплярами БІС криптографічного захисту інформації в електронно-обчислювальних машинах [63]. Світовий же ринок таких систем розвивається високими темпами і пропонує різноманітні системи захисту, починаючи від дверних замків і закінчуючи захистом банківських рахунків. До найвідоміших АДІС можна віднести французьку систему "Morfo", яка впроваджена в практику поліції Франції, Німеччини, Ізраїлю, Словаччини, Росії та інших країн, американські системи "Printrak" та "Kogent", японську систему "Nec".

Хоча й існує велика кількість публікацій, більшість із них зосереджено на методах опису і розпізнавання дактилоскопічних зображень за особистими ознаками. Такі ознаки і методи розпізнавання відображають процес порівняння відбитків, який проводиться експертами-криміналістами. На жаль, ці ознаки є суб'єктивними і не повністю описують наявну на зображенні інформацію. Як результат, системи ідентифікації не працюють з фрагментами папілярних узорів відбитків, на яких є мало особистих ознак. Інші ж методи, які повністю порівнюють зображення відбитків з еталонами, не забезпечують необхідних експлуатаційних параметрів.

Відомі алгоритми і методи попередньої обробки дактилоскопічних зображень [135,142,153,154,160,188,204,234-236] розроблені на емпіричних засадах та не використовують для його обробки усієї наявної на зображенні інформації. Жодним з дослідників не проведено аналізу і математичного моделювання спотворень таких зображень.

Отже, особливо актуальною проблемою при створенні систем ідентифікації є розробка нових інформативних ознак і методів

попередньої обробки, які б повніше використовували наявну на зображенні інформацію.

Слід наголосити, що тільки детальний аналіз і математичне моделювання спотворень, які виникають під час формування дактилоскопічних зображень, дозволить розробити методи попередньої обробки, які б максимально покращили якість відбитка папілярного узору. Розробка ж систем інформативних ознак, які не включають суб'єктивного фактору і максимально описують наявну на зображенні інформацію, усуне недоліки існуючих систем. Це дасть змогу проводити ідентифікацію за зображеннями з малою площею папілярного узору в БІС і робити пошук злочинців за малорозмірними слідами в АДІС.

Основна галузь, в якій традиційно проводилися дослідження папілярних узорів, – дактилоскопія. Як правило, її об'єктами дослідження є сліди пальців, долонь, ступні ноги. Для реєстрації особи використовуються лише відбитки пальців і долонь.

Основні властивості папілярного узору такі [34,36,91,113,122,123, 138,145,172,192,207,229,247]:

- **Індивідуальність.** Узор шкіри індивідуальний і має відносну стійкість зовнішньої будови. На цій особливості наголошували як засновники дактилоскопії Гальтон, Генрі, так і сучасні науковці [209, 243].
- **Стабільність.** Стійкість проявляється в збереженні рисунка у відносно незмінному стані з моменту формування (при розвитку плода в утробі) і протягом усього життя людини.
- **Регенеративність.** Усі поверхневі пошкодження призводять лише до тимчасової зміни узору й у подальшому відновлюються разом із шаром шкіри.

Відбитки папілярних узорів у силових структурах зберігаються у вигляді картотеки слідів і картотеки дактилокарт (рис.1.18 а, б).

Рельєф шкіри пальця - неоднорідний, його елементами є: міжфалангові складки, вузькі складки-зморшки, пори, папілярні лінії і міжпапілярні впадини (рис.1.19).

Міжфалангові складки появляються в результаті згину пальців і, в основному, не є інформативними складовими узору. Ними послуговуються в дактилоскопії для приблизної орієнтації відбитка. Вузькі складки-зморшки утворюються через часткову втрату шкірою притаманної їй еластичності. Такі складки тимчасові й їх використання для ідентифікації можливе в короткому проміжку часу між формуванням еталонного та вхідного відбитків. Найдрібнішими

елементами рельєфу є пори – отвори потоків потових залоз. Їх розмір знаходиться в межах 0,08...0,25 мм, а форма і взаєморозташування є ключовою інформацією в пороскопії [129]. Якщо порівняти кількість пор і особистих ознак папілярних ліній, то пор значно більше. Проте розвиток пороскопії стримує складність алгоритмів, техніки і високі вимоги до якості відбитків.

Основним елементом рельєфу зовнішнього шару шкіри долонь і пальців є папілярні лінії і міжпапілярні впадини. Групуючись між собою, вони створюють різні за складністю й рисунком узори. Розрізняють узори пальців (трьох фаланг), долонь і ступні ноги. Основу ж систем ідентифікації складають узори останніх фаланг пальців, оскільки кількість ознак на одиницю площі в них найбільша.

Узори пальців розташовані з внутрішньої сторони долоні останніх фаланг і формуються декількома потоками папілярних ліній, які "заповнюють" основу, центр, вершину й краї (рис.1.20 а). Крім того, узор розділяється на структурні зони (рис.1.20 б).

Якщо розглянути алгоритмічну базу АДІС, то вона включає в себе чотири режими ідентифікації (пошуку кандидатів) (рис.1.21).

Усі режими роботи АДІС можуть забезпечуватися двома типами алгоритмів:

- **Слід-Слід** (в режимах Слід-Карта вхідний слід порівнюватиметься з кожним відбитком дактилокарти у базі даних, Карта- Слід – кожен відбиток вхідної дактилокарти вважатиметься слідом і порівнюватиметься зі слідами у базі даних).
- **Карта-Карта.**

Алгоритм пошуку типу Карта-Карта відрізняється тим, що в ньому враховується додаткова інформація про розподіл типів узорів на кожному пальці (так звана декадактилоскопія). Такий етап в алгоритмах Карта-Карта дозволяє порівнювати дактилокарти з однаковими типами узорів відбитків (тут і далі відбитком вважатимемо рисунок папілярного узору з дактилокарти), що значно пришвидшує роботу. Якщо ж дактилокарт з однаковими типами узорів декілька, то підключається алгоритм типу Слід-Слід. Отже, найважливіша ланка алгоритмів ідентифікації в АДІС – алгоритм Слід-Слід, а з практичної точки зору криміналістів найвагомішим режимом роботи АДІС - Слід-Карта. БІС - системи, які проводять ідентифікацію особи на основі специфічних фізичних або динамічних (рухових) характеристик людини. БІС, на відміну від криміналістичних, повинні не тільки забезпечувати необхідні параметри пошуку, але і бути психологічно

2754 1013 – 2771

Подольский 2063

Місце для наклейки ідентифікаційного коду

Прізвище [redacted] Дата народження [redacted] 78

Ім'я Максим Місце проживання Киев. пр [redacted]

По батькові Николаевич [redacted] ив [redacted]

Місце народження Киев Місце прописки таможн.

Професія

ПРАВА РУКА

1. Великий	2. Вказівний	3. Середній	4. Безіменний	5. Мізинець
				

Лінія згину

ЛІВА РУКА

6. Великий	7. Вказівний	8. Середній	9. Безіменний	10. Мізинець
				

Лінія згину

КОНТРОЛЬНІ ВІДБИТКИ

Ліва рука	Великий	Великий	Права рука
			

Підпис особи, що дактилоскопіюється

Карта заповнена 4.6. 1999 р.

Карту склав (вказати де і в якому органі. П.,І.,Б., посада, підпис) ИВС

Рис. 1.18 а. Фронтальна сторона дактилокарти.

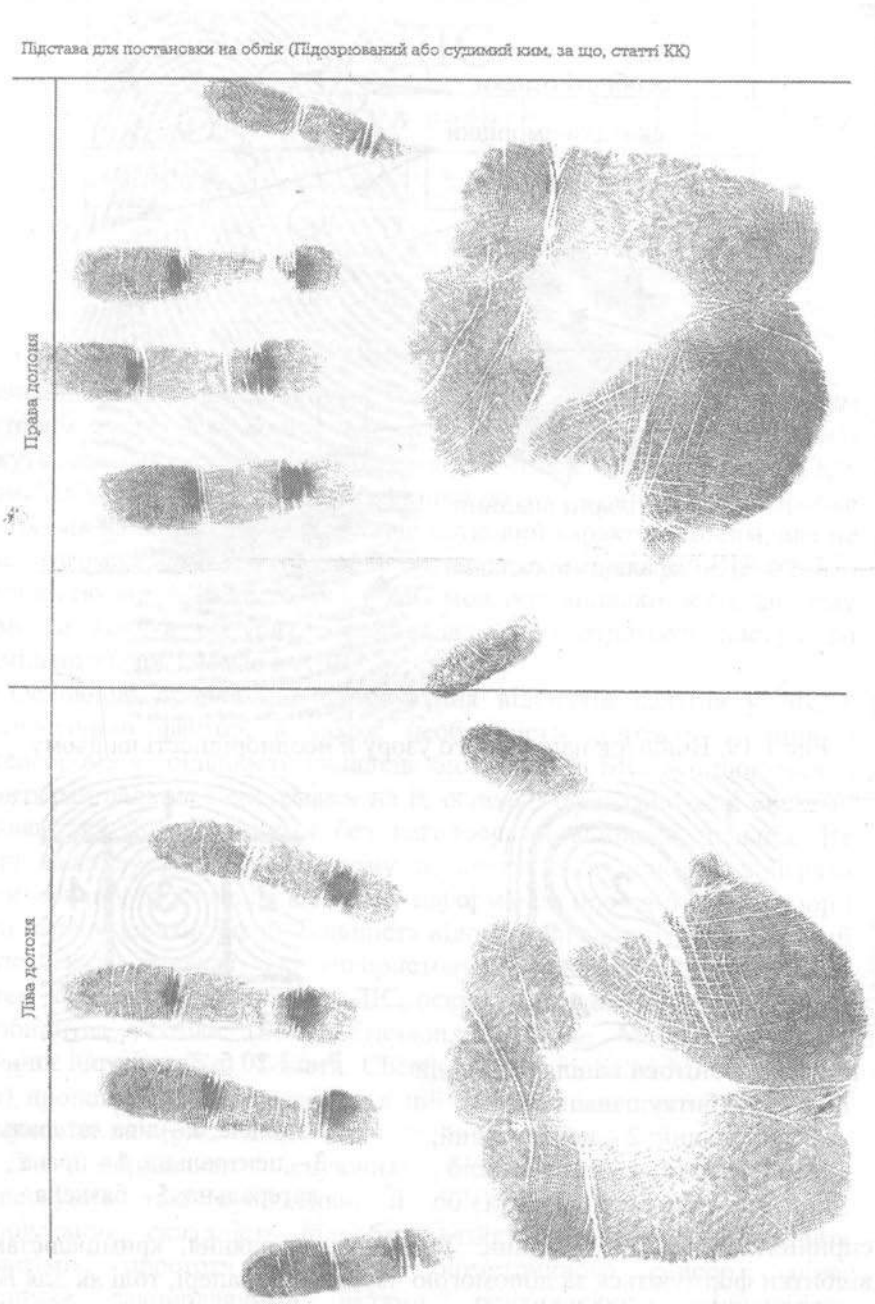


Рис. 1.18 б. Зворотна сторона дактилокарти.

Рис.1.19. Відбиток папілярного узору й неоднорідності на ньому.

Рис.1.20 а. Потоки папілярних ліній на відбитку пальця руки:
1 – дистальний; 2 – центральний; 3 – дельта; 4 – базисний.

Рис.1.20 б. Структурні зони відбитка:
1 – дистальна; 2 – ліва латеральна 3 – центральна; 4 – права латеральна; 5 – базисна.

сприйнятливими для людини. Так, для порівняння, криміналістами відбитки формуються за допомогою чорнила на папері, тоді як для БІС така технологія – неприйнятна як у плані дискомфорту, так і часу

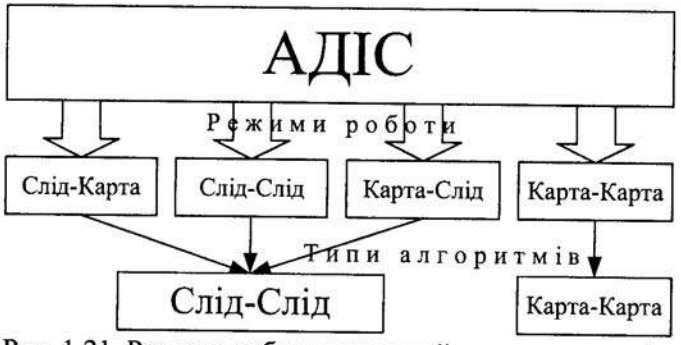


Рис. 1.21. Режими роботи системи й типи алгоритмів.

виконання необхідних процедур. Тому в цих системах дуже важливим фактором є зручність користування. Біометричні характеристики, які можуть забезпечувати високі показники ідентифікації, але незручні для формування образу, будуть мати менший попит на ринку, тож розробка алгоритмів на їх основі матиме лише науковий характер. Іншим, але не менш вагомим фактором, є ціна системи ідентифікації. Ще однією відмінністю від АДІС є те, що у БІС можливі випадки, коли систему навмисне хочуть обдурити (наприклад, щоб отримати доступ до приміщення), чого немає в АДІС.

Основною проблемою застосування відбитків пальців у БІС є психологічний фактор, а також необхідність контакту людини з біосенсором. У більшості випадків біометрія й БІС асоціюються з відбитками пальців і системами на їх основі. Переважно такі системи називаються біометричними без наголосу на відбитки пальців. Не менш важливу роль у швидкому розвитку таких систем відіграла дактилоскопія, яка надала вичерпну інформацію про папілярний узор і деякі методи ідентифікації. Більшість відомих алгоритмів ідентифікації базуються на ознаках, які використовують дактилоскопісти. Таких систем набагато більше, аніж АДІС, оскільки визнані провідні фірми з виробництва техніки (Sony, Ericsson, Samsung, Mirae, FingerKey, Biologon, Compaq, Nec, Testech, Cherry, Keytronic, SCM Microsystems і інші) пропонують свої розробки в цій галузі – сенсори та програмні продукти до них (рис. 1.22).

Для порівняння існуючих біометричних характеристик застосовують такі суб'єктивні й об'єктивні критерії: зручність використання, складність підробки, стійкість, простота виконання алгоритмів, простота виконання біометричного сенсора, ціна, підтримка законодавчими актами, психологічна прийнятність

людиною, точність систем на їх базі [151]. Якщо зіставити всі наведені критерії, то за попередньою оцінкою [151], оптимальним варіантом є БІС на основі відбитків пальців.

1.4.1. Особливості попередньої обробки в системах ідентифікації

Процедура обробки зображення зводиться до виконання певного набору операцій для візуального покращання зображення або приведення його до більш зручної для машинного аналізу форми. Для систем розпізнавання цей етап вводиться з єдиною метою - забезпечити такі характеристики зображень, при яких результати розпізнавання будуть найкращими. Це можливо за умови, якщо обробка дозволяє виділити максимальну кількість корисної інформації про об'єкт, який представлений на зображенні. Часто трапляється, що зображення після обробки в системах розпізнавання виглядає неякісним і з суб'єктивної точки зору, і за об'єктивними критеріями якості (контраст, гістограма, яскравість), які використовуються в обробці зображень, але забезпечує найкращі імовірнісні показники системи [71]. Вони є об'єктивним критерієм оцінки обробки в системах розпізнавання. Обробка зображень у таких системах будується на апріорній інформації про об'єкт розпізнавання та процес формування образу [94]. Наприклад, у системах розпізнавання літаків найбільшу корисну інформацію несуть: форма літака, згини, контур, а фонове заповнення взагалі не розглядається [83]. У БІС на основі відбитків пальців і АДІС (далі будемо вживати скорочену назву – дактилоскопічні й біометричні системи (ДБС)) основна інформація отримується з відбитка папілярних ліній, їх траєкторії, точок початку й кінця, злиття й розгалуження і т.д.

Обробка в ДБС орієнтована на те, щоб максимально точно виділити лінії без врахування їх спотворення (товщини й пор).

Загальновживаним терміном вважається попередня обробка зображень (ПОЗ), оскільки вона передує основному етапові розпізнавання.

1.4.2. Способи формування зображення

Успішне вирішення задачі обробки й розпізнавання об'єктів, у першу чергу, залежить від вибору моделі формування зображення за набором його відомих проекцій, апріорної й емпіричної інформації. Такий підхід використовується у випадках, коли неможливо отримати точний опис об'єкта й процесу формування зображення об'єкта [83].

Рис. 1.22. Біометричні сенсори і системи.

Будемо вважати, що двовимірне зображення незалежно від його природи описується функцією $g(x, y)$. Тоді процес формування нового зображення об'єкта $O(x, y, z)$ зводиться до тривимірного перетворення за допомогою оператора P. Ця операція записується таким чином:

$$g(x, y) = PO(x, y, z). \qquad (1.1)$$

Оператор P відображає як перетворення тривимірного об'єкта у двовимірне зображення, так і спотворення, що виникають на етапі його формування. В основному P визначається способом формування тривимірного узору на двовимірній плоскій поверхні сенсора або

паперу. Він також відображає спотворення, викликані специфікою відбиття, а саме: шуми, обумовлені фарбою, сенсором, пошкодженнями шкіри пальця, геометричними спотвореннями типу "губка".

Незважаючи на велику кількість публікацій на тему ПОЗ в ДБС, ще жоден із авторів не проводив аналізу й моделювання процесу формування зображення.

Для відбитків пальців розрізняють три типи процесу формування.

- Формування відбитка пальця на плоскій поверхні паперу за допомогою дактилоскопічних фарб із подальшим оцифровуванням сканером (АДІС "Сонда", "Дакто-2000") або відеокамерою (АДІС "DEX", "Калина").
- Формування відбитка на плоскій поверхні за рахунок речовин (фарба, піт, вода, тощо), які випадково потрапили на шкіру пальця. Оцифровка проводиться аналогічно, як і в попередньому пункті. Такий процес характерний для формування зображень слідів з місця злочину.
- Пряме формування зображення біометричними сенсорами. Використовується в БІС, хоча є спроби застосування й в АДІС (АДІС "Сонда", "Дакто-2000").

Для різних типів процесу формування зображення характерні свої спотворення та якість зображення (рис. 1.23).

Зображення прокатаних за допомогою чорнила пальців відрізняються від інших великою областю папілярного узору, але вони мають найбільші геометричні спотворення, і якщо не дотримуватися правил відкатки, то характеризуються поганою якістю. На даний час криміналістами вироблено чіткі правила прокатування відбитків і їх подальшого зберігання. Такий спосіб формування виправдовує себе в АДІС і не може бути застосованим у БІС. Другий спосіб формування відбитка за допомогою чорнила – простий відтиск верхньої фаланги пальця. Цим способом отримуємо менші геометричні спотворення, але й меншу область відображеного папілярного узору.

Зображення, отримані біосенсорами, відрізняються високою якістю і малими геометричними спотвореннями. До переваги таких методів відноситься миттєве формування зображення. До недоліків – менша площа папілярного узору, що відображається. Для БІС цей метод формування зображення – єдиний можливий в плані психологічного фактора.

Сенсори для папілярного узору відрізняються між собою принципом дії [62] і працюють на основі оптичного відбиття, зміни ємності між електродами, провідності шкіри, ультразвукового

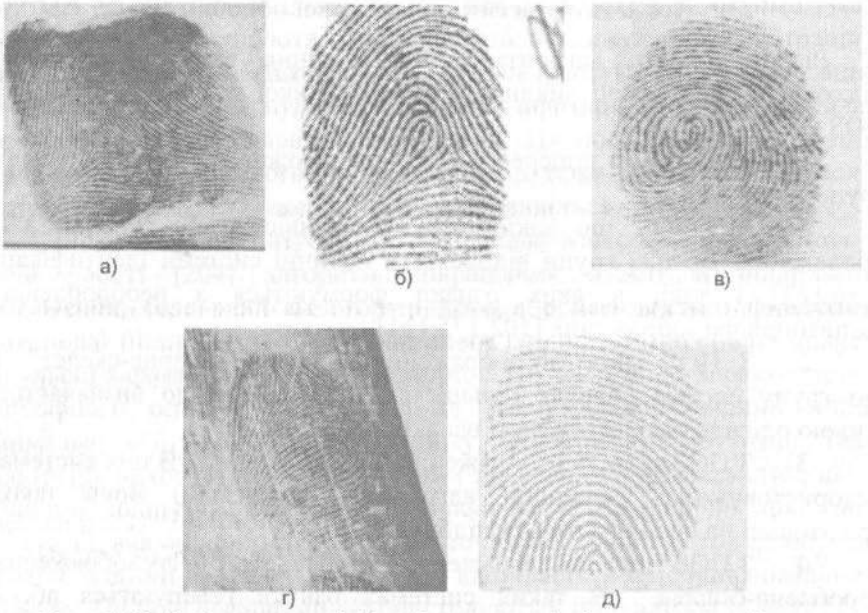


Рис. 1.23. Зображення відбитків, отримані різними способами: а) – прокатаний за допомогою чорнила відбиток пальця, оцифрований за сканером; б) – відбиток пальця, отриманий за допомогою чорнила простим натиском верхньої фаланги пальця з подальшою оцифровкою сканером; в) – зображення, отримане біосенсором Digital Biometrics; г) – латентний слід, проявлений хімічним шляхом; д) – зображення, отримане за допомогою твердотільного оптичного сканера.

сканування внутрішніх шарів шкіри, вимірювання температурної різниці. Сенсори, побудовані на принципі оптичного відбиття променів світла, дозволяють сканувати великі поверхні папілярного узору, але мають громіздку оптичну систему. Сенсори з ультразвуковим скануванням відображають папілярний узор навіть при пошкодженні верхніх шарів шкіри, але також ускладнені апаратним виконанням [154]. Найбільшого поширення набули сканери з використанням ефекту зміни ємності та провідності шкіри [63].

Надзвичайно трудомісткий і часозатратний спосіб отримання зображення має місце у випадку прихованих слідів. Зображення відрізняються найгіршою якістю і додатковими спотвореннями, а саме: змазуванням, накладанням двох узорів, присутністю фонових предметів і структури слідонесучої поверхні.

1.4.3. Алгоритми попередньої обробки

Різноманітність алгоритмів розпізнавання відбитків і різних підходів до цієї задачі викликало появу великої кількості алгоритмів ПОЗ.

Усі БІС за типом попередньої обробки можна поділити на чотири групи.

1. Без ПОЗ, що викликано неможливістю або складністю її проведення. До цієї групи відносяться оптичні системи ідентифікації [136,163] і такі, в яких ознаки формуються з необробленого напівтонового зображення [102,175,181].

2. З ПОЗ типу "вх.зображення-оброблене-бінарне-скелет". В цю групу систем попадає більшість БІС і АДІС, що визначається їхньою орієнтацією на особисті ознаки відбитків.

3. З ПОЗ типу "вх.зображення-бінарне-скелет". В цих системах використовуються складніші алгоритми бінаризації. Вони також орієнтовані на особисті ознаки відбитків.

4. З ПОЗ типу "вх.зображення-оброблене", або "вх.зображення-оброблене-бінарне". В таких системах ознаки генеруються або з обробленого, або з бінаризованого зображення. Сюди попадають системи, які базуються на особистих та інших типах ознак.

Розглянемо детальніше алгоритми обробки останніх трьох типів систем.

Для систем другої групи основною проблемою є бінаризація зображення. Даній проблемі присвячена велика кількість публікацій [83,208,211] і додатково кожен розробник ДБС намагається її удосконалювати та пристосовувати під власні потреби. В загальному, всі зображення характеризуються різною яскравістю та контрастом, тому використовують бінаризацію з адаптивним порогом. Типовою рисою біометричних зображень є те, що зміна яскравості та контрасту можлива локально, і тому іншим варіантом є локальна адаптивна бінаризація. У більшості випадків в АДІС і часто у БІС якість вхідного зображення є низька, що приводить до поганих результатів навіть при локальній адаптивній бінаризації. В таких ДБС усі етапи, що передують бінаризації й скелетизації, виконуються з метою покращання її результатів.

Проведемо короткий огляд відомих алгоритмів обробки типу "вх.зображення-оброблене-бінарне-скелет".

1. Ітераційний алгоритм, що базується на теорії нечітких множин [43] і бінаризації з адаптивним порогом [254]. Зображення

ділиться на малі блоки, кожен із яких обробляється окремо. Над кожним блоком виконуються такі операції: згладжування (фільтрація), нечітке кодування (fuzzy coding), контрастування, бінаризація, обчислення кількості нулів і одиничок, нечітке декодування (fuzzy decoding), адаптація параметрів обробки. Ця послідовність операцій здійснюється для кожного блоку до тих пір, поки кількість одиничок і нулів у бінарному зображенні блоку не зрівняється.

2. Огормен і Нікерсон (O'Gorman and Nickerson) пропонують у своїй роботі [204] алгоритм покращання якості й бінаризації зображення, базований на згортці його з орієнтованими фільтрами (directional filters), згідно із зображенням орієнтації (directional image). Імпульсні характеристики (ІХ) фільтрів адаптуються до характеристик папілярного потоку: мінімальної та максимальної ширини ліній, мінімального й максимального періоду, максимальної крутизни. Така фільтрація виконується з урахуванням локальних характеристик, які є стійкими до шумів, оскільки визначаються відповідно до локальної орієнтації, яка оцінюється з високою точністю. Даний метод фільтрації вимагає згортки великих масивів, що відбивається на обчислювальних затратах. Подібні алгоритми використовують й інші автори [132,187].

3. Група вчених (Sherlock, Monroe, Millard) [234,235] розробила алгоритм покращання якості зображення за допомогою спрямованої частотної фільтрації з урахуванням локальної орієнтації з наступною бінаризацією. Група інших учених (Wilson, Watson, Paek) [259] опрацювали подібний підхід, в якому зображення, які розбиваються на блоки розміром 32×32 точки, фільтруються орієнтованими фільтрами й підсилюють домінуючі частоти. Блоки зображення формуються з перекриттям для зменшення краєвих ефектів. Дещо змінений алгоритм запропонований у роботі [135], де результуюче зображення формується з набору профільтрованих згідно із зображенням орієнтації.

4. Найбільшого поширення, завдяки універсальності, набув алгоритм, розроблений групою вчених Мічіганського університету [160]. Його основним етапом є обробка зображення спрямованим фільтром Габора. Алгоритм складається з етапів: нормалізації, оцінки зображення орієнтації, оцінки зображення періоду папілярних ліній, сегментації, фільтрації, бінаризації, скелетизації. Такий алгоритм найповніше серед існуючих використовує наявну інформацію на зображенні для подальшої обробки [110].

5. Хонг (Hong) [151] запропонував алгоритм обробки зображення, який передбачає такі етапи: фільтрація зображення набором фільтрів Габора, екстрагування чорних і білих ліній на

зображенні, сегментація та оцінка орієнтації зображення алгоритмом мажоритарної вибірки, компонування результуючого зображення з профільтрованих. Цей алгоритм є найскладнішим, тому час обробки одного зображення неприпустимо великий, адже необхідно реалізовувати фільтрацію зображення набором фільтрів.

6. Алгоритм, який базується на операторі розмиття (Scale-Space Operator), адаптується до структури папілярних ліній [142]. Процедура визначення параметрів оператора передбачає оцінку локальної ширини папілярних ліній і адаптації рівня розмиття до рівня шуму. Додатково проводиться оцінка якості папілярних ліній, яка відображає, наскільки добре структура зображення відповідає моделі папілярних ліній.

Розглянемо алгоритми типу "вх.зображення-бінарне-скелет". Орієнтованість такої обробки на побудову скелета зображення чітко прив'язує їх до систем, що працюють з особистими ознаками або ознаками, що описують скелет.

1. Алгоритми такого типу запропоновані вже згаданою групою вчених Мічіганського університету. Перший [219] відноситься до простих алгоритмів, оскільки передбачає локальну бінаризацію з адаптивним порогом. Основна відмінність від найпростіших алгоритмів полягає в тому, що під час бінаризації враховується напрямок папілярних ліній, згідно з яким вибирається поріг бінаризації. Продовженням роботи вчених цього університету став алгоритм [244], в якому додатково здійснюють детектування ліній.

2. Ітераційно застосовувати оператор Лапласа й два динамічних пороги для бінаризації пропонують у праці [191]. На кожному кроці ітерації зображення згортається з оператором Лапласа, а точки, яскравість яких виходить за межі динамічного діапазону, відмічаються нулем або одиницею. Далі поріг змінюється на величину, яка забезпечує збіжність алгоритму. Подібне вирішення задачі підтримують й інші розробники [217,261], які після операції згортки вибирають локальні динамічні пороги у відповідності до локального контрасту.

3. Алгоритм із бінаризацією за контурами ліній вхідного зображення запропоновано в роботі [119]. Контури формуються за допомогою оператора Марра-Хілдрета.

4. Використовувати комплексний метод відновлення та покращання відбитків, враховуючи динамічну нелінійну систему, яка названа M-Lattice, що базується на реакційно-дифузійній моделі (reaction-diffusion model), пропонують автори роботи [236].

Четвертий тип алгоритмів не передбачає формування скелета. Такі алгоритми орієнтовані на генерування набору ознак із напівтонового або бінарного зображення.

1. Ученими Болонського університету запропоновано алгоритм відслідковування папілярних ліній на напівтоновому зображенні [181]. Цей процес проводиться згідно до напрямку градієнта яскравості. Набір стартових точок визначається накладанням прямокутної сітки на вхідне зображення. Для кожної стартової точки алгоритм відслідковує лінію до її закінчення або злиття з іншою (що і є особистими ознаками).

2. В роботі Вебера [255] вхідне зображення фільтрується смуговим фільтром у частотній області й бінаризується з локальним порогом. Далі запропоновано визначати особисті ознаки узору на бінарному зображенні без формування скелета.

3. Визначення особистих ознак за дивергенцією зображення орієнтації описане в роботі [246]. Алгоритм базується на використанні оператора дивергенції для визначення розривів в узорі, які й відповідають ознакам. Алгоритм забезпечує задовільні результати лише для якісних зображень.

Як видно з короткого опису існуючих алгоритмів, всі вони орієнтовані на системи з векторами особистих ознак. Лише алгоритми ПОЗ типу "вх.зображення-оброблене-бінарне-скелет" можуть бути використані для отримання напівтонових оброблених зображень. Алгоритми, базовані на нечітких множинах і на операторі розмиття, не забезпечують такої якості вихідного зображення, як алгоритми, що використовують спрямовану фільтрацію. Найкращі результати забезпечує алгоритм Хонга, але через високі обчислювальні затрати він є неприйнятним.

З метою розробки алгоритму та методів ПОЗ за базу взято праці [135,153,234,235,259], оскільки вони забезпечують якісну ПОЗ без великих обчислювальних затрат. Загальна структура ПОЗ представлена на рис.1.24.

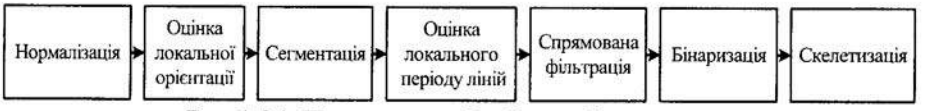


Рис.1.24. Попередня обробка зображення.

1.4.4. Методи попередньої обробки

а) Нормалізація. Цей етап не змінює папілярного узору, а зменшує варіацію яскравості самих зображень. В алгоритмі [153,160] застосовується глобальна нормалізація яскравості, а в алгоритмі [259] перетворення гістограми – її розтягування. Ці два методи вирішують одну і ту ж задачу, але різними способами. Обидва методи борються лише з глобальними спотвореннями кривої яскравості і не усувають локальних.

б) Оцінка локальної орієнтації. Даний етап обробки заслуговує на більшу увагу, оскільки існує велика різноманітність методів.

Що ж таке орієнтація папілярної лінії й яка взагалі може бути орієнтація кривої? Мова йде не про числове значення орієнтації, а про зображення орієнтації, яке визначає орієнтацію $\theta(i,j)$ дотичної до папілярної лінії у будь-якій точці $g(i,j)$ вхідного зображення (рис.1.25). Якщо точка оцінки орієнтації знаходиться між папілярними лініями, то оріентація визначається за ними.

Концепцію зображення орієнтації для відбитків пальців розвинули Метре, Марсі, Кепур [188], які вважають, що зображення орієнтації це не що інше, як перетворене вхідне зображення, а оцінка орієнтації – математичне перетворення. Їхній алгоритм відрізняється простотою, малими обчислювальними затратами і низькою точністю оцінки.

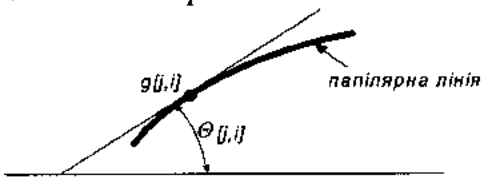


Рис.1.25. Орієнтація папілярної лінії.

На даний час найчастіше використовуються методи, які базуються на оцінці орієнтації за градієнтами яскравості вхідного зображення. Градієнт яскравості напівтонового зображення - орієнтований вектор, який вказує напрям і швидкість зміни яскравості в околі точки зображення. Локальну орієнтацію лінії за орієнтацією градієнтів обчислюють декількома способами, які, в свою чергу, є продовженням роботи Рао [221].

Група авторів [166,219] пропонує оцінювати орієнтацію ліній за усередненим напрямком градієнтів. Альтернативним варіантом є вагова схема оцінки [186]. Добрі результати оцінки забезпечує середньоквадратичний метод [115], а також використання власних

значень і власних векторів автоковаріаційної матриці [100]. Продовженням роботи над цими методами стали ітераційні методи [153,159,160], які включають у себе попередню обробку. Так, запропоновано оцінювати орієнтацію методом усереднення кута градієнтів, визначати її середньоквадратичне відхилення, і якщо воно більше за певний поріг, то проводити повторну оцінку, але вже у більшому околі [159]. Існує й дещо складніший алгоритм [153,160]: орієнтація оцінюється усередненням кутів градієнтів, зображення орієнтації переводиться у неперервну площину (косинусів і синусів орієнтації), здійснюється низькочастотна фільтрація, відновлюється профільтроване зображення орієнтації.

Огляд згаданих методів і алгоритмів оцінки вказує на перевагу градієнтних методів над іншими, крім алгоритму Хонга, який є точнішим, але непомірно збільшує обчислювальні затрати. Метод оцінки на основі автоковаріаційної матриці [100] також вимагає великих часозатрат. З градієнтних методів найкращий результат забезпечує оцінка з фільтрацією орієнтації [153,160], який покладемо в основу розробки власного.

в)Сегментація зображення. Сегментація передбачає поділ зображення на дві області: інформативну, в якій наявний папілярний узор, і неінформативну (ще її називають фоновою), в якій відбиток відсутній.

Для різних типів систем і зображень використовують свої специфічні методи сегментації. Проте для зображень відбитків методи дещо відрізняються від класичних [209,211].

Метре, Марі і Кепур [188] пропонують розбивати зображення на блоки, будувати гістограму середньоквадратичного відхилення яскравості зображення для 16 напрямків орієнтації, визначати пік гістограми, і якщо він перевищує порогове значення, то блок зображення відносити до інформативної області, інакше – до неінформативної. У своїй роботі [186] вони згадують, що їх перший метод коректно працює лише для якісних зображень й дає неправильну сегментацію в областях зображення з великою крутизною ліній. Замість нього, пропонують проводити блочну сегментацію за дисперсією яскравості зображення. Якщо дисперсія яскравості перевищує апріорно заданий поріг, то блок відмічається як інформативний, інакше – як неінформативний. Дещо удосконалений варіант полягає у тому, що дисперсія яскравості обчислюється вздовж напрямку орієнтації і перпендикулярно до нього [219]. Якщо різниця між ними перевищує порогове значення, то блок відмічається як інформативний, інакше – як неінформативний. Блоки, які належать до

фонової області, характеризуються малою дисперсією в обох напрямках. Запропоновано цілий алгоритм блочної сегментації [259], який передбачає сегментацію за порогом, що визначається адаптивна до мінімальної та максимальної яскравостей повного зображення, три етапи ерозії й формування замкнутої інформативної області. Недоліком його є неспроможність відкидати неякісні області зображення. Вважається доцільним використовувати відразу три параметри для сегментації (в даному випадку це уже класифікація) [101]: когерентність ліній, середнє значення та дисперсію яскравості у блоці. Далі проводять класифікацію на підставі лінійної вирішуючої функції [90] з апріорно визначеними ваговими коефіцієнтами. Іноді також використовують три параметри класифікації [154]: амплітуду яскравості (різниця між середнім значенням яскравості папілярних ліній і міжпапілярних впадин), частоту ліній (обернене значення до періоду) і дисперсію яскравості, які характеризують структуру папілярних ліній. Класифікація проводиться методом найближчого сусіда по шести еталонах для кожного класу. Оскільки оцінка частоти папілярних ліній є нестійкою до шумів на зображенні, то і класифікація блоків теж буде нестійкою.

Зважаючи на недоліки певних методів і алгоритмів сегментації, можемо стверджувати, що найкращим вибором будуть методи сегментації за когерентністю потоку папілярних ліній.

г) Оцінка локального періоду папілярних ліній. Локальний період папілярних ліній - це віддаль між ними (рис. 1.26).

В літературі описаний лише один метод оцінки локального періоду папілярних ліній [153,160]. Він передбачає побудову проекції фрагмента папілярної лінії в околі точки оцінки на вісь перпендикулярну до її орієнтації. Далі на одновимірній проекції, яка в ідеальному випадку повинна бути гармонічною хвилею, шукають піки і за віддалю між ними оцінюють середній період в околі точки. У блоках, де період не був оцінений, він визначається за періодом у сусідніх блоках. Останньою процедурою оцінки є низькочастотна фільтрація зображення локального періоду. Такий метод забезпечує точну оцінку періоду для якісних зображень із чіткими паралельними папілярними лініями. У зашумлених областях для папілярних потоків із міжпапілярними включеннями, точок із непаралельними лініями цей метод неправильно або взагалі не оцінює періоду. Це відбувається через утрату проекцією гармонічного характеру.

Рис.1.26. Локальний період папілярних ліній.

Метод оцінки глобального (середнього) періоду для всього зображення [46-49] передбачає формування восьми січень зображення і за їх одновимірними представленнями оцінку середнього періоду ліній. Цей метод простіший, але менш точний від попереднього, оскільки січення можуть проходити через фонову або зашумлену область зображення відбитка, а також уздовж папілярних ліній для деяких типів узорів.

Огляд існуючих методів указує на їх недостатню стійкість і точність.

д) Спрямована фільтрація. Першими фільтрацію до відбитків пальців застосували розробники АДІС PrintRac. Зображення розбивалося на блоки 32×32 точки, які перекривалися. Кожен блок фільтрувався смуговим фільтром із підсиленням домінуючих частот. Недоліком цього фільтра є поява артефактів на вихідному зображенні.

Спрямовані фільтри були спочатку розроблені для сегментації текстурних зображень [156], за допомогою яких на зображенні виділялися лінії, розташовані під певним кутом. Для зміни спрямованої властивості фільтра його амплітудно-частотна характеристика (АЧХ) (рис.1.27) повертається на необхідний кут.

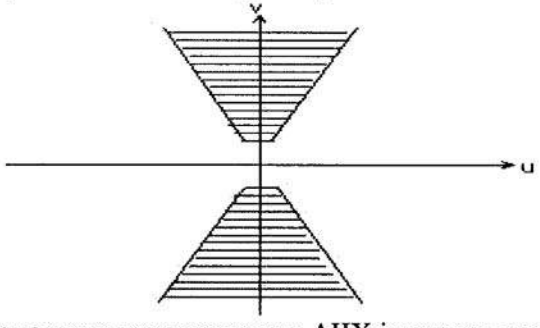
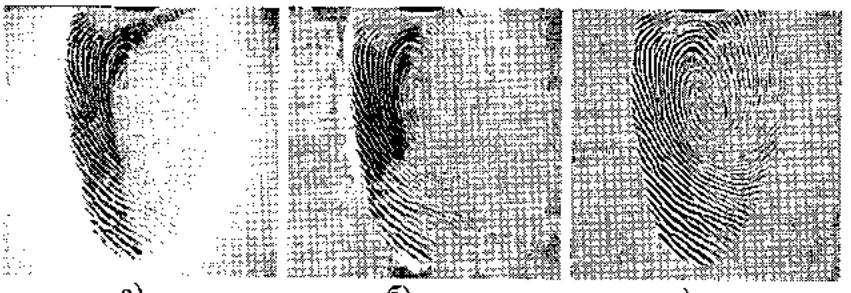


Рис.1.27. Схематичне представлення АЧХ ідеального спрямованого просторового фільтра.

Обробка зображень ідеальним спрямованим частотно-смуговим фільтром [259] призводить до спотворення ліній і значних краєвих ефектів. У вдосконаленому фільтрі [235] АЧХ розбита на дві незалежні складові. Перша складова фільтра відповідає за частотну смугову фільтрацію і представляє собою смуговий фільтр Батерворта, настроєний на середній період папілярних ліній, а друга - за спрямовану фільтрацію і є не чим іншим, як синусоїдальним фільтром [3]. Результуюче зображення комбінується мажоритарним алгоритмом із профільтрованих десяти зображень. Застосування такої АЧХ дозволило зменшити краєві ефекти, але не позбутися їх повністю. Перспективніше використовувати для комбінування результуючого зображення не мажоритарний алгоритм, а зображення орієнтації [135]. Усі розглянуті методи спрямованої фільтрації передбачають багатократне виконання швидкого перетворення Фур'є (ШПФ), що є основним стримуючим фактором широкого застосування цих алгоритмів. Також зауважимо, що краєві ефекти виникають у всіх згаданих методах.

Значно кращі результати забезпечує фільтрація спрямованим фільтром Габора (рис.1.28) [153,160], АЧХ й ІХ якого є краще локалізовані.

Просторова локалізованість ІХ фільтра Габора повністю усуває проблему краєвих ефектів і зменшує обчислювальні затрати на згортку. На відміну від методів обробки спрямованими фільтрами Фур'є у цьому методі повне зображення згортається один єдиний раз, але ІХ фільтра адаптується до періоду та орієнтації у кожній точці зображення. Така адаптація дозволяє більш точно локалізувати основну



а) б) в)

Рис.1.28. Необроблене зображення (а), профільтроване спрямованим ідеальним (б) і спрямованим фільтром Габора (в).

спектральну складову і відфільтрувати інші, які вважаються шумовими.

Огляд фільтрів указує пріоритет використання фільтра Габора на етапі ПОЗ. Єдиним недоліком буде необхідність оцінки зображень періоду й орієнтації папілярних ліній.

1.4.5. Інформативні ознаки й методи розпізнавання

а) Класифікація методів розпізнавання. Системи ідентифікації можна розділити за інформацією, яку вони описують векторами інформативних ознак і методами їх порівняння (рис.1.29).

Кожна з наведених систем має свої переваги й недоліки. Додатково до розглянутих використовуються ще класифікаційні ознаки.

б) Класифікаційні ознаки й методи. Класифікаційні ознаки – це форма узору папілярів (завитки, кола, спіралі тощо), напрям їх потоку (спіралі з правим обертанням, лівим тощо), особливості будови елементів узору (положення дельт, будова центрального узору тощо), кількість включень (папілярних ліній) між елементами узору (між дельтою й центром узору, в серцевині узору).

За класифікаційними ознаками узори діляться за системою Гальтона-Генрі на три типи: дуговий, завитковий і петльовий (рис. 1.30).

Петльові узори з ймовірністю появи 0,639 складають найпоширенішу групу. Простою кластеризацією за класифікаційними ознаками можна досягти значного зменшення множини зображень, які необхідно порівнювати точнішими, а отже, і більш часозатратними методами.

У криміналістиці для порівняння дактилокарт за класифікаційними ознаками використовується дактилоформула, яка, у свою чергу, поділяється на основну й додаткову. При записі основної й додаткової дактилоформули використовується десятипальцева система опису – декадактилоскопія. Дактилоформула представляє собою вектор інформативних ознак. Порівняння відбувається шляхом зіставлення вектора шуканої дактилокарти з еталонною, а умовою відповідності є їх рівність. Максимальна імовірність появи двох однакових дактилоформул для різних дактилокарт рівна 0,164 [80].

Дактилоформули використовуються в АДІС при пошуку в режимі Карта-Карта. Клас узору відбитків в АДІС виставляється автоматично з корекцією оператором або відразу оператором.

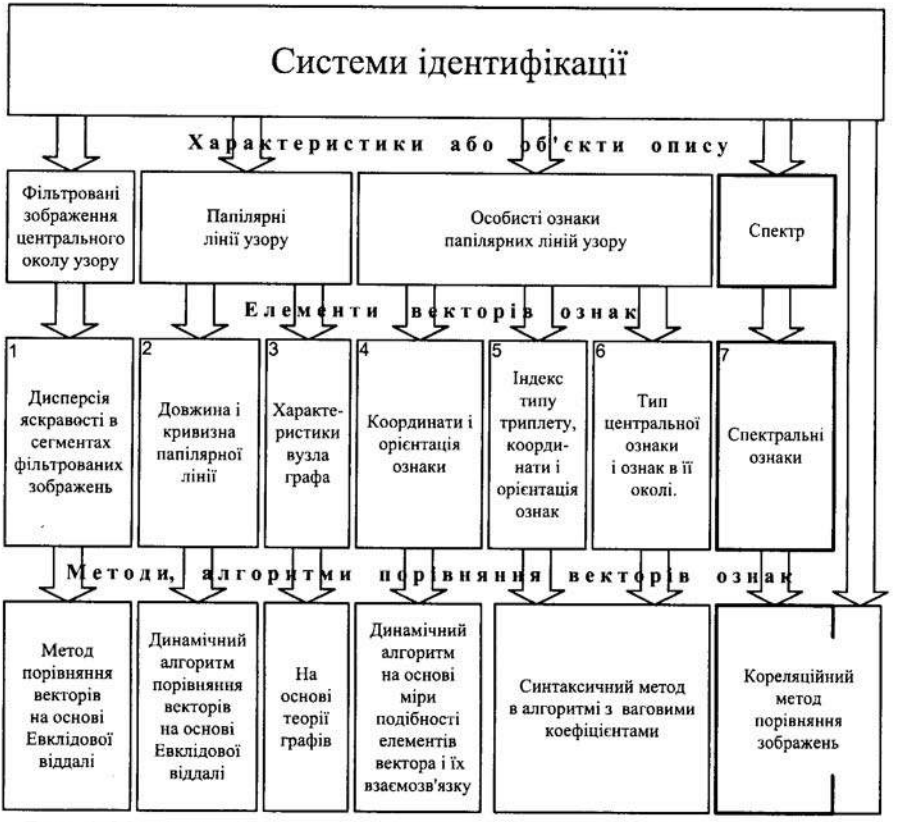


Рис. 1.29. Класифікація систем ідентифікації. Потовщеною лінією виділена гілка систем, до якої відносяться розроблені методи.

а) б) в)

Рис. 1.30. Типи папілярних узорів:
а) – дуговий; б) – завитковий; в) – петльовий.

Розробники деяких біометричних систем пропонують використовувати класифікаційні ознаки для грубої кластеризації бази даних еталонів із подальшим розпізнаванням вхідного зображення по тому кластеру, до якого воно належить. Такий метод прямо запозичений з криміналістики і не завжди точно відображає усе розмаїття узорів.

Прямим відображенням класифікації на автоматизовані системи можна вважати метод запропонований у [115], в якому класифікація відбувається емпірично побудованим алгоритмом: шукаються сингулярні точки узору – центр і дельти, їх кількість, взаєморозташування, індекс Пуанкаре для центра. На основі цієї інформації структурним алгоритмом проводиться класифікація. Алгоритм дозволяє класифікувати лише добре виражені типи узорів і дає неправильні результати для перехідних або важких для класифікації типів. Неточність алгоритму виражається 7-11% неправильно класифікованими узорами.

Запропоновано використовувати метод, який для класифікації бере до уваги одну сингулярну точку – центр узору та окіл навколо неї [216]. Далі окіл ділиться на 80 сегментів, у кожному з яких проводиться нормалізація яскравості. Окіл фільтрується набором з 8 спрямованих фільтрів Габора, формуючи 8 фільтрованих зображень. Формується вектор з 640 ознак за дисперсію в кожному сегменті околу для 8 зображень. Відбиток класифікується методом k-найближчих сусідів або нейронними мережами. Точність цього методу в межах 5...7%. Помилки в основному виникають під час класифікації перехідних типів узорів. Метод не чутливий до зсуву і до повороту в межах ±12°.

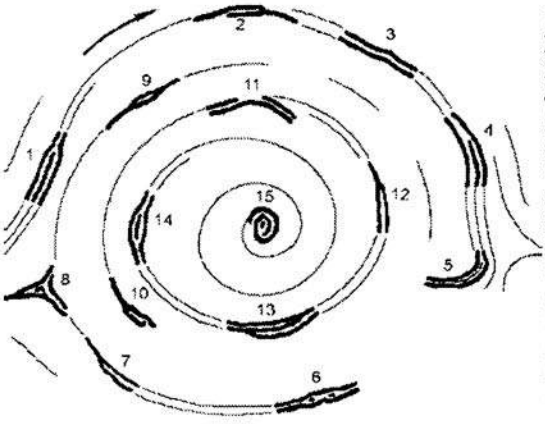
Якщо використовувати вектор зі 112 інформативних ознак, які формуються перетворенням Карунена-Лоєва із зображення орієнтації [112] класифікація проводиться різними типами класифікаторів: за мінімальною віддаллю до еталона, параметричним, найближчого сусіда, найближчих декількох сусідів, нейронним, статистичним нейронним. Найкращий результат дає статистичний нейронний класифікатор – 7% хибних класифікацій. Для коректної роботи такого класифікатора відбиток повинен бути просторово нормалізований і відображений повністю.

Відомо декілька методів і ознак для класифікації [118]. За першим методом зображення орієнтації розбивається на блоки і кожному з них, згідно з його домінуючою орієнтацією, присвоюється індекс. Вектор інформативних ознак формується з усіх записаних підряд індексів.

Другий метод оперує ознаками на основі просторового спектра зображення. Спектр розбивається на сегменти за кутом і частотою гармонічних складових. У кожному сегменті обчислюється сумарна енергія, з яких формується вектор ознак. Для цих двох векторів ознак застосовують різні типи класифікаторів, однак похибка класифікації знаходиться в межах 10...20%. Використання таких ознак на практиці недоцільне через їх чутливість до афінних перетворень і до неповного відбиття узору. Окрім цього класифікацію можна здійснювати шляхом кореляції зображення з еталонними. Кореляцію проводять бінарних, бінарних згладжених, скелетизованих, скелетизованих згладжених зображень. Похибка класифікації, відповідно, складає 25%, 25%, 10%, 5%. Цей метод, як і попередні, чутливий до афінних перетворень, але вже значно менше до неповного відбиття узору.

Наслідком невисокої точності методів класифікації типів узорів є майже цілковита відмова розробників БІС від їх застосування. Вони широко використовуються в АДІС, оскільки оператор системи вручну коректує неправильно визначений тип. У БІС доцільним може виявитися швидкий метод попереднього просіювання кандидатів на ідентифікацію замість класифікації. Такий метод повинен характеризуватися мінімальною ІНН і достатньо малою ІНІ для забезпечення пришвидшення роботи системи. Один із варіантів побудови такої системи буде описано далі.

в) Особисті ознаки. З літературних джерел [34,36,91] відомо про різні набори особистих ознак, тому наведемо їх загальний опис (рис. 1.31).



1 – закінчення;
2 – зустрічне розташування;
3 – згин;
4 – початок;
5 – міжпапілярна лінія;
6 – точки;
7 – злиття;
8 – дельта;
9 – око;
10 – гачок;
11 – розрив;
12 – розгалуження;
13 – місток;
14 – фрагмент;
15 – центр узору.

Рис. 1.31. Схематичне представлення особистих ознак.

Під час розпізнавання зображень відбитків за допомогою особистих ознак основною інформацією є не наявність чи відсутність ознак, а їхнє взаєморозташування. У ході експертної розробки відбитка пальця криміналістами формальний опис зводиться до визначення кутів розташування ознак, а також кількості ліній, що розташовані між ознакою й центром узору. Далі фіксується послідовність із числових позначень ознак, кутів і віддалей (кількості папілярних ліній між ними) [36].

У ДБС для того, щоб при формальному описі зображення відбитка не виникало ситуацій, коли відбиток не має жодної інформативної ознаки, використовують ознаки з великою імовірністю появи. Для уникнення помилок, викликаних неправильною ідентифікацією ознак, задіюють ознаки, які стійкі до спотворень слідотворення і на які можна розкласти складніші – це закінчення-початок і злиття-розгалуження. В більшості алгоритмів ідентифікації не робиться поділ на типи ознак, а реєструється лише їх положення і взаєморозміщення.

Коротко розглянемо існуючі вектори ознак і методи ідентифікації, побудовані на їх основі.

Найпростіший вектор ознак [115,151,159,171] (блок №4 рис.1.29) описується так:

$$\begin{aligned} \mathbf{V} &= (\mathbf{V}_i'),\ i = 1..N\ , \\ \mathbf{V}_i' &= (x_i, y_i, \varphi_i)\ , \end{aligned} \tag{1.2}$$

де $\mathbf{V}_i'$ – вектор ознак i-ї особистої ознаки узору з координатами x_i, y_i та орієнтацією φ_i; N – кількість особистих ознак.

Такий вектор не потребує попередньої підготовки до розпізнавання, наприклад, сортування елементів, що відбивається на складності алгоритмів порівняння.

Найпростіший, проте дуже швидкий алгоритм [115] передбачає три етапи порівняння векторів $\mathbf{V}_1$ і $\mathbf{V}_2$, описаних виразом (1.2):

- перебір усіх можливих комбінацій афінних перетворень другого порядку (зсув і поворот), які елемент вектора $\mathbf{V}_1$ перетворюють в елемент вектора $\mathbf{V}_2$. На основі цього визначається комбінація параметрів афінних перетворень одного зображення в інше;
- просторова нормалізація вектора $\mathbf{V}_1$ зворотнім до визначеного афінним перетворенням;
- обчислення кількості ознак, що збігаються з певним допуском, яка і відповідає рівню подібності узорів.

Недоліком алгоритму є чутливість до нелінійних геометричних спотворень ("губки") і низька точність визначення параметрів афінного перетворення при малій кількості особистих ознак.

Алгоритм, подібний до розглянутого побудований на основі використання генетичних алгоритмів із нечіткою логікою [171]. Коефіцієнт подібності ознак обчислюється за Гаусівською кривою, а подібність двох векторів визначає їх сума.

Додатково описувати відрізок скелета папілярної лінії, до якого належить особиста ознака, запропоновано в роботах Хонга [151,159]. Вектор ознак набуває вигляду:

$$\mathbf{V} = (\mathbf{V}_i'),\ i = 1..N\ ,$$
$$\mathbf{V}_i' = (x_i, y_i, \varphi_i, \mathrm{L}_i)\ , \qquad (1.3)$$

де L_i – опис відрізка скелета. Відрізок папілярної лінії використовується як додаткова ознака і для визначення параметрів афінного перетворення.

Адаптивний алгоритм порівняння двох векторів $\mathbf{V}_1$ і $\mathbf{V}_2$, описаних формулою (1.3), складається з трьох етапів.

1. Оцінюються параметри афінного перетворення елемента вектора $\mathbf{V}_1$ в елемент вектора $\mathbf{V}_2$. Оцінка проводиться за описом $\mathbf{L}_i$ відрізка скелета. Визначається подібність відрізків скелетів. Якщо вона більша від заданого порогу, то переходять до наступного етапу, якщо ні, то вибирають іншу пару елементів векторів $\mathbf{V}_1$ і $\mathbf{V}_2$.

2. Особисті ознаки, для яких збіглися їх описи на попередньому етапі, визначаються як центральні. Проводиться просторова нормалізація вектора $\mathbf{V}_1$ зворотним, до визначеного, афінним перетворенням. Елементи векторів $\mathbf{V}_1$ і $\mathbf{V}_2$ сортуються за кутом відносно центральних ознак. Опис їх позицій переводиться у полярну систему координат із центром у центральних ознаках.

3. Базуючись на мірі подібності, порівнюють відсортовані та перетворені вектори. Порівняння проводять попарно з корекцією при появі або зникненні ознак. Одночасно, у ході порівняння ознак, коректуються допуски для адаптації до нелінійних геометричних спотворень. Якщо сума мір подібності більша від порога, приймається рішення про ідентифікацію.

Цей алгоритм забезпечує кращі результати. Єдиним недоліком у ньому є те, що адаптація проводиться під час зміни кута до ознак, що порівнюються, і не проводиться при зміні віддалі до них.

Існує дещо складніший вектор ознак на основі їх триплетів [171] (блок №5 рис.1.29). У векторі ознак **V** узору відбитка кожен елемент є вектором ознак триплету

$$\begin{aligned}&\mathbf{V} = (\mathbf{V}_i'),\ \ i = 1..N\ ,\\ &\mathbf{V}_i' = ((x^1{}_i, y^1{}_i, \varphi^1{}_i), (x^2{}_i, y^2{}_i, \varphi^2{}_i), (x^3{}_i, y^3{}_i, \varphi^3{}_i), \mathbf{I}_i)\ ,\end{aligned} \tag{1.4}$$

де $(x^1{}_i, y^1{}_i, \varphi^1{}_i), (x^2{}_i, y^2{}_i, \varphi^2{}_i), (x^3{}_i, y^3{}_i, \varphi^3{}_i)$ – координати та орієнтації ознак, які складають *i*-й триплет; $\mathbf{I}_i$ – індекс триплету, й описується так:

$$\mathbf{I}_i = ((S^1{}_i, S^2{}_i, S^3{}_i), (\theta^1{}_i, \theta^2{}_i, \theta^3{}_i), (C^1{}_i, C^2{}_i, C^3{}_i))\,, \tag{1.5}$$

де $S^1{}_i, S^2{}_i, S^3{}_i$ – довжини ребер трикутника, побудованого на *i*-му триплеті; $\theta^1{}_i, \theta^2{}_i, \theta^3{}_i$ – відносна орієнтація ознак до найдовшої сторони трикутника; $C^1{}_i, C^2{}_i, C^3{}_i$ – кількість папілярних ліній, що перетинають ребра трикутника.

Алгоритм порівняння простий і включає три етапи.

1. Методом синтаксичного порівняння зіставляють індекси двох векторів. Пари елементів з однаковими індексами зберігаються. Якщо кількість індексів, що збіглися, достатня то переходять до наступного етапу.
2. Визначають параметри афінного перетворення одного вектора в інший. Відкидають всі пари триплетів, які збігаються з іншими параметрами афінного перетворення.
3. Рішення про ідентифікацію приймається на основі кількості триплетів, що збіглися.

Цей алгоритм забезпечує високу швидкість порівняння, адже порівняння двох триплетів за індексами вимагає незначних обчислювальних затрат. Суттєвим його недоліком є залежність індексів триплетів від нелінійних геометричних спотворень і похибки визначення позиції ознак, що призводить до високого рівня ІНН.

Запропоновано й алфавіт ознак [155] (блок №6 рис.1.29) із восьми символів

$$\mathbf{A} = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}\,, \tag{1.6}$$

кожен символ якого відповідає окремому типові особистих ознак (рис.1.31): точка, закінчення-початок, розвилка, око, гачок, перетин ліній (який автори вважають ознакою, а криміналісти – ні), місток, фрагмент. Далі кожна ознака описується реченням, яке включає символ алфавіту **A** і символи булевого алфавіту {0,1}

$$\mathbf{T} = (\mathbf{A}, f(a_1), f(a_2), f(a_3), f(a_4), f(a_5), f(a_6), f(a_7), f(a_8))\,, \tag{1.7}$$

де $f(a_1), f(a_2), f(a_3), f(a_4), f(a_5), f(a_6), f(a_7), f(a_8)$ – булеві функції, які визначають, чи в певному околі ознаки, що описується, є ознака з відповідним символом алфавіту **A**. Узор описується вектором ознак, який є словом із символів алфавіту **T**. Порівнюються два слова, а міра подібності визначається кількістю букв, які присутні в обох словах.

Такий опис і порівняння забезпечують високу швидкодію алгоритмів, проте не гарантують належної якості ідентифікації. Тут не враховано, що ознаки нестабільні, оскільки як після обробки, так і під час поганого відображення узору ознаки можуть міняти тип (наприклад, розвилка стане закінченням, фрагмент – двома розвилками) [155]. Це означає, що похибка визначення типу ознак буде відбиватися на точності ідентифікації.

На жаль, усім алгоритмам, побудованим на особистих ознаках, притаманні декілька спільних недоліків [80]:

- використовується не вся наявна для ідентифікації інформація, а лише структура розміщення й типи ознак;
- для ідентифікації необхідна певна кількість ознак, що не завжди можливе на практиці;
- нестабільність положення ознаки на зображеннях із поганою якістю призводить до втрати точності.

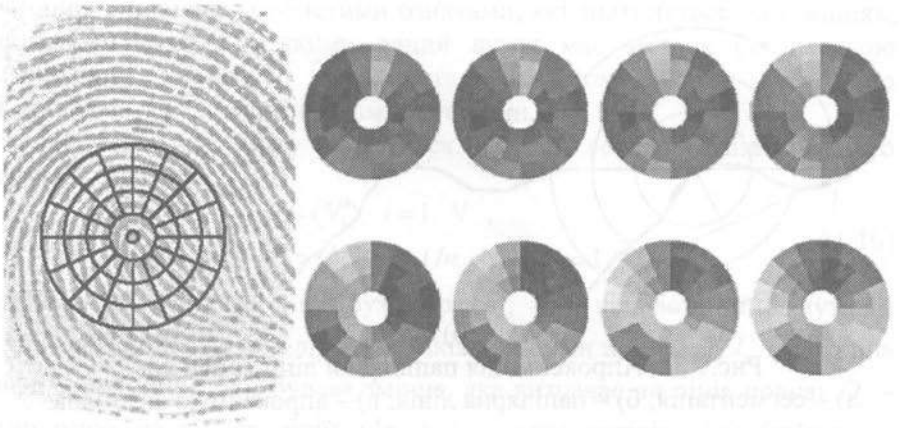
г) Ознаки на основі профільтрованих зображень центрального околу узору. Такий тип ознак був розроблений Пребхеке (Prabhakar) із Мічіганського університету [162,216] (блок №1 рис.1.29). Він запропонував використовувати їх для класифікації й розпізнавання. Під час класифікації, як було зазначено раніше, вектор ознак поступає на класифікатор, а при розпізнаванні – порівнюються два 640-значні вектори ознак. Схематичне представлення ознак відображено на рис.1.32.

Вектор ознак описується так:

$$\mathbf{V} = (D_i), \quad i = 1..640, \tag{1.8}$$

де D_i – дисперсія яскравості в i-му сегменті центрального околу. На рис.1.32.б схематично представлено дисперсію сегментів, оброблених вісьмома спрямованими фільтрами Габора з орієнтацією 0°, 22,5°, 45°, ... 157,5°.

Порівняння двох векторів проводиться за Евклідовою віддалю між ними. Якщо віддаль менша від заданого порога, то приймається рішення про ідентифікацію. Для забезпечення інваріантності до повороту генерується 10 векторів для 10 кутів повороту околу.



а) б)

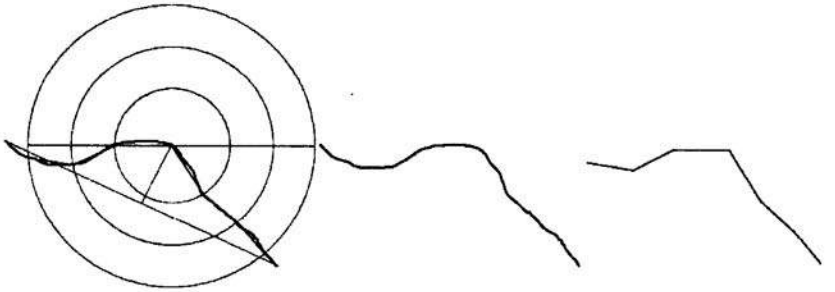
Рис.1.32. Зображення відбитка з центральним околом, розбитим на сегменти (а), й ілюстрація вектора ознак (б).

Перевагою такого вектора ознак є те, що проводиться детальний опис узору. Дисперсія яскравості є стійкою до геометричних спотворень типу "губка". Не потрібна попередня обробка зображення, хоча, з іншого боку, вона присутня в етапі генерування ознак. Цьому методу притаманні велика швидкодія на фоні простоти виконання, а також можливість розпаралелення обчислень.

Недоліками методу є чутливість алгоритму до неточності визначення центра узору й шумів у центральному околі. Він не забезпечує високих імовірнісних показників ідентифікації, що виникає через подібність дисперсій яскравості в сегментах околу однакових узорів. Як зазначає сам автор [162], такий метод доцільно використовувати з іншими ознаками, що покращує загальні результати роботи систем ідентифікації.

д) Ознаки папілярних ліній. Щоб описати папілярні лінії повністю (блок №2 рис.1.29) їх розбивають на сегменти й апроксимують ламаною кривою [99] (рис.1.33).

Для апроксимації знаходиться середина папілярної лінії як точка, яку перетинає перпендикулярна пряма, проведена посередині відрізка, що з'єднує кінці папілярної лінії. В центрі будуються концентричні кола, які утворюють сегменти і розбивають папілярну лінію на криві, кожна з яких апроксимується відрізком. Два відрізки одного сегмента утворюють пару, яка описується двома кутами. Вектор ознак узору запишеться так:



а) б) в)

Рис.1.33. Апроксимація папілярної лінії ламаною:
а) – сегментація; б) – папілярна лінія; в) – апроксимуюча ламана.

$$\begin{aligned} \mathbf{V} &= (\mathbf{V}_i'), \quad i = 1..N \ , \\ \mathbf{V}_i' &= (\varphi_{ij}, \theta_{ij}), \quad j = 1..M_i \ , \end{aligned} \tag{1.9}$$

де N – кількість папілярних ліній; M_i – кількість сегментів в i-й папілярній лінії; $\mathbf{V}_i'$ – вектор ознак i-ї папілярної лінії; φ_{ij} – кут між парою сегментів; θ_{ij} – кут між відрізками j-го і $(j\text{-}1)$-го сегментів.

Алгоритм порівняння двох зображень включає в себе обчислення кількості ліній, що збіглися. Для порівняння двох ліній обчислюється середньоквадратична похибка між векторами ознак ліній $\mathbf{V}'$. Якщо похибка менша від порога, то приймається рішення про ідентичність ліній на основі кількості ідентичних ліній.

Перевагою представленого вектора інформативних ознак є його інваріантність до афінних перетворень другого порядку, що, в свою чергу, спрощує алгоритм порівняння.

Недоліки цього методу суттєвіші, ніж переваги. Метод не набув поширення через невисоку точність, позаяк лінії для однакових типів узорів дуже подібні, а лінії для одного і того ж відбитка, але з нелінійними геометричними спотвореннями, сильно відрізняються. Розірвані лінії не зіставляються з повними.

Запропоновано також описувати не самі лінії, а їх взаєморозташування методом графів [157] (блок №3 рис.1.29). Кожна папілярна лінія асоціюється з вузлом графа (рис.1.34). Зв'язок між вузлами означає, що дві лінії, які відповідають вузлам, є сусідніми (суцільна лінія) або з'єднуються (пунктирна лінія). Кожен вузол графа додатково описується: довжиною лінії; булевою змінною, яка визначає

чи лінія є повною; особистими ознаками, які знаходяться на її кінцях; номерами вузлів, із якими даний вузол має зв'язок (за часовою стрілкою); довжиною фрагмента, протягом якого лінії, що відповідають з'єднаним вузлам, є сусідами.

Вектор ознак узору описується набором векторів ознак кожного вузла графа:

$$\begin{aligned} &\mathbf{V} = (\mathbf{V}'_{\mathrm{i}}),\ i = 1..N\ , \\ &\mathbf{V}'_{\mathrm{i}} = (l_i, B_i, O_i, (In_{ij}, ls_{ij})),\ j = 1..M_i\ , \end{aligned} \tag{1.10}$$

де $\mathbf{V}'_{\mathrm{i}}$ – вектор ознак лінії (вузла графа); N – кількість ліній (вузлів); M_i – кількість сусідніх ліній (зв'язків з іншими вузлами); l_i – довжина папілярної лінії; B_i – булева змінна, яка визначає чи лінія повна; O_i – тип ознак на кінцях лінії; (In_{ij}, ls_{ij}) – опис сусідів лінії (зв'язків з іншими вузлами); In_{ij} – індекс j-го сусіда i-го вузла; ls_{ij} – довжина відрізка лінії, вздовж якого i-та та In_{ij} -та лінії є сусідами.

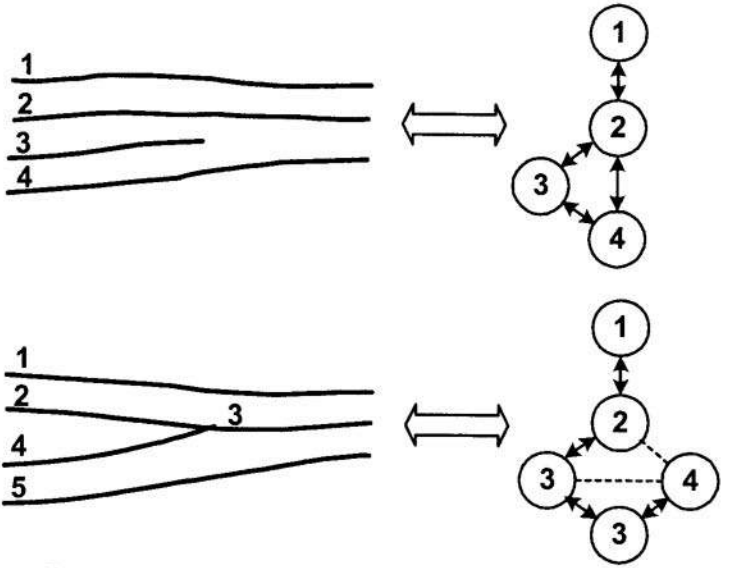


Рис.1.34. Фрагменти папілярного узору і їх графи.

Алгоритм порівняння включає три етапи.

1. Побудова карти відповідності вузлів. Кожен вузол одного графа порівнюється з кожним вузлом іншого (це еквівалентно зіставленню елементів одного вектора з елементами іншого). На цьому

етапі порівнюються три параметри: l_i, кількості In_{ij}, які більші і які менші від індексу вузла. Якщо різниця між параметрами лежить у визначених межах, то елемент карти відповідності приймає значення одиниці.

2. Розрідження карти відповідності. Порівнюються зв'язки з іншими вузлами, їх опис і значення елементів карти відповідності. Розрідження проводиться рекурсивним ітераційним методом доти, поки є можливість відкидання неправильних елементів карти відповідності.

3. Обчислення кількості вузлів, які збігаються, двох графів методом побудови двох дерев.

Перевагами такого опису є: інваріантність до афінних перетворень, нечутливість до нелінійних геометричних спотворень.

Недоліки такі: чутливість опису до розривів папілярних ліній, їх неправильного з'єднання, перетворення типів ознак. Це відбивається на складності автоматизації процесу ідентифікації.

1.4.6. Кореляційні методи

Кореляційні методи, які широко використовуються в інших системах розпізнавання [12,70], знайшли своє застосування і в ДБС. На відміну від кореляційних методів для структурного опису образів [70] тут корелюються зображення, а не вектори ознак. Кореляційну функцію в таких системах обчислюють двома способами – оптичними кореляторами [136,144,168] або за допомогою ШПФ [103]. Обидва способи математично описуються класичним виразом кореляції [86]. Векторів ознак як таких в цьому типі систем немає або їх роль відіграють фрагменти зображень [103]. В оптичних системах використовуються два типи кореляторів: Вандерлюхта [136] і оптичний корелятор із взаємно-модульованими зображеннями [144,168].

Для досягнення інваріантності кореляційного методу на основі оптичного корелятора Вандерлюхта використовують не одне статичне зображення, а відеопослідовність кадрів [136]. У кожному кадрі присутнє повернуте на певний кут зображення відбитка.

Незважаючи на високу продуктивність оптичні корелятори мають вагомі недоліки: висока собівартість і габарити апаратної частини. Щодо застосування кореляційних методів для систем ідентифікації, то появляється ще один недолік – висока чутливість до геометричних спотворень (ефекту "губки"). Особливо сильно впливають геометричні спотворення при кореляції двох великих зображень.

Більш доступним є метод кореляції на основі ШПФ, який може бути виконаний на обчислювальних машинах або мікропроцесорах. Іншою проблемою в цьому випадку є високі обчислювальні затрати для ШПФ.

Один із виходів із цієї ситуації – використання кореляції п'яти фрагментів вхідного зображення розміром 24×24 точки з еталонним зображенням [103]. Алгоритм реалізується в три етапи.

1. На вхідному зображенні вибирають п'ять фрагментів, які знаходяться поблизу центра узору і мають найменший коефіцієнт кореляції з іншими фрагментами зображення. Описується п'ятигранник, утворений центрами вибраних фрагментів.

2. Кожен фрагмент корелюється за допомогою ШПФ із зображенням з БД і визначаються координати піка кореляційної функції. Він окреслює область зображення, яка найбільше подібна до фрагмента вхідного зображення. Аналогічно встановлюються координати решти чотирьох фрагментів. Описується п'ятигранник побудований за визначеними координатами.

3. Рішення про ідентифікацію приймається шляхом зіставлення двох п'ятигранників. Порівнюються кути й ребра. Прийняття рішення відбувається на основі еліптичної вирішуючої функції.

Як зазначають самі розробники, цей метод вимагає великих обчислювальних затрат незважаючи на застосування ШПФ, тому пропонують використовувати його для підтвердження ідентифікації (fingerprint verification).

Перевагою саме такого застосування кореляційних методів розпізнавання є зменшення чутливості до геометричних спотворень, оскільки вони незначно спотворюють узор у межах фрагментів 24×24 точки.

Недоліків є декілька. Перший аналогічний недоліку ознак, побудованих на порівнянні папілярних ліній, – узори однакового типу мають дуже подібні фрагменти і розташовані за таким же п'ятигранником. Другий недолік полягає в тому, що метод є неінваріантний до повороту, хоча менш чутливий до нього. Це досягається малим розміром фрагментів. Авторами заявляється інваріантність у межах 10 градусів, що недостатньо для БІС. Загальним недоліком кореляційних методів порівняння є необхідність зберігання повних еталонних зображень. Цього недоліку позбавлені ознаки і кореляційний метод описані далі.

1.4.7. Комбіновані методи

Одним із шляхів подальшого вдосконалення систем ідентифікації є використання декількох типів векторів ознак і методів порівняння. Комбінування типів ознак дозволяє більш детально описати узор відбитка, а методів – краще налаштувати систему на всю гамму узорів [161]. Іншим способом підвищення точності ідентифікації є комбінування біометричних характеристик людини (наприклад, відбитків пальців і зображення обличчя тощо) [152].

У роботі [108] запропоновано використовувати три методи порівняння. Автор використовує методи, представлені на рис.1.29 в блоках з номерами 1, 5, і метод на основі розкладу Карунена-Лоєва [112]. Для формування кінцевого рішення про ідентифікацію порівнюються два методи комбінування результатів порівнянь, а саме формування рішення за найкращим результатом (у розумінні такого, що вказує на максимальну подібність) і на підставі зваженої суми результатів усіх трьох методів. Експериментально встановлено, що найефективнішою комбінацією є застосування всіх трьох методів із прийняттям рішення про ідентифікацію за найкращим результатом.

Дослідження комбінацій чотирьох методів проведені в роботі [216]: три методи ґрунтуються на особистих ознаках (блок №4 рис.1.29) і метод на основі фільтрації центрального околу узору набором фільтрів Габора (блок №1 на рис.1.29). Найкращою виявилась комбінація двох методів, базованих на особистих ознаках [115,151] і методі на основі фільтрів Габора [162,216]. Висновком досліджень проведених є твердження, що для підвищення точності ідентифікаційних систем необхідно комбінувати методи, що зужитковують різні типи ознак, які доповнюють одні одних. Це твердження повністю збігається з інформаційним підходом до оцінки корисності ознак на основі ентропії за диференційним критерієм ефективності [83].

1.5. Огляд криптографічних засобів

Важливість інформації у сучасному світі важко переоцінити. Наведемо доводи такого твердження: 1) володіння певним цифровим кодом може відкрити доступ власникові до значних матеріальних цінностей та послуг – це сталось завдяки інформатизації банківської діяльності; 2) утворилась справжня індустрія інформаційних послуг – інформація стала пересічним товаром, тобто об'єктом купівлі-продажу;

3) звичними стали приклади розорення фірм та цілих корпорацій після розголошення критично важливої конфіденційної інформації.

Особливий, нематеріальний характер інформації робить надто легким її копіювання та модифікацію, у зв'язку з чим вона стає привабливим об'єктом для різного типу зловживань.

Висока вразливість інформаційних технологій до різноманітних злочинних дій створила гостру необхідність у засобах протидії цьому, що привело до виникнення та розвитку галузі "криптографія" як невід'ємної частини сучасної інформаційної індустрії. Усі задачі захисту інформації засобами криптографії вирішуються методами, ніяким чином не пов'язаними з характеристиками матеріальних носіїв інформації, які грунтуються лише на маніпуляції самою інформацією та використовують тільки її іманентні властивості.

Як правило об'єктами дослідження криптографії є:

- криптографічний алгоритм – шифр – спеціальний метод перетворення інформації з метою її представлення у формі, недоступній для потенційного злочинця;
- криптографічний протокол – це процедура взаємодії користувачів криптографічних алгоритмів, у результаті якої користувачі досягають певну ціль, а потенційний зловмисник – не досягає;
- система управління ключами – комплекс заходів для генерації, відновлення, зберігання, розповсюдження та знищення ключів криптоалгоритмів.

Засобами сучасної криптографії вирішуються такі три основні проблеми [58]:

- забезпечення конфіденційності (секретності);
- забезпечення аутентифікації інформації та джерела повідомлень;
- забезпечення анонімності (наприклад, приховування переміщення електронних грошей від одного суб'єкта до іншого).

Схематично будь-яка криптографічна ситуація має вигляд, зображений на рис. 1.35 [189].

Учасниками криптографічного процесу можуть бути суб'єкти (окремі люди, групи законних користувачів, комп'ютери тощо), які пересилають, приймають чи обробляють інформацію, що потребує захисту.

У будь-якій криптосистемі, окрім легальних користувачів зв'язку, береться до уваги наявність потенційного суперника (інакше злочинець, ворог, опонент), який намагається стати учасником інформаційного обміну, оволодіти конфіденційною інформацією,

використати її у своїх інтересах. Таке припущення виникає через те, що у процесі обміну інформацією у більшості випадків використовуються фізично незахищені канали зв'язку.

Фізично захищеним каналом називається канал, який не є фізично доступним для суперника. Реалізація подібних каналів зв'язку виходить за межі методів, якими оперує криптографія. Такими каналами можуть бути: особиста зустріч, послуги довірених кур'єрів, побудова виділених каналів зв'язку, що знаходяться під цілодобовою охороною.

При розгляді криптографічних методів вводиться поняття захищеного каналу зв'язку, в якому захист інформації базується не на методах, згаданих вище, а на сучасних досягненнях фундаментальних наук і, в першу чергу, математики.

У найпростішому випадку розглянемо схему налагодження таємного зв'язку двома сторонами (рис.1.35). З них один постає відправником, а другий – адресатом повідомлення, хоча в реальних умовах кожному з них доводиться бути як і відправником, так і адресатом. Відправник намагається сформувати і відправити адресату повідомлення m. Адресат отримує повідомлення і намагається його зрозуміти. Для того щоби суперник не зміг ознайомитися зі змістом перехопленого повідомлення, відправнику необхідно застосувати до повідомлення деякий криптографічний алгоритм $E(\,)$ таким чином, щоб ніхто, за виключенням законного адресата і, залежно від криптографічної ситуації, відправника, не зміг відновити вихідне повідомлення. Послідовність дій, якої дотримуються користувачі описаної вище системи, формує криптографічний протокол.

Криптографічний алгоритм, інакше шифр, представляє собою математичну функцію, яка використовується для шифрування та дешифрування повідомлень. Звичайно це дві взаємопов'язані функції: одна для шифрування, а інша для дешифрування. При цьому по каналу зв'язку передається вже не саме повідомлення, а результат його перетворення за допомогою шифру – криптотекст c. Після чого для суперника виникає складне завдання ламання шифру. Згідно з традиційною термінологією, він мусить провести атаку на шифр.

Зв'язок між вихідним повідомленням, інакше відкритим текстом, m, криптотекстом c і алгоритмом шифрування $E(\,)$ формально виражається наступним чином:

$$c = E(m). \qquad (1.11)$$

Законний адресат, отримавши криптотекст, мусить застосувати до нього алгоритм дешифрування:

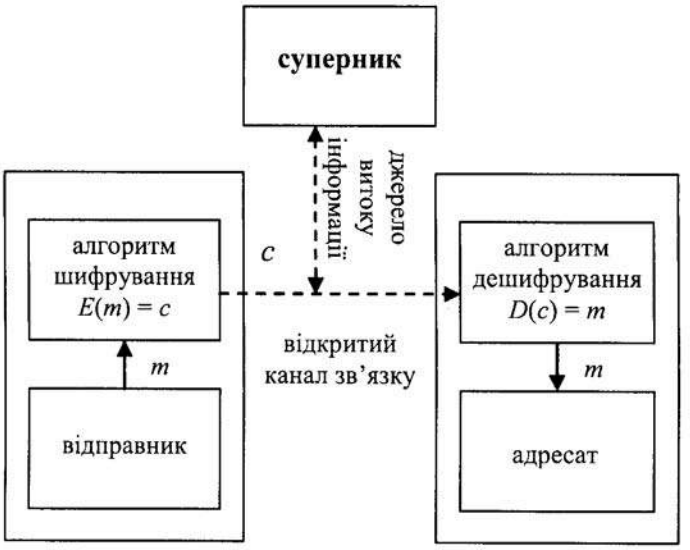


Рис. 1.35. Криптографічна схема з двома учасниками.

$$m = D(c). \qquad (1.12)$$

Якщо безпека алгоритму (за традиційною термінологією – стійкість алгоритму) ґрунтується на збереженні алгоритму в таємниці, тоді це обмежений алгоритм. Розробка сучасного стійкого криптографічного алгоритму – це тривала інтелектуальна робота групи спеціалістів. Тому "період життя" шифру мусить бути якомога більшим. Обмежені алгоритми на даний час мають лише історичний інтерес, і вони не відповідають теперішнім стандартам захисту інформації. Велика група користувачів не може використовувати такі алгоритми, оскільки як тільки один з членів групи покидає її, то інші користувачі змушені переходити на новий алгоритм. Іншою небезпекою є те, що суперник уже розгадав шифр і має можливість читати конфіденційну інформацію.

Стійкість новітніх криптосистем ґрунтується не на секретності алгоритму, а на секретності деякої інформації порівняно невеликого об'єму, яка називається криптографічним ключем. Ключ використовується для керуванням процесом криптографічного перетворення та є легкозмінним елементом криптосистеми. Ключ може бути змінений користувачем у будь-який момент часу, а алгоритм шифрування залишається довготривалим елементом системи. Викладені принципи відповідають "правилам стійкості шифру" сформульованим криптографом Керкхоффом ще у XIX ст.

Цей факт вносить зміни у криптографічну схему (рис.1.35). Тепер законні користувачі перед інформаційною взаємодією змушені обмінятися ключами (e і d), використовуючи системи управління ключами. А в суперника з'являється нове завдання – визначити ключ, за допомогою якого можна легко прочитати криптотекст. Так, метод повного перебору суперником усіх можливих ключів називається брутальною атакою [15].

Формули опису (1.11) та (1.12) з урахуванням ключової інформації мають вигляд:

$$c = E(m,e),\ m = D(c,d).$$

Сучасна криптографія залежно від способу використання ключа має класифікацію методів, представлену на рис 1.36.

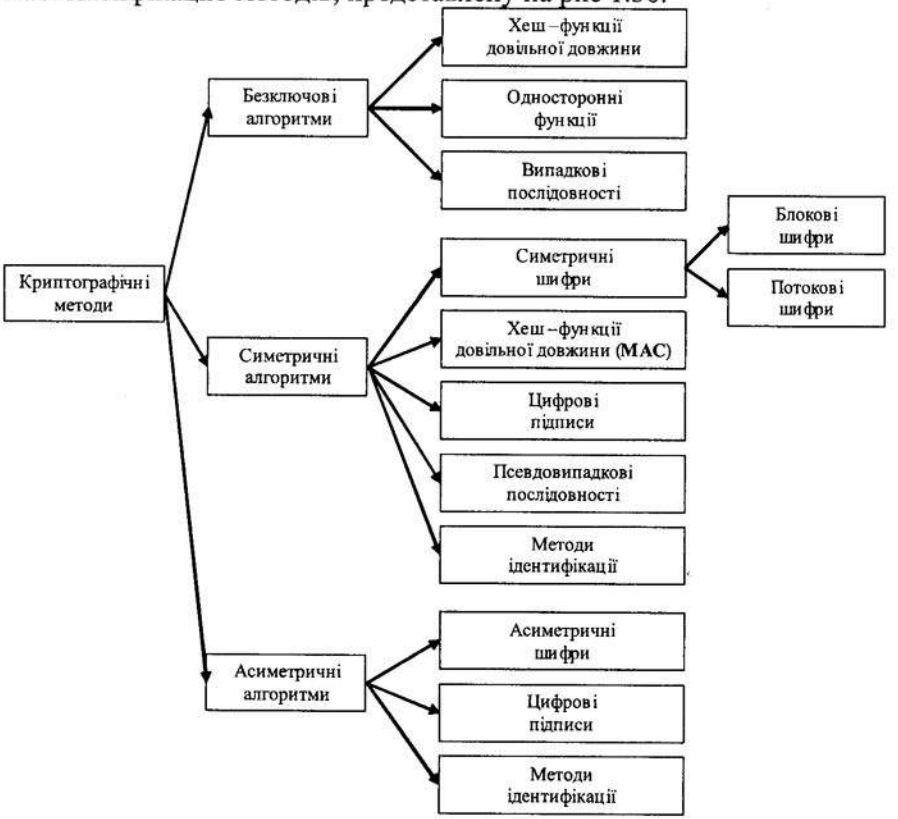


Рис.1.36. Класифікація криптографічних методів.

а) Симетричні алгоритми (інакше умовні алгоритми, алгоритми з одним ключем, алгоритми з таємним ключем) представляють собою

алгоритми, в яких ключ шифрування може бути розрахований по ключу дешифрування і навпаки ($e = d$). У більшості симетричних алгоритмів ключ шифрування та дешифрування той самий. У криптографічну схему (рис.1.35) вводиться недоступний для суперника таємний канал зв'язку для обміну ключами.

Для побудови криптографічно стійких симетричних алгоритмів використовують два загальних принципи: розсіювання та перестановки [93]. Прикладами успішної реалізації ідеї симетричного шифрування є DES [137], ГОСТ 28147-89 [32], RC6 [224], SPECTR-H64 [57], IDEA [170], AES [124], NewDES [121] RC5 [223], BLOWFISH [237].

б) Довжина ключа симетричних алгоритмів. Розрахувати складність ламання симетричної криптосистеми за допомогою брутальної атаки нескладно. Якщо використовується 8-ми бітовий ключ, тоді існує 2^8, або 256, можливих ключів. Отже, необхідно здійснити максимум 256 спроб для знаходження дійсного. У випадку 56 бітового ключа (алгоритм DES) – кількість можливих ключів 2^{56}. Сучасний персональний комп'ютер, виконуючи 10^8 перевірок ключів у секунду, знайде необхідний ключ у середньому за 23 роки. Для 64-х бітового ключа – 5600 років.

Отримані оцінки помилково вказують на значну стійкість криптографічних алгоритмів. Та з використанням сучасних технологій, локальних та глобальних мереж, суперскалярності новітніх комп'ютерів можливо на порядки зменшити часові затрати на злам системи. Ще у 1993 році криптограф Майк Вінер [260] розробив спеціалізовану обчислювальну машину для зламу криптоалгоритму DES. Він оцінив, що, витративши $1 000 000, можливо зламати шифр у середньому за 3,5 години. Беручи до уваги закон Мура про подвоєння кожних 18 місяців обчислювальної потужності у два рази, оцінимо затрати на злам симетричних систем на сьогодні:

Кошти, тис. $	Довжина ключа, біт				
	56	**64**	**80**	**112**	**128**
1	35 год	1 рік	$7\ 10^4$ років	10^{14} років	10^{19} років
10	3,5 год	37 днів	$7\ 10^3$ років	10^{13} років	10^{18} років
...					
$\mathbf{10^8}$	1 мс	0,3 с	6 год	10^6 років	10^{11} років

У роботах [141,148,218,256] проаналізовано інші технології зламу симетричних криптосистем – від використання вірусів, нейронних мереж, Китайської лотереї до біотехнологій та генетичних алгоритмів.

Також було знайдено верхню реальну оцінку довжини ключа. Злам 256 бітового ключа, враховуючи термодинамічні обмеження, реальні умови існування матерії та простору і часу, неможливий.

За звичайних умов роботи симетричних криптографічних алгоритмів в інформаційних системах рекомендовано застосування ключів з мінімальною довжиною 80 біт [58].

в) Асиметричні алгоритми. Основною проблемою, що виникає при використанні симетричних алгоритмів, є не надійність самого алгоритму, а створення безпечного каналу обміну ключами. Тобто, навіть при використанні у криптографічних алгоритмах довгих ключів, постає та ж проблема існування фізично захищеного каналу зв'язку. Якщо користувачів криптосистеми двоє, ключ може бути передано, наприклад, при їхній особистій зустрічі. Але при зростанні кількості користувачів до n кількість ключів збільшується до $\frac{n(n-1)}{2}$ (наприклад, для 10-ти користувачів деякої захищеної мережі необхідно 45 ключів). Очевидно, що особиста зустріч користувачів у такій ситуації втрачає свою раціональність. Вирішенням проблеми ні в якому разі не може бути використання одного ключа для всіх користувачів. Адже це збільшує ймовірність розкриття ключа пропорційно до кількості користувачів, а також дозволяє читати інформацію, призначену одному з членів групи, всім іншим користувачам.

Такі обмеження та недоліки, а також виникнення цілком нових криптографічних задач (цифровий підпис, ідентифікація та інші) привели до створення у другій половині 70-х років принципово нових підходів для вирішення проблем конфіденційності. Основою є ідея використання властивостей деяких математичних функцій, які мають різну складність виконання у "прямому" та "зворотному" напрямках. Скажімо, якщо задана така математична функція $f(\,)$ та аргумент (прообраз) x, то знайти значення (образ) $y = f(x)$ – легко. Обернена операція, тобто знаходження прообразу по відомому образу, є дуже важкою математичною задачею.

Прикладами важких математичних задач (і назв схем, у яких вони використовуються) є:

- розклад великих складених чисел на прості співмножники (RSA) [225];
- обчислення дискретних логарифмів у скінченному полі (ElGamal) [133];
- пошук квадратних коренів по модулю складеного числа (Rabin) [258]

та деякі інші.

У схемі шифрування виконується за допомогою "відкритого" ключа, а дешифрування – таємним ключем, який має лише адресат. Визначення таємного ключа представляє собою дуже складну проблему, що й зумовлює стійкість криптосистеми.

Згадані алгоритми носять назву алгоритмів з відкритим ключем, або асиметричних алгоритмів. У такій криптографічній схемі канал обміну ключами є незахищеним, ключ шифрування не рівний ключу дешифрування ($e \neq d$), ключ шифрування не є таємним елементом шифру і звичайно публікується учасником обміну для того, щоби будь-хто міг послати йому шифроване повідомлення. Повертаючись до ситуації обміну ключами у мережі з n учасниками, то з використанням нових принципів криптографії необхідно лише n пар ключів.

г) Довжина ключа асиметричних алгоритмів. У асиметричній криптографії застосовують ключі завдовжки більше 256 біт, тому можливість тотального перебору множини ключів не розглядається. Стійкість системи оцінюється через мінімальну кількість операцій, необхідну для знаходження прообразу.

Проаналізуємо стійкість найбільш вживаного алгоритму RSA. Найпотужнішими методами розкладу деякого числа на множники є:

- метод еліптичних кривих (ECM, розклад максимум 140 бітних чисел) [198,199];
- метод квадратичного сита (QS, розклад максимум 366 бітних чисел) [214,215];
- метод сита загального числового поля (GNFS, розклад чисел довших 366 біт) [173,174];
- метод сита спеціального числового поля (SNFS, найпотужніший на даний момент метод факторизації) [205].

Потужність комп'ютерів прийнято обчислювати у MIPS - роках (one-million-instruction-per-second, MIPS), що дорівнює 3·1013 операціям. Згідно визначення 1 MIPS - рік — це кількість операцій, здійснених комп'ютером DEC VAX 11/780 із швидкодією 1 млн. операцій на секунду за рік безперервної роботи. Швидкодія сучасних комп'ютерів 1000 MIPS - років. У таблиці 1.2. наведено необхідну обчислювальну потужність для факторизації методами GNFS і SNFS відповідно ключа асиметричного алгоритму RSA [205].

Отже, використовуючи для зламу системи RSA сучасний персональний комп'ютер, за 55 днів можливо здійснити факторизацію 512 бітового числа методом SNFS. А застосувавши технологію розподілених обчислень, адміністратор мережі великої організації з

кількістю комп'ютерів більше 1000 виконає факторизацію 768 бітового ключа менш ніж за місяць.

Очевидно, що наведені у таблиці 1.2 дані не є кінцевою оцінкою стійкості асиметричної криптосистеми. На відміну від симетричних систем, максимальну довжину ключа яких було визначено вище, для двоключових систем неможливо вказати верхню межу довжини. У роботі [107] авторами наведено довгостроковий прогноз (таблиця 1.3) необхідної довжини ключа. Звичайно, що довжина ключа відповідатиме цінності та мінімальному необхідному періоду життя конфіденційних даних, зашифрованих за допомогою цього ключа. Тобто непотрібно використовувати довгі ключі для захисту даних, цінність яких невелика, або період життя вимірюється кількома годинами. Рекомендовані довжини ключів на даний час наведені у таблиці 1.4.

Таблиця 1.2. Дані для факторизації методами GNFS і SNFS

Довжина ключа, біт	Потужність, MIPS – років	
	GNFS	SNFS
512	$3 \cdot 10^4$	150
768	$2 \cdot 10^8$	$1 \cdot 10^5$
1024	$3 \cdot 10^{11}$	$3 \cdot 10^7$
1280	$1 \cdot 10^{14}$	$3 \cdot 10^9$
1536	$3 \cdot 10^{16}$	$2 \cdot 10^{11}$
2048	$3 \cdot 10^{20}$	$4 \cdot 10^{14}$

Таблиця 1.3. Довгостроковий прогноз розкладу на множники

Рік	Довжина ключа, біт
2005	2048
2015	4096
2025	8192
2035	16384
2045	32768

Таблиця 1.4. Рекомендовані довжини ключів (у бітах)

Рік	Невеликі фірми	Корпорації	Держави
2005	1280	1536	2048
2010	1280	1536	2048
2015	1536	2048	2048

Вважається доцільним використовувати ключі з мінімальною довжиною 1280 біт.

д) Змішані алгоритми. У часи зародження асиметричної криптографії висловлювалися думки, що за декілька років вона повністю замінить свою попередницю, але цього не сталося з наступних причин.

1. Симетричні алгоритми значно простіше реалізуються як програмно, так і апаратно. Тобто при однакових вимогах ефективності та надійності складність, а отже, і пов'язана з нею ціна апаратних засобів, які реалізують шифр з відкритим ключем, набагато вищі, ніж у симетричних криптосистемах. У програмних реалізаціях на одному і тому ж типі процесора симетричні шифри працюють у 1000 разів швидше за асиметричні.

2. Надійність алгоритмів з відкритим ключем обґрунтована на даний час дещо слабше, ніж надійність алгоритмів із таємним ключем. Немає гарантії, що через деякий час вони не будуть розкриті, як це було з оригінальною криптосистемою Меркла-Хеллмана, яка ґрунтується на задачі укладки рюкзака [210,212].

3. Асиметричні системи вразливі до атаки використанням відкритого тексту. Якщо відомо $c = E(m,e)$, де m – відкритий текст із k можливих, тоді криптоаналітику необхідно зашифрувати усі k за допомогою відомого відкритого ключа та порівняти результат з c. Тобто здійснюється пошук відкритого тексту, а не ключа шифрування. За умови обмеженого простору можливих відкритих текстів даний метод атаки є дуже ефективним.

Враховуючи переваги та недоліки кожної криптографічної схеми, приходять до поняття так званих змішаних (гібридних) криптографічних систем. При організації шифрованого зв'язку в одній криптосистемі використовують як і симетричний, так і асиметричний алгоритми. Власне, саме повідомлення перед пересилкою його адресатові шифрується за допомогою сеансового ключа симетричного алгоритму. Далі сам ключ шифрується відкритим ключем адресата, опублікованим у певній відкритій базі ключів. Зашифроване повідомлення об'єднується із зашифрованим ключем і передається відкритим каналом зв'язку. Для того, щоби отримати вихідний текст повідомлення, адресат дешифрує за допомогою свого таємного ключа сеансовий ключ, який використовує для дешифрування самого повідомлення. При кожному наступному сеансі зв'язку генерується новий сеансовий ключ.

Вищеописана гібридна криптографічна система з успіхом використовується у сучасних криптосистемах PGP [264], ISDN [130,206], SESAME[185,213], PEM[140,177].

1.5.1. Стійкість класичних криптографічних алгоритмів

Здатність шифру протистояти різноманітним атакам на нього називають його стійкістю. Поняття стійкості шифру є центральним для криптографії. Якісно зрозуміти його досить легко, але отримати математично доведені оцінки стійкості для кожного конкретного шифру – проблема досі невирішена. Це пояснюється тим, що на даний момент немає необхідних для вирішення такої проблеми математичних результатів. Тому стійкість конкретного шифру оцінюється лише шляхом різноманітних спроб його ламання. Таку процедуру називають криптоаналізом шифру. Успішно проведений криптоаналіз може розкрити відкритий текст або ключ. Існує чотири основних типи атаки на шифр:

- атака за допомогою лише криптотексту;
- атака з використанням відкритого тексту;
- атака з вибраним відкритим текстом;
- атака з вибраним криптотекстом.

Більшість сучасних криптоалгоритмів загальнодоступні. Закладені в них принципи або відкрито розголошуються компанією – виробником, або їх можна вирахувати за допомогою аналізу тексту програмної реалізації, шляхом цілеспрямованого тестування системи, подаючи на її вхід спеціальні тести [169]. Але широко публікувати криптографічні алгоритми, тим більше з контрольними прикладами та програмними чи апаратними реалізаціями, неправильно. Використаний у криптосистемі алгоритм – це один з потенційних рубежів захисту від дій суперника. Якщо йому доведеться відновлювати алгоритм по тексту exe-файла чи тестуванням "чорного ящика", то для цього йому знадобляться певні зусилля і час. Необхідність відновлення алгоритму може вичерпати його ресурси ще до того, як він почне безпосереднє ламання шифру. Тому при розробці алгоритму потрібно обмежуватися розголошенням лише загальних даних, які підтверджують надійність алгоритму. Таке твердження не суперечить вищезгаданому принципу Керкхоффа. Воно лише вносить корективи у зростаючі вимоги до надійності криптосистем.

Стійкість відомих криптосистем визначається не стійкістю конкретного потужного криптоалгоритму чи параметрами

використаного ключа, а, насамперед, стійкістю найслабшої ланки у всій архітектурі криптографічного захисту. Тобто більшість систем "підводять" через помилки в організації криптографічного процесу, реалізації взаємодії користувача з криптосистемою, непродуманості криптографічних протоколів.

Навіть якщо система гарантує надійний захист при правильній експлуатації, користувачі можуть випадково порушити її. Інакше цю ситуацію називають атакою з врахуванням "людського фактора". Атака такого виду, виявляється, є значно ефективнішою, ніж місяці копіткого аналізу алгоритмів.

Класична криптографія ґрунтується на застосуванні рівномірно розподілених випадкових стрічок (ключі, хеші, цифрові підписи тощо). Але використання таких стрічок у реальних системах захисту суттєво ускладнюється необхідністю постійної генерації, зберігання та надійного відтворення у процесі взаємодії із системою. Як приклад розглянемо випадок парольної ідентифікації користувача у клієнт-серверній системі (рис.1.37).

Ідентифікація та аутентифікація вважається основою програмно-технічних засобів безпеки, оскільки усі інші засоби криптографії функціонують саме завдяки коректності роботи цих алгоритмів. Ідентифікація та аутентифікація – це перші лінії оборони систем захисту.

Ідентифікація дозволяє суб'єктові (користувачу; процесу, що діє від імені конкретного користувача, або іншому програмно-апаратному компоненту) назвати себе (повідомити свій ідентифікатор). За допомогою аутентифікації (інакше перевірки автентичності) інша сторона переконується, що суб'єкт дійсно є тим, за кого себе видає, тобто відповідає зареєстрованому раніше ідентифікатору.

У мережевому середовищі, коли сторони ідентифікації територіально рознесені, розглядаються два аспекти процесу:

- що служитиме аутентифікатором (тобто, що використовується для підтвердження автентичності суб'єкта);
- як організовано (захищено) обмін даними ідентифікації.

Суб'єкт може підтвердити особу, надавши принаймні одну з можливих сутностей (аутентифікаторів):

- дещо, що він знає (пароль, особистий ідентифікаційний номер, криптографічний ключ);
- дещо, що він має (особисту картку, ідентифікаційний токен);
- дещо, що є частиною його самого (голос, відбитки пальців, тобто біометричну інформацію).

У відкритому мережевому середовищі між сторонами ідентифікації, як зазначалося вище, не існує фізично захищених каналів зв'язку, тобто ідентифікаційні дані, що передаються суб'єктом по каналу зв'язку, можуть не відповідати даним, отриманим іншою стороною. Отже, необхідно використати криптографічні методи захисту від пасивного та активного прослуховування мережі, перехоплення та внесення змін у дані.

Повернемося до схеми на рис.1.37. Нехай користувачу (клієнт) в процесі реєстрації надано ключ симетричного алгоритму для обміну інформацією із сервером, а також пару відкритий/закритий ключ для забезпечення процесів, пов'язаних із цифровим підписом. Максимальний рівень надійності досягається лише за повної секретності застосовуваних ключів. За умови використання сучасних криптоалгоритмів та відповідних довжин ключів користувачеві необхідно тримати в таємниці до 1400 біт інформації (128 біт AES, 1280 біт – RSA). Очевидно, що запам'ятати послідовність такої довжини нереально. Тому ключі записуються на електронному носії інформації та захищаються додатковими методами захисту (блокування). Найбільш популярними методами блокування є методи, що ґрунтуються на використанні пароля, певної достатньо короткої для запам'ятовування фрази. Отже, уся система захисту виглядає таким чином. Клієнт надає пароль *W*, за допомогою пароля звільняється ключ *M*, який служитиме для шифрування конфіденційних даних. Для здійснення процесу аутентифікації клієнт посилає серверу запит на взаємодію, надаючи особистий ідентифікатор *ID* та хеш пароля *h(W)*. Порівнюючи дані, сервер надає (чи відхиляє) доступ до ресурсів (наприклад, бази даних тощо).

Виходячи із закону криптографії, що надійність системи захисту визначається надійністю її найслабшої ланки, отримуємо: конфіденційні дані, які захищені надійним криптоалгоритмом, є безпечними лише настільки, наскільки безпечним є пароль. Тобто короткі паролі – низький рівень захисту, довгі – рівень захисту високий, але виникає складність для запам'ятовування. Ще однією проблемою є відсутність будь-якого зв'язку між паролем доступу до системи і власником цього пароля. Іншими словами, будь-кого, хто знає пароль користувача, система ідентифікує саме як цього користувача. Тому останнім часом при розробці криптографічних систем захисту спостерігається зміщення акцентів у процесах управління ключами до застосування здобутків біометричної аутентифікації.

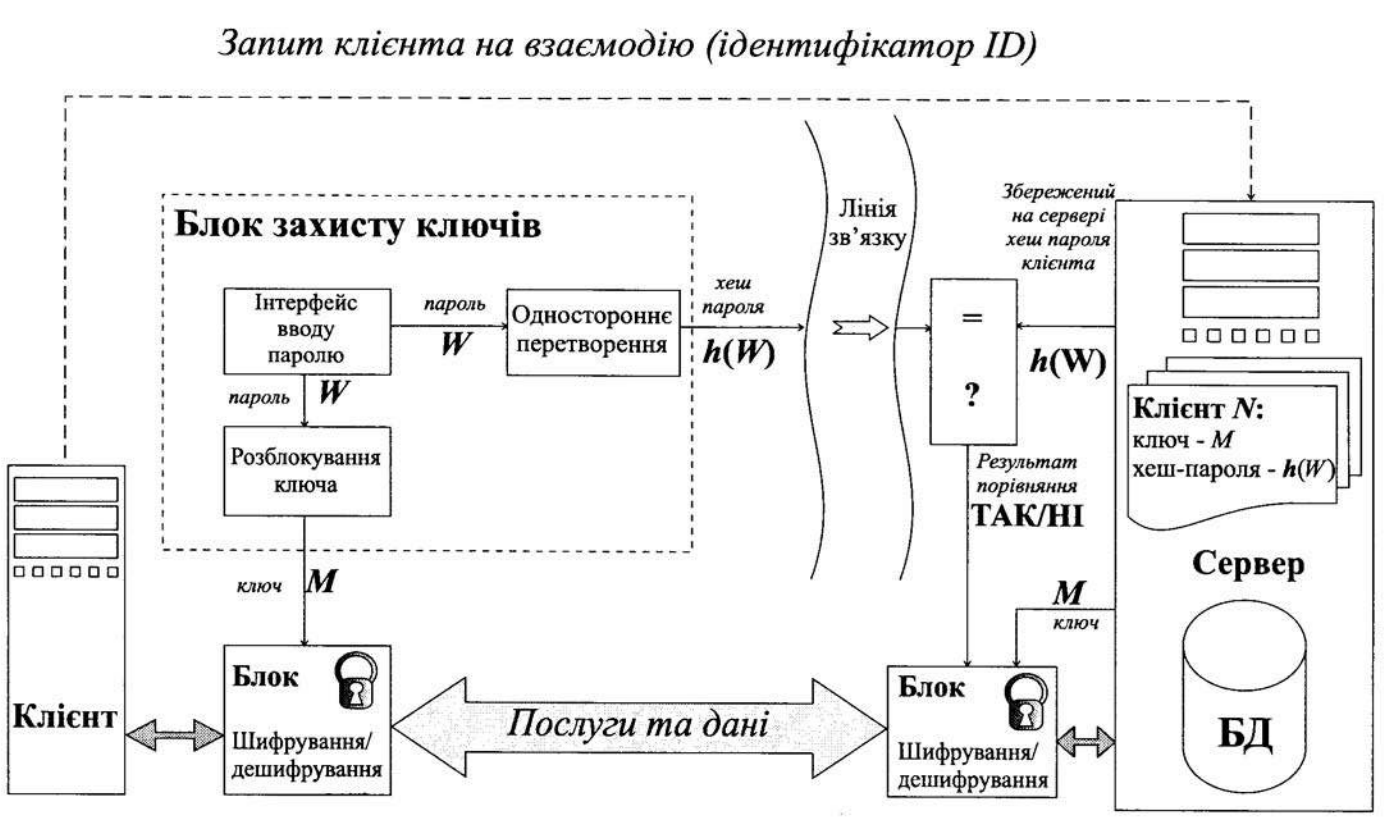


Рис.1.37. Структурна схема типової клієнт-серверної системи

Протягом останнього десятиріччя відбувся значний прорив у галузі біометричної аутентифікації [62]: на зміну громіздким обчислювальним блокам прийшли мікропроцесори, громіздким сканерам – сенсорні пластини товщиною декілька міліметрів. Ціна ж подібних систем знизилася до такого рівня, що вони конкурують з високоякісними професійними і побутовими системами захисту, область застосування яких обмежується лише фантазією розробника.

1.5.2. Біометричні системи

Жоден із об'єктів біометрії не є оптимальним, кожен має свої переваги та недоліки. Додатково системи біометричної ідентифікації, на відміну від парольних систем, вимагають складних алгоритмів розпізнавання зображень, що збільшує вартість систем захисту.

Біометричні сигнали та їхні відображення (наприклад, обличчя та форма його представлення на комп'ютері) надзвичайно відрізняються залежно від застосовуваних методів сканування, апаратури сканування, взаємодії користувачів із приладами отримання біометричних даних.

Наведемо фактори впливу на величину відмінності сигналу та його відображення.

а) Відмінності у наданні біометричних даних. Сигнал, отриманий з ідентифікатора, залежить як від характерних особливостей використовуваного біометричного об'єкта, так і від способу його надання системі користувачем. А саме, отриманий біометричний сигнал є недетермінованою композицією фізіологічних (рис. 1.38), характерної поведінки користувача та способу взаємодії носія з інтерфейсом біометричної системи.

Наприклад, тривимірна конфігурація пальця залежить від сили натиску, властивостей контактної поверхні скануючого пристрою, від орієнтації пальця у момент сканування, а також від методу перетворення у двовимірне зображення. У випадку ідентифікації по обличчю відображення залежатиме від позиції та нахилу голови і т.д.

Рис 1.38. Відбитки одного пальця.

б) Відмінності у послідовних зчитуваннях біометричних даних. На відміну від

штучних ідентифікаторів (карток, токенів, радіобрелоків) об'єкти біометрії є схильними до пошкоджень та зносу. Старіння тканин, нещасливі випадки, вплив шкідливих речовин, порізи наносять шкоду пальцям, змінюючи назавжди структуру папілярного узору. Ручна робота, носіння прикрас змінює геометрію руки. Малюнок судин ока значно залежить від стану здоров'я людини. Температура навколишнього середовища змінює голос. Виснаженість впливає на динаміку роботи з клавіатурою та чіткість підпису і т.д.

Усі наведені вище факти сприяють виникненню значних відмінностей у послідовних зчитуваннях біометричних даних однієї людини.

в) Особливості апаратури та алгоритмів отримання біометричних даних. У реальних умовах одержання біометричних даних супроводжується так би мовити технологічними шумами.

Наприклад, нещільний контакт з поверхнею сканування дає відбитки поганої якості. Причиною неідеальності контакту можуть бути: сухість шкіри; невиразність структури папілярних ліній та впадин; зникнення певних областей структури, пов'язане зі старінням; пітливість; бруд тощо. У випадку отримання зображення із прокатаних за допомогою чорнила пальців відображення мають значні геометричні спотворення і характеризуються низьким контрастом та великою кількістю фіктивних ознак.

Різниця в освітленні суттєво впливає на відображення обличчя. Використаний тип апаратури позначатиметься на якості підпису. Ширина смуги пропускання каналу впливатиме на звуковий сигнал і т.д.

Додатково помилки вноситимуться алгоритмами виділення особистих ознак. Різноманітні алгоритми обробки зображень вносять певні зміщення у реальне розташування ознак. Через недосконаліть алгоритмів обробки схожі ідентифікатори різних людей матимуть однакове відображення.

г) Біометричні ключі. Основною ідеєю криптографічних систем з біометричним захистом ключів є створення ланок біометричного блокування (розблокування) ключів подібно до ланок парольного захисту (блокування) ключів (рис.1.39) [189].

У таких системах криптографічний ключ зберігається як частина запису в базі даних разом із ім'ям, біометричними даними, привілеями доступу користувача. У випадку позитивного порівняння біометричних даних, збережених у базі, з даними, поданими в процесі ідентифікації, користувачеві розблоковується ключ та надаються відповідні права.

Окреслимо ряд проблем, які виникають під час роботи даної системи.

1. Необхідним є безпосередній доступ до біометричних даних для здійснення порівняння.

2. Ідентифікація користувача та розблокування ключа – це два відокремлених процеси.

3. (випливає з попередніх). Біометричні дані записуються системою локально (на магнітних носіях, брелоках і т.д.).

Рис.1.39. Структура реалізації парольної (а) та біометричної (б) схем блокування.

Очевидно, що найслабшим місцем такої системи захисту є саме носії інформації, адже викравши смарт-картку з біометрією, зловмисник отримує необмежений доступ до ключових даних, а також, що найважливіше, повністю компрометуються біометричні дані користувача [114]. На відміну від паролів чи PIN-коду, які можна змінити, біометричні дані не змінюються.

Наступною проблемою є застосування користувачем одного "ключа" (біометричних даних) у різних системах, що значно збільшує імовірність успішної атаки.

Враховуючи, що ідентифікація користувача здійснюється окремо від процесу розблокування ключа та на виході отримується лише результат "**ТАК**"/"**НІ**", подібні системи є вразливі до атак з використанням "троянських коней" (віруси, які можуть замінити підсистему біометричної ідентифікації та постійно видавати результат "**ТАК**" на вхід підсистеми розблокування ключа).

Для успішного вирішення наведених проблем, необхідно дати відповіді на такі запитання:

- чи реально створити біометричну систему, у якій неможливо скомпрометувати біометричні дані?
- чи ймовірно створити метод застосування однакових біометричних даних по-різному у різних системах?
- чи можливо, щоб система була безпечною та зручною у користуванні?

Вирішенню поставлених проблем присвячено ряд праць [125-127, 134,164,178,193-196,220,239,240,253]. Перед розглядом конкретних конструкцій зупинимось на ідеях закладених у них.

Нехай у процесі реєстрації біометричною системою зберігається не сам біометричний сигнал w, а його відображення $h(w, K)$, де K – це криптографічний ключ, який захищається системою. Трансформація $h(\,)$ – це, у певному сенсі, аналог криптографічної хеш-функції, тобто для різних входів w отримуються різні виходи, а отримання w або K із $h(w, K)$ є важкою проблемою.

Одні вчені [126] результат трансформації $h(w, K)$ називають "таємний шаблон" (private template) (рис.1.40), інші [220] – "скасовувана біометрія" (cancelable biometric). У літературі за процесом трансформації закріпився термін "зв'язування ключа" ("key binding").

Згідно нової постановки задачі у процесі ідентифікації відбувається трансформація вхідного біометричного сигналу користувача w' за допомогою функції $h(\,)$, а порівняння здійснюється у просторі відображень.

У різних системах ідентифікації, які реалізують саме такий метод, необхідно використовувати різні перетворення або те ж перетворення $h(\,)$, але з різними параметрами. І якщо у будь-якій із систем скомпрометовано $h(w, K)$, то інші системи, що базувались на тих же біометричних даних але з іншими ключами, функціонуватимуть далі без внесення змін.

У випадку застосування необоротних функцій (хеш-функції, односторонні перетворення) стійкість $h(\,)$ є доведено високою, але FRR такої системи є великою. Причина – відмінність у послідовних зчитуваннях біометричних даних. Очевидно, що для різних біометричних даних w' та w відображення $h(w')$ та $h(w)$ теж будуть різними.

За умови використання оборотних функцій (шифрування з ключем) FRR системи на рівні звичайної біометричної системи ідентифікації, але безпека біометричних даних є пропорційною

Рис.1.40. Ідентифікація з використанням "таємних шаблонів": а) – аналог парольної системи; б) – біометрична система.

стійкості оборотної функції, тобто знову виникають проблеми, пов'язані з управлінням ключами. Враховуючи вказані проблеми, конкретна конструкція трансформації $h(\ )$ повинна:

- враховувати властивості виду біометрії та можливості її представлення;

- мати оцінене параметрами системи значення втрати стійкості криптографічного ключа K у разі розголошення відображення $h(w, K)$ (т.зв. втрата ентропії);

- забезпечувати якомога меншу залежність ключа від біометричних даних. Іншими словами, необхідно забезпечити вибір будь-якого ключа незалежно від конкретних біометричних даних конкретного користувача.

Розглянемо відомі на теперішній час методи зв'язування криптографічних ключів із біометричними даними.

У своїх роботах [239-241] Сутар (Soutar) запропонував алгоритм зв'язування ключа у кореляційній системі розпізнавання відбитків пальців. Алгоритм "інтегрує" у процесі реєстрації користувача в системі криптографічний ключ K у функцію кореляції. На підставі т.зв. тренувальних відбитків пальців (автор пропонує мінімум п'ять) формується кореляційна функція $H(u) = |H(u)|\ e^{-i\varphi_H(u)}$. Далі відкидається модуль $H(u)$, а добуток фази та випадкового комплексного числа утворює нове значення фази для величини, що записується на сервері, $H_{stored}(u)$ (відповідає $h(\,)$). Модуль $|H_{stored}(u)|$ утворюється з деякого випадково вибраного ключа K. Крім H_{stored} на сервері записується хеш ключа. Повна структура даних, що відповідає конкретному користувачу, називається *Bioscrypt*. У процесі ідентифікації користувач надає свої відбитки пальців (теж мінімум п'ять раз), які корелюються за допомогою функції кореляції. Виконавши оригінальну процедуру відновлення, що використовує коди корекції помилок, автор виділяє ключ, який хешується та порівнюється із хешем, записаним у *Bioscrypt*. Результатом відновлення є або реальний ключ, або відмова у декодуванні. Алгоритм ніколи не видає неправильний ключ.

Недоліки методу:

- не розраховано втрати ентропії криптографічного ключа, який зв'язується даним методом;

- не наведено значень залежностей FAR та FRR системи розпізнавання;

- непривабливим для користувачів системи є необхідність кількаразового сканування пальця;

- низькі коректуючі властивості (до 5% помилок). З підвищенням коректуючих властивостей методу збільшується імовірність неправильної ідентифікації.

Девіда (Davida) [126,127] запропонував алгоритм з використанням біометрії рогівки ока та розглянув відображення рисунка рогівки у

2048 бітну двійкову послідовність (*IrisCode* [125]). У процесі ідентифікації розрахував віддаль Хемінга між наданою користувачем та збереженою у базі даних біометрією. Автор показав, що відмінність між різними взірцями однієї рогівки може досягати 10% (204 біт), а відмінність між рогівками різних людей – 45% (922 біт). У ході реєстрації користувача в системі отримуються декілька зображень рогівки ока та для кожної генерується відповідний K бітний *IrisCode*. Із отриманих кодів за допомогою мажоритарного декодера утворюється "канонічний" *IrisCode* **T** довжини K. Далі вибирають (N, K) – код корекції помилок довжиною N, завадостійкі властивості якого дозволяють коректувати до 10% помилок. Кодове слово C, що відповідає послідовності **T**, хешують, підписують цифровим підписом системи та записують у базі даних разом із $R = N - K$ перевірочними бітами, доданими до **T** під час кодування. У процесі ідентифікації користувач надає *IrisCode* **T'**, до якого додається R, утворена двійкова послідовність вважається спотвореним кодовим словом. Застосувавши функцію декодування, отримують кодове слово C', яке хешується, підписується цифровим підписом. Результат порівнюється з даними, збереженими у базі. Автор стверджує, що *IrisCode* може використовуватись як криптографічний ключ, а для збільшення ентропії пропонується вживати додатковий символьний пароль. Алгоритм є дуже швидким та надійним настільки, наскільки надійною є застосовувана хеш-функція. У методі чітко окреслена величина втрати ентропії використовуваного ключа (10% згідно використовуваного коду корекції помилок)

Недоліки алгоритму:

- на відміну від попереднього даний метод розглядається як метод генерації ключа, тобто біометричним даним користувача можливо поставити у відповідність лише один ключ;
- на жаль, як показано у роботі [125], відмінність між різними взірцями однієї і тієї ж рогівки може досягати 30%, що відповідно свідчить про низькі коректуючі властивості методу або необхідність збільшення втрати ентропії до 30% для збільшення коректуючих властивостей.

Монроуз (Monrose) [196] запропонував об'єднати пароль користувача з біометрією динаміки роботи з клавіатурою. Це дослідження є продовженням попередніх [180,197], у яких обгрунтовано метод рандомізації паролів перед хешуванням. Під рандомізацією, у даному випадку, розуміється приєднання до пароля (*psw*) випадкової послідовності довжиною s-біт, у результаті

утворюється т.зв. "зміцнений" пароль (*hpsw*). У процесі реєстрації користувача системою зберігається наступна інформація:

- випадкове число r довжиною k біт;
- "таблиця інструкцій" зашифрована за допомогою *psw*. Таблиця інструкцій містить інформацію про генерацію з r та *psw* значень *hpsw*. Процес генерації є толерантним до певної кількості помилок (параметр системи);
- "файл історії", зашифрований з використанням *hpsw*.

У ході ідентифікації користувач надає *psw'*. Під час набору пароля отримується біометрія. Обидві величини утворюють *hpsw'*, яке використовується для розшифрування файла історії. У разі невдачі система розшифровує таблицю інструкцій за допомогою наданого пароля та за схемою розподілу таємниці Шаміра генерує інше значення *hpsw'*, яке знову застосовується для спроби розшифрування. Процес повторюється n раз, де n – параметр безпеки алгоритму.

Автор пропонує використовувати *hpsw* як ключ шифрування. Але, насправді, отримані таким чином біометричні дані лише на 15 біт збільшують ентропію пароля, що несуттєво збільшує ефективність звичайної парольної системи ідентифікації. У наступних модифікаціях алгоритму [194,195] Монроуз на підставі біометрії голосу збільшив додаткову ентропію до 60 біт. Позитивним фактором тут слід визнати незалежність вибору ключа від біометричних даних, недоліком – відсутність інформації про втрату ентропії ключа.

Тайлз (Tuyls) [178,253] розробив алгоритм захисних функцій для збільшення конфіденційності ("Shielding Functions to Enhance Privacy"). У процесі реєстрації користувачем вибирається довільний криптографічний ключ S, який у вигляді хешу V записують у базі даних. Далі знаходять таке значення W, яке задовольняє умові $G(W, X) = S$, де X – біометрія користувача; $G(\,)$ – функція "δ-зв'язування", яка для усіх X', що знаходяться у δ-околі значення X, видає S. Автор вказує, що будь-яка детермінована функція володіє властивістю 0-зв'язування, ∞-зв'язуванням володіє функція $G(W, X) = \text{const}$. Величина W вноситься у базу даних. У процесі ідентифікації користувачем надається біометрія X', а сервером ідентифікації величина W, які подаються у $G(W, X')$. Отримане значення S' хешується та порівнюється із V. На основі результату приймається рішення про ідентифікацію. Робота функції δ-зв'язування ґрунтується на використанні завадостійкого кодування. Робота Тайлза носить суто теоретичний характер. Не проводились дослідження із

застосуванням конкретного виду кодів корекції, не розраховувались значення втрати ентропії, не вказано рівень стійкості системи.

У схемі "нечіткого зв'язування" (fuzzy commitment) [164] Джулс і Ватеннберг (Juels and Wattenberg) продовжили дослідження Девіди для покращання коректуючих властивостей алгоритму. У процесі реєстрації користувач вибирає секретний ключ C, який одночасно є кодовим словом БЧХ коду. Нехай d – це відстань між C та $\mathbf{T}$ – біометричною двійковою послідовністю. Структура fuzzy commitment містить d та хеш ключа C. Під час ідентифікації користувач надає біометрію $\mathbf{T}'$. З допомогою d знаходять найближче кодове слово C', яке хешується та порівнюється з записаним на сервері. Перевагами цього алгоритму є простота його реалізації та можливість використання будь-якого коду корекції помилок. Однак алгоритм має ряд суттєвих недоліків:

- автор пропонує використовувати метод із будь-яким типом біометрії, але не вказує жодного методу перетворення біометрії у бітову послідовність ключа **T**;
- алгоритм не працює при перестановці символів у **T**, що відповідає спотворенням, які пов'язані зі скануванням; алгоритм вимагає рівномірного закону розподілу ключа, що неможливо для біометричних даних;
- вибір ключів обмежений множиною кодових слів.

У таблиці 1.5 наведено порівняльну характеристику конструкцій. Трансформації біометричних даних класифікуються як зв'язуючі (З) та генеруючі (Г). Більш ширше застосування мають зв'язуючі функції, які дозволяють вибрати довільний ключ, незалежний від біометричних даних.

Таблиця 1.5. Порівняння реалізацій біометричного захисту ключів

Алгоритм	Тип біометрії	Класифікація	Безпечність	Практичність	Чутливість до помилок	Стійкість
Сутар	Пальці	З	В	С	В	Не досліджувалася
Девіда	Рогівка	Г	В	В	Н	С
Монроуз	Клавіатура, голос	З	В	В	В	Не досліджувалася
Тайлз	Не визначено	З	В	Н	Н	Не досліджувалася
Джулс	Не визначено	Г	В	В	Н	С

РОЗДІЛ 2. ГОЛОСОВА АУТЕНТИФІКАЦІЯ

2.1. Визначення інформативних ознак розпізнавання мовних сигналів

Як правило, у завданнях розпізнавання мовних сигналів першим етапом аналізу є визначення особливостей, які характеризують цей сигнал. На даний час існує багато підходів одержання інформативних ознак – компактної множини чисел, котра відображає характерні риси відповідного сигналу.

Один з таких підходів базується на застосуванні дискретного перетворення Фур'є, яке обчислюється у вікні фіксованого розміру вздовж сигналу, причому для вирішення проблеми виявлення локальних інформативних областей, що утворюються на границі вікон, використовують стратегію перекривання вікон. Із отриманих спектральних коефіцієнтів формуються кепстральні коефіцієнти, які компактно представляють заданий тип сигналів.

Основним недоліком віконного перетворення Фур'є є його фіксована часово-частотна роздільна здатність, тобто вікно має фіксований розмір і його важко пристосувати під коректне представлення локальних особливостей сигналу. Крім того, базисна функція розкладу залишається гармонічною, а тому не здатна описувати локальні зміни сигналу. Єдиним способом опису локальних змін є різке збільшення спектральних складових, що приведе до зміни форми сигналу за межами локальної особливості.

Використання вейвлет-аналізу для розпізнавання мовних сигналів є потужнішим методом порівняно з Фур'є-аналізом [2,35,39,64], оскільки вейвлет-перетворення оперують функціями, локалізованими як у часовій, так і в частотній областях, на відміну від Фур'є - функцій, які добре локалізовані в частотній області, але погано локалізовані в часовій області та не здатні описувати локальні особливості сигналу.

Нехай задано множину $V_n = \{S_1, S_2, S_3, ...S_s\}$, елементами якої є послідовності $S_k = \{x_1, x_2, x_3, ...x_l\}$, де x_i – відліки відповідних функції $X_s(t)$ в дискретні моменти часу, $t_i = i \cdot \Delta T$, ΔT – період дискретизації. Функції $X_s(t)$ – це реалізації обраної команди, які озвучуються *n*-ним диктором.

Суть задачі полягає в тому, що із заданих послідовностей S_s необхідно визначити множину O_n, яка б компактно представляла

множину V_n, тобто $O_n \subset S_1$, $O_n \subset S_2$, $O_n \subset S_s$. Широка різноманітність мовних сигналів приводить до появи великої кількості проблем, які виникають при розв'язанні задач такого класу. Це пов'язане з тим, що на формування мовних сигналів впливають різного роду фактори, які важко описати аналітично.

У загальному випадку математична модель, яка відображає мовні сигнали на виході мікрофона, повинна враховувати всю багатогранність і основні детерміновані закономірності перетворення сигналів такого класу, які зумовлені особливостями мови та її діалектів, фонемного складу, індивідуальними й емоційними особливостями, нелінійною зміною темпу й інтенсивності відтворення, явищами коартикуляції та редукції. Така модель повинна відображати процеси мовотворення й не суперечити відомим даним про сприйняття мови людиною. Вона має враховувати акустику приміщення й перетворюючі властивості мікрофона.

Очевидно, що розробити ефективну математичну модель, яка б ураховувала всі перелічені вище фактори дуже складно, оскільки важко встановити межі й характер розподілу деяких факторів, а також їхню взаємозалежність або вплив один на одного. Тому для розв'язку поставленої задачі необхідно ввести ряд спрощень, які є адекватними для заданої ситуації.

Приймаємо, що модифікація основних складових мови під дією явища коартикуляції й редукції є незначною, а зміна темпу відбувається лінійно. Крім того, вважатимемо, що шум, спричинений цим трактом, є адитивним і розподілений за нормальним законом.

Отже, для виділення множини O_n, яка компактно репрезентує множину сигналів V_n, необхідно провести процес декомпозиції – розклад S_s послідовностей по базису заданих функцій і представлення множини O_n вибраними за відповідним критерієм коефіцієнтами розкладу того чи іншого рівня композиції.

Вибір способу розкладу і типу базисних функцій є принципово важливим, оскільки від цього залежить інформативність представлення множини V_n. Декотрі з базисних вейвлетів відносяться до ортогональних і дозволяють проводити повну реконструкцію сигналу, інші цього не дозволяють зробити, проте краще описують локальні особливості сигналів.

Як було сказано раніше, використання гармонічних функцій у якості базисних (Фур'є-аналіз) не є досить ефективним.

Основним чинником при виборі базисних вейвлетів для задачі розпізнавання мови є можливість кращого виявлення тонких особливостей сигналів порівняно з іншими вейвлетами (табл. 2.1).

Базис функцій, який використовується у вейвлет - аналізі, утворюється шляхом зсуву $\Psi_0(t-b)$ й масштабування $\Psi_0(t/a)$ заданої функції Ψ_0, яка називається материнським вейвлетом, тобто

$$\Psi = a^{-1/2} \cdot \Psi_0\left(\frac{t-b}{a}\right).$$

Зменшення параметра масштабування a дозволяє ефективно задіяти базисні функції для аналізу високих частот, а його збільшення – для аналізу низьких частот, тобто з'являється можливість адаптивного до сигналу вибору базисних функцій.

Число використаних при розкладанні базисів задає рівень декомпозиції сигналу, причому за нульовий рівень приймається сам сигнал, а рівні декомпозиції – вниз спадаюче дерево того або іншого виду. Материнською функцією вейвлетів можуть бути різні функції, у тому числі ті, які нагадують модульовані імпульсами синусоїди, функції зі стрибками рівня, а це у свою чергу забезпечує легке представлення сигналів з локальними особливостями, набором базисів (вейвлетів) того чи іншого типу.

Основою для визначення множини O_n є використання багаторівневого аналізу (multiresolution analyze).

Такий аналіз грунтується на представленні сигналу на кожному з рівнів декомпозиції сумою з двох складових – грубої (апроксимуючої) та детальної (деталізуючої), тобто

$$X_s(t) = \sum_k c_{m,k}\varphi_{m,k}(t) + \sum_{m \geq m,k} d_{m,k}\Psi_{m,k}(t)$$

де $c_{m,k}$ й $d_{m,k}$ – коефіцієнти, які визначаються наступним чином:

$$c_{m,k} = \int X_s(t)\varphi_{m,k}(t)dt\,,$$

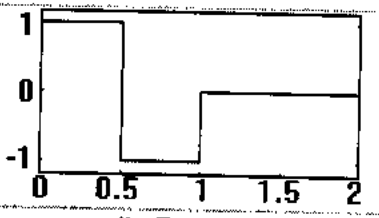
$$d_{m,k} = \int X_s(t)\Psi_{m,k}(t)dt\,.$$

Функція $\varphi(t)$ (скейлінг функція) визначає грубе наближення (апроксимацію) сигналу й породжує коефіцієнти апроксимації, функція $\varphi(t)$ властива не всім вейвлетам, а тільки тим, які відносяться до ортогональних.

Таблиця 2.1. Приклади базисних вейвлетів

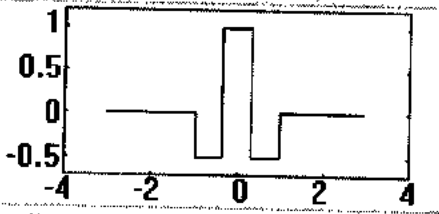
HAAR - вейвлет

$$\psi(t)=\begin{cases}1, & 0\le t<1/2\\ -1, & 1/2\le t<1\\ 0, & t<0, t\ge 1\end{cases}$$



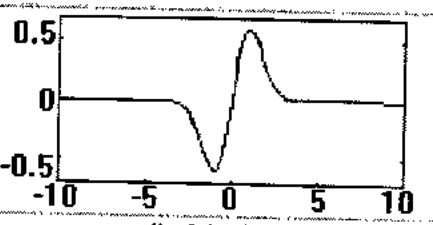
FHAT - вейвлет ("Французька шапка" - French hat)

$$\psi(t)=\begin{cases}1, & |t|\le 1/3\\ -1/2, & 1/3<|t|\le 1\\ 0, & |t|>1\end{cases}$$



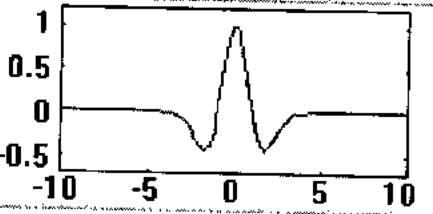
Wave - вейвлет

$$\psi(t)=t\exp\left(-\frac{t^2}{2}\right)$$



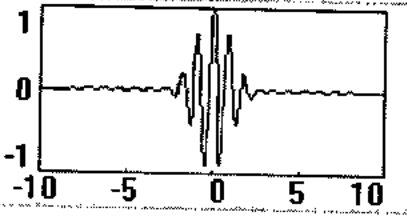
MHAT - вейвлет ("Мексиканська шапка" - Mexican hat)

$$\psi(t)=\left(1-t^2\right)\exp\left(-\frac{t^2}{2}\right)$$



Вейвлет Морле

$$\psi(r)=\exp\left(ik_д r-\frac{r^2}{2}\right)$$



Функція $\Psi(t)$, як було описано вище, створюється на основі тієї чи іншої материнської функції $\Psi_0(t)$, визначає деталі сигналу та породжує коефіцієнти деталізації.

Тобто представлення сигналу при використанні багаторівневого аналізу – це спадаюче дерево коефіцієнтів апроксимації й деталізації заданого рівня розкладу, формування дерева розкладу може відбуватися за допомогою алгоритму Маллата або використання алгоритму пакетного вейвлет - перетворення.

У звичайному алгоритмі Маллата швидкого вейвлет-перетворення (ШВП) при переході з масштабного рівня m на рівень $m+1$ функція апроксимуючих коефіцієнтів $c_{m,k}$ розділяється на низькочастотну $(c_{m+1,k})$ і високочастотну $(d_{m+1,k})$ частини спектрального діапазону, і при наступному збільшенні масштабних рівнів аналогічно проводиться розклад, проте лише для низькочастотних (апроксимуючих) функцій [179] (рис. 2.1 а).

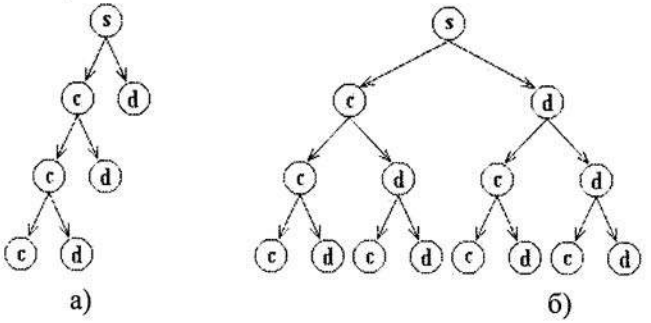


Рис. 2.1. Швидке вейвлет-перетворення: а) – алгоритм Маллата; б) – пакетні вейвлети.

Це обумовлено тим, що високочастотні функції (деталізуючі) є малоінформативними порівняно з низькочастотними (апроксимуючими), однак такий підхід не є ефективним, оскільки відкидання високочастотних функцій приводить до видалення шумів не тільки, але й характерних локальних особливостей сигналу, які можуть бути використані для компактного представлення заданого сигналу.

У пакетному алгоритмі ШВП операція послідовного частотного розщеплення застосовується як для низькочастотних, так і для високочастотних (деталізуючих) коефіцієнтів [37,52]. У результаті виникає дерево розкладу, приклад якого показаний на рис. 2.1 б.

При такому розкладі вейвлети кожного наступного рівня утворяться з вейвлета попереднього рівня поділом на два нових вейвлета:

$$\Psi_1 = \sum_n h_n \Psi(t-n),\ \Psi_2 = \sum_n g_n \Psi(t-n),$$

де g_n, h_n – відповідні вагові коефіцієнти.

Нові вейвлети також локалізовані, але на двічі ширшому інтервалі. Відповідно повний набір вейвлетних функцій розкладу називають вейвлет - пакетом.

Пакетне вейвлет - перетворення є адаптивним, тобто дозволяє точніше врахувати особливості сигналів шляхом вибору відповідного дерева оптимальної форми розкладу, що забезпечує мінімальну кількість вейвлет - коефіцієнтів при заданій точності реконструкції сигналу, тим самим виключаючи інформаційно - надлишкові та непотрібні деталі сигналів.

Оцінка інформативності сукупності вейвлет - коефіцієнтів:

$$E = \exp(-\sum_n p_n \cdot \log(p_n)),\ p_n = |x_n|^2 \| x \|^{-2}.$$

Будь-яке усереднення коефіцієнтів збільшує ентропію. При аналізі дерева обчислюється ентропія вузлів і його розділених частин c і d. Якщо при розділенні вузла ентропія не зменшується, то подальший розклад цього вузла не має сенсу.

Таким чином, використавши алгоритм пакетного розкладу для кожної складової множини V_n, можна визначити сукупність вузлів, ентропія яких не зменшується у випадку наступного розкладання цього вузла. Із сукупності вузлів для кожної складової множини V_n необхідно вибрати ті вузли, які є найбільш схожими за заданим критерієм. Таким критерієм може бути мінімум Евклідової відстані та близькість параметрів розподілу функції у вузлі.

Вибрану подібним способом функцію у вузлі можна вважати компактним поданням множини V_n. Далі над отриманою функцією проводиться операція стиску динамічного діапазону, в якості якої може бути використана нелінійна операція логарифмування.

Для одержання коефіцієнтів розпізнавання виконаємо операцію кепстрального аналізу:

$$C_s(m) = \frac{1}{N} \sum_{n=0}^{N-1} In|S(n)|^2 e^{i\frac{2\pi}{N}nm} \quad ,m = 0,1,...,2N-1.$$

Отримані значення – це ознаки для розпізнавання n-го диктора по заданій команді.

2.2. Алгоритм визначення ознак розпізнавання мовних сигналів у біометричних системах

На першому етапі алгоритму (рис. 2.2) здійснюється запис реалізацій команди шляхом п'ятиразового озвучення обраного слова диктором, з використанням вугільного мікрофона марки Y345D фірми GENIUS. Параметри реєстрації сигналу: частота дискретизації – 22,05 кГц; кількість біт, які використовуються для квантування значень сигналу, – 8; кількість каналів запису сигналу – 1 (Mono).

Рис. 2.2 Блок-схема методу визначення ознак розпізнавання

При виконанні процедури запису слід дотримуватися таких вимог:

- відстань від губ диктора до мікрофона – 3...5 см;

- команди озвучувати спокійним тоном з рівномірною інтонацією.

Експериментально було встановлено, що ефективність розпізнавання системи покращується у випадку озвучення диктором тексту, який складається з певної послідовності речень. Кожне речення в своєму складі містить команду, яку потрібно записати. Далі проводиться аналіз кожного речення з наступним виділенням озвученої реалізації команди.

Такий підхід зумовлений психофізіологічним станом диктора в момент запису, тобто при озвученні окремо взятої команди людина переходить у стан зацікавленості й здивування, що накладає свій слід на формування голосу та формування команди. Реалізація запису команди методом виділення з відповідних озвучених речень дозволяє стабілізувати психофізіологічний стан диктора, оскільки його увага не буде сконцентрована на окремо взятому слові (команді), а розподілятиметься по всьому тексту.

Другий етап – виділення команди з потоку слів. Він базується на визначенні двох простих характеристик: енергії й кількості переходів через нуль. Визначення енергії відбувається у рухомому вздовж усього сигналу вікні. Формально записується як

$$E_n = \sum_{m=n-N+1}^{n} x^2(m) \cdot w(n-m),$$

де $x(m)$ – відліки дискретизованого мовного сигналу із частотою дискретизації $f_д = 22{,}05$ кГц;

$$w(n) = \begin{cases} 1, & 0 \le n \le N-1 \\ 0, & \text{в іншому випадку} \end{cases}$$ – функція вікна.

Таким чином, миттєва енергія сигналу в момент n є сумою квадратів N відліків від $n - N + 1$ до n.

Загасання за межами вікна залежить від типу вікна й несуттєво від його ширини. Якщо N приймає малі значення (порядок періоду основного тону або менше), то E_n буде змінюватися дуже швидко, відповідно до тонкої структури мовного сигналу. Якщо N приймає великі значення (порядок декількох періодів основного тону), то E_n змінюватиметься повільно та не буде адекватно описувати зміни особливостей мовного сигналу. Це означає, що не існує єдиного значення N, яке б задовольняло всі перераховані вище умови, адже період основного тону може змінюватися від 20 відліків для високих жіночих і дитячих голосів до 500 відліків для дуже низьких чоловічих

голосів. На практиці N вибирають рівним 200...400 відліків при частоті дискретизації 22,05 кГц.

Характеристика E_n дозволяє відрізнити вокалізовані мовні сегменти від невокалізованих, а у випадку високоякісного мовного сигналу (з високим значенням відношення сигнал - шум) функцію енергії можна використовувати для відділення мови від пауз.

Одним із недоліків функції миттєвої енергії є чутливість до великих рівнів сигналу, оскільки кожний відлік підноситься до квадрата. Внаслідок чого значно спотворюється співвідношення між значеннями послідовності $x(m)$. Простим способом позбавлення цього недоліку є перехід до функції середнього значення у вигляді

$$M_n = \sum_{m=-\infty}^{\infty} |x(m)| \cdot w(n-m), \qquad (2.1)$$

де замість суми квадратів обчислюється зважена сума абсолютних значень ($|x(m)|$ – абсолютне значення сигналу).

Другою характеристикою, яка дозволяє виділити команду з потоку слів, є функція середнього числа переходів через нуль. Розглянемо спосіб визначення цієї величини:

$$Z_n = \sum_{m=-\infty}^{\infty} | sign[x(m)] - sign[x(m-1)] | \cdot w(n-m), \qquad (2.2)$$

де

$$sign[x(n)] = \begin{cases} 1, & x(n) \geq 0 \\ -1, & x(n) < 0 \end{cases}$$ – функція визначення знака;

і

$$w(n) = \begin{cases} 1/2N, & 0 \leq n \leq N-1 \\ 0, \text{ в іншому випадку} \end{cases}$$ – функція вікна.

Оскільки енергія вокалізованих сегментів мовного сигналу концентрується на частотах, менших, ніж 3 кГц, що зумовлено спадаючим спектром сигналу збудження, а для невокалізованих сегментів більша частина енергії лежить в області високих частот, існує тісний зв'язок між числом нульових переходів і розподілом енергії по частоті.

Очевидно, що великій кількості переходів через нуль відповідають невокалізовані сегменти, а малій кількості – вокалізовані сегменти мовного сигналу.

Опишемо роботу алгоритму виділення команди з потоку речення на основі використання згаданих вище характеристик.

Приймається, що перші 100 мс не містять мовного сигналу. На цьому відрізку обчислюються середнє значення й дисперсія кожної з величин (2.1), (2.2) для оцінки статистичних параметрів шуму. Потім, із урахуванням цих параметрів і максимального середнього значення на відрізку, обчислюються пороги для середнього числа нульових переходів і енергії сигналу. Визначається фрагмент коливань, на якому траєкторія середнього значення перевищує деякий поріг (P_1). Допускається, що початок і кінець команди лежать поза границями цього фрагмента. Далі, рухаючись у протилежну сторону по осі часу від моменту, де M_n вперше перевищив поріг P_1, визначають момент, коли M_n вперше виявився менше нижнього порога P_2. Цей момент вибирають як початок. Подібним чином визначається закінчення команди N_2.

Наступний крок – це переміщення вліво від N_1 (вправо від N_2) і порівняння числа переходів через нуль із порогом P_1. Це переміщення не повинне перевищувати 25 інтервалів ліворуч від N_1 (праворуч від N_2). Якщо число переходів через нуль перевищує поріг у 3 і більше раз, то початок команди переноситься туди, де крива нульових переходів уперше перевищила поріг. Аналогічно роблять із N_2.

Третім етапом методу визначення ознак розпізнавання є часова нормалізація образів. Як відомо, для реалізації системи розпізнавання необхідно сформувати класи образів розпізнавання. Кількість образів, які представляють обраний клас, залежить від інформативності ознак, котрі їх описують. Системи розпізнавання мовних сигналів відзначаються широкою мінливістю образів, які представляють обраний клас, тому очевидним є те, що для підвищення ефективності роботи таких систем розпізнавання намагаються максимально інформативно описати всі наявні класи. Інформативність описів класу найчастіше досягається шляхом застосування ефективних алгоритмів визначення ознак розпізнавання, однак поліпшити інформативність опису можна також збільшенням кількості образів, які представляють даний клас.

Очевидно, що для побудови системи розпізнавання необхідно, щоб усі образи мали однакову розмірність. Тому для часової нормалізації образів застосовується лінійний метод регуляції темпу мовних сигналів, запропонований Гарві [38].

Четвертий етап – це розклад кожного образа з використанням алгоритму пакетного вейвлет - розкладу. У якості материнського вейвлета використовується вейвлет Добеші 9-го порядку. Оскільки цей базис ортонормований, то є можливість реалізувати швидкий алгоритм

обчислення вейвлет - коефіцієнтів на кожному частотному рівні через уже знайдені коефіцієнти на рівні з більш високою частотою.

На рис. 2.3. показане розкладання однієї з реалізацій команди "zero" на підставі пакетного вейвлет-алгоритму.

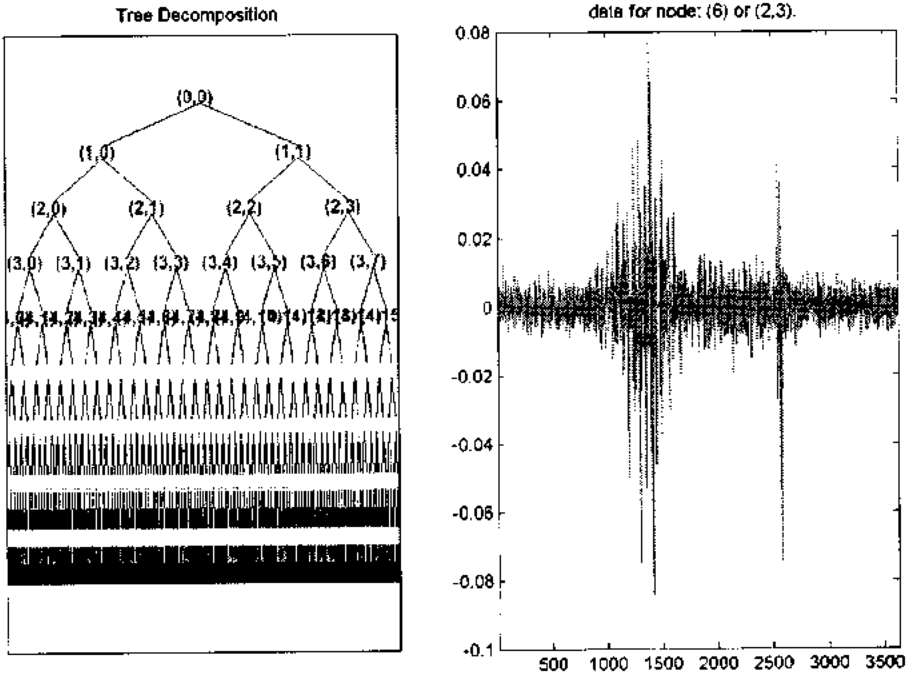


Рис. 2.3. Розклад реалізації звукової команди "zero" з використанням пакетного вейвлет – алгоритму.

У лівій частині малюнка зображене вейвлет-дерево 9-го порядку, а у правій – вид сигналу у вузлі (2,3).

П'ятий етап – оптимізація вейвлет-дерева за критерієм ентропії, проводиться аналіз і розрахунок ентропії вузлів дерева і розділених частин. Якщо ентропія вузлів не зменшується, то розклад такого вузла надалі не проводиться.

На рис. 2.4 у лівій частині представлене оптимізоване за критерієм ентропії вейвлет - дерево. У правій частині зображена часова залежність сигналу в одному з термінальних (кінцевих) вузлів.

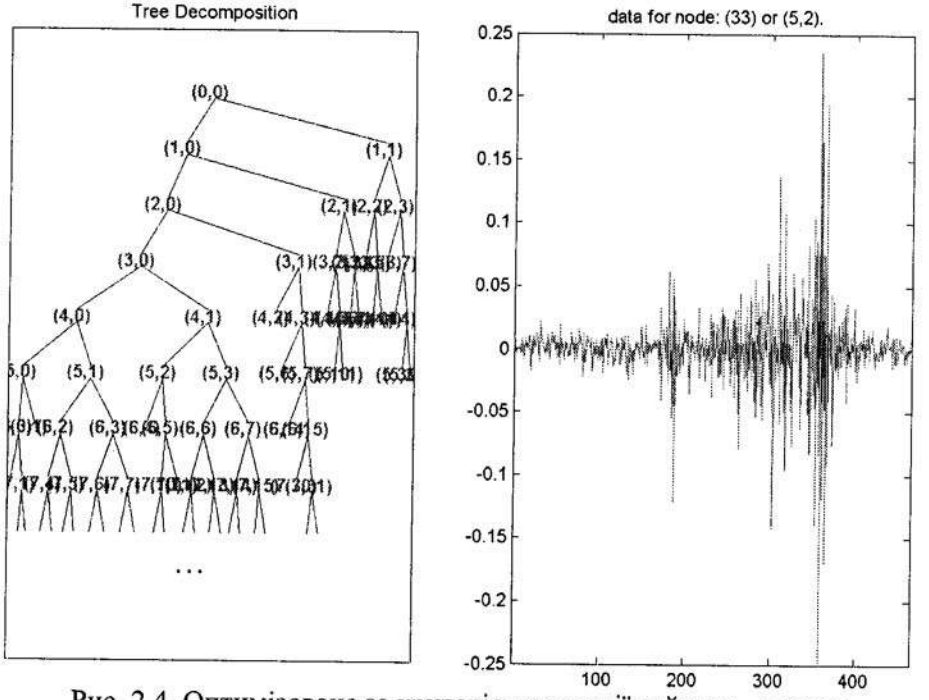


Рис. 2.4. Оптимізоване за критерієм ентропії вейвлет – дерево.

Шостий етап – пошук оптимальних термінальних вузлів для формування класу розпізнавання. У свою чергу цей етап можна розділити на кілька кроків.

Перший крок –визначення списку всіх термінальних вузлів, які знаходяться в оптимізованих вейвлет - деревах кожного з образів відповідного класу розпізнавання.

Другий крок – порівняння термінальних вузлів з однаковими номерами для різних образів заданого класу. Як критерій порівняння використовується швидкість зміни кількості переходів через нуль. У випадку, коли номери термінальних вузлів для різних образів одного класу не збігаються, проводиться порівняння термінального вузла з вузлами, які не є термінальними й знаходяться в інших образах того ж класу, але номери яких рівні номерам термінальних вузлів.

Третій крок – визначення номера вузла із заданого переліку (може бути як термінальним, так і не термінальним), який буде представляти даний образ у класі. Критерієм вибору є максимальний збіг значення функції зміни швидкості переходів через нуль із такими ж функціями, отриманими для інших образів.

Таким чином, наприкінці шостого етапу ми одержуємо часові залежності, які характеризують даний клас.

Сьомий етап - визначення векторів розпізнавання, які є векторами однакової розмірності. Для цього використовують операцію дискретного кепстрального аналізу. Кількість коефіцієнтів розкладу приймається рівним 20.

2.3.Оцінка вірогідності роботи системи розпізнавання людини по голосу на основі диференціальних імовірностей правильного (неправильного) розпізнавання

Обчислення помилки виявлення класифікації здійснюється за допомогою відстані Махаланобіса. Зв'язок між відстанню Махаланобіса й помилкою виявлення описується наступною формулою:

$$p(e)=\frac{1}{2}\Phi(-\frac{1}{2}\sqrt{r_{ij}})+\frac{1}{2}\left[1-\Phi(\frac{1}{2}\sqrt{r_{ij}})\right]=\frac{1}{2}\int_{\frac{1}{2}\sqrt{r_{ij}}}^{\infty}\frac{1}{\sqrt{2\pi}}\exp(-\frac{y^2}{2})dy +$$

$$+\frac{1}{2}\left(1-\int_{-\infty}^{\frac{1}{2}\sqrt{r_{ij}}}\frac{1}{\sqrt{2\pi}}\exp(-\frac{y^2}{2})dy\right) = \int_{\frac{1}{2}\sqrt{r_{ij}}}^{\infty}\frac{1}{\sqrt{2\pi}}\exp(-\frac{y^2}{2})dy.$$

Відповідну залежність подано на рис. 2.5.

У тестуванні використано 5 класів образів, один із яких правильний. Оцінка помилки для найбільш несприятливого класу становить порядку 30%, а для найменш несприятливого – близько 5%. Оцінка середньої помилки виявлення для всіх класів складає порядку 20%.

Очевидно, що дана вибірка в статистичному розумінні є малою. У загальному випадку діапазон невеликої вибірки за результатами численних досліджень числових послідовностей становить від 10...15 до 200. За таких обставин не доводиться сподіватися на регулярність статистичних характеристик середнього значення й дисперсії ймовірностей правильного (неправильного) розпізнавання. Відомо, що ймовірність правильного розпізнавання є величиною меншою від 1 для вибірок довільного розміру. Однак класичні статистичні підходи не настільки чутливі для того, щоб в умовах малих вибірок надійно уникати одиничної (нульової) події щодо ймовірностей правильного (неправильного) розпізнавання. Довільна класична статистична оцінка

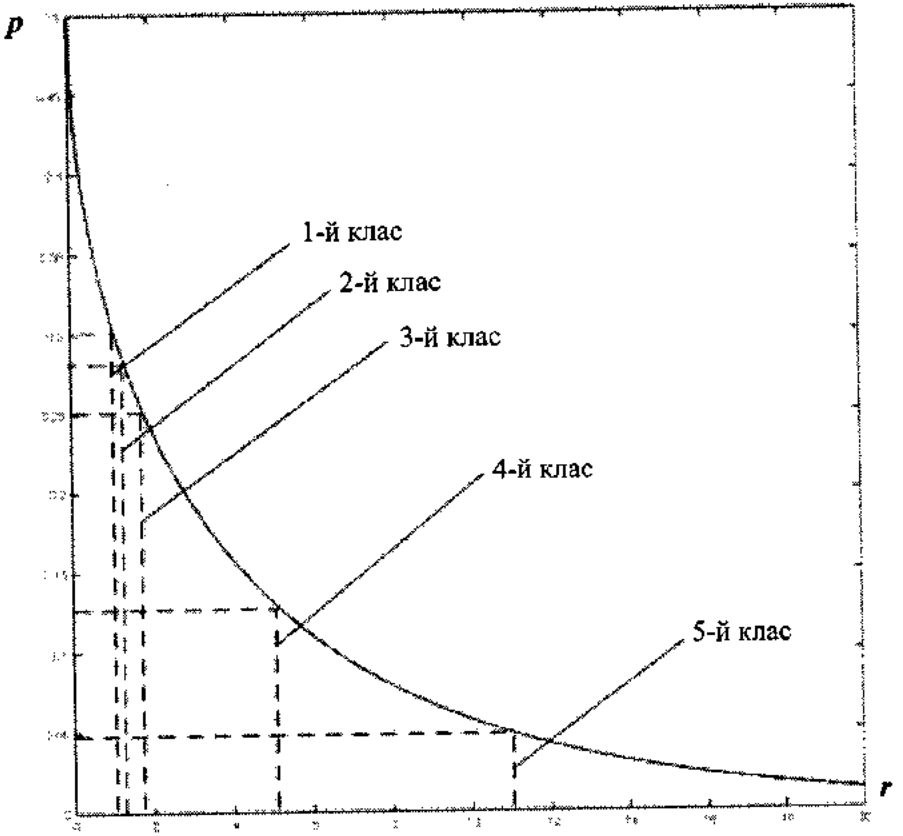


Рис. 2.21 Залежність імовірності помилки виявлення від величини відстані Махаланобіса

в умовах невеликих вибірок характеризується більшими значеннями дисперсій, що значно погіршує імовірність самої статистичної оцінки.

Для запобігання проблем оцінювання за допомогою статистичних підходів були застосовані методи диференціального оцінювання ймовірності правильного (неправильного) розпізнавання [40-42,226]. Доведено, що усереднена за базою даних диференціальна ймовірність правильного (неправильного) розпізнавання рівна ймовірності правильного (неправильного) розпізнавання алгоритму в цілому. При цьому дисперсія побудованої в такий спосіб оцінки ймовірності правильного (неправильного) розпізнавання може в кілька разів бути меншою, ніж у випадку класичних статистичних оцінок. На завершення слід відзначити, що оцінка середньої ймовірності

неправильного розпізнавання на рівні 20 % відповідає класу такого роду біометричних систем.

2.4. Методи компресії мовних сигналів

При побудові біометричних систем класифікації та розпізнавання мовних сигналів важливого значення набуває розробка ефективних методів компресії мовних образів [53,86-88]. У першу чергу це пов'язано з тим, що пропускна здатність сучасних ліній зв'язку є обмеженою. Тому актуальним є створення таких методів компресії, які б із мінімальними спотвореннями проводили завадостійкий стиск мовних образів.

Методи компресії мовних сигналів можна розділити на дві загальні групи: без втрати якості (вони в основному базуються на усуненні послідовності однакових фрагментів) та з частковою втратою якості сигналу (рис. 2.6). Останні й набули найбільшого застосування через свою гнучкість і можливість досягати великого ступеня компресії при достатній якості.

Широкої популярності у системах аутентифікації з використанням мовних сигналів отримали методи компресії на основі ортогональних перетворень.

Будь-який реально існуючий мовний сигнал має нерівномірний спектр з переважаючою більшістю низькочастотних складових. Виходячи з цього припустимо можливість утворення деякого гіпотетичного ортогонального перетворення, яке не синтезується взагалі. Розклад сегмента сигналу на коефіцієнти дає однакові за амплітудою коефіцієнти в певному інтервалі u.

Кожний сегмент оцифрованого мовного сигналу можна представити коефіцієнтами розкладу в дискретному базисі ортогональних функцій без усякої втрати форми й параметрів сигналу. Це дозволяє використовувати більш гнучкі методи компресії, а також збільшити якість компресованих сигналів. Функції є ортогональними при виконанні умови

$$\int_{-\infty}^{\infty} \varphi_i(t)\varphi_j(t)dt = 0, \quad i \neq j, j, i = 1,...,N.$$

При використанні цифрового представлення умова ортогональності має вигляд:

$$\sum_{n=-\infty}^{\infty} \varphi_i(n)\,\varphi_j(n) = 0, \qquad i \neq j, j, i = 1,...,N.$$

Рис. 2.6. Ієрархія методів компресії мовних сигналів.

Прямий дискретний розклад в ортогональному базисі записується:

$$F(m) = \sum_{n=1}^{N} x(n)A(m,n),$$

де N – кількість вибірок у сегменті перетворення; $A(m,n)$ – ядро прямого перетворення (матриця $N \times N$).

Зворотне перетворення має вигляд:

$$\tilde{x}(n) = \sum_{m=1}^{N} F(m)B(n,m),$$

де $B(n,m)$ – ядро зворотного перетворення.

У матричному представлені пряме й зворотне перетворення записуються

$$f = Ax,$$
$$\tilde{x} = Bf.$$

Для унітарних перетворень матриця $B = A^{-1} = A^T$. Матриці A і B називають операторами прямого й зворотного перетворення.

Відома велика кількість ортогональних перетворень, таких як Фур'є, Уолша, синусне, косинусне та ін. Вибравши відповідне перетворення, можна досягти різних результатів щодо компресії і якості самого компресованого сигналу. Від цього залежить форма спотворень, що виникають під час компресії.

Далі розглянемо відомі базиси ортогональних функцій (БОФ) для компресії мовних сигналів. Для більш глибокого представлення властивостей БОФ введемо поняття середньостатистичного рівня коефіцієнтів розкладу (СРКР) сегмента сигналу, який знаходиться шляхом усереднення кожного i - го коефіцієнта розкладу для великої кількості сегментів сигналу і сформований різними дикторами та при різних ситуаціях.

Математично це записується так:

$$U(i) = \frac{\sum_{k=0}^{M-1} |f(i+kN)|}{\sum_{k=0}^{M-1}\sum_{n=1}^{N} |f(n+kN)|},$$

де M – кількість сегментів розкладу; N – кількість коефіцієнтів розкладу сегмента; $f(\,)$ – розклад сегмента сигналу в БОФ.

БОФ, у якому максимальні значення СРКР зосереджуються у вузькій області, має більші можливості для якісної компресії. Для практичного знаходження СРКР утворений сигнал, який складається із фраз, вимовлених одинадцятьма різними дикторами, має 2 659 328 вибірок та тривалість 5,5 хв.

2.4.1. Базиси ортогональних функцій

а) Перетворення Фур'є. Розклад сигналу в БОФ Фур'є найбільш відомий в радіотехніці, за допомогою якого можливе знаходження спектра сигналу.

Ядро прямого дискретного перетворення Фур'є [69] визначається як

$$A(j,k) = e^{\frac{2\pi . i}{N} . jk}, \quad k, j = 0...N-1 \quad .$$

У загальному випадку ортогональні функції Фур'є мають комплексний характер, на рис. 2.7 представлено модуль шести перших функцій Фур'є.

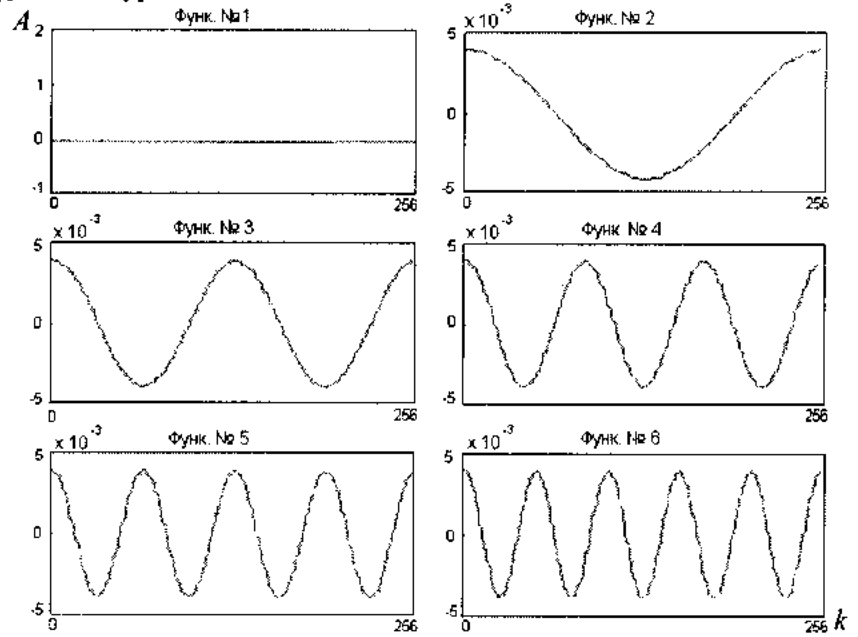


Рис. 2.7. Модуль перших шести ортогональних функцій Фур'є.

СРКР для дискретного перетворення Фур'є зображено на рис. 2.8 (через симетричність спектра та для наочності результатів нульовий коефіцієнт (відносна частота) перенесений на середину графіка). Середина інтервалу відповідає нульовій частоті, а кінцеве значення припадає на частоту 4 кГц, отже, мовний сигнал є низькочастотним.

У цьому й у наступних описах перетворень буде представлено тільки пряме перетворення, оскільки знайти зворотну матрицю ортогонального перетворення чисельними методами не є складним завданням, а також для всіх перетворень функції прямого й зворотного перетворення є ідентичними.

б) Синусне перетворення. Синусне перетворення формується на основі тригонометричної функції синуса, ядро прямого дискретного перетворення якого обчислюється як

$$A(j,k) = \sqrt{\frac{2}{N+1}} \sin\left[\frac{(j+1)(k+1)\pi}{N+1}\right], \quad k, j = 0,\ldots,N-1 \quad .$$

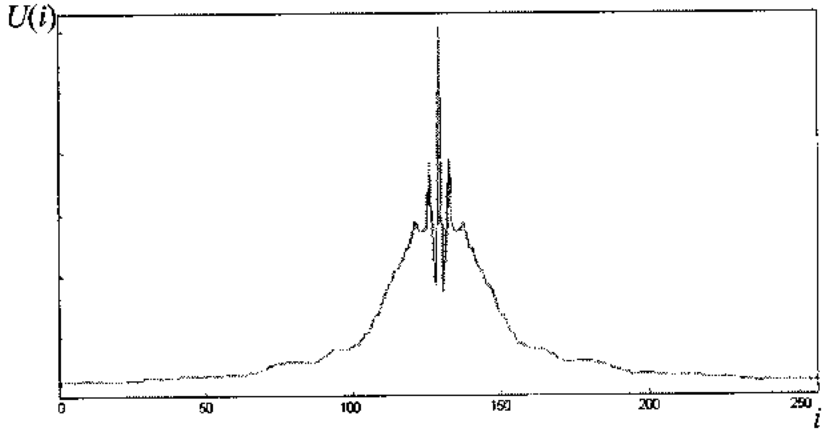


Рис. 2.8. СРКР перетворення Фур'є.

Функції синусного перетворення та СРКР мають вигляд представлений на рис. 2.9 та рис. 2.10:

в) Парне симетричне косинусне перетворення. Якщо сегмент сигналу, який піддається перетворенню в БОФ, можна записати як

$$X_s(j)=\begin{cases}x(j) & j\geq 0\\ x(-1-j) & j<0\end{cases},$$

тоді сегмент симетричний щодо точки -½, провівши аналітичне перетворення цього вектора та врахувавши симетричність, одержуємо ядро парного симетричного косинусного перетворення

$$A(j,k)=\frac{2}{N}c(k)\cos\left(\frac{\pi}{N}k(j+\frac{1}{2})\right),\ k,j=0,...,N-1\ ,$$

де

$$c(k)=\begin{cases}\frac{1}{\sqrt{2}} & k=0\\ 1 & k=1,...,N-1\end{cases}.$$

Функції парного симетричного косинусного перетворення графічно представлені на рис. 2.11, а СРКР – на рис. 2.12.

г) Непарне симетричне косинусне перетворення. Подібно до попереднього випадку представимо сегмент перетворюваного сигналу як:

$$X_s(j)=\begin{cases}x(j) & j\geq 0\\ x(-j) & j<0\end{cases}.$$

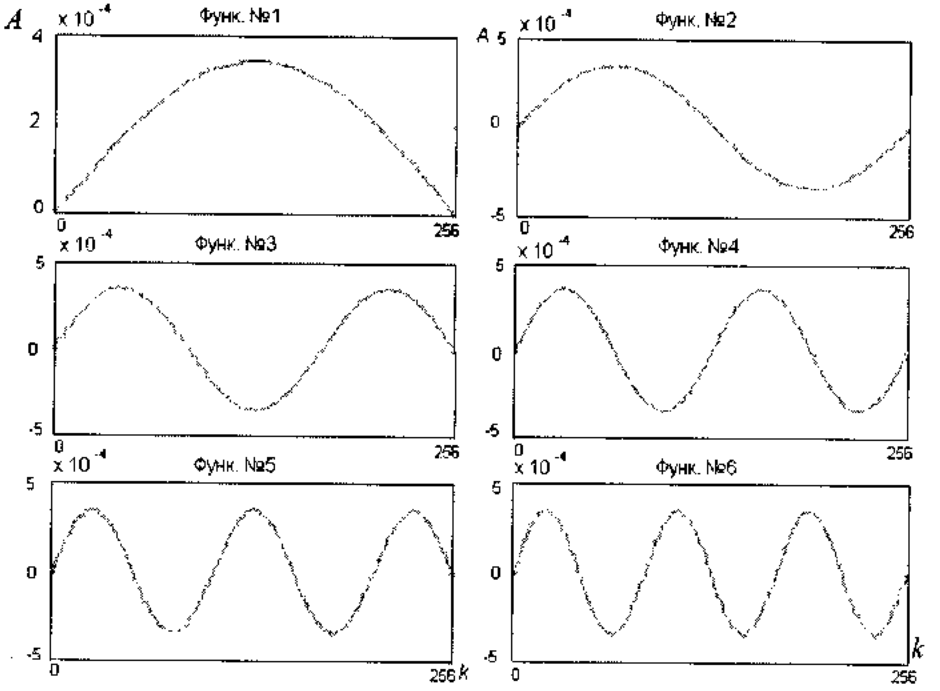


Рис. 2.9. Шість перших функцій синусного перетворення.

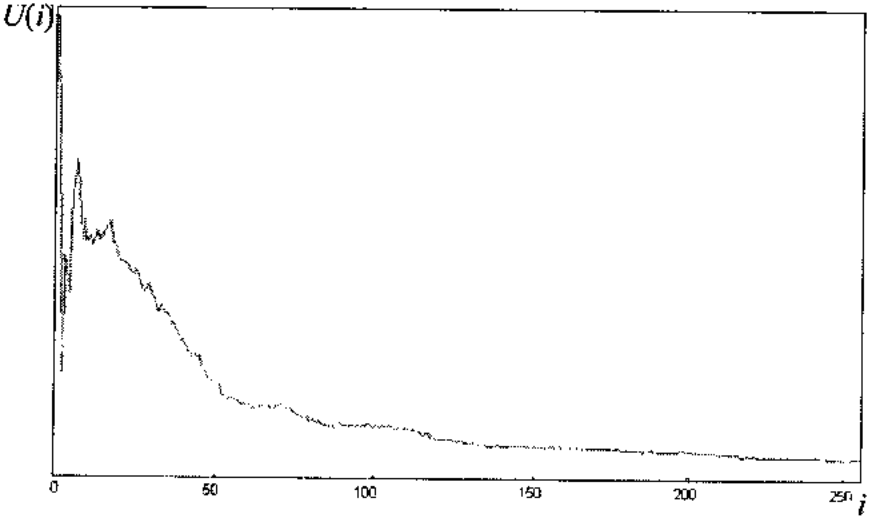


Рис. 2.10. СРКР синусного перетворення.

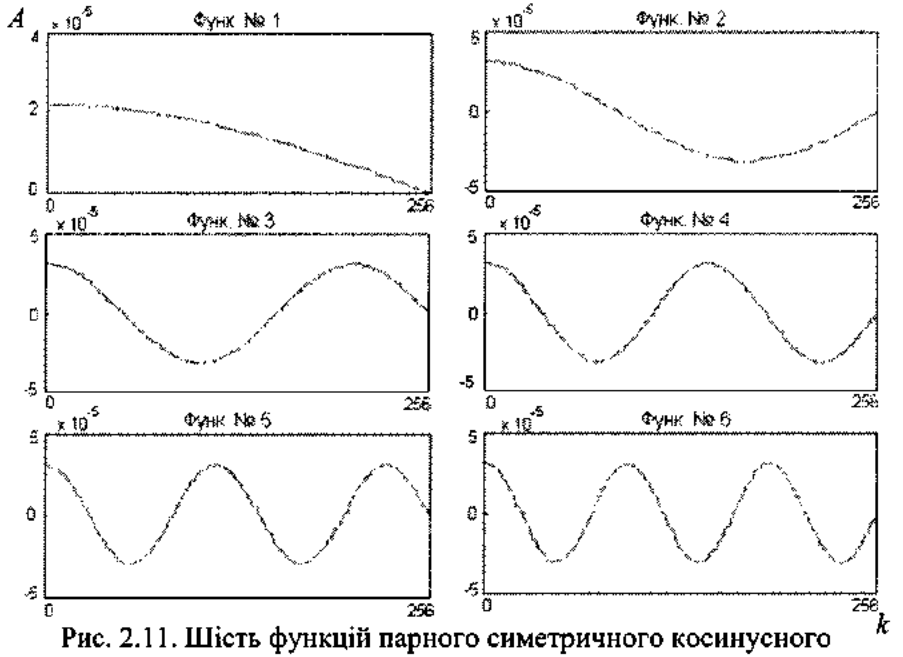


Рис. 2.11. Шість функцій парного симетричного косинусного перетворення.

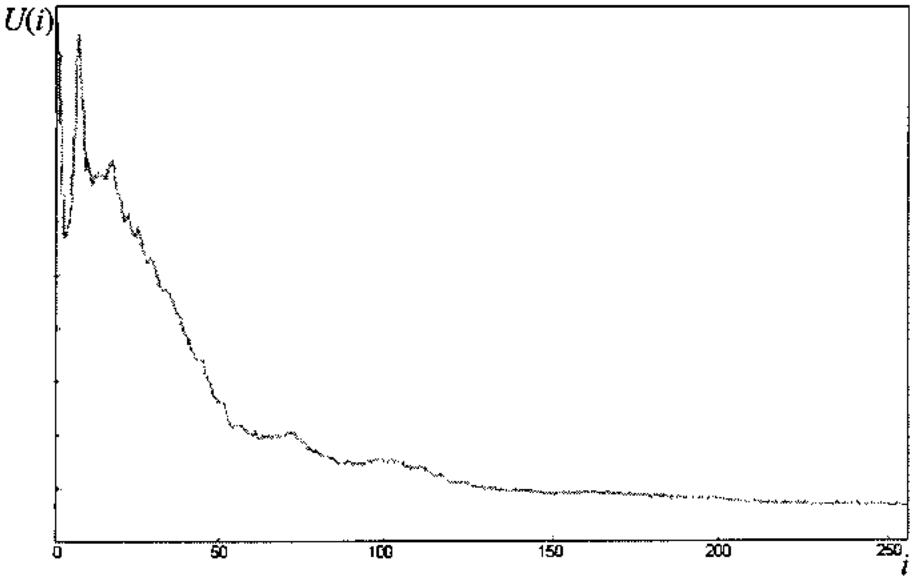


Рис. 2.12. СРКР парного симетричного косинусного перетворення.

Тепер вектор X_s симетричний щодо нуля, провівши знову аналітичне перетворення Фур'є та врахувавши симетричність, одержимо ядро непарного симетричного косинусного перетворення

$$A(j,k)=\begin{cases}\dfrac{1}{N} & j=0\\ \dfrac{2}{N}\cos\left(\dfrac{2\pi}{2N-1}jk\right) & j\neq 0\end{cases}, \text{ де } \quad k,j=0,...,N-1 \ .$$

Графічне представлення шести перших функцій непарного симетричного косинусного перетворення наведене на рис. 2.13, а СРКР – на рис. 2.14.

д) Перетворення Адамара. Як і попереднє перетворення, ядро прямого перетворення Адамара (Уолша) також задається матричним представленням за допомогою таких рекурентних формул:

$$A_2=\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix},$$

$$A_{2N}=\frac{1}{\sqrt{2}}\begin{bmatrix}\|A_N\| & \|A_N\|\\ \|A_N\| & \|-A_N\|\end{bmatrix} \ .$$

На рис. 2.15 зображено шість перших рядків ядра прямого перетворення Адамара для матриці $A(32\times 32)$, а на рис. 2.16 – СРКР для вікна перетворення 256 вибірок.

Як видно з рисунків, перетворення Адамара має досить широке розосередження максимальних рівнів СРКР. Тому при компресії з обнуленням мінімальних коефіцієнтів будуть виникати значні спотворення сигналу, що є неприпустимим у розпізнаванні мовних сигналів. Отже, синусне й косинусне перетворення мають більші потенційні можливості.

2.4.2. Ортогональні перетворення на основі теореми Карунена - Лоєва

а) Рівняння Карунена-Лоєва. Питання вибору БОФ є дуже важливим при компресії сигналу, оскільки оптимальний базис дає можливість зменшити помилку компресії сигналу й збільшити чіткість мови. Теорема Карунена-Лоєва дозволяє синтезувати оптимальний БОФ для випадкового сигналу з відомою кореляційною функцією. Як уже було сказано, мовний сигнал можна вважати стаціонарним випадковим процесом на деякому проміжку часу. Інтегральне рівняння Карунена-Лоєва має вигляд [92,203]

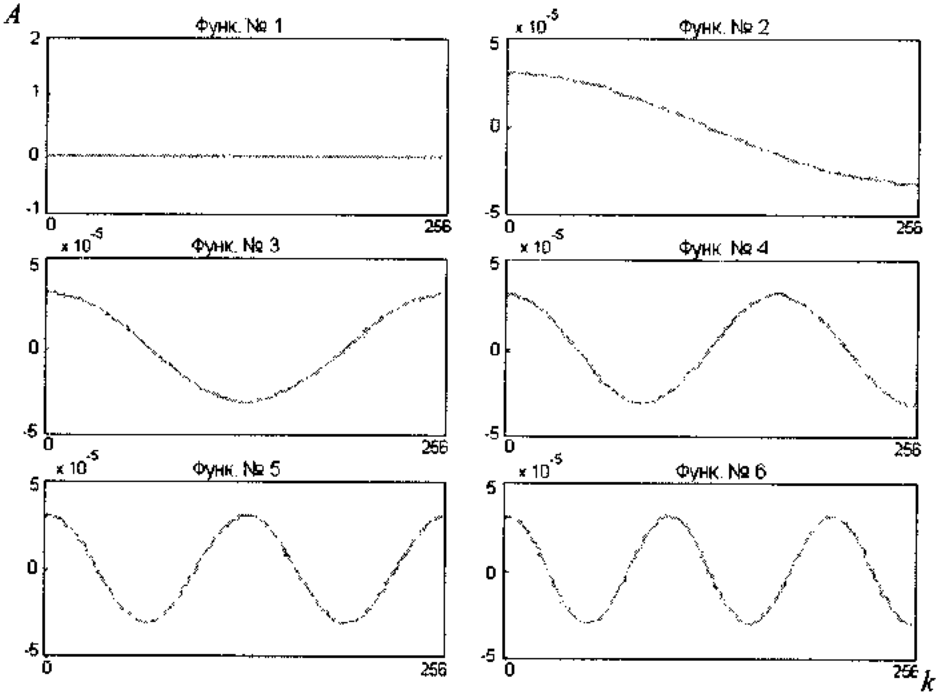


Рис. 2.13. Шість перших функцій непарного симетричного косинусного перетворення.

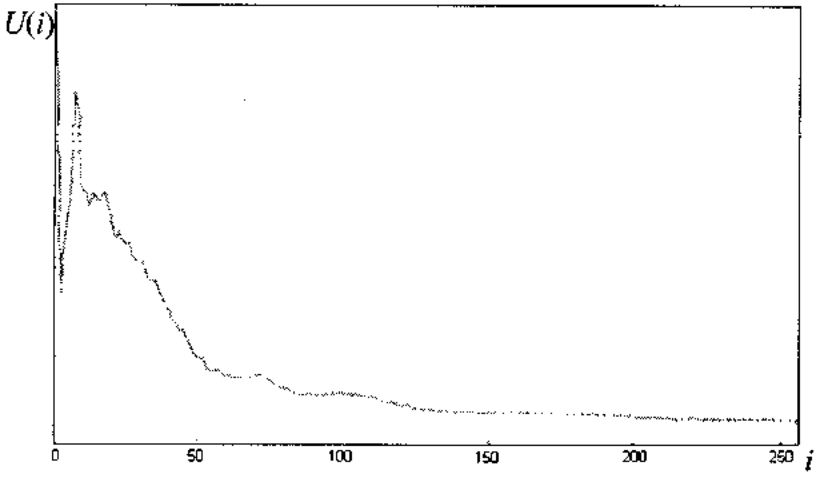


Рис. 2.14. СРКР непарного симетричного косинусного перетворення.

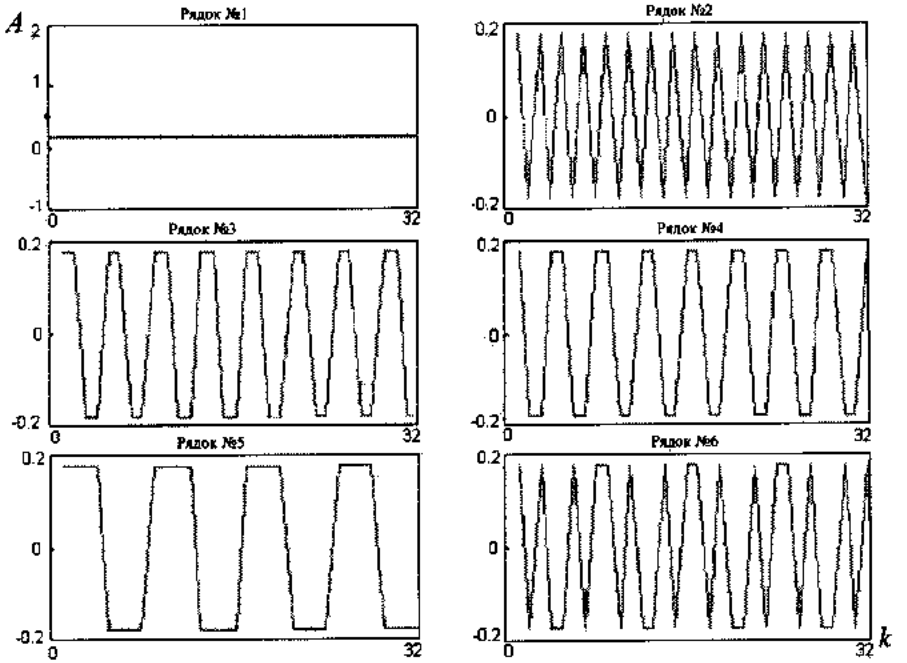


Рис. 2.15. Шість перших рядків ядра прямого перетворення Адамара.

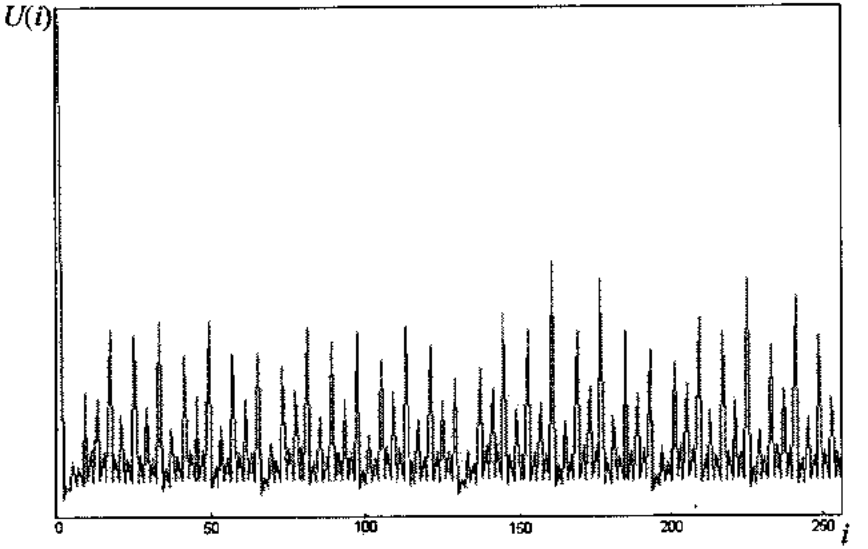


Рис. 2.16. СРКР перетворення Адамара.

$$\int_{-T}^{T} K_{xx}(t,s)\varphi_i(s)ds = \lambda_i \varphi_i(t),$$

де K_{xx} – двомірна автокореляційна функція випадкового процесу; $\varphi_i(s)$ – оптимальний БОФ для даного сигналу; λ_i – власні значення оператора на основі автокореляційної функції.

Розклад сигналу з використанням функції $\varphi_i(s)$ називається розкладом Карунена-Лоєва.

Нехай маємо вектор Y, який представляє вхідний сигнал. Створимо вектор $\widetilde{Y}$, використавши ортогональне перетворення з матрицею $P^T(N \times N)$, тобто $\widetilde{Y} = P^T Y$ або в координатній формі [60]

$$\widetilde{Y} = \sum_{i=1}^{N} P_{i,j} Y_i, \qquad i,j = 1,...,N. \tag{2.3}$$

Кореляційна матриця $\widetilde{K}$ вектора $\widetilde{Y}$ при цьому

$$\widetilde{K} = E\widetilde{Y}\widetilde{Y}^T = EPYY^T = PKP^T = \sum_{i=1}^{N}\sum_{j=1}^{N} K_{i,j} p_i p_j ,$$

де $P_i(i = 1...N)$ – вектори - стовпці матриці P.

При декорелюючому перетворенні (2.3) матриця $\underline{K}$ діагональна, тобто

$$\widetilde{K} = \Lambda = \left\| \widetilde{\sigma}_k^2 \delta_k^2 \right\|, \qquad k,j = 1...N,$$

де $\widetilde{\sigma}_k^2$ – дисперсія елементів вектора Y, і тому

$$\sum_{i=1}^{N}\sum_{j=1}^{N} K_{i,j} p_i p_j = \Lambda \ . \tag{2.4}$$

Помноживши праву й ліву частини (2.4) на вектори p_k й з огляду на їхню ортогональність, одержимо систему векторних рівнянь:

$$\sum_{i=1}^{N} K_{i,k} p_i = \Lambda p_k, \qquad k = 1,..., N. \tag{2.5}$$

У матричному вигляді вираз (2.5) перепишемо як

$$KP = PD, \tag{2.6}$$

де D – матриця, на діагоналі якої перебувають власні значення λ_i.

б) Перетворення Карунена-Лоєва для марковського процесу. Мовний сигнал можна розглядати як гаусівський марковський процес із певним коефіцієнтом кореляції між сусідніми відліками r [60]. Для даного процесу кореляційна матриця записується

$$K = \sigma^2 \left[r_{i,j} \right],$$

$$r_{i,j} = r^{|i-j|}, \qquad i, j = 1,\ldots,N,$$

де r – коефіцієнт кореляції між сусідніми відліками.

У такому випадку рівняння Карунена-Лоєва можна вирішити в явному вигляді та представити власні значення λ_i й власні вектори матриці K

$$\lambda_i = \frac{(1-r^2)}{(1-2r\cos(v_i)+r^2)}, \qquad i = 1,\ldots,N,$$

$$P_{i,j} = \left[\frac{2}{N+\lambda_i^2} \right]^{\frac{1}{2}} \sin\left[v_j \left(i - \frac{N+1}{2} \right) + \frac{i\pi}{2} \right], \qquad i, j = 1\ldots N,$$

де v_i – корінь трансцендентного рівняння

$$\operatorname{tg}(Nv) = \frac{(1-r^2)\sin(v)}{(1+r^2)\cos(v) - 2r}.$$

Далі представлено шість функцій прямого перетворення (рис. 2.17) та СРКР (рис. 2.18).

З рисунків видно, що зміна коефіцієнта кореляції між сусідніми відліками r незначно змінює форму ортогональних функцій перетворення і практично не впливає на групування максимальних елементів розкладу.

в) Перетворення Карунена-Лоєва для мовного сигналу. Для мовного сигналу існує апроксимаційна формула усередненої автокореляційної функції, на основі якої можливий синтез БОФ, повинний оптимально підходити для розкладу випадкового сигналу з характеристиками, що відповідають мовному.

Кореляційна матриця розраховується як

$$K_{i,j} = e^{-\alpha \left| \frac{i-j}{f_d} \right|} \cos\left(2\pi f_0 \left| \frac{i-j}{f_d} \right| \right), \qquad i, j = 0\ldots N-1,$$

де $\alpha = 10^3$ 1/Гц; $f_0 = 400$ Гц; $f_д = 8000$ Гц.

Враховуючи, що при розв'язку рівняння більш високочастотні власні вектори (ортогональні вектори, рядки матриці ядра) знаходяться в перших рядках ядра перетворення, на рис. 2.19 представлено шість останніх рядків, і відповідно до синтезованого перетворення на рис. 2.20 – СРКР.

Порівнявши попередні СРКР і представлений на рис. 2.20, можна констатувати високу зосередженість максимальних рівнів, що

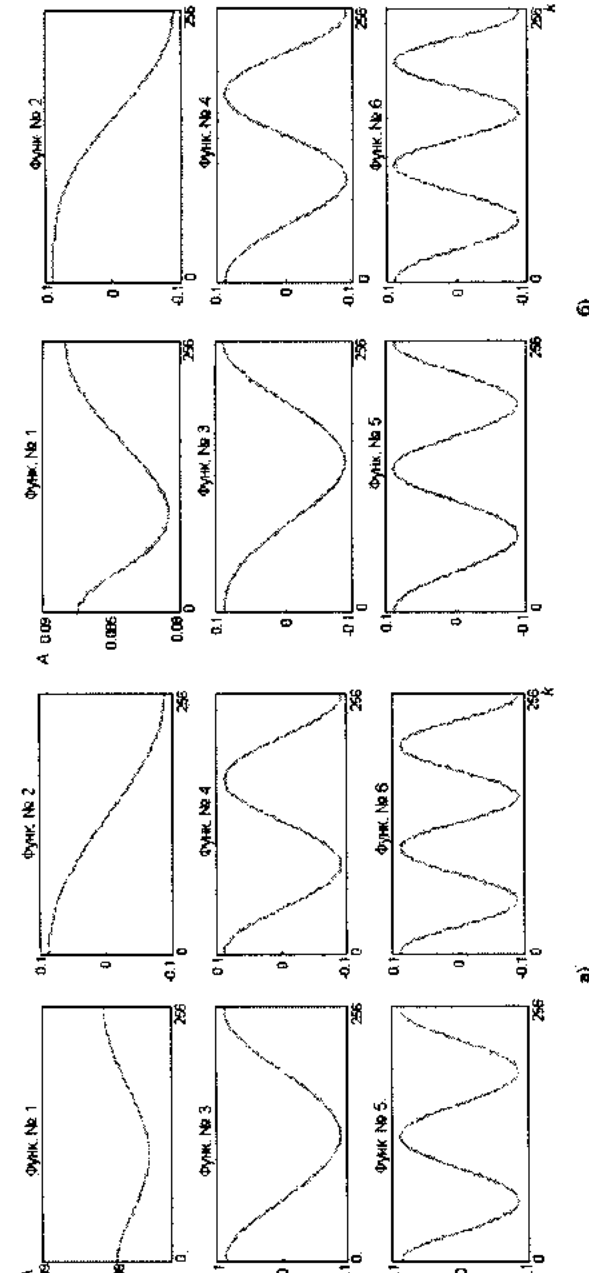


Рис. 2.17. Шість перших функцій розкладу Карунена-Лоєва для марковського процесу при $r = 0{,}1$ (а) і $r = 0{,}4$ (б).

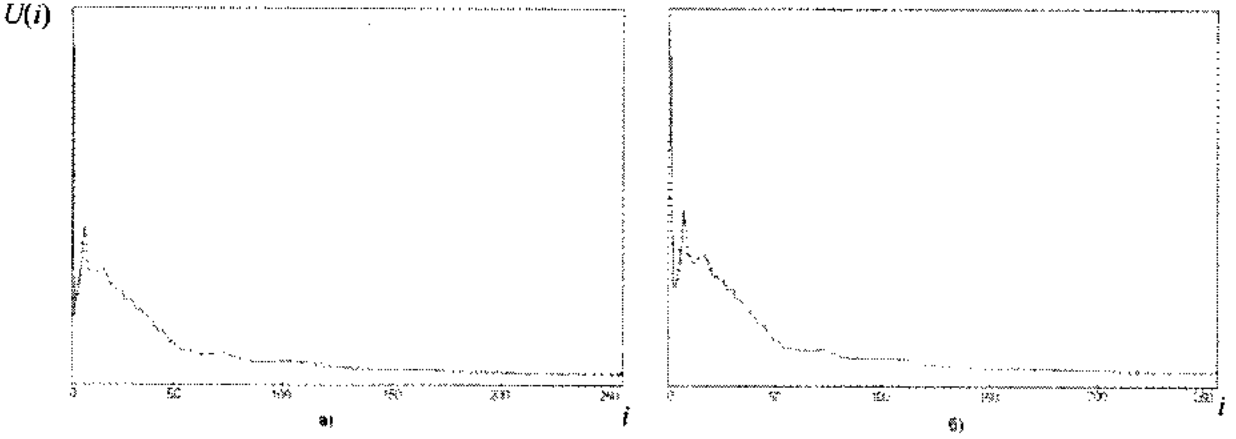


Рис. 2.18. СРКР перетворення Карунена-Лоєва для марковского процесу при $r = 0,1$ (а) і $r = 0,4$(б).

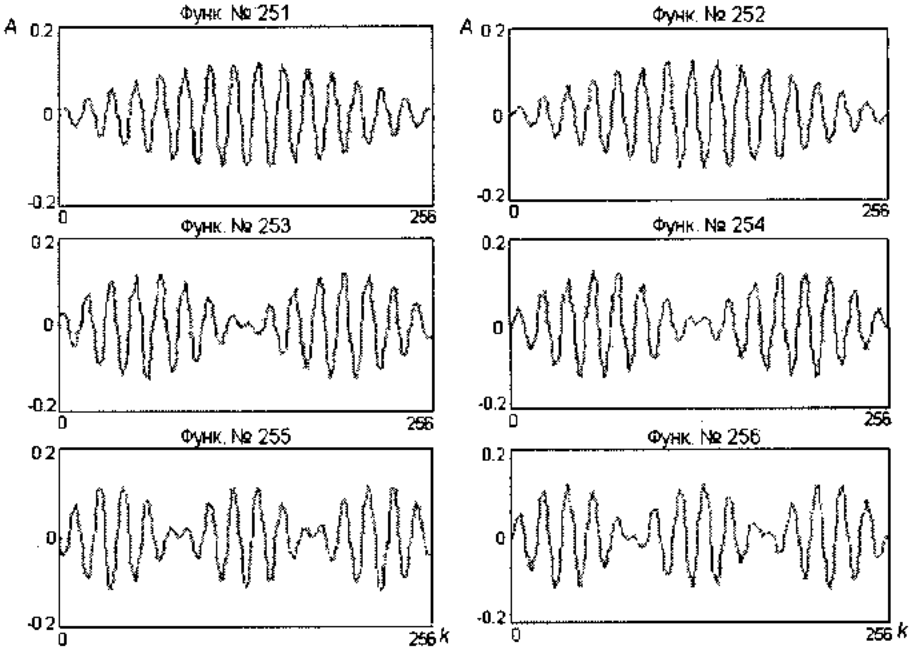


Рис. 2.19. Шість останніх рядків ядра прямого перетворення Карунена-Лоєва для мовного сигналу.

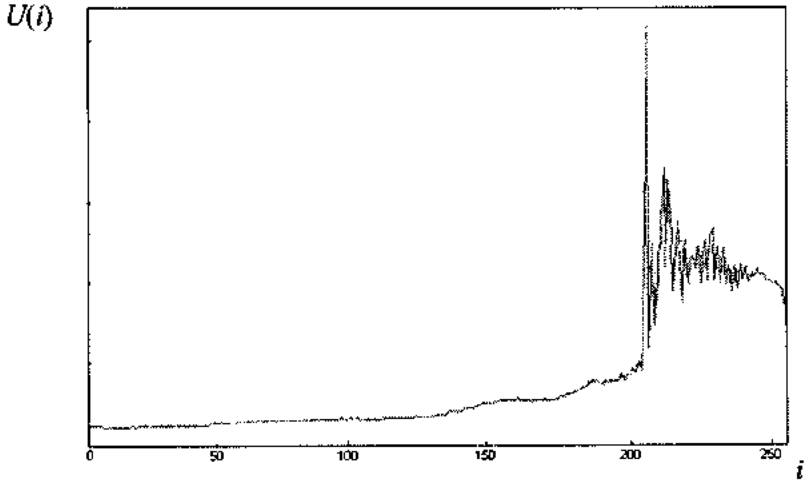


Рис. 2.20. СРКР перетворення Карунена-Лоєва для мовного сигналу.

істотно відіб'ється на якості компресованого сигналу. Крім того, синтезоване перетворення відрізняється від попереднього специфічністю ортогональних векторів, які утворяться не з одного фрагмента гармонійного коливання, а з декількох з'єднаних між собою фрагментів.

2.4.3. Компресія з виключенням сукупності мінімальних коефіцієнтів розкладу

Даний метод компресії передбачає ортогональне перетворення сегмента сигналу з наступним виключенням сукупності найменших за модулем коефіцієнтів розкладу незалежно від порядку їхнього розташування. Додатково зберігається інформація про розташування коефіцієнтів. Загальна кількість біт додаткової інформації дорівнює розміру вікна перетворення, а коефіцієнт компресії [60]

$$K = \frac{BN}{BU + N},$$

де B – кількість біт, виділених на кожний коефіцієнт; N – кількість вибірок у сегменті обробки; U – кількість переданих коефіцієнтів розкладання.

У результаті в системі обробки мовних сигналів утворяться два інформаційних потоки: перший відповідає потоку інформації про коефіцієнти розкладу, а другий – інформації про розміщення цих коефіцієнтів ($K(n)$ та $q(n)$ на рис. 2.21). Несуттєве місце розташування

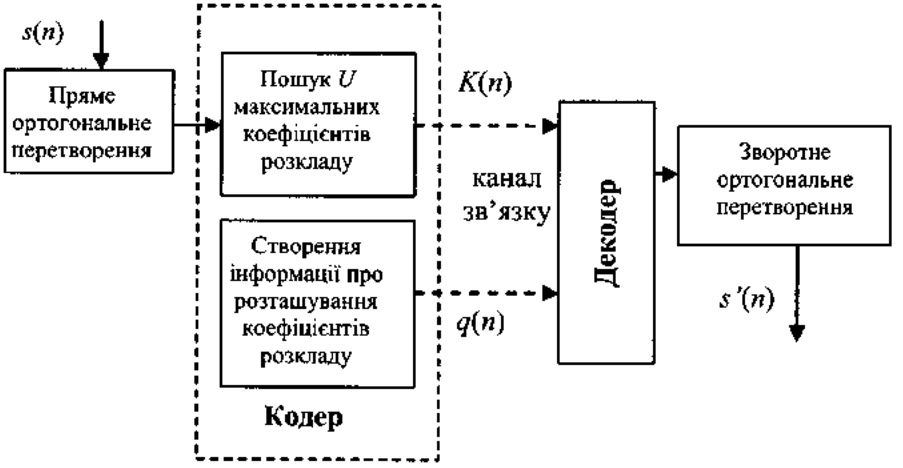


Рис. 2.21. Структурна схема компресії-декомпресії методом виключення сукупності мінімальних коефіцієнтів.

максимальних коефіцієнтів розкладу, важливе лише їхнє значення порівняно з іншими в утвореній множині коефіцієнтів одного сегмента.

Перевагою запропонованого методу компресії є його повна нечутливість до місця розташування максимальних коефіцієнтів, тобто існує можливість використовувати перетворення, у яких максимальні значення коефіцієнтів можуть бути розкидані по всій множині косфіцієнтів розкладу.

Шляхом математичного моделювання системи компресії й декомпресії мовного сигналу отримано відношення залежноті сигнал/спотворення (с/сп) від коефіцієнта компресії для сегментів перетворення 64, 128, 256 вибірок (рис. 2.22). Зрівнявши результати (рис.2.22 а-в), можна зробити висновок, що при двократному збільшенні розміру сегмента перетворення, наприклад з 64 до 128 вибірок, вдається тільки незначно поліпшити якість компресії (щонайбільше на 4 дБ), а в деяких випадках навіть і погіршити.

Графіки для усіх досліджених перетворень подібні: спостерігається зменшення крутизни спаду с/сп зі збільшенням коефіцієнта компресії. Тому навіть невелике покращання базису ортогональних функцій зумовить підняття всієї залежності, а отже, відчутно збільшиться можливий коефіцієнт компресії.

Порівняємо допустимий коефіцієнт компресії для ортогональних перетворень, зафіксувавши відношення с/сп на рівні 30 дБ [13]. Якщо під час обчислень неможливо досягнути 30 дБ, то усунемо коефіцієнти розкладу та визначимо коефіцієнт компресії за допомогою лінійної інтерполяції між двома сусідніми значеннями [45]. Результати обчислень представлено на рис.2.23.

При суб'єктивному порівнянні якості передачі (на слух) спотворення з використанням перетворень Адамара і нахиленого мають вигляд широкосмугового шуму, що пояснюється їх специфічною структурою (Адамара – дворівневі цифрові функції, нахилене – функції трикутноподібної форми). Після більш гармонічних перетворень – синусного, косинусних і Карунена-Лоєва – сигнал стає неприродно "металічним" і через сильне збільшення коефіцієнта компресії неприродність посилюється та повністю втрачається чіткість сприйняття деяких фрагментів звуків фрази. Зі збільшенням розміру вікна перетворення спотворення стають тривалішими і захоплюють

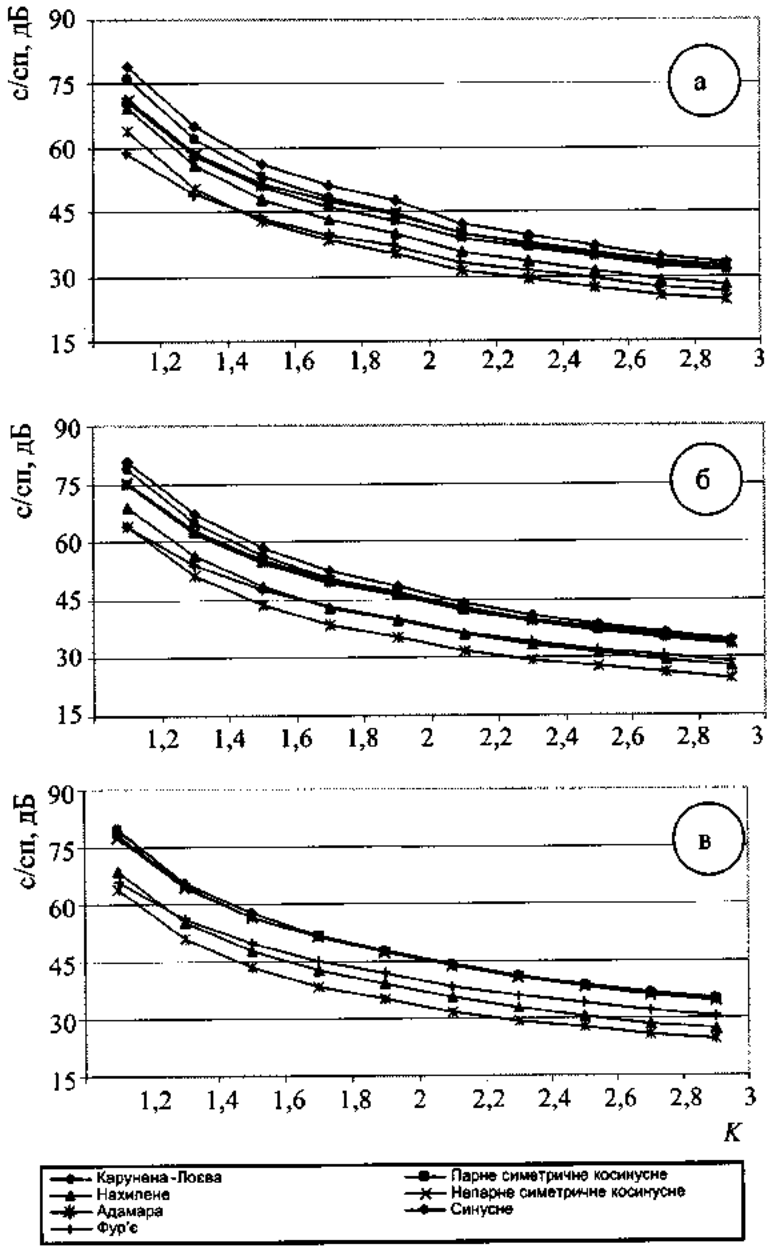


Рис. 2.22. Залежність відношення с/сп від коефіцієнта компресії для сегмента перетворення розміром 64 (а); 128 (б) і 256 (в).

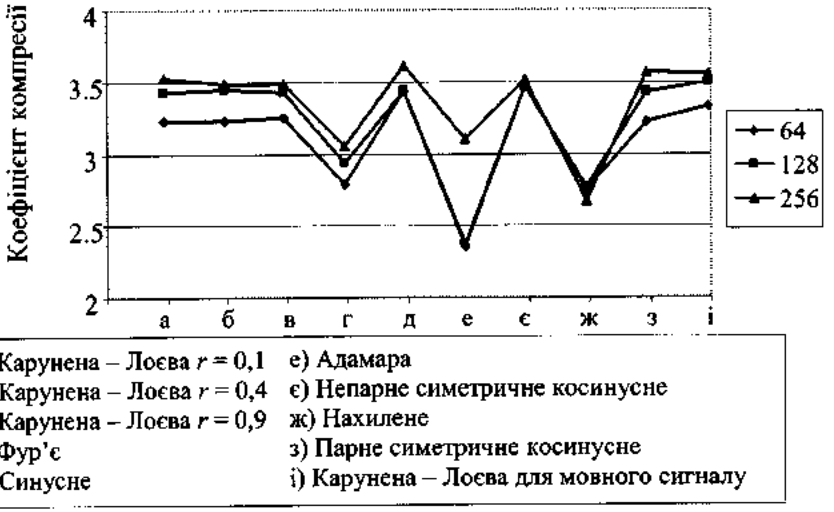


Рис. 2.23. Допустимі коефіцієнти компресії для досліджених ортогональних перетворень при розмірі 64, 128, 256 вибірок.

декілька звуків, але їх рівень не зменшується і чіткість мови загалом не покращується.

Порівнявши одержані значення за різних ортогональних перетворень, можна сказати, що невелика перевага синтезованого базису над відомими простежується тільки тоді, коли сегмент перетворення становить 128 вибірок. У разі інших розмірів вікна перетворення (64 і 256) синтезований базис дає гірші результати.

Якщо суб'єктивно визначити межу якісного сигналу для синтезованого перетворення Карунена - Лоєва, то вона досягається за коефіцієнта компресії $K = 2,8$ (розраховане відношення с/сп = 36 дБ).

Використання синтезованого перетворення забезпечує більшу чіткість компресованого сигналу, що зумовлене врахуванням апріорної статистичної інформації про мовний сигнал, зокрема, синтез базису ортогональних функцій за середньостатистичною автокореляційною функцією мовного сигналу.

2.4.4. Критерії оцінки якості компресії

а) Об'єктивні критерії. В останні роки, коли стало можливим проведення досліджень із застосуванням ЕОМ, перше місце серед оцінок якості компресії посіли об'єктивні оцінки, які грунтуються на

статистичних математичних параметрах сигналів, для яких не потрібно значних матеріальних і часових затрат.

Нехай $x(n)$ і $y(n)$ – є мовні сигнали в дискретному часі перед компресією та після декомпресії.

Для оцінки якості передачі довільного сигналу використовується відношення сигнал/шум, у випадку компресії не завжди утворюється шумова похибка, тому приймемо за критерій порівняння відношення с/сп, що в загальному рівнозначне відношенню середньоквадратичного відхилення (СКВ) сигналу до СКВ похибки, виражене в децибелах:

$$\rho_1 = 10\lg\left[\frac{\sum x(n)^2}{\sum (x(n)-y(n))^2}\right] . \qquad (2.7)$$

Вважається, що при відношенні с/сп рівному 30 дБ, шум практично не відчутний на слух [7,26]. Ґрунтуючись на цьому подальшу межу якості, значення с/сп, приймемо саме такою.

Обробка мовного сигналу часто здійснюється сегментовано. У такому випадку відношення с/сп має вигляд [3,70]

$$\rho_2 = \frac{1}{N}\sum_{k=0}^{N-1}\left[10\lg\left\{\frac{\sum_{n=1}^{N}(x(n+kN))^2}{\sum_{n=1}^{N}(x(n+kN)-y(n+kN))^2}\right\}\right], \qquad (2.8)$$

де N – число вибірок сигналу в сегменті обробки.

Для зменшення чутливості цього показника якості до зміни рівня сигналу існує ще одна формула розрахунку:

$$\rho_3 = \frac{1}{M}\sum_{k=0}^{M-1}\left[10\lg\left\{\frac{\Re_k^2}{1-\Re_k^2}\right\}\right], \qquad (2.9)$$

де M – кількість сегментів обробки; $\Re_k = \Re_{xx}^{(k)}(0)$ – оцінка взаємного співвідношення кореляції $\Re_{xx}^{(k)}(0)$ в k-му сегменті, який розраховується за формулою

$$\Re_{xx}^{(k)}(\tau) = \frac{N\sum_{n=1}^{N-\tau}[x(n+kN).y(n+\tau+kN)] - \sum_{n=1}^{N}x(n+kN).\sum_{n=1}^{N}y(n+kN)}{\sqrt{\left[N\sum_{n=1}^{N}x(n+kN)^2 - \left(\sum_{n=1}^{N}x(n+kN)\right)^2\right]\left[N\sum_{n=1}^{N}x(n+kN)^2 - \left(\sum_{n=1}^{N}y(n+kN)\right)^2\right]}}.$$

У системах обробки мовного сигналу, які застосовують компресію, для зменшення надлишковості інформації використовується

комплексний показник якості, який враховує як відношення с/сп, так і коефіцієнт компресії. Коефіцієнтом компресії вважатимемо відношення вихідної до вхідної швидкості передачі інформації кодера $K = \frac{V_{x(n)}}{V_{z(n)}}$, де $V_{x(n)}$ й $V_{z(n)}$ – швидкості передачі інформації на вході та виході кодера відповідно.

Ґрунтуючись на формулах для ρ_1, ρ_2, ρ_3, сформуємо три різні комплексні показники якості $\xi = K\vartheta$, де ϑ – це відношення с/сп:

$$\xi_1 = K\frac{\sum x(n)^2}{\sum (x(n)-y(n))^2},$$

$$\xi_2 = \frac{K}{N}\sum_{k=0}^{N-1}\left[\frac{\sum_{n=1}^{N}(x(n+kN))^2}{\sum_{n=1}^{N}(x(n+kN)-y(n+kN))^2}\right],$$

$$\xi_3 = \frac{K}{M}\sum_{k=0}^{M}\left[\frac{\Re_k^2}{1-\Re_k^2}\right].$$

Використовуючи комплексний показник якості можна лише об'єктивно оцінити методи компресії. Для повної оцінки якості потрібно визначити також деякі суб'єктивні категорії, які дадуть можливість врахувати властивості слухового апарату людини.

б) Суб'єктивні критерії. У цифрових системах обробки мовних сигналів чіткість сигналу переважно висока і у поняття "якості звучання" вкладають такі суб'єктивні характеристики, як натуральність, можливість розпізнавання диктора за голосом і т.д. Існують експериментальні способи визначення кількісних мір якості звучання, які оцінюються за градаціями: "відмінно", "добре", "задовільно", "не задовільно". Кожній градації при формуванні кількісних оцінок приписується певна кількість балів.

Були здійснені суб'єктивно - статистичні експерименти, на підставі яких стало можливим зв'язати суб'єктивні оцінки з розрахованими об'єктивними за допомогою рівняння [59]

$$\chi = \alpha\rho + \beta\ , \qquad (2.10)$$

де χ –суб'єктивна оцінка якості, зроблена слухачами та виражена в балах; α, β –коефіцієнти регресії, які знаходяться методом найменших квадратів за статистичними даними.

Якість компресії оцінювалась градаціями "недопустимо" – "відмінно". Кожній вказаній градації якості разом із проміжними типу "відмінно – добре" були приписані бали від 1 ("недопустимо") до 9 ("відмінно"). Обробкою звучання 288 речень, вимовлених різними дикторами у різних умовах передачі, було отримано оціночні значення $\alpha' = 0{,}156$ і $\beta' = 2{,}702$ для оцінки якості за формулою (2.7). Коефіцієнт кореляції між суб'єктивною оцінкою χ та розрахованою χ' за допомогою рівняння (2.10) складає 0,667 при середньоквадратичному відхиленні 1,202. Відтак дійсно існує зв'язок між χ та χ', однак не настільки тісний, як цього можна очікувати.

При використанні виразу (2.8) коефіцієнти регресії склали $\alpha' = 0{,}247$ і $\beta' = 1{,}369$ [59], коефіцієнт кореляції – 0,873 при середньоквадратичному відхиленні 0,787. У випадку показника якості (2.9) – $\alpha' = 0{,}336$ і $\beta' = 0{,}486$, коефіцієнт кореляції – 0,911, відхилення – 0,665. Таким чином, зв'язок цього показника з суб'єктивною оцінкою уже стає більш точним.

При наявності стороннього впливу (корисного сигналу) відбувається зміна порогу чутливості слуху людини (до спотворень), такий факт називається ефектом маскування завад корисним сигналом. Грунтуючись на цьому, можна говорити про недопустимість оцінки якості компресії на підставі винятково об'єктивних критеріїв. Для повної оцінки якості системи необхідно проводити наукові суб'єктивно-статистичні дослідження із залученням фахівців сфери акустики.

У таблицю 2.2. зведено результати порівняння методів компресії мовних сигналів з використанням ортогональних перетворень.

Застосовуючи перетворення Адамара й нахилене, можна домогтися високого ступеня компресії, але при цьому значно погіршити якість компресованого сигналу. Спотворення при цих методах мають вигляд широкосмугових шумів, що пояснюється специфічною побудовою їхніх ортогональних функцій.

А в наступній таблиці 2.3. представлено порівняння методів компресії при повному і неповному виключенні коефіцієнтів розкладу.

Таблиця 2.2. Порівняння методів компресії при використанні різних базисів ортогональних перетворень

Перетворення	Переваги	Недоліки	K
Фур'є	• можливість знайти миттєвий спектр; • легке визначення частотних параметрів сигналу	• комплексність коефіцієнтів розкладання; • чутливість до усунень коефіцієнтів розкладання (УКР)	3,06
Синусне	• універсальність; • існування алгоритму швидкого перетворення	• одногармонічність[1] ортогональних функцій; • чутливість до УКР	7,83
Парне симетричне косинусне	• універсальність; • існування алгоритму швидкого перетворення	• одногармонічність ортогональних функцій; • чутливість до УКР	7,43
Непарне симетричне косинусне	• універсальність; • існування алгоритму швидкого перетворення	• одногармонічність ортогональних функцій; • чутливість до УКР	7,24
Нахилене	• існування алгоритму швидкого перетворення	• значні шумові спотворення при УКР	7,15
Адамара	• існування алгоритму швидкого перетворення	• значні шумові спотворення при УКР; • дворівневі цифрові ортогональні функції.	6,54
Карунена-Лоєва для марковського процесу $r = 0,1; 0,4; 0,9$	• універсальність; • можливість зміни ортогональних функцій зміною коефіцієнта кореляції між сусідніми відліками.	• одногармонічність ортогональних функцій; • відсутність алгоритму швидкого перетворення	7,15 7,3 7,27
Карунена-Лоєва, синтезований для мовного сигналу	• врахування апріорної інформації про мовний сигнал; • багатогармонічність[2] ортогональних функцій	• відсутність алгоритму швидкого перетворення	8,5

[1] ортогональні функції утворюються одним гармонійним коливанням з різною фазою й періодом.

[2] ортогональні функції утворюються декількома гармонійними функціями.

Таблиця 2.3. Порівняння методів компресії

Метод	Переваги	Недоліки	Три кращих базиси
Повне виключення малозначимих коефіцієнтів розкладу	• незалежність від заздалегідь заданого розміщення максимальних коефіцієнтів розкладу	• необхідність передачі додаткової інформації про розміщення максимальних коефіцієнтів розкладу; • більша складність через необхідність пошуку мінімальних коефіцієнтів розкладу; • малий коефіцієнт компресії (< 3,5); • значні спотворення сигналу	• синусне; • Карунена-Лоєва для мовного сигналу; • непарне симетричне косинусне
Неповне виключення малозначимих коефіцієнтів розкладу	• досягнення значного коефіцієнта компресії (> 8); • розподіл спектра помилки по всьому частотному діапазоні; • висока суб'єктивна оцінка якості; • можливість удосконалення	• залежність від СРКР; • використання однакового розподілу бітів на коефіцієнти вокалізованих і невокалізованих звуків	• Карунена-Лоєва для мовного сигналу; • синусне; • парне симетричне косинусне

РОЗДІЛ 3. ДАКТИЛОСКОПІЧНА АУТЕНТИФІКАЦІЯ

3.1. Спотворення, характеристики й особливості дактилоскопічних зображень

За природою спотворень процес слідотворення дактилоскопічних зображень описується нелінійним оператором P (1.1).

Позначимо зображення $\hat{g}(x,y)$ як ідеально відтворений образ тривимірного об'єкта – папілярного узору. У більшості випадків під ідеальним формуванням зображення відбитка розуміють строго паралельну проекцію узору на плоску поверхню. Далі моделювання спотворень, які виникають під час проектування, зводиться до моделювання спотворень реального зображення відносно ідеального $\hat{g}(x,y)$. Такий підхід викликаний не тільки необхідністю спрощення, але і тим, що спотворення можна оцінити лише за набором реальних зображень, оскільки немає опису об'єкта досліджень. Отримати тривимірний опис папілярних ліній пальця апаратно важко. Додатково зазначимо, що форма пальця деформується при різних його положеннях.

Отже, загальна формула (1.1), із урахуванням вищесказаного, набуде вигляду

$$g(x,y) = P_{\varsigma}\hat{g}(x,y), \qquad (3.1)$$

де $g(x,y)$ – реальне спотворене зображення; P_{ς} – оператор спотворення ідеального зображення $\hat{g}(x,y)$, який відображає усі спотворення, що наявні на зображенні $g(x,y)$.

Розглянемо спотворення [85], які виникають у процесі формування зображення відбитка.

а) Невідповідний контакт папілярного узору і слідонесучої поверхні, ефект "губки". Такий тип спотворень визначається порядком відображення (прокатування) тривимірного папілярного узору на двовимірній слідонесучій поверхні та еластичністю шкіри людини. На цьому етапі виникають геометричні спотворення й змазування узору. Каменем спотикання при вирішенні оберненої задачі усунення таких спотворень є неконтрольованість процесу формування образу папілярного узору. Це призводить до формування різних образів одного і того ж папілярного узору під час повторного відбиття (рис.3.1).

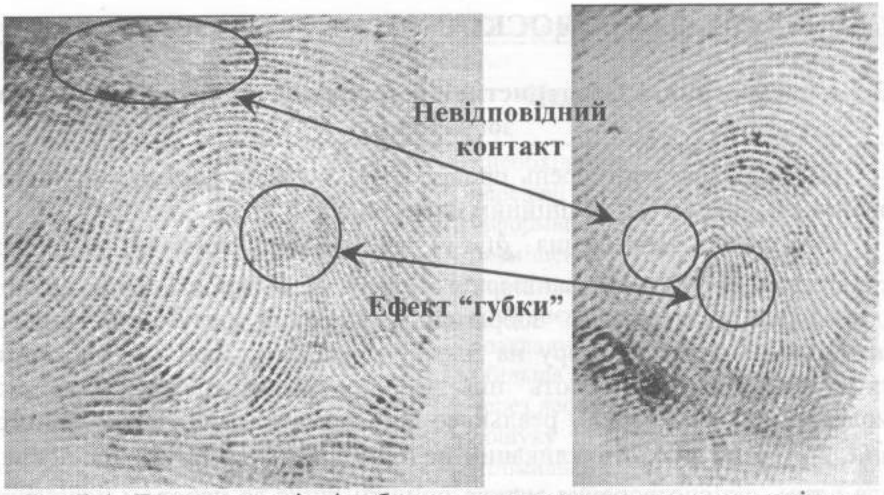


Рис.3.1. Дактилоскопічні зображення одного пальця, отримані при різних умовах слідотворення.

На зображенні рис.3.1 виділено області, в яких проявляється ефект "губки". Таким чином, вираз (3.1) для геометрично спотвореного зображення матиме вигляд

$$g(x,y) = \Re\hat{g}(r_x(x,y), r_y(x,y)), \qquad (3.2)$$

де $r_x(x,y), r_y(x,y)$ – функції геометричних спотворень (найчастіше нелінійні). У найпростішому випадку $r_x(x,y)=m_x \cdot x$, $r_y(x,y) = m_y \cdot y$, що відповідає масштабуванню по осях OX і OY у декартовій системі координат (ДСК); m_x, m_y – масштабні коефіцієнти; $\Re$ – функціонал нелінійних негеометричних спотворень (наприклад, змазування).

б) Нерівномірний контакт. Структура папілярних ліній може бути відображена повністю, якщо вони мають надійний контакт із поверхнею слідотворення й слідотвірна речовина рівномірно розподілена на папілярах. Дійсно, такі фактори, як сухість шкіри, хвороби, піт та бруд призводять до утворення фрагментів відбитка з нерівномірним відображенням. Можливі випадки, коли певні ділянки папілярних ліній не мають достатнього для відбиття контакту з поверхнею, а на інших ділянках отримуємо відбиття міжпапілярних борозен. Цей тип спотворень зумовлює погіршення контрасту регіонів зображення в областях його локалізації, що чітко представлено на рис.3.1. світлими або темними плямами. Шуми в цьому випадку є теж наслідком дії такого спотворення, але в областях зображення, менших

за розміром від періоду папілярних ліній. Візуально такий шум сприймається як зміна яскравості папілярних ліній в околі декількох точок або їх розриви. Часто шумоподібний тип спотворення викликаний не зовнішніми факторами, а структурою папілярних ліній (саме наявністю пор і рельєфності на папілярах). Особливістю спотворення є те, що у більшості випадків зміна контрасту не виключає дії спотворення шумоподібної природи, а також дії одночасно декількох таких спотворень із різними характеристиками. Остаточно зміну контрасту описуємо наступним масштабним перетворенням з обмеженнями [69] і мультиплікативним шумом:

$$g(x,y)=\left[\begin{cases} G_{\max}, & якщо \quad \hat{g}(x,y) > I_{\max} \\ T(\hat{g}(x,y)), & якщо \quad I_{\min} \le \hat{g}(x,y) \le I_{\max} \\ G_{\min}, & якщо \quad \hat{g}(x,y) < I_{\min} \end{cases}\right] \cdot m(x,y), \text{для } (x,y) \in E, \quad (3.3)$$

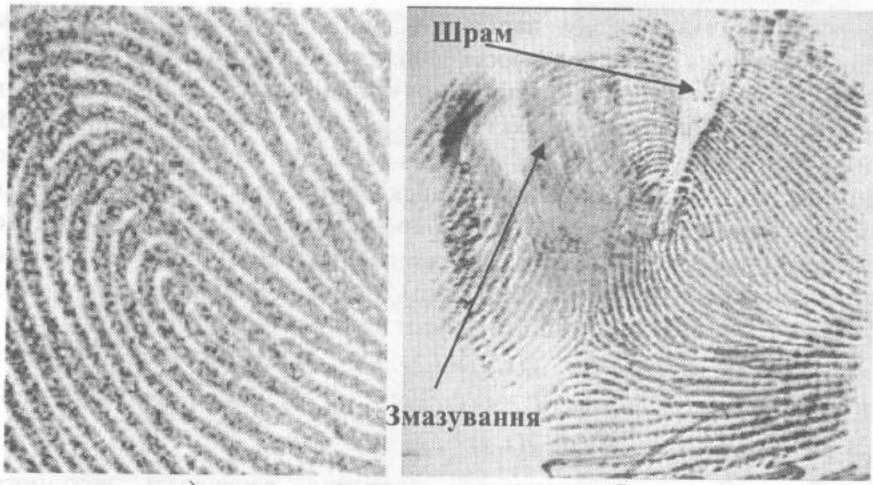
де $G_{\min}$, $G_{\max}$ – екстремальні значення яскравості вихідного зображення; $I_{\min}$, $I_{\max}$ - границі обмеження яскравості; $T(\hat{g}(x,y))$ – функція масштабування яскравості в області локалізації спотворення E; $m(x,y)$ - мультиплікативний шум, що відповідає дії спотворення в околах, менших за розміром від періоду папілярних ліній.

Необхідно зазначити, що функція масштабування яскравості може бути як лінійною, так і нелінійною. Лінійна функція масштабування яскравості записується таким виразом:

$$T(\hat{g}(x,y)) = \frac{G_{\max} - G_{\min}}{I_{\max} - I_{\min}} \cdot \hat{g}(x,y) + \frac{G_{\min} \cdot I_{\max} - G_{\max} \cdot I_{\min}}{I_{\max} - I_{\min}}.$$

Під час практичного дослідження зображень, отриманих за допомогою сканера з сенсорною пластиною, яка працює на основі провідності пальця, виявлено, що люмінесцентна пластина має нерівномірне свічення, а також існують точки, в яких відсутній ефект свічення. Такі спотворення зображення теж моделюються мультиплікативним шумом (рис.3.2 а).

в) Пошкодження папілярних ліній. Ручна праця, поранення шкіри, зморшки вносять неконтрольовані спотворення папілярного узору. Сюди також варто віднести спотворення, викликані недотриманням правил прокатування відбитків, і спотворення слідотворення, які виникають при спонтанному відбитті слідів на поверхні. З іншого боку, неглибокі поранення шкіри призводять до тимчасового спотворення, бо після регенерації узор повністю відновлюється. Таким чином, ці пошкодження можуть спричиняти спотворення картини ознак



а) б)

Рис.3.2. Фрагмент зображення відбитка, отриманого біосенсором фірми Testech з мультиплікативним шумом (а), і відбиток з дефектом відкатування та пошкодженням папілярних ліній (б).

відбитків на період, який менший від часу регенерації. Тобто будуть формуватися неіснуючі й пропадати реальні ознаки (рис.3.2 б).

Математичне моделювання таких спотворень є надто громіздкою задачею, оскільки поранення шкіри призводить до спотворення тривимірного об'єкта. Картина узору після регенерації може бути понівечена шрамом, який описується як новий об'єкт. У разі стирання папілярних ліній, наприклад, внаслідок ручної праці з шорсткими поверхнями, спотворення узору будуть аналогічні до спотворень нерівномірного контакту. Зморшки не означають втрати ділянок папілярних ліній, а лише їх місцевий розрив, і можуть бути описані виразом геометричних перетворень (3.2), в якому функції $r_x(x,y), r_y(x,y)$ матимуть нелінійний характер і втрачають неперервність.

г) Спотворення, викликані способом отримання дактилоскопічних зображень. У даному випадку говоримо про шуми й спотворення, які виникають на етапі формування відбитка (зерниста структура слідотвірної речовини, шорсткість слідонесучої поверхні та інші) й етапі перетворення відбитка у зображення (шуми та спотворення в апаратурі вводу зображення). До шумів на етапі вводу зображення відносимо не тільки шуми апаратури, але й шуми та збої програмного забезпечення та каналу передачі зображень. Якщо порівняти способи

отримання дактилоскопічних зображень, то найкращі результати забезпечують "живі сканери" (live-scanner), основані на ефекті оптичного відбиття від скляної поверхні і на ефекті зміни ємності між матрицею електродів і папілярними лініями. Найбільш поширеним, однак, способом отримання відбитків є відбиття їх за допомогою чорнила на папері й наступним вводом. Тому, розробляючи алгоритм попередньої обробки орієнтуємося, на зображення, сформовані саме таким способом, оскільки вони характеризуються найгіршою якістю.

Наближено спотворення такого типу опишемо шляхом уведення в зображення адитивного шуму:

$$g(x,y) = \hat{g}(x,y) + n(x,y), \tag{3.4}$$

де $n(x,y)$ – адитивний шум.

Загальну математичну модель одержання зображення з урахуванням (3.2)-(3.4) запишемо так:

$$g(x,y) = \left\{ \begin{array}{cc} G_{\max}; & g\left(r_x(x,y), r_y(x,y)\right) > I_{\max} \\ T\left(\Re\hat{g}\left(r_x(x,y), r_y(x,y)\right)\right); & I_{\min} \le g\left(r_x(x,y), r_y(x,y)\right) \le I_{\max} \\ G_{\min}; & g\left(r_x(x,y), r_y(x,y)\right) < I_{\min} \end{array} \right\} \times \tag{3.5}$$

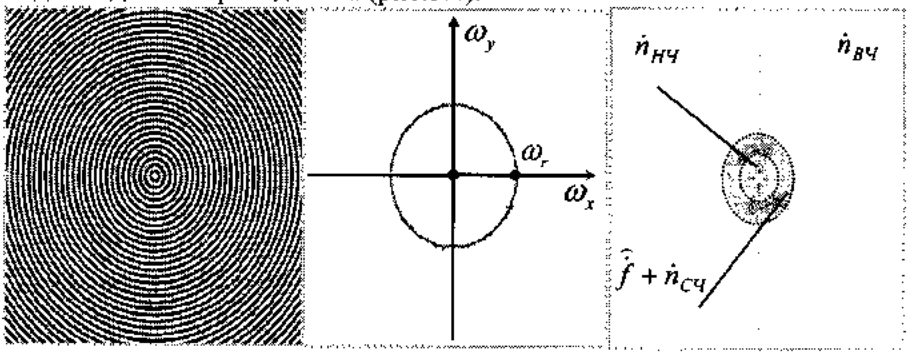
$$\times m(x,y) + n(x,y), \quad \forall (x,y) \in E .$$

Моделювання спотворень проводиться з метою побудови алгоритму попередньої обробки. Її ж метою є розв'язання оберненої задачі – усунення наявних спотворень.

Геометричні спотворення (3.2) усуваються, якщо відомі функції $r_x(x,y), r_y(x,y)$. Ці функції отримують шляхом зіставлення двох зображень або за описом процесу формування зображення. Оскільки процес формування математично не описаний, тому другий спосіб відпадає. Оцінювати $r_x(x,y), r_y(x,y)$ на основі набору тестових зображень є недоцільно, адже такі спотворення непостійні, і тому неможливо узагальнити модель. Висновком із цих суджень є те, що неможливо усунути геометричні спотворення, а необхідно адаптувати алгоритми розпізнавання до них. Подібна ситуація і з негеометричними спотвореннями (змазуванням). Як і щодо геометричних спотворень, цей процес також неконтрольований і його параметри невідомі системі ідентифікації та не можуть бути оцінені на етапі проектування ДБС.

Таке ж твердження можна б було зробити і для спотворень яскравості (3.2), якби не апріорні дані про зображення, на основі яких будується ПОЗ.

Вважається [176], що зображення відбитка є не що інше, як зображення спотвореної колової ґратки з відповідною аналогією їх характеристик. Спектр колової ґратки – коло радіусом ω_r (рис.3.3), а спектр спотвореної колової ґратки буде зосереджений в смузі частот, подібно до спектра відбитка (рис.3.4).



а) б)

Рис.3.3. Просторове (а) і частотне (б) представлення колової дифракційної ґратки.

Рис.3.4. Зображення спектра реального відбитка (наднизькі частотні складові не відображені).

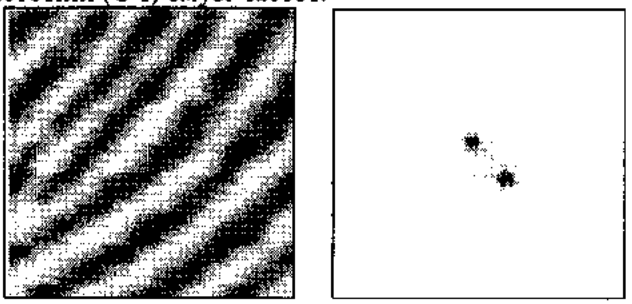
Пунктирними лініями на рис.3.4 виділено смугу частот, яка характерна для всіх дактилоскопічних зображень. Це, нарівні з проведеною аналогією, дозволяє припускати, що в НЧ і ВЧ областях спектра знаходяться лише спектральні складові шуму. Узявши до уваги, що мультиплікативний шум може бути замінений залежним від вхідного зображення адитивним шумом, запишемо спектр зображення $g(x,y)$ так:

$$\dot{f}(\omega_x,\omega_y) = \dot{\hat{f}}(\omega_x,\omega_y) + n_{СЧ}(\omega_x,\omega_y,\hat{g}) + n_{НЧ}(\omega_x,\omega_y,\hat{g}) + n_{ВЧ}(\omega_x,\omega_y,\hat{g}), \quad (3.6)$$

де $\dot{\hat{f}}(\omega_x,\omega_y)$ – спектр зображення $\hat{g}(x,y)$; $n_{СЧ}(\omega_x,\omega_y,\hat{g})$, $n_{НЧ}(\omega_x,\omega_y,\hat{g})$, $n_{ВЧ}(\omega_x,\omega_y,\hat{g})$ – спектральні складові шуму, які є залежними від вхідного зображення.

Розглянемо спектр фрагмента потоку папілярних ліній (рис.3.5).

Спектр (рис.3.5 б) показує локалізованість спектральних складових за частотою і орієнтацією. Така властивість дозволить надалі зменшити рівень шумових складових за допомогою орієнтованих фільтрів у середньочастотній (СЧ) смузі частот.



а) б)

Рис.3.5. Зображення фрагмента потоку папілярних ліній (а) і його спектра (б).

Аналогія відбитка з дифракційною граткою, а фрагмента з гармонічною просторовою хвилею дає підставу для ще двох припущень. Так, зображення гармонічної хвилі має гістограму у вигляді параболи (аналогічно до параболічного розподілу гармонічного сигналу [3,70]), а значення мінімальної й максимальної яскравості будь-якого фрагмента зображення є постійними.

На основі проведеного аналізу встановлено такі головні особливості зображень відбитків, із якими додатково можна ознайомитися в роботі [85]:

- колова анізотропія спектра повного зображення і точкова анізотропія зображення фрагмента потоку папілярних ліній;
- зображення папілярних ліній локально нормалізовані за яскравістю, у будь-якому регіоні зображення, який за розміром більший від періоду папілярних ліній, значення максимальної й мінімальної яскравості є постійними;
- гістограма яскравості зображення відбитка описується параболічною кривою.

Отже, критерієм вибору етапів попередньої обробки є наближення характеристик реальних зображень до критеріїв ідеального зображення з наведеними вище особливостями.

3.2. Методи попередньої обробки

3.2.1. Сегментація дактилоскопічних зображень

Етап сегментації часто називають визначенням маски зображення. Сегментація передбачає поділ зображення на дві області: інформативну Ψ (область зображення, де присутня або може бути відновлена інформація про папілярні лінії) і неінформативну Ξ (область зображення, де відсутня або не може бути відновлена інформація про папілярні лінії). Таке застосування сегментації дозволяє не проводити обробку фонової області зображення й усунути неінформативні об'єкти з нього.

Актуальність цього етапу в ПОЗ визначається використанням локальної нормалізації, яка в області Ξ спричиняє значне підвищення шуму. При розробці даного методу виходять із властивості збереження енергії гармонічного сигналу при проходженні ним диференціюючої ланки. В свою чергу, папілярні лінії мають характер плоскої двовимірної гармонічної хвилі, а отже, диференціювання зображення призводить не до втрати енергії зображення в інформативній області Ψ, а тільки до пониження енергії в області фону. Як правило, сегментація проводиться за нормою $G(i,j)$ градієнта яскравості, який обчислюється за допомогою оператора Кірша:

$$G(i,j) = \left\| \partial_x(i,j), \partial_y(i,j) \right\|, \tag{3.7}$$

$$\partial_x = \mathbf{g} * \mathbf{H}_2, \quad \partial_y = \mathbf{g} * \mathbf{H}_1, \tag{3.8}$$

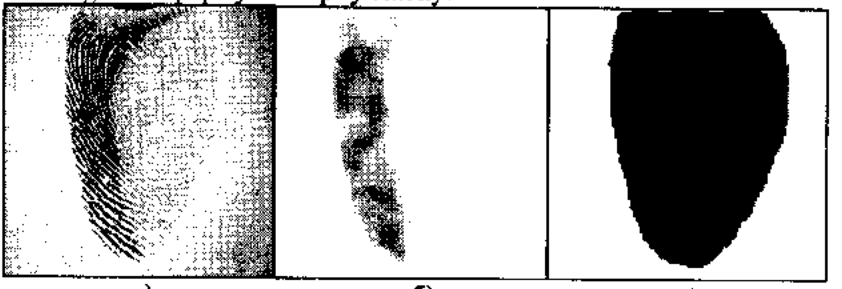
$$\mathbf{H}_1 = \begin{pmatrix} 5 & 5 & 5 \\ -3 & 0 & -3 \\ -3 & -3 & -3 \end{pmatrix}, \quad \mathbf{H}_2 = \begin{pmatrix} 5 & -3 & -3 \\ 5 & 0 & -3 \\ 5 & -3 & -3 \end{pmatrix}, \tag{3.9}$$

$$\left\| \partial_x(i,j), \partial_y(i,j) \right\| = \left| \partial_x(i,j) \right| + \left| \partial_y(i,j) \right|, \tag{3.10}$$

де $\mathbf{H}_1, \mathbf{H}_2$ – оператори Кірша; ∂_x, ∂_y – масиви дискретних похідних по відповідних осях зображення. Вектор градієнта яскравості для точки (i,j) описується в ДСК вектором $\begin{bmatrix} \partial_x(i,j) \\ \partial_y(i,j) \end{bmatrix}$. Для обчислення можна використовувати як прості оператори Собела, Робертса, Превітта, Кірша, так і складний – Марра-Хілдрета [83]. Маска обчислюється так:

$$mask(i,j) = \begin{cases} 1; & \underset{i,j \in K \times K}{med}\left(G(i,j)\right) \geq c \\ 0; & \underset{i,j \in K \times K}{med}\left(G(i,j)\right) < c \end{cases}, \ \forall (i,j) \in \mathbf{R}, \qquad (3.11)$$

де c – порогова величина (визначається експериментально); $\mathbf{R} = \Psi + \Xi$ – уся область зображення; $K \times K$ – розмір вікна фільтрації ($K = 24$). Медіанна фільтрація [69] застосовується для згладження дії імпульсних шумів і утворення плавної картини градієнта яскравості (рис.3.6 б). Останньою операцією є порогова бінаризація результату фільтрації (рис.3.6 в), яка і формує бінарну маску.



а) б) в)

Рис.3.6. Вхідне зображення (а), градієнт зображення після медіанної фільтрації (б) і маска інформативної області зображення (в).

Розроблений метод виділення інформативної області Ψ гнучкіший у використанні і простіший у виконанні, ніж існуючі. Попіксельне обчислення маски дозволило більш точно виділяти інформативну область на зображенні, а ніж блочні методи. На відміну від методу, базованого на когерентності ліній[101], розроблений не дає збоїв у центральних областях узору, де лінії мають сильну крутизну (отже, і малу когерентність).

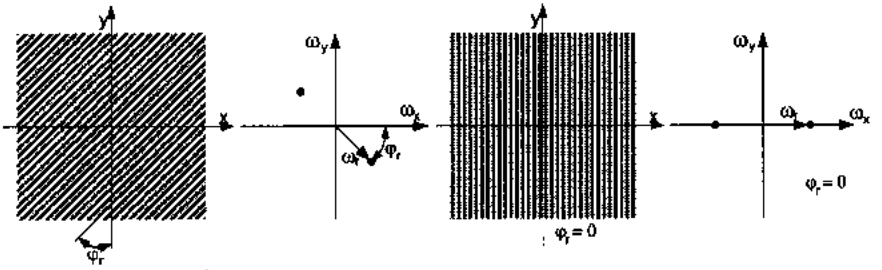
3.2.2. Квазіоптимальна фільтрація

Класичний квазіоптимальний просторовий фільтр з АЧХ у вигляді $f(i,j)^2$ забезпечує добрі результати на якісних зображеннях із рівномірним контрастом. Якщо ж його використати для зображень відбитків пальців із низькоконтрастними зонами, тоді ці зони будуть придушені шляхом зменшення енергії їх спектральних складових, що зумовлено просторовою селективністю фільтра.

Для усунення наведеного недоліку взамін просторово-частотного квазіоптимального фільтра з обмеженою смугою пропускання

необхідно використати частотно-селективний квазіоптимальний фільтр з обмеженою смугою пропускання.

Якщо розглянути зображення гармонічної хвилі, яка має напрям під кутом φ до осей координат, то її основна гармоніка на спектрі буде розташована під таким самим кутом, а віддаль ω_r (яка відповідає радіальній частоті) від центра спектра відповідає її частоті (рис.3.7 а).



а) б)

Рис.3.7. Зображення й структура спектрів нахиленої (а) і направленої вздовж осі OX гармонічної хвилі (б).

Спектр зображення гармонічної хвилі $g_z(x,y) = A\cos(Tx)$, направленої вздовж осі OX (рис.3.7 б), запишеться так:

$$f(\omega_x,\omega_y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g_z(x,y)e^{-j(x\omega_x+y\omega_y)}dxdy = A\pi(\delta(\omega_r - x, y) + \delta(\omega_r + x, y)), \quad (3.12)$$

де $\delta(x,y)$ – функція Дірака; $T = \dfrac{2\pi}{\omega_r}$ – період гармонічної хвилі; A – амплітуда гармонічної хвилі.

Для нахиленої гармонічної хвилі (рис.3.7 а)

$$g_z(x,y) = A\cos(T(x\cos\varphi + y\sin\varphi))$$

спектр буде таким:

$$f(\omega_x,\omega_y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} g_z(x,y)e^{-j(x\omega_x+y\omega_y)}dxdy = \quad (3.13)$$

$$= A\pi(\delta(\omega_r\cos\varphi - x, \omega_r\sin\varphi + y) + \delta(\omega_r\cos\varphi + x, \omega_r\sin\varphi - y))$$

де φ – кут нахилу гармонічної хвилі. Вона може бути представлена як хвиля вздовж координатної осі OX, повернутої на φ ДСК, в якій спектр записується виразом (3.12). Якщо спектр перевести в циліндричну систему координат (ЦСК), то формули спектрів (3.12) і (3.13) матимуть вигляд:

$$f(r,\theta) = A\pi(\delta(\omega_r - r, \theta) + \delta(\omega_r - r, \theta - \pi)), \quad (3.14)$$

$$f(r,\theta) = A\pi(\delta(\omega_r - r, \theta - \varphi) + \delta(\omega_r - r, \theta - \varphi - \pi)), \quad (3.15)$$

де r,θ – координати в ЦСК. На основі представлень (3.14) і (3.15) розділяють просторові і частотні координати гармонік. Координата r відповідає за частоту гармонічної складової, а φ – за її орієнтацію. В такому випадку, якщо АЧХ фільтра в ЦСК залежить від φ, то він має просторову селективність, а якщо від r – то частотну.

Просторово і частотно-селективні фільтри для спектрів, описаних формулами (3.14), (3.15), матимуть такі АЧХ:

$$h(r,\theta) = \begin{cases} 1; & \forall(r = \omega_r) \wedge (\theta = 0 \vee \theta = \pi), \\ 0; & \forall(r \neq \omega_r) \vee (r = \omega_r \wedge (\theta \neq 0 \vee \theta \neq \pi)), \end{cases} \quad (3.16)$$

$$h(r,\theta) = \begin{cases} 1; & \forall(r = \omega_r) \wedge (\theta = \varphi \vee \theta = \varphi + \pi), \\ 0; & \forall(r \neq \omega_r) \vee (r = \omega_r \wedge (\theta \neq \varphi \vee \theta \neq \pi)). \end{cases} \quad (3.17)$$

АЧХ частотно-селективних фільтрів однакова для обох спектрів (3.14), (3.15)

$$h(r,\theta) = \begin{cases} 1; & \forall r = \omega_r, \\ 0; & \forall r \neq \omega_r. \end{cases} \quad (3.18)$$

АЧХ просторово-частотного та частотно-селективного фільтрів, для зображення колової дифракційної гратки, буде однакова й опишеться формулою (3.18), оскільки на ньому є спектральні складові з орієнтацією в усьому діапазоні кутів $\theta \in [0,\pi]$.

У разі побудови фільтрів для дактилоскопічних зображень необхідно брати до уваги, що їх спектр нерівномірно розподілений у смузі частот (рис.3.4). Просторово-селективний фільтр зменшуватиме рівень неосновних гармонік зображення, які відповідають папілярним лініям з орієнтацією, відмінною від основної. Цього не буде лише в ідеальному випадку, коли основні гармоніки зображення розподілені рівномірно за орієнтацією, що характерно виключно для колової дифракційної гратки.

Формування АЧХ частотно-селективного фільтра передбачає інтегральну оцінку основних гармонік по всіх напрямах. Тоді пропускатимуться папілярні потоки з основним періодом, що відповідає спектральним складовим, в яких зосереджена найбільша енергія зображення, і зменшуватимуться з іншим періодом.

Розглянемо побудову АЧХ квазіоптимального фільтра для дактилоскопічних зображень. Нехай $g(x,y)$ – зображення, а $f(\omega_x,\omega_y)$ – його спектр. Для інтегральної оцінки розподілу гармонічних

складових зображення необхідно спектр $f(\omega_x,\omega_y)$ описати в ЦСК - $f(\omega_r,\theta)$ і знайти інтегральну проекцію на вісь $o\omega_r$ (рис.3.8).

Проекція оцінюється так:

$$p(\omega_r)=\int_{-\pi}^{\pi}\left|f(\omega_r,\theta)\right|d\theta. \qquad (3.19)$$

АЧХ квазіоптимального частотно-селективного фільтра в ЦСК опишеться формулою

$$h'(\omega_r,\theta)=\frac{p(\omega_r)}{\max(p(\omega_r))}. \qquad (3.20)$$

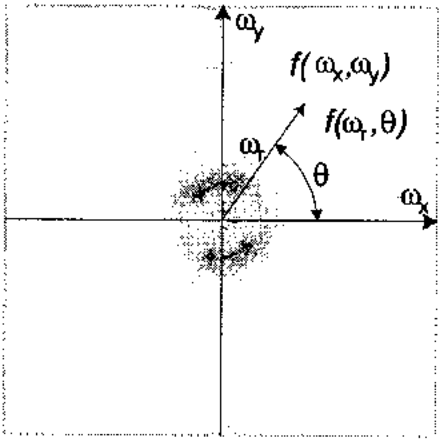


Рис.3.8. Зображення спектра в ДСК і ЦСК.

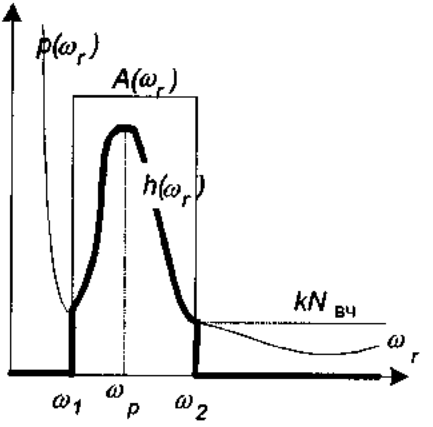


Рис.3.9. Структура проекції спектра на вісь $o\omega_r$ $p(\omega_r)$, АЧХ смугового $A(\omega_r)$ і квазіоптимального $h(\omega_r)$ фільтрів.

З урахуванням першої особливості дактилоскопічних зображень енергія інформативних спектральних складових зосереджена в середньочастотній смузі. Отже, квазіоптимальний фільтр для таких зображень повинен пропускати їх без послаблення, згідно визначення квазіоптимального фільтра [3].

Якщо обробляти зображення фільтром з АЧХ (3.20), то отримаємо зображення з придушеними середньо- і високочастотними складовими, оскільки основна енергія спектра зосереджена в НЧ складових. У випадку обробки дактилоскопічних зображень квазіоптимальний частотно-селективний фільтр має пропускати без зміни спектральні

складові з частотою ω_p (ω_p – координата піка в області СЧ) (рис.3.9). Згідно ж із формулою (3. 6), шуми поділені на НЧ, СЧ і ВЧ, отже, скомбінувавши ідеальний смуговий фільтр (проекція АЧХ $A(\omega_r)$ якого представлена на рис.3.9) і квазіоптимальний, досягнемо кращого результату пониження рівня НЧ, ВЧ і частково СЧ шумів. Комбінацію ідеального смугового і квазіоптимального фільтра з просторово-частотною селективністю було застосовано раніше [259], але не враховано, що відбитки мають різний середній період, а відтак і смугу основних складових спектра. Замість емпірично визначеної смуги пропускання пропонуємо використовувати адаптивну смугу пропускання, що додатково описано у роботі [81]. У такому випадку фільтр буде квазіоптимальним частотно-селективним із адаптивною смугою пропускання.

Нижня межа смуги пропускання ω_1 визначається як координата локального мінімуму на відрізку $[0,\omega_p]$ проекції $p(\omega_r)$. Для встановлення верхньої частоти пропускання ω_2 робимо припущення, що спектр $n_{ВЧ}(\omega_x,\omega_y)$ – рівномірний і дорівнює $N_{ВЧ}$. Тоді частота відповідатиме перетину кривої $p(\omega_r)$ і прямої $kN_{ВЧ}$ (величина k визначається експериментально й коливається в межах 1,2..1,5) (рис.3.9). Таке припущення з певною похибкою підтверджується практичними дослідженнями.

АЧХ квазіоптимального частотно-селективного фільтра з адаптивною смугою пропускання в неперервному просторі ЦСК опишеться формулою

$$h(\omega_r,\varphi)=\begin{cases}\dfrac{p(\omega_r)}{p(\omega_p)}; & \forall\,\omega_r\in[\omega_1,\omega_2],\\ 0; & \forall\,\omega_r\notin[\omega_1,\omega_2]\end{cases} \tag{3.21}$$

або в ДСК

$$h(\omega_x,\omega_y)=\begin{cases}\dfrac{p\left(\sqrt{\omega_x^2+\omega_y^2}\right)}{p(\omega_p)}; & \sqrt{\omega_x^2+\omega_y^2}\in[\omega_1,\omega_2],\\ 0; & \sqrt{\omega_x^2+\omega_y^2}\notin[\omega_1,\omega_2].\end{cases} \tag{3.22}$$

У просторовій області частота ω_p обернено пропорційна середньому періоду папілярних ліній.

У дискретному просторі для зображення **g** зі спектром **f** АЧХ квазіоптимального частотно-селективного фільтра з адаптивною смугою пропускання запишемо таким чином:

$$h(i,j)=\begin{cases}\dfrac{p\left(\sqrt{i^2+j^2}\right)}{p(\nu_p)}; & \sqrt{i^2+j^2}\in[\nu_1,\nu_2]\ ,\\ 0; & \sqrt{i^2+j^2}\notin[\nu_1,\nu_2]\ ,\end{cases} \tag{3.23}$$

$$p(\nu)=\sum_{l=\nu-1}^{\nu+1}p'(l)\,, \tag{3.24}$$

$$p'(\nu)=\sum_{i,j}\begin{cases}|f(i,j)|; & \sqrt{i^2+j^2}\in[(\nu-0{,}5),(\nu+0{,}5))\,,\\ 0; & \sqrt{i^2+j^2}\notin[(\nu-0{,}5),(\nu+0{,}5))\,,\end{cases}$$

де $p'(\nu)$ – проекція спектра, аналог $p(\omega_r)$; $p(\nu)$ – згладжена усереднюючим фільтром проекція $p'(\nu)$; ν_p – частота основних гармонік зображення, аналог ω_p (детальніше про її оцінку див п.3.2.5); ν_1,ν_2 – нижня й верхня межа смуги пропускання фільтра, аналоги ω_1,ω_2. Усереднююча фільтрація проекції $p'(\nu)$ проводиться для забезпечення гладкості кривої.

Квазіоптимальний частотно-селективний фільтр із адаптивною смугою пропускання, що додатково описаний у літературі [81], усуває НЧ, ВЧ та придушує СЧ шуми на дактилоскопічних зображеннях, не зменшуючи рівня основних корисних гармонік спектра зображення.

3.2.3. Оцінка зображення локальної орієнтації

Якщо паралельні папілярні лінії розглядати як гармонічну хвилю, то їх напрям буде перпендикулярний до кута розташування спектральних складових хвилі і перпендикулярний до напрямку градієнтів яскравості.

За основу взято метод середньоквадратичної оцінки, який удосконалено. Середньоквадратична оцінка передбачає визначення орієнтації за векторами піднесених до квадрата градієнтів.

Нехай у полярній системі координат градієнт описується вектором $\begin{bmatrix}\rho\\ \phi\end{bmatrix}$, а в декартовій $\begin{bmatrix}\partial_x\\ \partial_y\end{bmatrix}$, тоді

$$\begin{bmatrix}\rho\\ \phi\end{bmatrix}=\begin{bmatrix}\sqrt{\partial_x^{\,2}+\partial_y^{\,2}}\\ \tan^{-1}\partial_y/\partial_x\end{bmatrix}, \tag{3.25}$$

а вектор у квадраті, довжина якого піднесена до квадрата й кут подвоєний, за допомогою комплексних змінних

$$(\partial_x + j\partial_y)^2 = (\partial_x^{\,2} - \partial_y^{\,2}) + j(2\partial_x\partial_y)\,. \tag{3.26}$$

Обчислення середньоквадратичного значення орієнтації вектора проводиться в околі W точки оцінки за формулою

$$\varphi = \frac{1}{2}\angle\left(\sum_W\left(\partial_x^{\,2}-\partial_y^{\,2}\right),\sum_W\left(2\partial_x\partial_y\right)\right), \tag{3.27}$$

$$\angle(x,y)=\begin{cases}\tan^{-1}(y/x); & \forall x\ge 0\ ,\\ \tan^{-1}(y/x)+\pi; & \forall x<0\wedge y\ge 0\ ,\\ \tan^{-1}(y/x)-\pi; & \forall x<0\wedge y<0\ .\end{cases} \tag{3.28}$$

Орієнтація потоку папілярних ліній перпендикулярна до орієнтації градієнта і визначається з орієнтації ϕ

$$\theta=\begin{cases}\phi+\dfrac{\pi}{2}; & \forall\phi\le 0\,,\\ \phi-\dfrac{\pi}{2}; & \forall\phi>0\,.\end{cases} \tag{3.29}$$

Оцінка локальної орієнтації для дискретного зображення виконується блоками в декілька етапів.

1. Обчислюються масиви ∂_x і ∂_y для вхідного зображення **g** за формулами (3.8).

2. Зображення g розбивається на блоки $\mathbf{V}_{m,n}^{(4)}$ розміром 4×4 пікселі, і приймається, що папілярні лінії мають однакову орієнтацію в їх межах, $m=\overline{1,M/4}$, $n=\overline{1,N/4}$.

3. Оцінюється локальна орієнтація для блоків $\mathbf{V}_{m,n}^{(4)}$ у квадратному околі $\mathbf{W}_{m,n}^{(24)}$ розміром 24×24 пікселі, який центрований відносно $\mathbf{V}_{m,n}^{(4)}$ (рис.3.10). Спочатку знаходиться середньоквадратична орієнтація градієнтів яскравості $\phi(m,n)$ в блоках $\mathbf{W}_{m,n}^{(24)}$:

$$G_1(m,n)=\sum_{i,j\in W_{m,n}^{(24)}}2\partial_x(i,j)\partial_y(i,j)\ , \tag{3.30}$$

$$G_2(m,n) = \sum_{i,j \in W^{(24)}_{m,n}} (\partial_x{}^2(i,j) - \partial_y{}^2(i,j)), \tag{3.31}$$

$$\phi(m,n) = \angle\big(G_2(m,n),\ G_1(m,n)\big), \tag{3.32}$$

де $\angle(x,y)$ – обчислюється за формулою (3.28). Орієнтація $\Theta(m,n)$ для кожного блока $\mathbf{V}^{(4)}_{m,n}$ визначається з масиву Φ за формулою (3.29). Розмір масиву орієнтації Θ рівний $M/4 \times N/4$ пікселі.

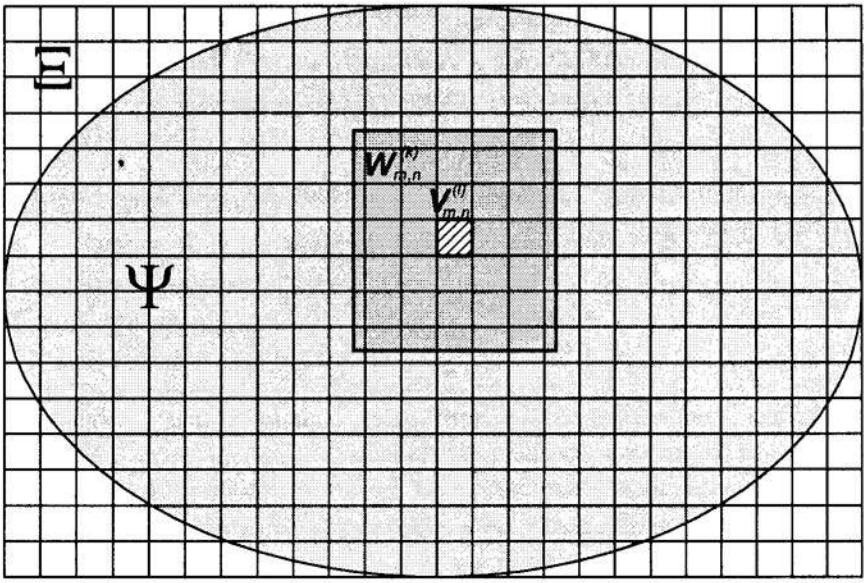


Рис.3.10. Схематичне представлення блочної оцінки.

Під блоком зображення розуміємо не що інше як зображення меншого розміру, котре рівне розміру блока й складається з елементів повного зображення. Наприклад, блок

$$\mathbf{V}^{(1)}_{m,n} \subset (g(i,j)),\ i = \overline{(m-1)*l, m*l},\ j = \overline{(n-1)*l, n*l}.$$

Використання блоків, які перекриваються для оцінки локальної орієнтації, дозволило збільшити точність оцінки, особливо в областях із локальними спотвореннями (шрам, рана, зморшка тощо), відмовитись від подальшого згладження зображення локальної орієнтації з переведенням її в неперервний простір, як це зазвичай роблять [153,235], не проводити ітераційної оцінки, як у праці [159], і

зменшити обчислювальні затрати. Докладніше цей метод викладено в роботі [85].

3.2.4. Локальна нормалізація яскравості

Використання локальної нормалізації яскравості замість глобальної, яка найчастіше застосовується в ПОЗ якісних зображень, дає змогу усунути варіацію яскравості зображення, викликану спотвореннями, описаними формулою (3.3).

Нормалізацію доцільно проводити в межах блока $\mathbf{V}_{m,n}^{(4)}$, оцінюючи параметри розподілу яскравості в $\mathbf{W}_{m,n}^{(24)}$ (див. п.3.2.3). Однією з умов локальної нормалізації згаданим методом є достатня точність визначення статистичних параметрів розподілу, тому квадрати, на які розбивається зображення, повинні бути більшими від періоду папілярних ліній (квадрат 24×24 повністю відповідає таким вимогам, оскільки практичні дослідження показали, що період не перевищує 20 дискретних точок для роздільної здатності пристрою вводу 500 точок на дюйм).

У відомих методах глобальної нормалізації припускають, що розподіл яскравості для вхідного зображення описується нормальним законом. Далі нормалізуються математичне очікування і середньоквадратичне відхилення яскравості зображення. На відміну від глобальної нормалізації точно оцінити параметри такого розподілу в малому околі важко. Замість цього, ґрунтуючись на третій особливості дактилоскопічних зображень, пропонуємо оцінювати максимальну та мінімальну яскравості блока $\mathbf{W}_{m,n}^{(24)}$, нормалізувати точки у межах блока $\mathbf{V}_{m,n}^{(4)}$ (рис.3.10) за формулою

$$g'(i,j) = \frac{g(i,j) - g_{\min}(i/4, j/4)}{g_{\max}(i/4, j/4) - g_{\min}(i/4, j/4)}, \qquad (3.33)$$

де $g_{\min}(m,n) = \min_{i,j \in \mathbf{W}_{m,n}^{(24)}}(g(i,j))$, $g_{\max}(m,n) = \max_{i,j \in \mathbf{W}_{m,n}^{(24)}}(g(i,j))$ – мінімальна й максимальна яскравості в межах блоків $\mathbf{W}_{m,n}^{(24)}$; g' – вихідне нормалізоване зображення. Яскравість точок вихідного зображення після нормалізації знаходиться в межах [0,1].

Застосування наведеного методу в областях дії спотворення, описаного формулою (3.3), майже повністю усуває його за умови, що область спотворення більша від розміру блоків $\mathbf{W}_{m,n}^{(24)}$ і функція

масштабування $T(\hat{g}(x,y))$ – лінійна. Якщо функція $T(\hat{g}(x,y))$ нелінійна, то локальна нормалізація покращить зображення, але не усуне спотворення повністю. Глобальна ж нормалізація в такому випадку не дає жодних результатів.

Додатково з цим методом можна ознайомитися в роботі[85].

3.2.5. Оцінка зображення локального періоду

Замість оцінки періоду просторовими методами [46] пропонуємо оцінювати його домінуючу гармоніку ν_p (див.п.3.2.2) спектра $\mathbf{f}$ за допомогою проекції $p(v)$ у полярній системі, яка обчислюється за формулою (3.24).

Пояснимо поняття частоти папілярних ліній. Під нею розуміємо частоту гармонічної хвилі, якою моделюється потік папілярних ліній зображення. Поняття частоти папілярних ліній не є точним і зустрічається рідко. Частіше вживається поняття періоду папілярних ліній, величина якого обернено пропорційна до частоти.

В п.3.2.2 описана глобальна оцінка частоти папілярних ліній, яка виправдовує себе у випадку малої площі відбиття узору й відсутності сильних геометричних спотворень типу "губка". Ці умови забезпечуються у БІС, а в АДІС – ні. Отже, ПОЗ для БІС може включати етап глобальної оцінки періоду папілярних ліній поєднаний з квазіоптимальною фільтрацією, а для АДІС потрібна оцінка локального періоду.

Локальна оцінка частоти папілярних ліній проводиться аналогічно до глобальної, але в межах блоків зображення, що перекриваються, подібно до оцінки орієнтації (рис.3.10). Враховуючи, що період папілярних ліній – величина повільнозмінна, приймаємо, що він у межах блоків 32×32 буде однаковим.

Глобальна оцінка частоти папілярних ліній включає кілька етапів:

1. Вхідне зображення g розбивається на блоки $\mathbf{V}_{m,n}^{(32)}$ розміром 32×32, $m=\overline{1,M/32}$, $n=\overline{1,N/32}$.

2. Оцінюється частота папілярних ліній у межах кожного блока $\mathbf{W}_{m,n}^{(128)}$ розміром 128×128 точки, який центрований відносно $\mathbf{V}_{m,n}^{(32)}$ (аналогічно, як у п.3.2.4 блоки $\mathbf{V}_{m,n}^{(4)}$ і $\mathbf{W}_{m,n}^{(24)}$):

   а) за допомогою ШПФ обчислюється спектр для блока зображення $\mathbf{f}_{m,n}^{(128)}=\Im\mathbf{W}_{m,n}^{(128)}$ ($\Im$ - ШПФ);

б) визначається розподіл частот папілярних ліній у блоці $\mathbf{W}_{m,n}^{(128)}$; для цього розраховується інтегральна проекція $p^{(128)}(v)$ Фур'є образу $\mathbf{f}_{m,n}^{(128)}$ на вісь $o\omega_r$ за формулою (3.24);

в) знаходиться пік проекції $p^{(128)}(v)$ в області СЧ (на практиці для зображень роздільною здатністю 500 точок на дюйм пошук проводиться в діапазоні $v \in [4, 30]$); пік повинен задовольняти умову

$$p^{(128)}(v_p - 2) \le p^{(128)}(v_p - 1) \le p^{(128)}(v_p) < p^{(128)}(v_p + 1) < p^{(128)}(v_p + 2),$$

якщо умова виконується, то в масив зображення локального періоду заноситься величина $\Pi(m,n) = \dfrac{128}{2v_p}$ (період вимірюється в кількості точок між двома папілярними лініями), інакше заноситься -1.

3. Точкам масиву $\Pi(m,n)$, в яких період не був оцінений, але в блоці $\mathbf{V}_{m,n}^{(32)}$ є хоча б одна точка, яка належить інформативній області Ψ, присвоюється значення, рівне середньому значенню періоду, оціненого у сусідніх блоків.

Перевагою частотного методу оцінки над відомими просторовими є їх універсальність, нечутливість до крутизни повороту папілярних ліній, міжпапілярних включень та нерегулярності в потоці (поблизу особистих ознак).

Усі ці недоліки притаманні відомим методам й усунуті в розглянутому завдяки використанню проекції спектра, яка не чутлива до:

- орієнтації й крутизни ліній, оскільки оцінюється розподіл основних спектральних складових спектра без урахування їх орієнтації;
- появи нерегулярностей потоку, що спричиняють лише збільшення енергії наднизьких частот у спектрі, але незначно впливають на основні складові;
- появи міжпапілярних включень, які переважно не є періодичними структурами, а отже, не призводять до виникнення на проекції додаткового піка.

3.2.6. Обробка спрямованим фільтром Габора

У малому околі папілярні лінії й впадини на зображенні мають форму двовимірної гармонічної хвилі вздовж напрямку орієнтації та

описуються локальним періодом і напрямком. Більшість смугових фільтрів зменшують рівень шумів та зберігають структуру ліній, як це, наприклад, робить квазіоптимальний фільтр, якому характерна лише добра частотна селективність (п.3.2.2). Фільтр Габора має частотно- і спрямовано-селективні властивості й водночас його АЧХ є просторово- та частотно-локалізована. Просторово-частотна локалізованість фільтра дозволяє проводити спрямовану й частотну фільтрацію без якихось краєвих ефектів, притаманних ідеальним фільтрам із погано локалізованими характеристиками.

Функція Габора є комплексною експонентою з Гаусівською огинаючою [200] і використовується як базис Wavelet розкладу зображень. В області обробки зображень застосовується її дійсна частина. Багатьма авторами ще вживається термін парносиметричного фільтра Габора. ІХ спрямованого фільтра Габора описується формулою

$$h(x,y)=\exp\left\{-\frac{1}{2}\left[\frac{x^2}{\delta_x^2}+\frac{y^2}{\delta_y^2}\right]\right\}\cos(\omega_g x)\,, \qquad (3.34)$$

де δ_x,δ_y – ширина гаусівської огинаючої ІХ уздовж і впоперек осі ОХ в ДСК і вибирається згідно з роздільною здатністю пристрою формування зображення (приймають 4,0 для пристрою вводу з роздільною здатністю 500 точок на дюйм); ω_g – частота, на яку налаштований фільтр.

Фільтр з ІХ (3.34) пропускає гармонічні складові спектра, які розташовані перпендикулярно до осі ОХ і мають частоту ω_g. Він адаптований до гармонічної хвилі $\omega_g=\omega_r$, представленої на рис.3.7 б.

Для зображень відбитків локальна орієнтація ліній та їх частота є змінними, і тому ІХ адаптують до них, відповідно, поворотом ІХ і зміною частоти ω_g.

ІХ фільтра Габора, який адаптується до параметрів папілярних ліній, запишеться в дискретному просторі так:

$$h(i,j,\varphi,\omega_g)=\exp\left\{-\frac{1}{2}\left[\frac{x'^2}{\delta_x^2}+\frac{y'^2}{\delta_y^2}\right]\right\}\cos(\omega_g x')\,, \qquad (3.35)$$

$$x'=j\cos\varphi+i\sin\varphi\,,$$

$$y'=-j\sin\varphi+i\cos\varphi\,,$$

$$i=-{}^{(N_g-1)}\!/_{2}\,..\,{}^{(N_g-1)}\!/_{2}\,,\ j=-{}^{(N_g-1)}\!/_{2}\,..\,{}^{(N_g-1)}\!/_{2}\,,$$

де φ – орієнтація фільтра Габора (його ІХ і АЧХ); $N_{БД}$ – розмір масиву ІХ. Оскільки ІХ просторово локалізована, то t_1, t_2 вибираються згідно значенням δ_x, δ_y.

АЧХ фільтра Габора, яка відповідає ІХ (3.35), має такий вигляд:

$$H_{gabor}(u,v,\varphi,\omega_g) = 2\pi\delta_x\delta_y \exp\left\{-\frac{1}{2}\left[\frac{v'^2}{\delta_{f_x}^2}+\frac{u'^2}{\delta_{f_y}^2}\right]\right\} + 2\pi\delta_x\delta_y \exp\left\{-\frac{1}{2}\left[\frac{v''^2}{\delta_{f_x}^2}+\frac{u''^2}{\delta_{f_y}^2}\right]\right\}, \quad (3.36)$$

$$v' = (v+\omega_g/2\pi)\cos\varphi + u\sin\varphi,$$

$$u' = -(v+\omega_g/2\pi)\sin\varphi + u\cos\varphi,$$

$$v'' = (v-\omega_g/2\pi)\cos\varphi + u\sin\varphi,$$

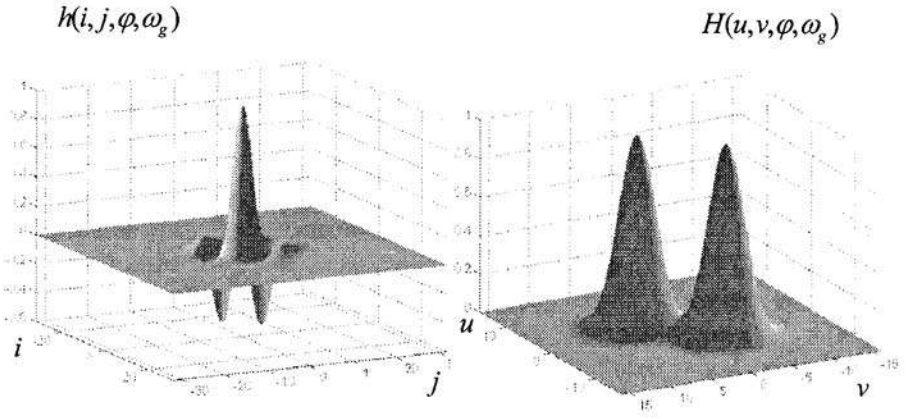
$$T' = t_1 N_{БД} + t_2 N_{БД} P_{мі}^{(1)},$$

де $\delta_{f_x} = 1/2\pi\delta_x$, $\delta_{f_y} = 1/2\pi\delta_y$ – ширина по осях частот експоненціальної складової АЧХ фільтра.

ІХ і АЧХ фільтра Габора адаптованого до орієнтації 45° і періоду 10 точок представлені на рис.3.11.

Якщо розглянути АЧХ фільтра Габора (рис.3.11 б) і спектр фрагмента потоку папілярних ліній (рис.3.5 б), то можемо говорити, що фільтр Габора адаптований до орієнтації й періоду потоку папілярних ліній. Він є квазіоптимальним фільтром, оскільки пропускає основні спектральні складові без змін і придушує інші. Як бачимо, АЧХ має виражену спрямовану й частотну селективність, яка дозволяє краще зменшувати рівень шумів, описаних формулою (3.6). На відміну від квазіоптимального фільтра (п.3.2.2) фільтр Габора зменшує рівень НЧ, ВЧ і гармонічних складових СЧ шумів, які мають орієнтацію, відмінну від орієнтації папілярних ліній. Така властивість дає підставу говорити про фільтр Габора як про квазіоптимальний просторово-частотний фільтр.

У роботі [135] пропонується застосовувати ШПФ для фільтрації зображення набором орієнтованих на 16 кутів фільтрів Габора і формувати вихідне зображення з профільтрованих. Такий підхід виправдовує себе для фільтрів із нескінченною ІХ. У випадку



а) б)

Рис.3.11. ІХ (а) і АЧХ (б) фільтра Габора, налаштованого на орієнтацію 45° і період 10 точок.

використання просторово локалізованої ІХ обчислювальні затрати будуть менші, якщо проводити пряму просторову згортку. Це пов'язано з тим, що розмір масиву ІХ значно менший від розміру зображення.

Враховуючи оцінені зображення локальної орієнтації й періоду, спрямовану фільтрацію зображення можна описати такою формулою згортки:

$$g'(i,j)=\sum_{k=-\frac{N_g-1}{2}}^{\frac{N_g-1}{2}}\sum_{l=-\frac{N_g-1}{2}}^{\frac{N_g-1}{2}} h\left(k,l,\Theta\left(\frac{i}{4},\frac{j}{4}\right),\frac{2\pi}{\Pi\left(\frac{i}{32},\frac{j}{32}\right)}\right)\cdot g(i-k,j-l), \quad (3.37)$$

де g' – профільтроване зображення; Θ – зображення локальної орієнтації (п.3.2.3); Π – зображення локального періоду (п.3.2.5). Для БІС доцільно послуговуватися глобальним періодом $\Pi(i,j)=\frac{1}{2v_p}$ (п.3.2.2.), що зменшує часозатрати на ПОЗ.

Використання фільтра Ґабора, адаптованого до локальних властивостей папілярних ліній узору, дозволяє підвищувати якість

зображення, що, у свою чергу, покращує результати подальшої роботи з ними.

3.2.7. Перетворення гістограми

Однією з найбільш поширених характеристик, за допомогою якої вирішують задачу поліпшення якості зображення, є гістограма. На жаль, в області обробки дактилоскопічних зображень їй не приділяють великої уваги і лише окремі дослідники використовують в алгоритмах обробки методи розтягування гістограми. Якщо ж провести спрощення і припустити, що гістограма спотвореної дифракційної гратки мало чим відрізняється від гістограми неспотвореної дифракційної гратки, то вираз для гістограми ідеального нескінченного зображення матиме вигляд:

$$h(I) = \frac{1}{\pi\sqrt{1-(I-1/2)^2}}, \tag{3.38}$$

де $I \in [0,1]$ – інтенсивність яскравості зображення.

Експериментальні дослідження гістограм реальних зображень показали, що більшість із них мають характер гаусівської кривої, а отже, одним із способів покращання якості зображення є перетворення його гістограми. Для перетворення гістограми зображення було використано детально описаний у літературі й програмно реалізований спосіб перетворення гістограми [69].

Перетворення гістограми дозволяє максимально наблизити гістограму реального зображення до ідеального, про що додатково наголошено в роботі [85].

3.3. Критерії застосування двоетапного методу розпізнавання

Усі розробники, які цікавляться двоетапними методами розпізнавання, ставлять за мету покращити імовірнісні показники системи. Як було з'ясовано в п.1.4.7, метою використання нами двох етапів порівняння є досягнення необхідних експлуатаційних та імовірнісних параметрів систем ідентифікації.

Концепція застосування двоетапного методу порівняння у розробленому алгоритмі полягає у забезпеченні швидкісних параметрів системи на першому етапі та імовірнісних на другому. Згідно з цим, загальний двоетапний метод збереже властивості кореляційного з одночасним усуненням його основного недоліку, а саме великих обчислювальних затрат. Зужитий на першому етапі швидкий, але менш

точний метод пришвидшує роботу алгоритму за рахунок скорочення кількості кандидатів на порівняння другим етапом. Кандидатом вважатимемо опис відбитка пальця особи, який зчитується з БД і порівнюється з описом вхідного відбитка пальця. Перший етап передбачає порівняння опису локальної орієнтації зображення, а другий – кореляційний метод порівняння за спектральними ознаками.

Процес порівняння для такого двоетапного методу відображається перевернутою пірамідою (рис.3.12).

На першому етапі вектор ознак вхідного зображення порівнюється з усіма $N_{БД}$ кандидатами з БД. Якщо кандидат має різницю між векторами, меншу від порогової, то він проходить перший етап і далі порівнюється другим етапом. На основі міри подібності, яка видається другим етапом, приймається рішення про ідентифікацію.

Взявши за мету збільшення швидкодії системи в цілому без зменшення її імовірнісних показників, ми тим самим визначилися з правилом комбінування результатів, отриманих на кожному з двох етапів. Таке комбінування називається І-правилом (AND-Rule), за яким вхідний відбиток вважається ідентифікованим, якщо обидва етапи дали позитивний результат.

Виведемо критерії доцільності застосування двоетапного методу порівняння зображень.

Нехай t_1, t_2 – часи порівняння векторів двох зображень першим і другим етапами. Припускаємо, що в базі даних є $N_{БД}$ кандидатів, кожен із яких описується двома векторами.

Перший критерій конкретизує вибір імовірнісних показників, тобто $P_{нн}^{(1)} = 0$, $P_{ні}^{(1)} < 1$. Імовірність $P_{нн}^{(1)} = 0$ вибрано для того, щоб перший етап не вносив додаткової похибки в результати роботи системи, а ІНІ $P_{ні}^{(1)} < 1$ – щоб забезпечити зменшення кількості кандидатів на порівняння другим етапом.

Час ідентифікації в системі без першого етапу обчислюється так:

$$T = t_2 N_{БД}. \tag{3.39}$$

У випадку застосування двоетапного методу час визначається виразом

$$T' = t_1 N_{БД} + t_2 N_{БД} P_{ні}^{(1)}. \tag{3.40}$$

Для того, щоб включення додаткового етапу порівняння забезпечило покращання часових показників системи, необхідно, аби $T' \le T$. Підставивши в наведену умову формули (3.39) і (3.40) та

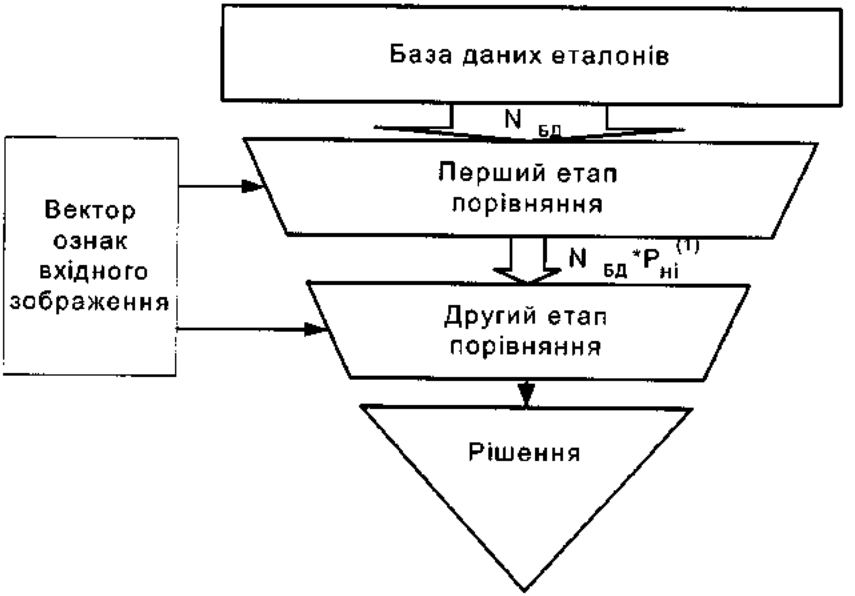


Рис.3.12. Процес порівняння зображень двоетапним методом.

провівши спрощення, отримаємо умову доцільності застосування двоетапного методу розпізнавання:

$$\frac{t_2}{t_1} > \frac{1}{1-P_{ni}^{(1)}} = \frac{1}{P_{ni}^{(1)}}, \qquad (3.41)$$

де $P_{ni}^{(1)}$ – імовірність правильної ідентифікації першим етапом.

Нерівність (3.41) вказує на те, що чим більше кандидатів проходить через перший етап порівняння, тим меншим повинен бути час порівняння t_1. Враховуючи, що добавлення додаткових ознак приводить до збільшення об'єму інформації, яку необхідно зберігати, ускладнення алгоритму й зростанню витрат на розробку, вираз (3.41) перепишемо так:

$$\frac{t_2}{t_1} >> \frac{1}{P_{ni}^{(1)}}. \qquad (3.42)$$

Нерівність (3.42) є другим критерієм доцільності застосування двоетапного методу й означає, що введення додаткового етапу повинно покращити параметри системи таким чином, щоб перекрити затрати на його розробку та функціонування.

Розглянемо імовірнісні характеристики системи з двоетапним методом порівняння.

Нехай $P_{ні}^{(1)}(T^{(1)}), P_{нн}^{(1)}(T^{(1)})$ – імовірнісні характеристики (див.п.1.2) першого, $P_{ні}^{(2)}(T^{(2)}), P_{нн}^{(2)}(T^{(2)})$ – другого етапу порівняння ($T^{(1)}, T^{(2)}$ – пороги ідентифікації для першого та другого етапів). Тоді загальні імовірнісні характеристики для І-правила комбінування результатів записуються так:

$$P_{ні}(\mathbf{T}) = P_{ні}^{(1)}(T^{(1)}) P_{ні}^{(2)}(T^{(2)}), \tag{3.43}$$

$$P_{нн}(\mathbf{T}) = P_{нн}^{(1)}(T^{(1)}) + P_{нн}^{(2)}(T^{(2)}) - P_{нн}^{(1)}(T^{(1)}) P_{нн}^{(2)}(T^{(2)}), \tag{3.44}$$

де $\mathbf{T} = \begin{bmatrix} T^{(1)} \\ T^{(2)} \end{bmatrix}$.

Вибір параметрів порівняння для першого етапу проводимо таким чином, щоб забезпечити перший критерій. У такому разі $P_{ні}(\mathbf{T})$ описується виразом (3.43), а вираз (3.44) набуває вигляду

$$P_{нн}(\mathbf{T}) = P_{нн}^{(2)}(T^{(2)}). \tag{3.45}$$

Отже, забезпечивши два наведені критерії, зменшимо час порівняння і заодно покращимо характеристику $P_{ні}(\mathbf{T})$ системи, не змінивши характеристики $P_{нн}(\mathbf{T})$.

Для подальшого пришвидшення роботи БІС (для АДІС така будова недоцільна) застосуємо сортування результатів порівняння на першому етапі. Для цього вхідний опис відбитка порівнюється з усіма кандидатами в БД, а далі формується список кандидатів у порядку зростання різниці між векторами. Переважно кандидат, який відповідає вхідному опису, має найменшу різницю між векторами й буде занесений у першій позиції. У такому випадку час порівняння у БІС визначатиметься формулою

$$T'' = t_1 N_{БД} + t_2 + t_{сорт}, \tag{3.46}$$

де $t_{сорт}$ – час сортування результатів першого етапу. Якщо взяти до уваги, що $(t_2 + t_{сорт}) << t_1 N_{БД}$, то загальний час (3.46) порівняння відбитків у двоетапному методі для БІС обмежуватиметься часом порівняння, затраченим на роботу першого етапу.

Якщо узагальнити наведені формули, то час порівняння для АДІС визначатиметься формулою (3.40), а для БІС лежатиме в межах $[T'', T']$ (3.40), (3.46).

Отже, введенні критерії доцільності вибору двоетапного методу ідентифікації є ще критеріями вибору системи інформативних ознак для першого етапу порівняння та його налаштування.

3.4. Вибір зони опису зображення

Розроблений двоетапний метод порівняння передбачає прив'язку генератора ознак до конкретної точки узору, а зона вибирається на підставі теорії інформації.

Кожен узор характеризується невизначеністю, яка описується ентропією. Поняття ентропії зручно використовувати для вибору оптимальної зони за критерієм мінімуму ентропії [90]. Зони узору, які зменшують невизначеність під час опису зображення, рахуються більш інформативними, ніж ті, що приводять до протилежного результату.

Якщо розглядати вибір найбільш інформативної зони для опису локальних орієнтацій відбитка, то необхідно звернути увагу на те, як вони відрізняються для відбитків одного і різних типів узору.

Розглянемо зони для подальшого опису локальної орієнтації у їх межах. Дистальна й латеральні зони (рис. 1.20) включають у себе дистальний потік папілярних ліній (рис. 1.19), який подібний для відбитків як одного, так і різних типів узорів. Це означає, що, описуючи локальну орієнтацію в цих зонах, ми досягнемо невеликого зменшення невизначеності ідентифікації, а в більшості випадків до її збільшення. Описувати локальну орієнтацію в базисній зоні нема сенсу, оскільки вона є однаковою для усіх типів відбитків. Лише в центральній зоні локальна орієнтація відрізняється для різних відбитків одного і, особливо, для різних типів узорів. Доцільність опису локальної орієнтації саме центральної зони підкреслюється і тим, що навколо неї формуються інші зони, тобто вони статистично залежні від неї.

Розглянемо визначення найбільш інформативної зони для кореляційного методу порівняння. Припустимо, що ідеальні узори не мають жодної особистої ознаки, далі проводимо їх порівняння. У такому випадку два відбитки одного типу і з однаковою локальною орієнтацією будуть добре корельовані. Корельованість визначає їхню подібність. Особисті ознаки ж формують у потоках папілярних ліній області нерегулярної поведінки. Кожна нерегулярність, яка розташована у потоці папілярних ліній і не присутня у двох зображеннях, що корелюються, призводить до зменшення їх подібності. Коли нерегулярність присутня в обох зображеннях, вона не змінює їх корельованості. Отже, кількість особистих ознак є непрямою мірою оцінки оптимальності вибору зони для кореляційного методу розпізнавання. Існує розподіл кількості особистих ознак для всієї

долоні [91]. Максимально багато ознак, як правило, на останній фаланзі пальця в його центральній зоні.

Проведений аналіз показує, що центральна зона відбитків є найінформативнішою, тому розроблені методи розпізнавання прив'язані до центра узору. Опрацьовано й метод визначення центра узору описаний в [61].

3.5. Система інформативних ознак зображення локальної орієнтації

Для розпізнавання зображень за їх контурами пропонують використовувати спіраль Архімеда або концентричні кола [83,89]. Ці два підходи не дадуть суттєвих результатів для дактилоскопічних зображень, оскільки точки перетину кривих (спіралі або кіл) будуть нестабільними. Девіація точок перетину може досягати декількох періодів папілярних ліній.

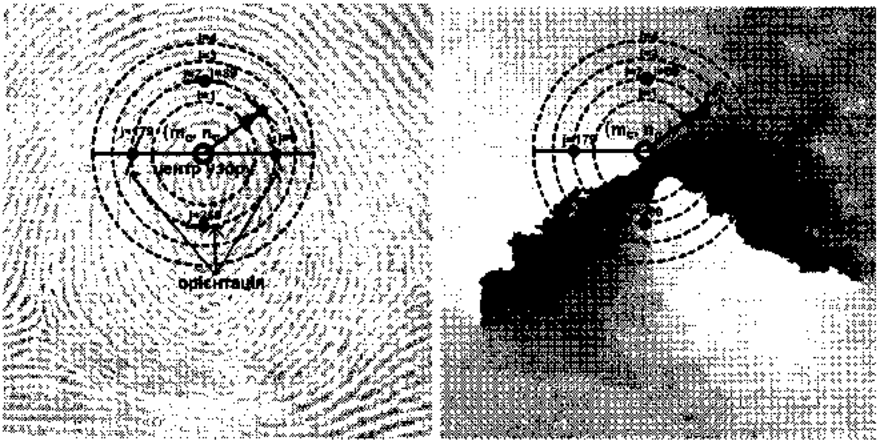
Якщо розглянути всі локальні характеристики зображень відбитків, то найбільш стійкими до шумів і геометричних спотворень є локальна орієнтація. Вона є інтегральною характеристикою узору і відображає поведінку потоків папілярних ліній. Описуючи її, ми, тим самим, оцінюємо потоки ліній, які є стійкішими формуваннями, аніж окремі папілярні лінії.

Використання концентричних кіл, розташованих у центрі узору (рис. 3.13 а), дозволяє досягти інваріантності ознак до зсуву й повороту (на етапі порівняння).

Для опису локальної орієнтації центральної зони зображення пропонуємо формувати вектор ознак із точок $c_j^{(i)}$ зображення орієнтації (рис.3.13 б), які лежать на чотирьох концентричних колах, розміщених у центрі узору відбитка.

Кола мають радіуси $R_j^{(i)}$, $i = 1,2,3,4$ – номер концентричного кола; $j = 0...359$ – номер точки на концентричному колі.

Орієнтація в самому центрі узору має велику похибку, яка викликана тим, що кут потоку папілярних ліній оцінюється шляхом усереднення напрямків градієнтів в околі, де потік є швидкозмінний. Виходячи з цього, радіус першого концентричного кола $R^{(1)} = 80$ дискретних відліків. Радіуси наступних кіл $R^{(i)} = R^{(1)} + 2\overline{\Pi}$ ($\overline{\Pi}$ – середній період папілярних ліній, який рівний 10 дискретним відлікам для зображень із роздільною здатністю 500 точок на дюйм) вибрані з огляду на те, що орієнтація папілярних ліній мало змінюється на



а) б)

Рис.3.13. Представлення концентричних кіл на дактилоскопічному зображенні (а) і зображенні локальної орієнтації (б).

віддалі одного періоду папілярних ліній, а на віддалі трьох періодів може кардинально змінитися.

Кількість точок на кожному колі вибрана однаковою для спрощення етапу порівняння векторів, а саме 360 для того, щоб оцінювати взаємну орієнтацію зображень із дискретністю в один градус.

Вектор інформативних ознак локальної орієнтації є масивом розміром 4×360, і описується так:

$$\mathbf{V}_{\text{орієнт.}} = (c_j^{(1)}, c_j^{(2)}, c_j^{(3)}, c_j^{(4)}). \qquad (3.47)$$

Оскільки на етапі попередньої обробки проводиться блочна оцінка локальної орієнтації, значення $c_j^{(i)}$ в точках концентричних кіл обчислюється ще раз. Розрахунок проводимо за формулами (3.28)-(3.32), приймаючи, що блок оцінки $\mathbf{W}_{m,n}^{(24)}$ розташований так, що його центр збігається з j-ю точкою i-го концентричного кола.

Розроблена система інформативних ознак, що базується на описі зображення локальної орієнтації, відрізняється від відомих високою стійкістю до шумів і геометричних спотворень та простотою процесу генерування вектора ознак. Такий вектор ознак характеризує потоки папілярних ліній, що іншими дослідниками робиться за допомогою класифікаційних ознак. На відміну від опису класифікаційними ознаками дана система відрізняється відсутністю суб'єктивізму і детальним описом потоків папілярних ліній.

На основі запропонованої системи інформативних ознак можна також проводити класифікацію узорів, але в цьому випадку погіршаться імовірнісні показники системи.

3.6. Система спектральних інформативних ознак

Як альтернатива класичному підходу були спроби використання просторового спектра зображення відбитка для формування ознак і розпізнавання. Одним із таких дослідників був Майк Фідді. За його методом формується вектор ознак, який інтегрально описує структуру спектра.

Непрямим способом використання спектра для опису зображення є кореляційний спосіб порівняння. Суттєвою перешкодою у його реалізації є необхідність збереження великої кількості інформації – повного зображення або його спектра. Якщо як вектор ознак зберігати спектр **f** обробленого зображення, то його розмір буде еквівалентний розмірові зображення.

Вирішення цієї проблеми базується на першій особливості зображень відбитків, а саме використання як вектора ознак не всього спектра зображення, а лише його частини, котра несе найкориснішу інформацію про зображення. Якщо розглянути спектр і типове зображення відбитка, то емпірично можемо припустити, що доцільно порівнювати складові зображення з найбільшою кореляцією відбитків одного пальця, отриманих різними способами. Шуми, як було зазначено в п. 3.1, не є інформативною складовою і належать до нестійких формувань на зображенні. Їм притаманна мінливість у часі (час між формуванням відбитків) і зміни випадкового характеру, які залежать від способу формування зображення. Як і в системі ознак [176], звертаємо увагу на інформативну область **A** (рис. 3.14), яка обмежується двома колами радіусів $r_{\min}$ і $r_{\max}$. Оскільки парно симетричні спектральні складові спектра є комплексно спряжені, то для опису зображення формуємо вектор ознак із елементів, розташованих у лівій половині області **A** (виділена жирною лінією):

$$\mathbf{V}_{\text{спектр}} = f(u,v),\ \forall(u \wedge v \in \mathbf{A}) \wedge (u < 0), \qquad (3.48)$$

де $u = -\overline{\frac{N}{2}, \frac{N}{2}}, v = -\overline{\frac{M}{2}, \frac{M}{2}}$ – дискретні відліки осей просторових частот.

Вектор ознак $\mathbf{V}_{\text{спектр}}$ описує не структуру папілярного узору, період, напрямки ліній, їх поведінку, а повне зображення. Тобто такий

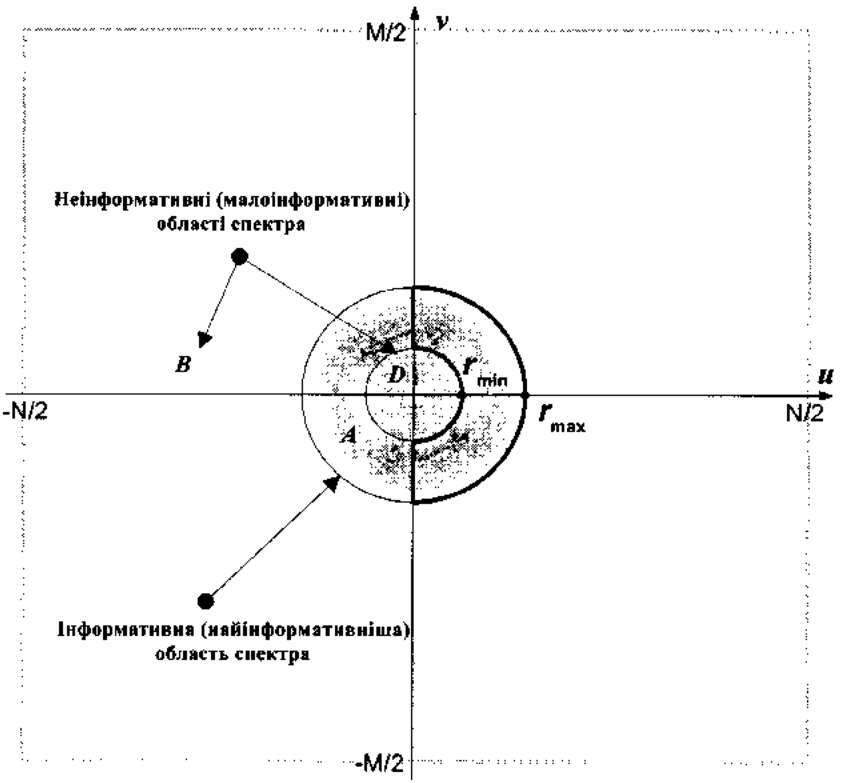
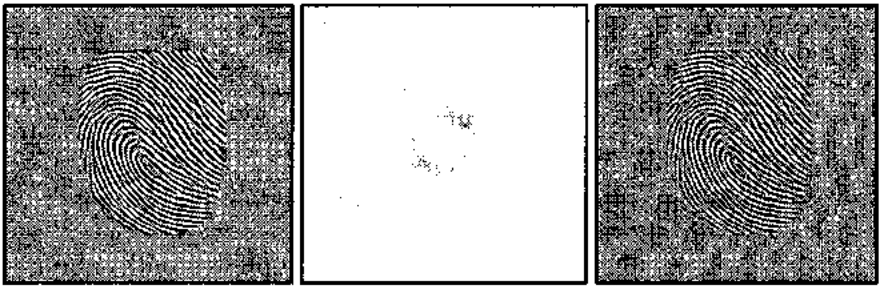


Рис.3.14. Зображення спектра та його інформативна (А) і неінформативні (В і D) області.

вектор максимально зберігає наявну на зображенні корисну інформацію. Щоб переконатися в цьому, наведемо спектр обробленого зображення та зображення, отриманого оберненим ШПФ (ОШПФ) зі спектральних складових вектора ознак $V_{спектр}$ (рис.3.15). Рисунки наочно показують, що втрати інформації про папілярні лінії є незначні і в основному стосуються високочастотних складових у регіонах аномальної поведінки папілярних ліній. Якщо розглянути такі ознаки з погляду компресії, то як і будь-який формальний опис зображення вектор ознак є не що інше, як скомпресоване зображення.

Використання вектора $V_{спектр}$ для кореляційних методів порівняння, про що мова йтиме нижче, усуває ще один недолік цих методів, а саме необхідність збереження великої кількості інформації. Завдяки тому, що корелюємо гармонічні складові, які відповідають



а) б) в)

Рис.3.15. Вхідне зображення після попередньої обробки (а) його спектр (б) і зображення (в), отримане зі спектральних складових, які формують вектор ознак (3.48).

області А спектра (рис. 3.14), досягаємо зменшення впливу шумів на результати розпізнавання [61].

3.7. Порівняння відбитків на основі системи інформативних ознак зображення локальної орієнтації

Вибираючи метод порівняння, врахуємо, що задача ідентифікації відрізняється від розпізнавання і що маємо $N_{БД}$ еталонних зображень у БД, які відповідають $N_{БД}$ класам за термінами теорії розпізнавання. Інший важливий фактор, який слід брати до уваги, – відсутність статистичних даних про відбитки, а отже, методи розпізнавання, в яких вони необхідні, не підходять для цієї задачі. Це накладає певні обмеження на вибір методу порівняння векторів $\mathbf{V}_{орієнт.}$, описаних формулою (3.47). Потрібно також врахувати, що зображення відбитків одного і того ж пальця будуть групуватися в просторі зображень навколо його ідеального зображення $\hat{g}$.

Проведений аналіз вказує, що для цього етапу можна застосовувати методи, базовані на віддалі в просторі ознак або різниці між векторами. Описані методи розпізнавання на основі віддалей у просторі ознак не можуть бути використані, оскільки збільшують обчислювальні затрати і є чутливими до збоїв оцінки локальної орієнтації. Вибір між віддаллю в просторі ознак і середньою різницею між елементами векторів зроблений на користь другого, бо декілька елементів вектора, які відповідають області зображення зі збійною оцінкою орієнтації, призводять до значного зростання віддалі, але невеликого зростання середньої різниці. Таку ситуацію необхідно

обов'язково враховувати через те, що в реальних системах вона зустрічається часто.

Вибір зупинено на середній різниці між двома векторами $\mathbf{V}_{\text{орієнт. вх.}}$ – для вхідного зображення і $\mathbf{V}_{\text{орієнт. етал.}}$ – для еталонних зображень у БД, яка обчислюється таким чином:

$$\overline{\Delta}_{\text{орієнт.}} = \frac{1}{N_{\text{орієнт}}} \sum_{i=0}^{4} \sum_{j=0}^{359} \left(V_{\text{орієнт. вх.}}(i,j) - V_{\text{орієнт етал.}}(i,j) \right), \qquad (3.49)$$

де $N_{\text{орієнт}} = 1440$ – кількість елементів векторів описаних, формулою (3.47).

Поворот зображення відносно еталонного викликає циклічний зсув елементів рядків вектора. Тобто поворот зображення на k градусів спричинить циклічний зсув елементів вектора $\mathbf{V}_{\text{орієнт. етал.}}$ на k позицій і формування вектора $\mathbf{V}_{\text{орієнт. вих.}}$, як це відображено на рис.3.16.

Для досягнення інваріантності до повороту необхідно обчислювати різницю (3.49) для циклічно зсунутих векторів і вибрати мінімальну величину $\overline{\Delta}_{\text{орієнт.}}$. Таким чином, різницю (3.49) між двома векторами інформативних ознак $\mathbf{V}_{\text{орієнт. вх.}}$ і $\mathbf{V}_{\text{орієнт. етал.}}$ слід визначати так:

$$\overline{\Delta}_{\text{орієнт.}} = \frac{1}{N_{\text{орієнт.}}} \min_{shift=-G,G} \left\{ \sum_{i=0}^{4} \sum_{j=0}^{359} \left(\begin{matrix} V_{\text{орієнт. вх.}}\left(i,(j+shift+360) \bmod 360\right) \\ -V_{\text{орієнт. етал.}}(i,j) \end{matrix} \right) \right\}, \qquad (3.50)$$

де G – кут у градусах, який окреслює межі інваріантності до повороту. Це значить, що, задавши значення кута G, отримуємо інваріантність першого етапу розпізнавання до повороту зображень у межах [- G,G].

Додатково пропонується встановлювати орієнтацію вхідного зображення відносно еталонного. Для цього обчислюється значення *shift*, для якого різниця мінімальна

$$\theta_{\text{вх.-етал.}} = shift;\ \overline{\Delta}_{\text{орієнт}} = \frac{1}{N_{\text{орієнт}}} \sum_{i=0}^{4} \sum_{j=0}^{359} \left(\begin{matrix} V_{\text{орієнт вх.}}\left(i,(j+shift+360) \bmod 360\right) \\ -V_{\text{орієнт етал.}}(i,j) \end{matrix} \right), \qquad (3.51)$$

$$shift \in [-G,G].$$

Отже, результатом порівняння першого етапу буде не тільки міра різниці між двома векторами ознак, яка відповідає мірі різниці між двома зображеннями локальної орієнтації, але й кут орієнтації вхідного зображення відносно іншого. Цей кут буде задіяно в наступному етапі порівняння для зменшення обчислювальних затрат.

$V_{орієнт\ етал.}(i,j)$

	j=0	j=1							j=358	j=359	
i=0	1	2	3	...	k-1	k	k+1	...	358	359	360
i=1	1	2	3	...	k-1	k	k+1	...	358	359	360
i=2	1	2	3	...	k-1	k	k+1	...	358	359	360
i=3	1	2	3	...	k-1	k	k+1	...	358	359	360

а)

$V_{орієнт\ пов.}(i,j)$

	j=0	j=1							j=358	j=359	
i=0	360-k+1	360-k+2	360-k+3	...	360	1	2	...	358-k	359-k	360-k
i=1	360-k+1	360-k+2	360-k+2	...	360	1	2	...	358-k	359-k	360-k
i=2	360-k+1	360-k+2	360-k+2	...	360	1	2	...	358-k	359-k	360-k
i=3	360-k+1	360-k+2	360-k+2	...	360	1	2	...	358-k	359-k	360-k

б)

Рис.3.16. Масив індексів вектора $\mathbf{V}_{орієнт.\ пов.}$ (б) зображення, яке повернуте на k градусів відносно іншого, представленого масивом вектора $\mathbf{V}_{орієнт.\ етал.}$ (а).

Усі розглянуті у першому розділі методи порівняння передбачають використання незмінного порога ідентифікації відбитка. На противагу такому методу пропонуємо застосовувати адаптивний поріг, адже задачею першого етапу порівняння є не стільки ідентифікація, скільки зменшення кандидатів для порівняння другим етапом.

Для адаптивного вибору порогу доцільно ввести об'єктивну кількісну оцінку якості зображення, а точніше – центральної області узору, для якої формується вектор $\mathbf{V}_{орієнт.\ вх.}$. Врахувавши першу особливість дактилоскопічних зображень (п.3.1), зробимо припущення, що якість зображення можна оцінювати потужністю спектральних складових спектра в області **A** (рис.3.14). Оскільки вектор $\mathbf{V}_{орієнт.\ вх.}$ описує локальну орієнтацію в центральній області, то необхідно оцінювати якість за спектром центральної області. Формула для чисельної оцінки якості матиме такий вигляд:

$$Q = \sum_{(i_c, j_c) \in A_{центр}} f_{центр}(i_c, j_c)^2, \qquad (3.52)$$

де $\mathbf{f}_{центр}$ – спектр центрального околу; $\mathbf{A}_{центр}$ – область корисних складових спектра $\mathbf{f}_{центр}$, аналогічна до області **A** спектра **f** (рис.3.14).

Обґрунтуємо застосування оцінки якості зображення. Такий спосіб оцінки можливий виходячи з того, що після попередньої обробки, зокрема спрямованої фільтрації, області зі спотвореннями (наприклад, змазування і злипання ліній) мають меншу потужність яскравості (тут і далі не враховуватимемо потужності постійної складової). Це пояснюється особливістю фільтра Габора. Після обробки ним області з відсутніми папілярними лініями матимуть $Q \to 0$. Водночас з тим, у випадку збою оцінки орієнтації фільтр Габора буде придушувати папілярні лінії, що призведе до зменшення потужності спектральних складових в області $\mathbf{A}_{\text{центр}}$. Збій оцінки орієнтації означає, що зображення локальної орієнтації має меншу якість. Отже, наведені приклади свідчать, що якість зображення (3.52) взаємопов'язана з якістю зображення локальної орієнтації. Тому, оцінюючи її за такою формулою, ми отримуємо якість узору відбитка (його локальної орієнтації й структури папілярних ліній).

На наступному кроці визначимося, який поріг необхідно адаптувати. Ввівши поняття якості, відразу можемо стверджувати, що зображення з максимальною якістю повинні забезпечувати мінімальне значення $\overline{\Delta}_{орієнт.}$ під час порівняння з його еталоном у БД. Тобто, якщо $Q \to Q_{\max}$ ($Q_{\max}$ – максимальна якість зображення, яка визначається максимально можливою потужністю яскравості зображення папілярних ліній), величина $\overline{\Delta}_{орієнт.} \to 0$ (коли порівнюються два зображення одного папілярного узору). В реальних задачах необхідно враховувати, що оцінка локальної орієнтації має похибку, викликану шумами, збоями оцінки і геометричними спотвореннями узору. І тому при $Q \to Q_{\max}$ – $\overline{\Delta}_{орієнт.} \to \overline{\Delta}_{орієнт.\min.}$. Адаптацію слід проводити до якості вхідного зображення, адже якість еталонного повинна бути високою (такі вимоги до ДБС).

Позначимо через $\overline{\Delta}_{орієнт.вх-еталон}$ різницю між векторами вхідного зображення і його еталоном із БД, а через $\overline{\Delta}_{орієнт.вх.min}$ мінімальну різницю між вектором вхідного зображення і будь-яким іншим еталонним, крім такого, що відповідає вхідному зображенню.

Що будемо розуміти під збоєм оцінки орієнтації? Збій – це значна похибка в оцінці орієнтації, яка локалізована в деякій області зображення і виникла через, наприклад, пошкодження, бруд, що присутні на пальці. В такому випадку збій є неконтрольованим

процесом, а оскільки орієнтація папілярних ліній статистично взаємозв'язана, то він порушує ці зв'язки. Кожен узор має унікальну картину потоків папілярних ліній, які характеризуються локальною орієнтацією. Особливістю потоків є те, що вони взаємозв'язані і не можуть змінювати свого напрямку довільним чином. А, отже, збій, який порушує взаємозв'язок між потоками, створює таку картину локальної орієнтації в області його дії, яка не притаманна жодному іншому узорові відбитка пальця. Це, у свою чергу, значить, що збій у своїй основі збільшуватиме різницю $\overline{\Delta}_{орієнт.вх.\min}$, бо подібної зони збою не буде на жодному з еталонних зображень. На рис.3.17 представлено можливий варіант збою оцінки орієнтації, викликаний зморшкою і пошкодженнями узору.

Іншим фактором, який спричиняє зміну локальної орієнтації, є нелінійні геометричні спотворення ("губка"). У цьому випадку орієнтація в одній і тій же точці на вхідному зображенні з геометричними спотвореннями та еталонному зображенні буде незначно відрізнятися. Тобто такі спотворення не порушують статистичних взаємозв'язків потоків папілярних ліній і цілісності картини локальної орієнтації. Цілком можливі ситуації, коли зростає $\overline{\Delta}_{орієнт.вх-еталон}$ і зменшується $\overline{\Delta}_{орієнт.вх.\min}$, оскільки геометричні нелінійні спотворення можуть призводити до того, що локальна орієнтація вхідного зображення буде подібна до орієнтації іншого відбитка з БД, який відповідає вхідному.

Найпростішим варіантом вибору адаптивного порога є адаптація його до якості зображення, тобто поріг буде функцією

$$\overline{\Delta}_{орієнт.пор.}(Q) = a_{\Delta_{орієнт.}} + \frac{b_{\Delta_{орієнт.}}}{Q}, \qquad (3.53)$$

де $a_{\Delta_{орієнт.}}, b_{\Delta_{орієнт.}}$ – параметри функції, які відповідають за адаптацію порога. Через те, що геометричні спотворення не змінюють якості зображення, за адаптацію до них відповідає величина $a_{\Delta_{орієнт.}}$. Оскільки збої оцінки орієнтації зумовлюють зменшення якості Q, то і за адаптацію до них відповідатиме величина $b_{\Delta_{орієнт.}}$.

Розглянемо ситуацію, коли вхідне зображення характеризується збоєм під час оцінки локальної орієнтації. На першому етапі розпізнавання ми маємо значення якості зображення, але не знаємо, наскільки відрізняється орієнтація в області збою від істинної. Наведемо приклад. Ситуація перша: нехай у певній зоні зображення є

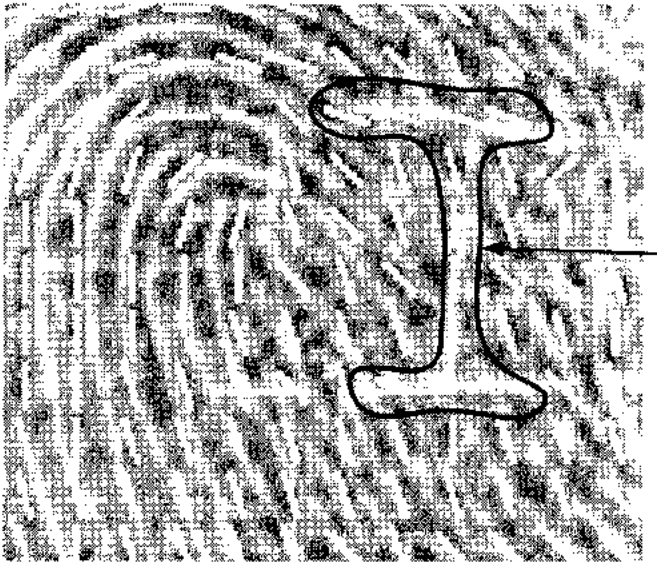


Рис.3.17. Збій в оцінці локальної орієнтації папілярних ліній.

збій оцінки, який характеризується похибкою орієнтації 70 градусів. Зважаючи на спрямовані характеристики фільтра Габора, папілярні лінії у цій області будуть повністю придушені й зображення матиме якість Q_1. Різниця (3.50) для вхідного зображення і його еталона становитиме $\overline{\Delta}_{орієнт.1}$. Ситуація друга: в певній зоні зображення є збій оцінки, який характеризується похибкою орієнтації 90 градусів. І за цих обставин папілярні лінії будуть повністю подавлені фільтром Габора і зображення матиме якість $Q_2 \approx Q_1$. Різниця (3.50) для вхідного зображення і його еталона складатиме $\overline{\Delta}_{орієнт.2}$, а оскільки похибка орієнтації більша, то і $\overline{\Delta}_{орієнт.2} > \overline{\Delta}_{орієнт.1}$. Не виключена ситуація, коли $\overline{\Delta}_{орієнт.1} < \overline{\Delta}_{орієнт.пор}(Q_1)$, а $\overline{\Delta}_{орієнт.2} > \overline{\Delta}_{орієнт.пор}(Q_2)$, і тоді в першій ситуації суперечимо першому критерієві з п.1.4, що є неприпустимо.

Врахуємо особливість збоїв для кращої адаптації порога до них. Розіб'ємо різниці $\overline{\Delta}_{орієнт.вх-еталон}$ і $\overline{\Delta}_{орієнт.вх.min}$ на два доданки:

$$\overline{\Delta}_{орієнт.вх-еталон} = \overline{\Delta}_{орієнт.вх-еталон\ обл.зб.} + \overline{\Delta}_{орієнт.вх-еталон\ решта}, \quad (3.54)$$

$$\overline{\Delta}_{орієнт.вх.min} = \overline{\Delta}_{орієнт.вх.min\ обл.зб.} + \overline{\Delta}_{орієнт.вх.min\ решта}, \quad (3.55)$$

де $\overline{\Delta}_{орієнт.вх-еталон\ обл.зб.}$, $\overline{\Delta}_{орієнт.вх.\min\ обл.зб.}$ – складові, які відповідають різниці елементів векторів, що описують орієнтацію в області збійної оцінки, $\overline{\Delta}_{орієнт.вх-еталон\ решта}$, $\overline{\Delta}_{орієнт.вх.\min решта}$ – складові, які відповідають різниці елементів векторів, що описують орієнтацію в області коректної оцінки.

Оскільки $\overline{\Delta}_{орієнт.вх-еталон\ решта}$ і $\overline{\Delta}_{орієнт.вх.\min решта}$ описують орієнтацію в незбійній області, а $\overline{\Delta}_{орієнт.вх.\min решта}$ відповідає похибці порівняння вхідного зображення не з його еталоном, то справедлива нерівність $\overline{\Delta}_{орієнт.вх-еталон\ решта} << \overline{\Delta}_{орієнт.вх.\min решта}$.

Величини $\overline{\Delta}_{орієнт.вх-еталон\ обл.зб.}$ і $\overline{\Delta}_{орієнт.вх.\min обл.зб.}$ подібні, оскільки імовірність того, що збій призведе до такого спотворення картини локальної орієнтації, що опис її в області збою буде подібний до опису орієнтації іншого зображення, прямує до нуля. На основі такого порівняння можемо чітко стверджувати, що зображення зі збоєм в оцінці орієнтації матиме різницю, визначену за формулою (3.50), мінімальну порівняно з його еталоном у БД.

На підставі проведеного аналізу збоїв і поведінки різниці (3.50) пропонуємо обчислювати адаптивний поріг за іншою формулою:

$$\overline{\Delta}_{орієнт.пор.}(Q,\overline{\Delta}_{орієнт.\min}) = \overline{\Delta}_{орієнт.\min} + a_{\Delta_{орієнт.}} + \frac{b_{\Delta_{орієнт.}}}{Q}. \qquad (3.56)$$

Запропонований адаптивний поріг (3.56) враховує проаналізовані впливи збоїв і геометричних спотворень на локальну орієнтацію. Як і в попередній формулі (3.50), константа $a_{\Delta_{орієнт.}}$ відповідає за адаптацію до різниці орієнтації, викликаної геометричними спотвореннями, а $\overline{\Delta}_{орієнт.\min}$ і $b_{\Delta_{орієнт.}}$ дозволяють адаптувати поріг до збоїв в оцінці орієнтації і якості зображення.

Для практичної реалізації необхідно знати константи $a_{\Delta_{орієнт.}}$, $b_{\Delta_{орієнт.}}$. Визначення їх проводиться за першим критерієм із п.3.3, що буде описано далі.

Підсумовуючи сказане, наведемо основні особливості застосування методу порівняння за різницею (3.50) з адаптивним порогом (3.56).

1. Якщо відповідно підібрати параметри виразу (3.56), метод порівняння за ознаками зображення локальної орієнтації забезпечить виконання першого критерію (п.1.4) і буде оптимізований за другим.

2. Обчислення міри різниці між векторами за формулою (3.50) дозволяє досягти інваріантності до повороту й одночасно оцінити кут повороту зображень за рівнянням (3.51). Цей кут буде використаний у другому етапі порівняння з метою пришвидшення його роботи.

3.8. Порівняння відбитків на основі системи спектральних ознак і кореляційного методу

Класичні кореляційні методи розпізнавання базуються на кореляції двох векторів ознак. В оптичних пристроях розпізнавання використовуються методи, що грунтуються на коефіцієнті взаємної кореляції двох зображень.

Кореляційні методи розпізнавання дозволяють вирішити дві задачі:

- розпізнавання зображення шляхом порівняння його з еталонним;
- визначення зміщення зображення, яке розпізнається, відносно еталонного.

В основу ж розробленого методу покладена формула нормованої взаємної кореляції двох зображень $g_{вх.}(x,y)$ і $g_{еталон}(x,y)$. У просторовій області вона записується виразом [76,86,88]:

$$K(x,y)=\frac{\int\limits_{-\infty-\infty}^{\infty\ \infty} g_{вх.}(x,y)g_{еталон}(x+x',y+y')dx'dy'}{E_{вх.}E_{еталон}}, \qquad (3.57)$$

$$E_{вх.}=\sqrt{\int\limits_{-\infty-\infty}^{\infty\ \infty} g_{вх.}(x,y)^2\,dxdy}=\sqrt{\int\limits_{-\infty-\infty}^{\infty\ \infty} f_{вх.}(\omega_x,\omega_y)^2\,d\omega_x d\omega_x},$$

$$E_{еталон}=\sqrt{\int\limits_{-\infty-\infty}^{\infty\ \infty} g_{еталон}(x,y)^2\,dxdy}=\sqrt{\int\limits_{-\infty-\infty}^{\infty\ \infty} f_{еталон}(\omega_x,\omega_y)^2\,d\omega_x d\omega_x},$$

де $f_{вх.}(\omega_x,\omega_y), f_{еталон}(\omega_x,\omega_y)$ – просторові спектри зображень $g_{вх.}(x,y)$ і $g_{еталон}(x,y)$; $E_{вх.}, E_{еталон}$ – енергії зображень $g_{вх.}(x,y)$ і $g_{еталон}(x,y)$.

З урахуванням теореми Парсеваля і теореми кореляції [29,248], вираз (3.57) у частотній області набуде вигляд:

$$K(\omega_x,\omega_y)=\frac{f_{вх.}(\omega_x,\omega_y)f_{еталон}{}^{*}(\omega_x,\omega_y)}{E_{вх.}E_{еталон}}, \qquad (3.58)$$

де $K(\omega_x,\omega_y)$ – частотний образ взаємокореляційної функції; $f_{еталон}^{*}(\omega_x,\omega_y)$ – комплексно спряжений спектр до $f_{еталон}(\omega_x,\omega_y)$.

Застосування формул кореляції (3.57) або (3.58) призведе до великої кореляції постійних складових зображень, що, своєю чергою, дасть неправильні результати порівняння зображень. Тому її усуваємо з процесу порівняння. Врахувавши сказане змінимо формулу (3.57):

$$K(x,y)=\frac{\int\limits_{-\infty-\infty}^{\infty\ \infty}(g_{вх.}(x,y)-\overline{g}_{вх.})(g_{еталон}(x+x',y+y')-\overline{g}_{еталон})dx'dy'}{E_{вх.0}E_{еталон0}}, \quad (3.59)$$

$$E_{вх.0}=\sqrt{\int\limits_{-\infty-\infty}^{\infty\ \infty}(g_{вх.}(x,y)-\overline{g}_{вх.})^2\,dxdy}=$$

$$=\sqrt{\int\limits_{-\infty-\infty}^{\infty\ \infty}f_{вх.}(\omega_x,\omega_y)^2\,d\omega_x d\omega_y-f_{вх.}(0,0)^2},$$

$$E_{еталон\,0}=\sqrt{\int\limits_{-\infty-\infty}^{\infty\ \infty}(g_{еталон}(x,y)-\overline{g}_{еталон})^2\,dxdy}=$$

$$=\sqrt{\int\limits_{-\infty-\infty}^{\infty\ \infty}f_{еталон}(\omega_x,\omega_y)^2\,d\omega_x d\omega_y-f_{еталон}(0,0)^2},$$

де $\overline{g}_{вх.},\overline{g}_{еталон}$ – постійні складові яскравості зображень; $E_{вх.0}$, $E_{еталон\,0}$ – енергії зображень $g_{вх.}(x,y)$ і $g_{еталон}(x,y)$ без урахування постійної складової. В частотному просторі вираз (3.59) матиме вигляд:

$$K(\omega_x,\omega_y)=\begin{cases}\dfrac{f_{вх.}(\omega_x,\omega_y)f_{еталон}^{*}(\omega_x,\omega_y)}{E_{вх.0}E_{еталон\,0}}; & \omega_x\wedge\omega_y\neq 0,\\ 0; & \omega_x\wedge\omega_y=0.\end{cases} \quad (3.60)$$

Проаналізуємо перший випадок, коли порівнюємо однакові зображення $g_{вх.}(x,y)=g_{еталон}(x,y)$. Тоді пік взаємокореляційної функції (3.59) буде розташований у точці з координатою (0,0) і рівний одиниці. Нормуючий множник буде рівний $E_{еталон\,0}^{\ 2}$.

Розглянемо тепер другий випадок, коли зображення $g_{вх.}(x,y)$ є частиною $g_{еталон}(x,y)$ (рис. 3.18). Тобто $g_{еталон}(x,y)\supset g_{вх.}(x,y)$. Тоді, в ідеалі (коли однакові значення локального середньоквадратичного відхилення яскравості в інформативних областях, що відповідає

однаковій локальній енергії зображення), отримаємо ситуацію, коли енергія $E_{вх.0} < E_{еталон\,0}$ у стільки разів, у скільки площа зображення $g_{вх.}(x,y)$ менша від площі зображення $g_{еталон}(x,y)$. Припустимо, що інформативна область **Z** зображення $g_{вх.}(x,y)$ в $n_{ZZ'}$ разів менша від інформативної області **Ξ** зображення $g_{еталон}(x,y)$. Отже, нормуючий знаменник $E_{вх.0}E_{еталон\,0}$ взаємокореляційної функції (3.59) буде менший у $n_{ZZ'}$ разів від нормуючого знаменника $E_{еталон\,0}^{\ 2}$ як у першому випадку. Враховуючи, що взаємокореляція інформативної області буде відбуватися в області зображення $\mathbf{Z}' \supset \mathbf{\Xi}$ (виділена штриховою лінією на рис.3.18), яка дорівнює області **Z** зображення $g_{вх.}(x,y)$, то значення чисельника у формулі (3.59) взаємокореляційної функції зменшиться в $n_{ZZ'}^{\ 2}$ разів. У сукупності зі зменшенням знаменника максимум взаємокореляційної функції зменшиться в $n_{ZZ'}$ разів. Ці твердження справедливі, коли яскравість кожної точки однакова для виразу (3.57) або однакова локальна дисперсія яскравості для виразу (3.59).

На практиці доволі важко сформувати відбитки з однаковими інформативними зонами, отже, при відбитті того ж папілярного узору, але меншою мірою, буде зменшуватись коефіцієнт кореляції

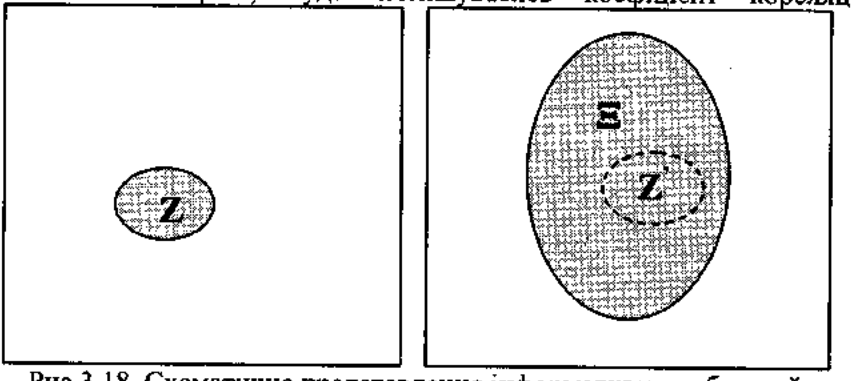


Рис.3.18. Схематичне представлення інформативних областей зображення $g_{вх.}(x,y)$ і $g_{еталон}(x,y)$.

зображень. Загалом таке твердження є справедливе, але і неприйнятне для ДБС, оскільки переважно доводиться порівнювати менше вхідне зображення (сліду) з більшим (відбиток із дактилокарти або еталон з БД). Вихід із цієї ситуації знайдений на основі припущення, що локальна дисперсія зображення папілярного візерунка є однаковою у

всій інформативній зоні зображення (це характерно для зображень із періодичною структурою, таких як колова дифракційна ґратка й паралельні папілярні лінії) і що з певними похибками (не більше 10%) забезпечується ПОЗ. Неточності цього твердження, в основному, спостерігаються в зонах аномальної поведінки ліній. Отже, запропонована вище попередня обробка забезпечує не тільки покращання структури папілярних ліній, а й забезпечує необхідні для розпізнавання характеристики зображення.

Враховуючи зроблені припущення, можемо вважати, що енергії зображення в областях **Z** і **Z**' рівні, тому формулу (3.59) переписуємо так:

$$K(x,y)=\frac{\int\limits_{-\infty}^{\infty}\int\limits_{-\infty}^{\infty}(g_{вх.}(x,y)-\overline{g}_{вх.})(g_{еталон}(x+x',y+y')-\overline{g}_{еталон})dx'dy'}{E_{вх.0}{}^{2}}. \quad (3.61)$$

Обчислений за формулою (3.61) коефіцієнт взаємної кореляції буде рівний одиниці, якщо $g_{еталон}(x,y)\subset g_{вх.}(x,y)$.

Узагальнивши задачу та розширивши можливості методу до порівняння як меншого фрагмента на великому $g_{еталон}(x,y)\subset g_{вх.}(x,y)$, так і вхідного зображення з більшою інформативною областю із зображенням із меншою інформативною областю $g_{вх.}(x,y)\subset g_{еталон}(x,y)$, вираз взаємокореляційної функції (3.61) представимо як

$$g_{вх.}(x,y), \quad (3.62)$$

а в частотній області вираз (3.60) зведемо до вигляду

$$K(\omega_x,\omega_y)=\begin{cases}\dfrac{f_{вх.}(\omega_x,\omega_y)f_{еталон}{}^{*}(\omega_x,\omega_y)}{\min(E_{вх.0}{}^{2},E_{еталон\,0}{}^{2})}; & \omega_x\wedge\omega_y\neq 0,\\ 0; & \omega_x\wedge\omega_y=0.\end{cases} \quad (3.63)$$

Вираз (3.63) для просторових спектрів $f_{вх.}(u,v), f_{еталон}(u,v)$ дискретних зображень $g_{вх.}(i,j)$ і $g_{еталон}(i,j)$ запишеться так:

$$K(u,v)=\begin{cases}\dfrac{f_{вх.}(u,v)f_{еталон}{}^{*}(u,v)}{\sqrt{\min\left(\begin{array}{l}\sum\limits_{u=1}^{M}\sum\limits_{v=1}^{N}\left(f_{вх.}(u,v)\right)^2-f_{вх.}(0,0)^2,\\ \sum\limits_{u=1}^{M}\sum\limits_{v=1}^{N}\left(f_{еталон}(u,v)\right)^2-f_{еталон}(0,0)^2\end{array}\right)}}; & u\wedge v\neq 0,\\ 0; & u\wedge v=0.\end{cases} \quad (3.64)$$

Звідки отримаємо вираз для порівняння відбитків за спектральними ознаками (3.48).

Маючи вектор спектральних ознак і знаючи, яким складовим спектра з області **A** (рис. 3.14) вони відповідають, можемо відновити основні спектральні складові зображення. Така задача є оберненою до задачі формування вектора ознак, а в термінах теорії компресії зображень відповідає декомпресії.

Оскільки парно симетричні складові спектра є комплексно спряжені, а у формулі (3.64) усі складові спектра вхідного зображення перемножуються зі складовими спектра еталонного, то парно симетричні складові спектра взаємокореляційної функції $K(u,v)$ теж будуть комплексно спряжені. Цю властивість використано для зменшення кількості операцій множення. Для цього обчислюємо добуток елементів двох векторів $\mathbf{V}_{\text{спектр. вх.}}$ та $\mathbf{V}_{\text{спектр. еталон}}$, що описують зображення $g_{вх}$ та $g_{еталон}$, і з нього формуємо спектр дискретної взаємокореляційної функції:

$$K\left(inv_u(l), inv_v(l)\right) = \frac{D_{доб.інф.скл.}(l)}{\min(E_{вх.0}^{інф.скл.\,2}, E_{еталон\,0}^{інф.скл.\,2})}, l = \overline{1, N_{спектр.}}, \tag{3.65}$$

$$K\left(-inv_u(l), -inv_v(l)\right) = \frac{D^{*}_{доб.інф.скл.}(l)}{\min(E_{вх.0}^{інф.скл.}, E_{еталон\,0}^{інф.скл.})}, \; l = \overline{1, N_{спектр.}}, \tag{3.66}$$

$$D_{доб.інф.скл.}(l) = V_{спектр.вх.}(l) V^{*}_{спектр.еталон}(l), \tag{3.67}$$

$$E_{вх.0}^{інф.скл.} = \sqrt{2\sum_{l=1}^{N_{спектр}} V_{спектр.вх.}(l)^2}, \tag{3.68}$$

$$E_{еталон0}^{інф\ скл} = \sqrt{2\sum_{l=1}^{N_{спектр}} V_{спектр.еталон}(l)^2}, \tag{3.69}$$

де $D_{доб.інф.скл.}(l)$ – добуток елементів векторів спектральних ознак (половини області **A** рис.3.14), що відповідає добутку найбільш інформативних складових зображень; $E_{вх.0}^{інф.скл.}$ і $E_{еталон0}^{інф.скл.}$ – енергії спектрів (їх найбільш інформативних складових) або зображень, які були б відновлені з їх спектральних ознак; $\mathbf{inv}_u$, $\mathbf{inv}_v$ – масиви індексів рядків і стовпців елементів області **A** (рис.3.14), які були занесені у вектори спектральних ознак. Множення на два під час обчислення енергій необхідне через те, що енергія визначається за половиною спектральних складових, які задіяні у формулах (3.65)-(3.67).

Таким чином, формули (3.65)-(3.69) дозволять оцінювати спектр взаємокореляційної функції за спектральними складовими, представленими у векторах ознак, що і необхідно було зробити.

Для того, щоб максимально зменшити обчислювальні затрати, а саме кількості операцій ділення, виконуватимемо операцію нормування не цілої функції, а її піка.

Остаточно формули для обчислення міри подібності двох зображень запишуться так:

$$K\left(inv_u(l), inv_v(l)\right) = D_{доб.інф.ел.}(l), l = \overline{1, N_{спектр.}}, \quad (3.70)$$

$$K\left(-inv_u(l), -inv_v(l)\right) = D_{доб.інф.ел.}^{*}(l), \; l = \overline{1, N_{спектр.}}, \quad (3.71)$$

$$K(i,j) = \Im^{-1} K(u,v), \quad (3.72)$$

$$K_{пік} = \frac{1}{\min\left(E_{вх.0}^{інф.скл.}, E_{еталон\,0}^{інф.скл.}\right)^2} \max_{\substack{i=\overline{1,M} \\ j=\overline{1,N}}} \left(K(i,j)\right). \quad (3.73)$$

За формулами (3.67)-(3.71) формується спектр $K(u,v)$ взаємокореляційної функції. Далі за допомогою ОШПФ $\Im^{-1}$ знаходиться взаємокореляційна функція $K(i,j)$. На підставі виразу (3.73) визначимо пік $K_{пік}$ і нормуємо його. Одночасно встановлюємо координати $(i_{пік}, j_{пік})$ піка

$$i_{пік} = i, j_{пік} = j; \; K_{пік} = \frac{1}{\min\left(E_{вх.0}^{інф.скл.}, E_{еталон\,0}^{інф.скл.}\right)} \left(K(i,j)\right); \forall i \in [1,N] \wedge j \in [1,M], \quad (3.74)$$

які відповідають зміщенню одного зображення відносно іншого.

Отже, результатом порівняння на другому етапі є міра подібності двох зображень, яка рівна коефіцієнту кореляції $K_{пік}$ (3.73), і зміщення зображень одне відносно іншого (3.74).

Використання для обчислень кореляційної функції елементів векторів спектральних ознак дозволяє не тільки зменшити об'єм інформації, яку необхідно зберігати в БД, але й оцінювати кореляцію за найбільш інформативними спектральними складовими зображень. Застосувавши кореляційний метод, таким чином додатково усуваємо НЧ складові спектрів із процесу порівняння, які є сильнокорельовані для зображень різних відбитків. Видалення ВЧ складових, підвищує ступінь взаємної кореляції зображень однакових відбитків, оскільки виключаються з процесу порівняння слабокорельовані ВЧ шуми зображень.

Отже, поєднання спектральних ознак і кореляційного методу дозволило максимально адаптувати його до задачі порівняння дактилоскопічних зображень.

Спосіб усунення неінваріантності цього методу до повороту буде розглянутий нижче.

Одночасне поєднання розроблених методів і векторів ознак дає можливість зберегти переваги кореляційних методів порівняння й позбутися їх недоліків [61].

3.9. Особливості реалізації попередньої обробки дактилоскопічних зображень

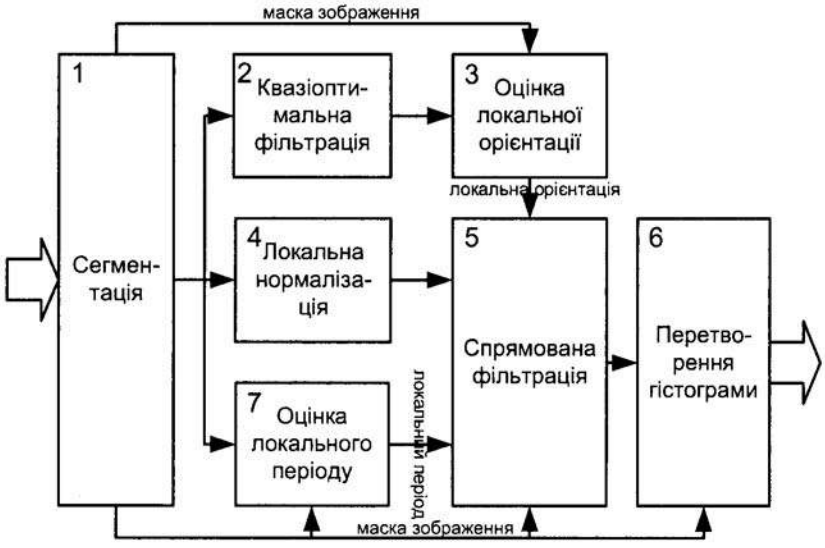
На підставі описаних вище методів, розроблено два типи ПОЗ – для БІС і АДІС (рис.3.19 а, б; головне вікно програми – рис.3.20). Попередню обробку побудовано таким чином, щоб забезпечити максимальне наближення параметрів реального зображення до ідеального. Опишемо коротко їхню роботу.

Вхідне зображення g (рис.3.21 а) проходить сегментацію в блоці №1, де зображення розбивається на інформативну Ψ і неінформативну Ξ зони. Елементам фонової області Ξ присвоюється середнє значення яскравості, яке обчислюється в межах зони Ψ. Це зроблено для того, щоб не появлялися спектральні складові з наднизькими просторовими частотами. Сегментація проводиться методом, описаним у п.3.2.1, за яким обчислюється маска зображення **mask** (рис.3.21 б). На виході отримуємо зображення g_1.

Для точнішої оцінки зображення локальної орієнтації сегментоване зображення g_1 подається на блок №2 квазіоптимальної фільтрації з адаптивною смугою пропускання, яка описана в п.3.2.2. Це дозволяє усунути НЧ і СЧ шуми, тим самим підвищити точність оцінки орієнтації. Профільтроване зображення g_2 (рис.3.21 в) подається на блок №3 оцінки зображення локальної орієнтації папілярних ліній. Паралельно оцінений глобальний період папілярних ліній подається на блок спрямованої фільтрації (для БІС). Оцінка зображення локальної орієнтації Θ проводиться за формулами (3.28)-(3.32). Зображення локальної орієнтації представлено на рис.3.21 г.

Сегментоване зображення g_1 також подається на блок №4 локальної нормалізації, в якому частково усуваються спотворення нерівномірного контакту з поверхнею. На виході отримуємо зображення g_3 (рис.3.21 д). Процедура локальної нормалізації перед

а)



б)

Рис. 3.19. Блок-схеми ПОЗ для БІС (а) та АДІС (б).

локальною оцінкою орієнтації й періоду є недоцільною, оскільки підвищиться вплив спотворених областей на результати оцінки. У випадку подачі на оцінювачі ненормалізованих зображень області дії спотворень нерівномірного контакту матимуть малі значення векторів градієнтів і енергію спектральних складових, а отже, під час оцінки їх вплив буде меншим. Завдяки такій побудові реалізовано вагові методи оцінки, в яких області з якісним узором чинитимуть більший вплив на оцінку орієнтації й періоду, ніж області з поганим узором.

В ПОЗ для АДІС сегментоване зображення g_1 подається на блок №7 оцінки локального періоду. Блок здійснює оцінку методом, описаним у п.3.2.5. Визначений період **П** подається в блок №5 спрямованої фільтрації.

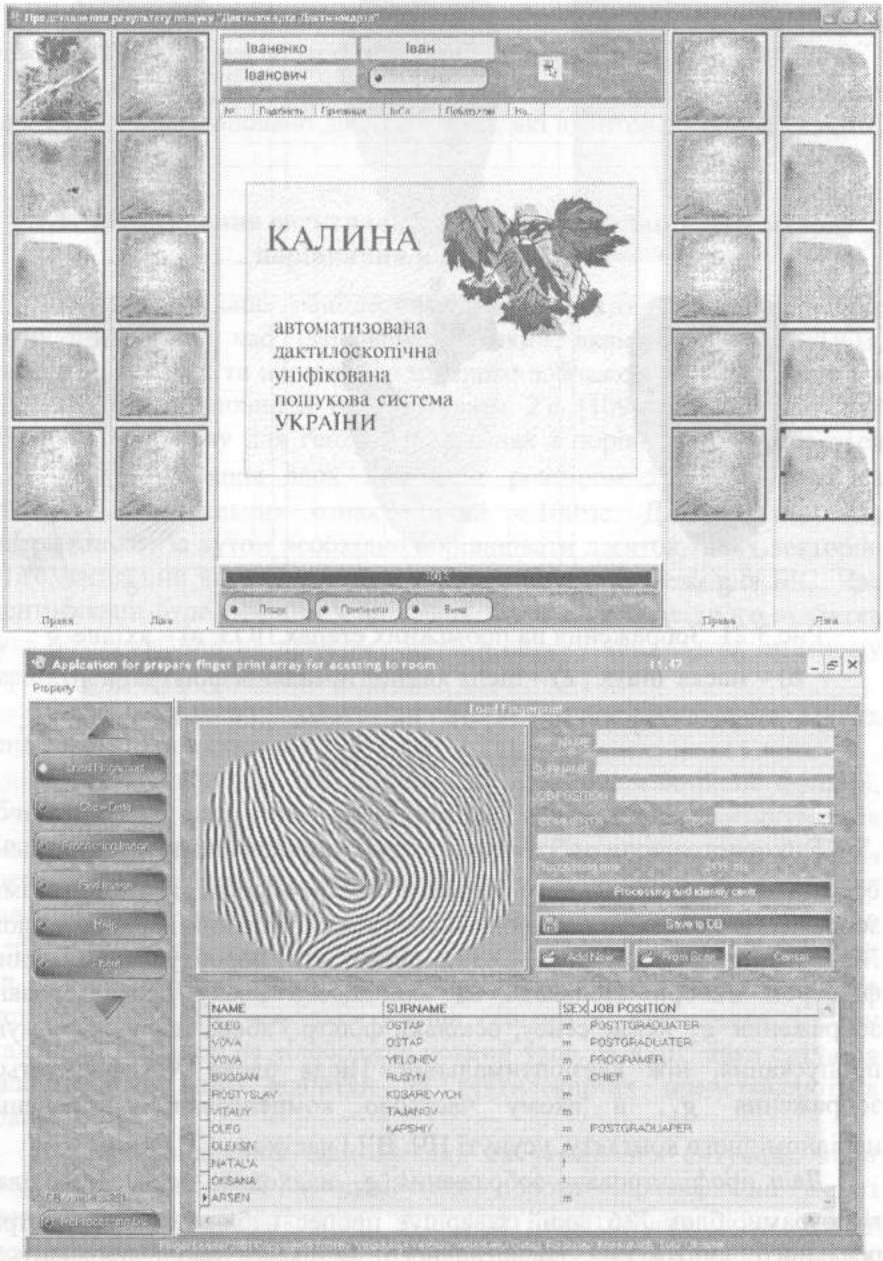


Рис. 3.20. Головне вікно програми.

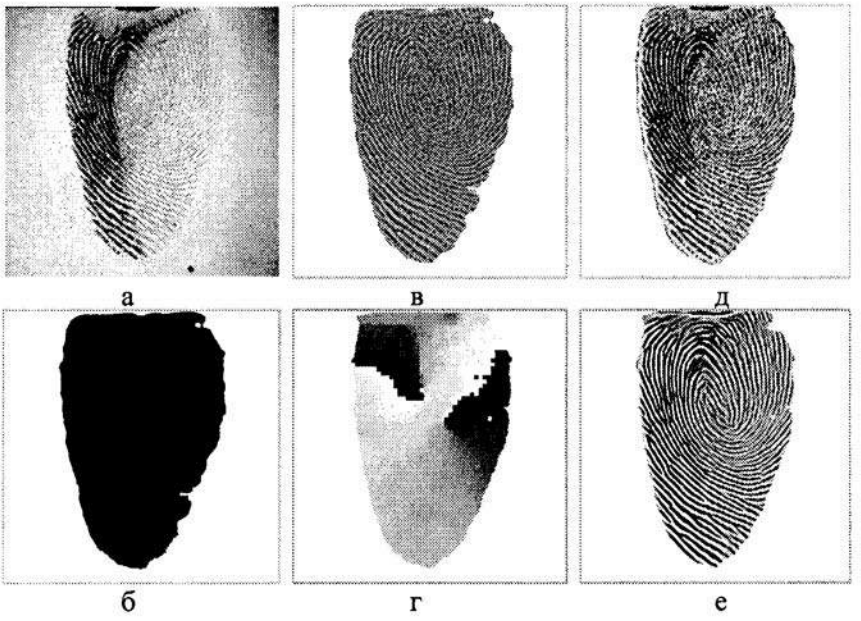


Рис.3.21. Зображення на проміжних етапах ПОЗ: а) – вхідне g; б) – маска **mask**; в) – після квазіоптимальної фільтрації g_2; г) – локальної орієнтації Θ; д) – після локальної нормалізації g_3; е) вихідне оброблене g'.

Використовуючи зображення вхідне, нормалізоване g_3, локальної орієнтації Θ і локального періоду **П** (в обробці для БІС взамін зображення локального періоду подається глобальний період), у блоці №6, згідно з формулою (3.37), проводять обробку спрямованим фільтром Габора. Подавати на вхід цього блоку профільтроване зображення g_2 немає сенсу, оскільки фільтр Габора має вужчу смугу пропускання, ніж квазіоптимальний. Після блока №5 формується зображення g_4, в якому частково компенсовані спотворення нерівномірного контакту, усунуті НЧ, ВЧ і частково СЧ шуми.

Далі профільтроване зображення g_4 надходить на перетворювач гістограми, блок №6, який завершує процес наближення параметрів реального зображення до ідеального. В цьому блоці проводиться обробка зображення, під час якої гістограма набуває вигляду параболи (п.3.2.7). На виході отримуємо оброблене зображення g' (рис.3.21 е).

Кожен етап обробляє або оцінює параметри зображення лише в межах інформативної області **Ψ**, що пришвидшує його роботу.

Таким чином, із метою забезпечення необхідних експлуатаційних параметрів запропоновано два типи ПОЗ, які адаптовані до задач АДІС і БІС.

3.9.1. Застосування спектральних ознак і кореляційного методу порівняння у БІС та АДІС

Як було згадано раніше, важливим фактором, що визначає зручність БІС, є час ідентифікації, який включає час на ПОЗ, генерування ознак та порівняння вхідного зображення з еталонними в БД. Цей час не повинен перевищувати 2 с [109]. Час попередньої обробки 0,8 с, тому для генерування ознак і порівняння залишається 1,2 с. Час порівняння двох зображень розміром 512×512 точок за вектором спектральних ознак рівний ≈ 100мс. Для забезпечення інваріантності за кутом необхідно порівнювати десяток таких векторів. Отже, загальний час буде перевищувати допустимі межі для БІС. Час ідентифікації буде меншим у випадках, коли еталон вхідного відбитка буде розташований на першому місці в списку кандидатів, виданому першим етапом розпізнавання (3.3).

Розглянемо ситуацію, коли порівнюються два зображення, в яких зона перекриття менша від 100% (рис.3.22).

У такому випадку пік нормованої взаємокореляційної функції, обчисленої за векторами спектральних ознак буде, зменшуватися відповідно до зменшення зони перекриття **Z**. Наприклад, якщо **A=B=Z,** коефіцієнт кореляції рівнятиметься одиниці, а якщо **Z** відповідає половині **A** і **B** зображення, то пік становитиме ≈ 0,5. Це значить, що відбиток не буде ідентифікованим, якщо поріг ідентифікації більший від 0,5. Ситуація, коли наявна мала зона перекриття, часто зустрічається у БІС, оскільки площа сенсора є обмеженою, і тому еталонний відбиток не відображає повний узор. В АДІС така ситуація малоймовірна, адже відбитки на дактилокартах представляються повністю.

Для пришвидшення ідентифікації та уникнення ситуацій, коли коефіцієнт подібності менший від порога ідентифікації через зменшення зони перекриття, описуємо центральну зону узору спектральними ознаками (чому саме центральну, обґрунтовано в п.3.4). Додатково наголосимо, що ця зона присутня у всіх відбитках. Для опису центральної зони вирізаємо окіл **C** центра узору у вигляді круга і

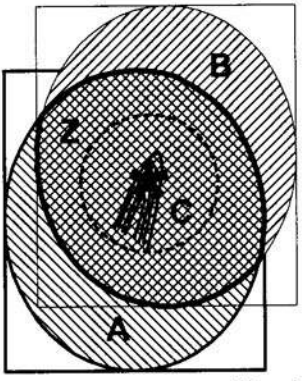


Рис.3.22. Представлення зони перекриття **Z** вхідного **A** і еталонного **B** зображень, в якій розташована центральна зона **C** узору. $\mathbf{Z} = \mathbf{A} \cap \mathbf{B}$, $\mathbf{C} \supset \mathbf{Z}$.

генеруємо для нього вектор спектральних ознак. Оскільки кореляція, яка обчислюється за спектрами зображень, є циклічною, то для уникнення краєвих ефектів, коли через неточність визначення центра узору появляються некорельовані області зображення, окіл на етапі вводу відбитків вибираємо більшим, ніж на етапі розпізнавання. Нами вибрано околи з діаметрами 100 і 120 точок. Околи вибрано у вигляді кругів для того, щоб зона кореляції **C** не змінювалася, коли вхідне зображення буде повернуте відносно еталонного.

Центр узору не є об'єктивно описаною величиною, бо немає чіткого розуміння, що це таке. Методи визначення центра узору побудовані на емпіричних засадах і включають суб'єктивний фактор. Це призводить до того, що визначення центра узору є неточним і має похибку, яка збільшується з погіршенням якості зображення. Порівняння двох центральних околів різних розмірів дозволило досягти нечутливості методу до похибки ±10 точок, проте, як показали практичні дослідження, інколи цього є недостатньо. Тому вводимо додатковий етап порівняння спектральних ознак околів центрів, але вже після корекції координат центра вхідного зображення за координатами піка (3.74) взаємокореляційної функції (3.73). Це дало змогу повністю виключити вплив суб'єктивних факторів на етап розпізнавання й уникнути збільшення ІНН через похибку визначення координат центра узору. Отже, тепер можемо говорити про нечутливість загального багатоетапного розпізнавання до похибки встановлення центра узору в межах, в яких пік взаємокореляційної

функції (3.73) не зменшиться до значення, меншого від порога ідентифікації другого етапу.

Ввід додаткових етапів передбачає вибір адаптивних порогів ідентифікації, налаштування яких буде проводитися за критеріями описаними в п.3.3.

Одним із важливих параметрів, які необхідно вибрати для формування спектральних ознак за формулою (3.48), є значення $r_{\min}, r_{\max}$ для околу інформативної зони **А** (рис.3.14). Для їх експериментального визначення введено поняття різниці між коефіцієнтом кореляції двох зображень ідентичних пальців, знятих у різний спосіб, K_{nik1-1} і коефіцієнтом кореляції двох зображень для різних пальців K_{nik1-0}

$$\Delta k = K_{nik1-1} - K_{nik1-0}. \qquad (3.75)$$

Міняючи значення $r_{\min}, r_{\max}$, ми дослідили залежність зміни Δk і вибрали точку з максимальною різницею, що відповідає максимальній віддалі в просторі ознак між множинами правильної та неправильної ідентифікації. Усереднену графічну залежність Δk від $r_{\min}, r_{\max}$ для 100 порівнянь відбитків одного узору і 100 різних представлено на рис. 3.23. З отриманої залежності вибрано значення $r_{\min} = 30$, $r_{\max} = 66$ дискретних відліків, при яких величина Δk максимальна й рівна 0,477.

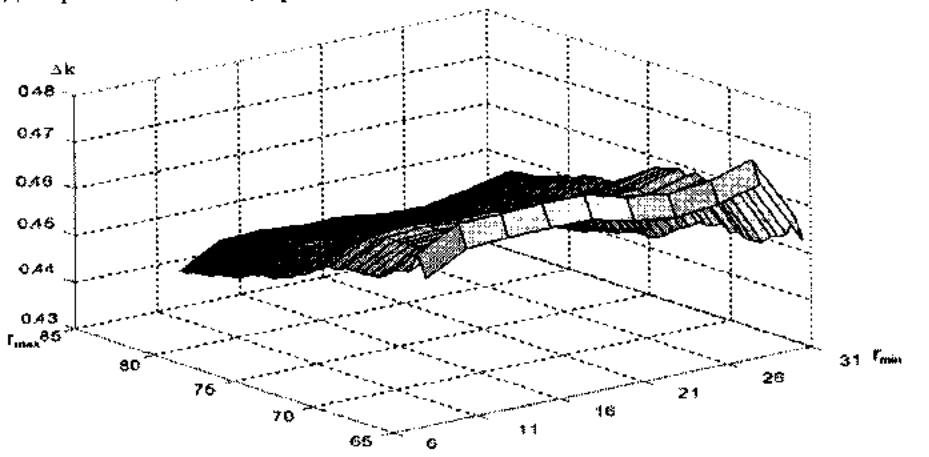


Рис.3.23. Графічна залежність Δk від $r_{\min}, r_{\max}$.

Наголосимо, що визначені параметри можуть бути перераховані для генерування спектральних ознак околу центра узору діленням на відношення розмірів зображення й околу, тобто на $512/120$.

Як уже згадувалося раніше в п.3.8, кореляційний метод порівняння за спектральними ознаками є неінваріантним до повороту зображень. Залежність коефіцієнта кореляції від кута одного зображення відносно іншого представлена на рис.3.24.

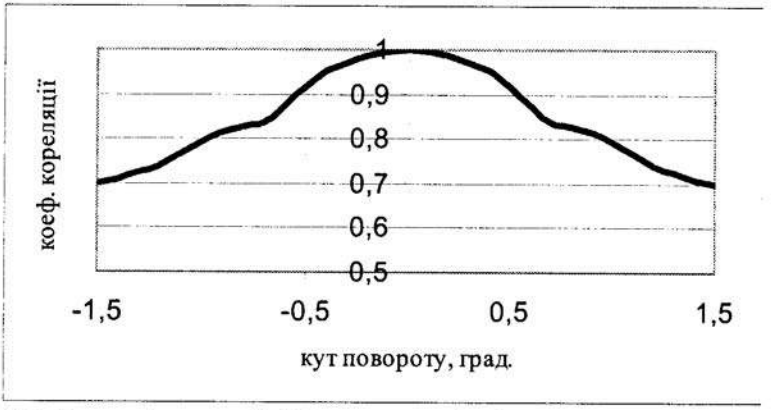


Рис.3.24. Залежність коефіцієнта кореляції від кута взаємного повороту зображень.

Із наведеної залежності видно, що для зображень, повернутих на половину градуса, коефіцієнт кореляції зменшується на 9%. Якщо на етапі ідентифікації формувати набір із $\mathbf{V}^{(angle)}_{\text{спектр. вх.}}$, $angle = \overline{(-G, G)} \cdot \Delta angle$ векторів ознак, кожен з яких відповідає опису повернутого на $angle$ зображення, а на етапі порівняння зіставляти їх з еталоном, то максимальний пік відповідатиме мірі подібності двох зображень. Якщо вважати, що зменшення міри подібності на 9% не є критичним, то, вибираючи $\Delta angle = 1^{\circ}$, ми отримаємо інваріантність кореляційного методу до повороту в межах $[-G, G]$ градусів.

Недоліком такого вирішення проблеми неінваріантності є збільшення обчислювальних затрат. Зважаючи на те, що перший етап дозволяє оцінити орієнтацію двох зображень, використавши її, зменшимо кількість порівнянь векторів. Нехай першим етапом визначена орієнтація $angle_1$, тоді на другому етапі необхідно порівняти лише вектори:

$$\mathbf{V}^{(angle)}_{\text{спектр. вх.}},\ angle = \overline{(angle_1 - \Delta_{angle}, angle_1 - \Delta_{angle})}$$

з еталоном, де $\Delta_{angle} = 2$ – ймовірна похибка визначення орієнтації на першому етапі.

Отже, застосовуючи спектральні ознаки описаним способом, можна забезпечити нечутливість кореляційного методу порівняння до похибки визначення центра узору. Цього не вдається зробити іншими згаданими раніше методами, в яких генератор ознак прив'язаний до центра узору. Незважаючи на те, що зона перекриття відбитків буває малою, їх ідентифікація буде проводитися з високою імовірністю, чого не можна сказати про кореляційні методи, які порівнюють повні зображення. Використання набору векторів $\mathbf{V}^{(\text{angle})}_{\text{спектр. ел.}}$ у поєднанні з визначенням кута орієнтації на першому етапі дозволяє досягти інваріантності кореляційного методу до повороту за рахунок незначного збільшення обчислювальних затрат.

Далі розглянемо блок-схеми етапу ідентифікації, які використовують описані тут способи формування ознак.

3.9.2. Етап запису векторів ознак у базу даних

На основі проведеного аналізу способів застосування ознак і методів у практичних задачах і шляхів їх реалізації розроблено блок-схему етапу вводу відбитків пальців у БД (рис. 3.25).

Розглянемо детальніше цей етап. Вхідне оцифроване зображення $\mathbf{g}$ подається на блок №2 попередньої обробки (п.3.9). На його виході отримуємо масиви обробленого зображення g', градієнтів яскравості $\mathbf{G}_1$, $\mathbf{G}_2$ і маски зображення **mask**, які обчислюються на проміжних етапах обробки. Далі зображення g' і масив орієнтації Θ подаються на блок №3 оцінки координат центра узору, на виході якого одержуємо координати (m_c, n_c). У блоці вирізання центральної області формується круговий окіл із діаметром 120 точок, який подається на блок №5 генерування спектральних ознак. На його виході дістаємо вектор $\mathbf{V}_{\text{спектр. еталон центр}}$. У блоці №6 обчислюється якість за вектором спектральних ознак. Для цього формулу (3.52) переписуємо таким чином:

$$Q_{\text{центр}} = \sum_l V_{\text{спектр. еталон центр}}(l)^2 . \qquad (3.76)$$

Оцінене значення $Q_{\text{центр}}$ в блоці №6 порівнюється з порогом $Q_{\text{центр пор.}}$. Якщо $Q_{\text{центр}} > Q_{\text{центр пор.}}$, то вектори ознак заносяться в БД.

Для вибору порога $Q_{центр\ пор.}$ були проведені практичні дослідження якості відбитків. Для цього було встановлене мінімальне значення $Q_{центр\ мін.} = 2.11 \cdot 10^{11}$ для БД з 1000 відбитків, які були передані в БД із візуальним контролем якості. Його прийнято за поріг для перевірки зображень за якістю. Така перевірка є більш важливою для БІС, ніж для АДІС, оскільки у БІС не описується повне зображення спектральними ознаками й ідентифікація проводиться за спектральними ознаками центральної зони. Генерування спектральних ознак для повного зображення в АДІС зроблено для того, щоб уможливити ідентифікацію особи за фрагментом відбитка, в якому відсутній центр узору. На виході блока формування спектральних ознак отримуємо вектор $\mathbf{V}_{\text{спектр. еталон}}$, який подається на блок перевірки якості зображення. Як і для блока перевірки якості центральної зони узору формула (3.52) перепишеться таким чином:

$$Q = \sum_{l} V_{спектр.\ еталон}(l)^2 . \qquad (3.77)$$

Визначена якість зображення Q порівнюється з порогом $Q_{пор.} = 20 \cdot 10^{11}$. Якщо $Q > Q_{пор.}$, то опис еталонного зображення заноситься в БД. Поріг вибраний так, щоб не пропускати зображення відбитків із неякісних дактилокарт.

Для генерування векторів ознак локальної орієнтації масиви $\mathbf{G}_1$, $\mathbf{G}_2$, **mask** і координати (m_c, n_c) подаються на блок генерування вектора ознак. Генерування вектора $\mathbf{V}_{\text{орієнт.еталон}}$ відбувається згідно з формулою (3.47). Додатково проводиться перевірка, чи точка концентричного кола, для якої оцінюється $c_j^{(i)}$, знаходиться в інформативній області $\mathbf{\Psi}$ зображення. Якщо вона розміщена в області $\mathbf{\Xi}$, то параметрові $c_j^{(i)}$ присвоюється значення –1. На етапі розпізнавання, під час визначення середньої різниці між векторами, вона не братиме участі в обчисленні різниці $\overline{\Delta}_{орієнт.}$. Вектор ознак $\mathbf{V}_{\text{орієнт.еталон}}$ заноситься у БД.

Рис.3.25. Блок-схема етапу вводу відбитків у БД. Штриховою лінією виділено блоки, які є лише в АДІС.

3.9.3. Етап ідентифікації

У п. 3.9.2 описано спосіб застосування спектральних ознак, який вимагає менших обчислювальних затрат і є практично нечутливий до геометричних спотворень. На його основі розроблено блок-схеми

етапів і загальну блок-схему ідентифікації для БІС й АДІС (рис.3.26 та рис.3.27).

Розглянемо коротко функціонування етапу генерування наборів векторів ознак перед ідентифікацією. Робота блоків ПОЗ, визначення центра узору, вирізання околу центра й формування векторів ідентична до роботи в блок-схемі етапу запису векторів ознак у БД (рис.3.25). Далі, на відміну від етапу запису, генеруються не два вектори ознак, а два набори векторів ознак. Вирізаний з повного зображення окіл центра узору подається на цикл по кутах діапазону інваріантності $[-G,G]$ (блок №5). В тілі циклу зображення околу центра подається на блок повороту зображення, в якому воно повертається на кут *angle*. Вихідне повернуте зображення околу центра подається на генератор ознак, на виході якого отримуємо вектор $\mathbf{V}_{\text{спектр. вх. центр}}$. У наступному блоці згенерований вектор ознак добавляється в набір $\mathbf{V}^{(\text{angle})}_{\text{спектр. вх. центр}}$. Далі у блоці №9 визначається якість за формулою (3.76) за довільним вектором із набору $\mathbf{V}^{(\text{angle})}_{\text{спектр. вх. центр}}$. Перевірка проводиться за наперед встановленим порогом $Q_{\text{центр поріг}} = 1.15 \cdot 10^{11}$. Якщо $Q_{\text{центр}} < Q_{\text{центр пор.}}$, то процес ідентифікації завершується видачею повідомлення про погану якість вхідного зображення. За поріг $Q_{\text{центр поріг}}$ узято мінімальну якість для набору вхідних зображень, які були ідентифіковані під час тестування. Поріг вибраний так, щоб не збільшувати ІНН за рахунок відкидання вхідних зображень.

Згенерований вектор $\mathbf{V}_{\text{орієнт. вх.}}$ ознак локальної орієнтації для вхідного зображення подається на подібний до описаного раніше циклу. В його тілі циклічним зсувом вхідного вектора $\mathbf{V}_{\text{орієнт. вх.}}$ формуються вектори ознак для кожного кута з діапазону інваріантності $[-G,G]$, які компонуються в набір векторів ознак локальної орієнтації $\mathbf{V}^{(\text{angle})}_{\text{орієнт. вх.}}$.

Етап генерування наборів векторів для АДІС є інакшим, оскільки повинен додатково генерувати набір векторів спектральних ознак повного зображення. Його блок-схема представлена на рис.3.27.

Цей етап в АДІС відрізняється від такого ж етапу для БІС тим, що в тілі циклу №4, де формується набір векторів спектральних ознак $\mathbf{V}^{(\text{angle})}_{\text{спектр. вх. центр}}$ околу центра узору, формується також набір

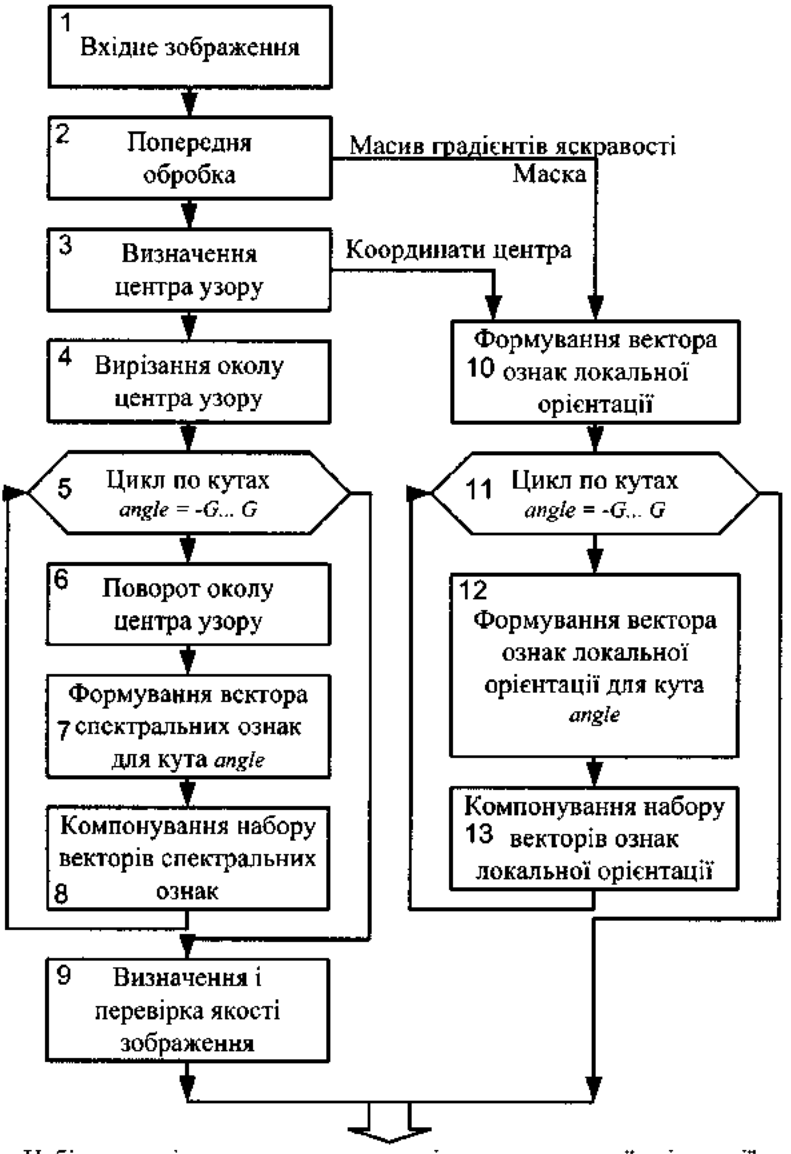


Рис.3.26. Блок-схема етапу генерування наборів векторів ознак перед ідентифікацією для БІС.

спектральних ознак $\mathbf{V}^{(angle)}_{спектр.\,вх.}$ повного зображення. Центральна зона узору вирізається з повернутого зображення. Перевірка якості проводиться за двома наборами спектральних ознак. Якщо якість околу центра менша від порога $Q_{центр\,поріг} = 1{,}15 \cdot 10^{11}$, то приймається, що у відбитка відсутній центр узору, внаслідок чого порівняння за спектральними ознаками околу центра узору не проводиться. В тому випадку, якщо якість повного зображення також менша від порога $Q_{поріг} = 1{,}15 \cdot 10^{11}$, то ідентифікація не проводиться, а видається повідомлення про низьку якість зображення.

Генерування набору векторів ознак локальної орієнтації здійснюється аналогічно, як і в блок-схемі для БІС (рис.3.26).

Результатом роботи розглянутого етапу є набори векторів: спектральних ознак околу центра узору $\mathbf{V}^{(angle)}_{спектр.\,вх.\,центр}$, ознак локальної орієнтації $\mathbf{V}^{(angle)}_{орієнт.\,вх.}$, спектральних ознак повного зображення $\mathbf{V}^{(angle)}_{спектр.\,вх.}$ (лише для АДІС) і додатково ще є оброблене зображення g', координати центра узору (m_c, n_c), якість околу центра узору $Q_{центр}$, які будуть використані на етапах ідентифікації.

Під час ідентифікації на першому етапі порівнюються вектори ознак локальної орієнтації. На цьому етапі не передбачено видачі рішення про ідентифікацію, формується лише список кандидатів, які будуть порівнюватися на другому етапі. Блок-схема першого етапу представлена на рис.3.28.

Для того, щоб обчислити адаптивний поріг за формулою (3.56) необхідно знати мінімальне значення $\overline{\Delta}_{орієнт.\min}$ середньої різниці між векторами ознак локальної орієнтації. Оскільки між набором вхідних векторів $\mathbf{V}^{(angle)}_{орієнт.\,вх.}$ і першим еталоном, описаним вектором $\mathbf{V}_{орієнт.\,еталон}$, різниця $\overline{\Delta}_{орієнт.\min}$ є невідома, то приймаємо в блоці №1, що $\overline{\Delta}_{орієнт.пор.} = \overline{\Delta}_{орієнт.\min} = 25^{\circ}$. Таке значення порога дозволяє ідентифікувати вхідні зображення з імовірністю $P_{нн}(T) = 0$ і, тим самим, забезпечити виконання першого критерію з п.3.3. Через те, що величина $\overline{\Delta}_{орієнт.\min}$ може змінитися під час порівняння, то й остаточне значення $\overline{\Delta}_{орієнт.пор.}$ буде визначатися ітераційно в тілі циклу.

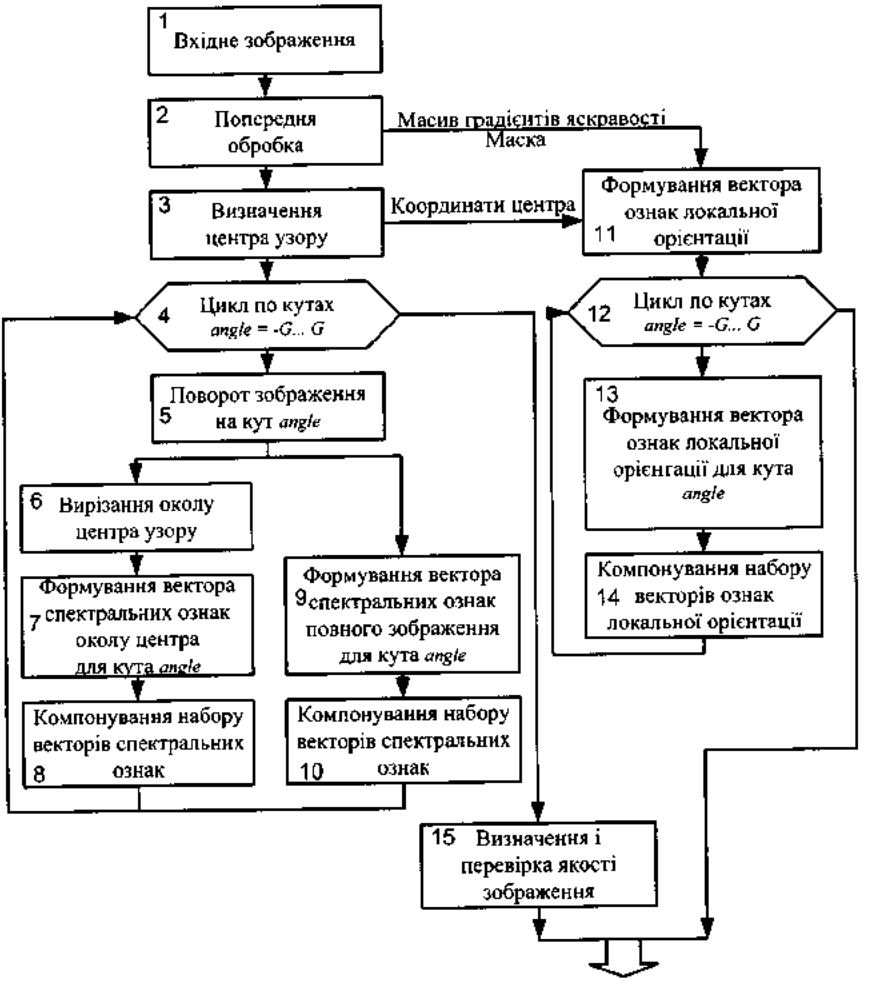


Рис.3.27. Блок-схема етапу попередньої підготовки до ідентифікації для АДІС.

Вхідними величинами для цього етапу (рис. 3.28) є набір векторів $\mathbf{V}^{(angle)}_{орієнт.\ вх.}$, якість околу центра $Q_{центр}$ і еталонні вектори $\mathbf{V}_{орієнт.\ еталон}$ з БД.

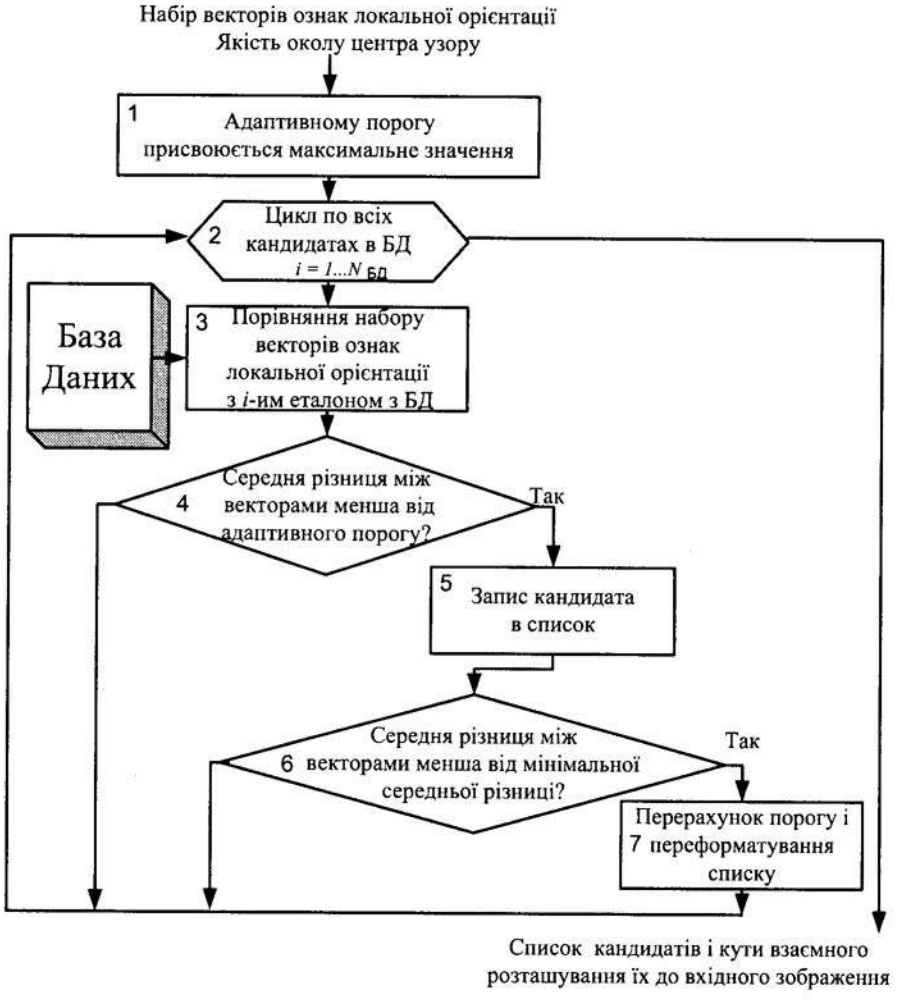


Рис.3.28. Блок-схема етапу ідентифікації за векторами ознак локальної орієнтації.

У першому блоці приймається $\overline{\Delta}_{орієнт.пор.} = \overline{\Delta}_{орієнт.\min} = 25^{\circ}$, що обгрунтовано вище. Далі $\mathbf{V}^{(angle)}_{орієнт.\,вх.}$ подається на цикл, в якому він порівнюється з кожним еталонним вектором $\mathbf{V}_{орієнт.\,еталон}$ і обчислюється різниця $\overline{\Delta}_{орієнт.}$ між векторами за формулою (3.50), а також кут між вхідним і еталонним зображеннями $\theta_{вх.-етал.}$ (3.51). Якщо

$\overline{\Delta}_{орієнт.} < \overline{\Delta}_{орієнт.пор.}$, то в наступному блоці в список кандидатів на ідентифікацію заносяться номер кандидата, значення $\overline{\Delta}_{орієнт.}$ для нього і кут $\theta_{вх.-етал.}$. Коли ж $\overline{\Delta}_{орієнт.} > \overline{\Delta}_{орієнт.пор.}$, то розглядається наступний вектор $\mathbf{V}_{орієнт.еталон}$ з БД. Якщо обчислене значення $\overline{\Delta}_{орієнт.} < \overline{\Delta}_{орієнт.min}$, то перераховується величина адаптивного порога $\overline{\Delta}_{орієнт.пор.}$, а значенню $\overline{\Delta}_{орієнт.min}$ присвоюється $\overline{\Delta}_{орієнт.}$. Така зміна значення порога вимагає перегляду списку кандидатів з метою усунення кандидатів, для яких $\overline{\Delta}_{орієнт.} > \overline{\Delta}_{орієнт.пор.}$. Список кандидатів формується ітераційно разом із визначенням кінцевого значення порога $\overline{\Delta}_{орієнт.пор.}$. Далі розглядається наступний опис еталона з БД до моменту порівняння вхідного набору $\mathbf{V}^{(angle)}_{орієнт.вх.}$ з $N_{БД}$ еталонними $\mathbf{V}_{орієнт.еталон}$.

На виході цього етапу ідентифікації отримуємо список із $N_{список№1}$ кандидатів, які описуються номером у БД, різницею $\overline{\Delta}_{орієнт.}$ і кутом $\theta_{вх.-етал.}$. Ці дані будуть використовуватися на наступному етапі ідентифікації.

Другий етап ідентифікації передбачає порівняння набору векторів спектральних ознак із еталонами з БД. Третій етап працює разом із другим у тілі одного циклу й відрізняється лише тим, що на його вхід подається не повний набір наново згенерованих векторів спектральних ознак, а набір із п'яти векторів. Блок-схема другого й третього етапів приведена на рис.3.29.

На основі формули (3.53) запишемо вирази для обчислення адаптивних порогів ідентифікації за спектральними ознаками:

$$K_{поріг№1}(Q_{центр}) = a_{центр1} + \frac{b_{центр1}}{Q_{центр}}, \qquad (3.78)$$

$$K_{поріг№2}(Q_{центр}) = a_{центр2} + \frac{b_{центр2}}{Q_{центр}}, \qquad (3.79)$$

де $a_{центр1}$, $b_{центр1}$, $a_{центр2}$, $b_{центр2}$ – коефіцієнти, які визначаються на етапі навчання системи на тестовому масиві зображень. Ці пороги потрібні для того, щоб вхідний відбиток був переданий на порівняння наступним етапом або відмічений, як неідентифікований.

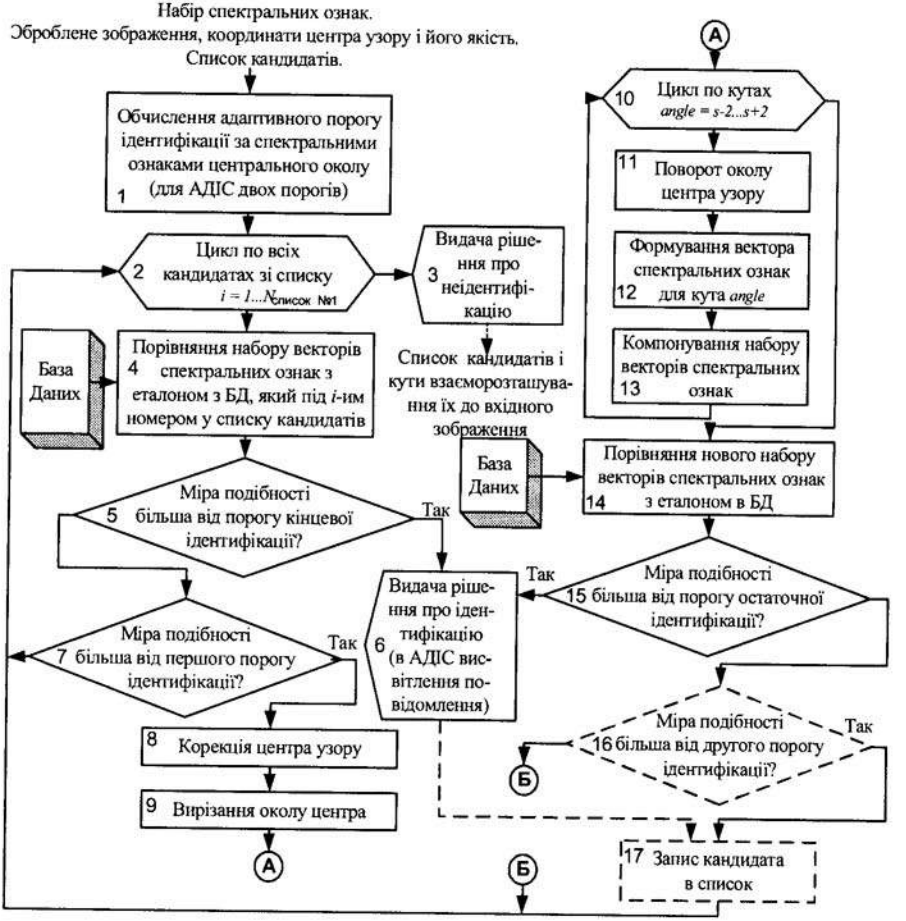


Рис.3.29. Блок-схема етапу ідентифікації за векторами спектральних ознак околу центра узору. Штриховими лініями зображено додаткові блоки, необхідні для роботи АДІС.

Крім того, є поріг T кінцевої ідентифікації, згідно з яким виноситься рішення про ідентифікацію системою, а не окремим етапом.

Формула (3.78) використовується в блоці №1 для розрахунку порога ідентифікації $K_{поріг\,№1}$ другим етапом, а (3.79) – порога ідентифікації $K_{поріг\,№2}$ третім етапом в АДІС. Далі всі вхідні величини й пороги ідентифікації подаються на цикл (блок №2), у тілі якого вхідний набір векторів спектральних ознак порівнюється з еталонними

векторами у БД, які занесені у список кандидатів, що сформований першим етапом ідентифікації. Як результат видається рішення про ідентифікацію у БІС або формується новий список кандидатів для АДІС. В тілі циклу набір $\mathbf{V}^{(angle)}_{\text{спектр. вх. центр}}$ порівнюється з вектором $\mathbf{V}_{\text{спектр. еталон центр}}$ кандидата. Під час порівняння враховується, що список кандидатів включає у себе кут взаємного розташування вхідного й еталонного зображень $\theta_{вх.-етал.}$. Тому, для зменшення кількості операцій обчислення коефіцієнта кореляції за формулою (3.73), його встановлюють для п'яти векторів із набору $\mathbf{V}^{(angle)}_{\text{спектр. вх. центр}}$ ($angle = \overline{\theta_{вх.-етал.} - 2, \theta_{вх.-етал.} + 2}$), вибирають максимальний $K_{пік\ центр}$ і визначають кут взаємної орієнтації S вхідного й еталонного зображень. Порівнюються п'ять, а не один вектор для того, щоб похибка у розрахунку кута $\theta_{вх.-етал.}$ першим етапом ідентифікації не вплинула на результати системи. Далі значення $K_{пік\ центр}$, тобто міра подібності двох зображень, порівнюється з порогом T. Якщо $K_{пік\ центр} > T$, то для БІС приймається рішення про ідентифікацію й робота системи закінчується, а в АДІС виводиться повідомлення про те, що знайдено подібний відбиток, і цикл продовжується далі для формування списку кандидатів. Якщо $K_{пік} < T$, то перевіряється, чи $K_{пік\ центр}$ більший від першого адаптивного порога $K_{поріг №1}$, який визначає доцільність корекції центра узору для повторної спроби ідентифікації третім етапом. Якщо ж $K_{пік\ центр} > K_{поріг №1}$, то проводиться корекція координат центра узору, вирізається окіл центра і генерується новий набір спектральних ознак $\mathbf{V}^{(angle)}_{\text{спектр. вх. центр кор.}}$. На відміну від генерування набору векторів ознак на етапі, відображеному блок-схемою на рис.3.26 та рис.3.27, у цьому випадку генеруються лише п'ять векторів спектральних ознак для $angle = \overline{s-2, s+2}$. Далі набір $\mathbf{V}^{(angle)}_{\text{спектр. вх. центр кор.}}$ подається на блок обчислення міри подібності, який видає значення $K_{пік\ центр\ кор.}$ і наново визначає кут s. Цю операцію можна назвати корекцією кута орієнтації двох зображень. Як і на другому етапі ідентифікації, на цьому етапі значення $K_{пік\ центр}$ порівнюється з порогом T. Якщо $K_{пік\ центр} > T$, то у БІС приймається рішення про ідентифікацію

й робота системи закінчується, в АДІС виводиться повідомлення про ідентифікацію, а кандидат заноситься у список. Цикл для БІС повторюється доти, поки вхідний відбиток не буде ідентифікований або всі кандидати зі списку, який сформований на першому етапі ідентифікації, не будуть переглянуті. Якщо всі кандидати переглянуті й жоден із них не забезпечив умови ідентифікації $K_{пік\ центр\ кор.} > T$, то видається рішення про неідентифікацію. Для АДІС після перевірки умови $K_{пік\ центр\ кор.} > T$ у випадку, коли $K_{пік\ центр\ кор.} < T$, порівнюється значення $K_{пік\ центр\ кор.}$ з другим адаптивним порогом ідентифікації $K_{поріг\ №2}$. Якщо $K_{пік\ центр\ кор.} > K_{поріг\ №2}$, то кандидат залишається в списку, інакше він видаляється. Така специфіка побудови розглянутих етапів ідентифікації викликана відмінністю задач ідентифікації у БІС й АДІС. На виході АДІС ми повинні отримати список найбільш подібних еталонних зображень, навіть якщо вхідне зображення не дає змоги проводити точну ідентифікацію, як це вимагається у БІС.

Адаптивний поріг ідентифікації $K_{поріг\ №1}$ дозволяє розрідити список кандидатів на ідентифікацію, вилучаючи з нього такі, для яких корекція центра узору не дасть позитивного результату. Як наслідок зменшується кількість операцій повторного генерування наборів векторів $\mathbf{V}^{(angle)}_{спектр.\ вх.\ центр\ кор.}$, що особливо важливо для БІС. Адаптивний поріг $K_{поріг\ №2}$ застосовується в АДІС для подальшого розрідження списку кандидатів і зменшення кількості операцій порівняння відбитків за спектральними ознаками повного зображення.

Для АДІС пропонується проводити четвертий етап ідентифікації. Його можна назвати етапом порівняння зображень за спектральними ознаками повного зображення. Актуальність вводу цього етапу ідентифікації пояснюється необхідністю порівняння відбитків, у яких відсутня центральна зона узору. Вхідними параметрами для цього етапу є список кандидатів із попереднього етапу ідентифікації, в якому вказані значення міри подібності $K_{пік\ центр\ кор.}$, кут орієнтації S та набір спектральних ознак повного зображення $\mathbf{V}^{(angle)}_{спектр.\ вх.}$ (рис. 3.30).

Циклом (рис. 3.30, блок №1) перебираються всі кандидати, які пройшли три попередні етапи ідентифікації. Якщо вхідне зображення не має центра узору, то цикл перебирає всі еталонні зображення з БД і $N_{список\ №2} = N_{БД}$. В тілі циклу порівнюється вхідний набір $\mathbf{V}^{(angle)}_{спектр.\ вх.}$

Рис.3.30. Блок-схема етапу ідентифікації за векторами спектральних ознак повного зображення.

векторів спектральних ознак з еталонним вектором спектральних ознак $\mathbf{V}_{\text{спектр. еталон}}$, який зчитується з БД для кожного кандидата. Міра подібності $K_{пік}$, яка відповідає коефіцієнтові кореляції, розраховується за формулою (3.73). Також визначаються координати піка кореляційної функції (3.74), які відповідають взаємному зсувові вхідного зображення відносно еталонного. Коефіцієнт кореляції обчислюється для п'яти векторів із вхідного набору $\mathbf{V}^{(\text{angle})}_{\text{спектр. вх.}}$, $angle = \overline{s-2, s+2}$, аналогічно як і в попередніх етапах ідентифікації. Якщо є потреба, то коректується значення кута взаємної орієнтації s.

На виході цього етапу отримуємо список кандидатів, кожен із яких описується значеннями мір подібності околів центрів $K_{пік\ центр\ кор.}$ (якщо ідентифікація за ними проводилася) і повних зображень $K_{пік}$, орієнтацією s і зсувом вхідного зображення відносно еталонного

$(i_{пік}, j_{пік})$. Дані про орієнтацію й зсув використовуються для виводу і візуального порівняння відбитків оператором АДІС.

На рис.3.31 наведені блок-схеми процесів ідентифікації для БІС (рис.3.31 а) та АДІС (рис.3.31 б).

Ці блок-схеми відображають суть роботи обох систем. У БІС на виході повинні отримати булеву змінну, яка визначає, ідентичний вхідний відбиток одному з еталонних чи ні. Відповідно до цього й побудована блок-схема ідентифікації. Під час обробки й генерування векторів ознак може видаватися рішення про неідентифікацію у разі поганої якості вхідного зображення. На першому етапі ідентифікації таке рішення може бути прийняте, якщо жоден з еталонів не ідентифікований за вектором ознак локальної орієнтації. Далі проводиться сортування списку в порядку збільшення різниці $\overline{\Delta}_{орієнт.}$. Це робиться для того, щоб кандидат із найменшою різницею порівнювався першим на наступному етапі (виграш у часі від введення сортування описано у п.3.3). Відсортований список подається на другий етап ідентифікації, де порівнюються спектральні ознаки околу центра. Якщо коефіцієнт кореляції $K_{пік\ центр} > T$, то приймається рішення про ідентифікацію. Якщо ж $K_{пік\ центр} < T$, але $K_{пік\ центр} > K_{поріг №1}$, то проводиться третій етап ідентифікації. На третьому етапі $K_{пік\ центркор.}$ порівнюється з T, якщо $K_{пік\ центркор.} > T$, то видається рішення про ідентифікацію. Якщо серед усіх кандидатів жоден не забезпечує виконання умови ідентифікації, то це означає, що вхідний відбиток не має еталона в БД і буде неідентифікований системою (у більшості БІС, отже, людина не отримає доступу до об'єкта, який захищається системою).

Блок-схема ідентифікації в АДІС подібна до блок-схеми для БІС. Результатом роботи АДІС є список кандидатів. Основна відмінність полягає в тому, що перших три етапи ідентифікації проводять розрідження списку кандидатів і не передбачають завершення ідентифікації, поки всі еталони не будуть переглянуті та не буде сформований кінцевий список кандидатів. Оскільки робота АДІС передбачає дослідження слідів, на яких часто немає центра узору, то проводиться перевірка на його наявність. Якщо він відсутній, то слід подається на четвертий етап ідентифікації, який у такій ситуації порівнює його з усіма зображеннями з БД. Далі список сортується в порядку спадання значення $K_{пік}$ і виводиться операторові. Якщо ж

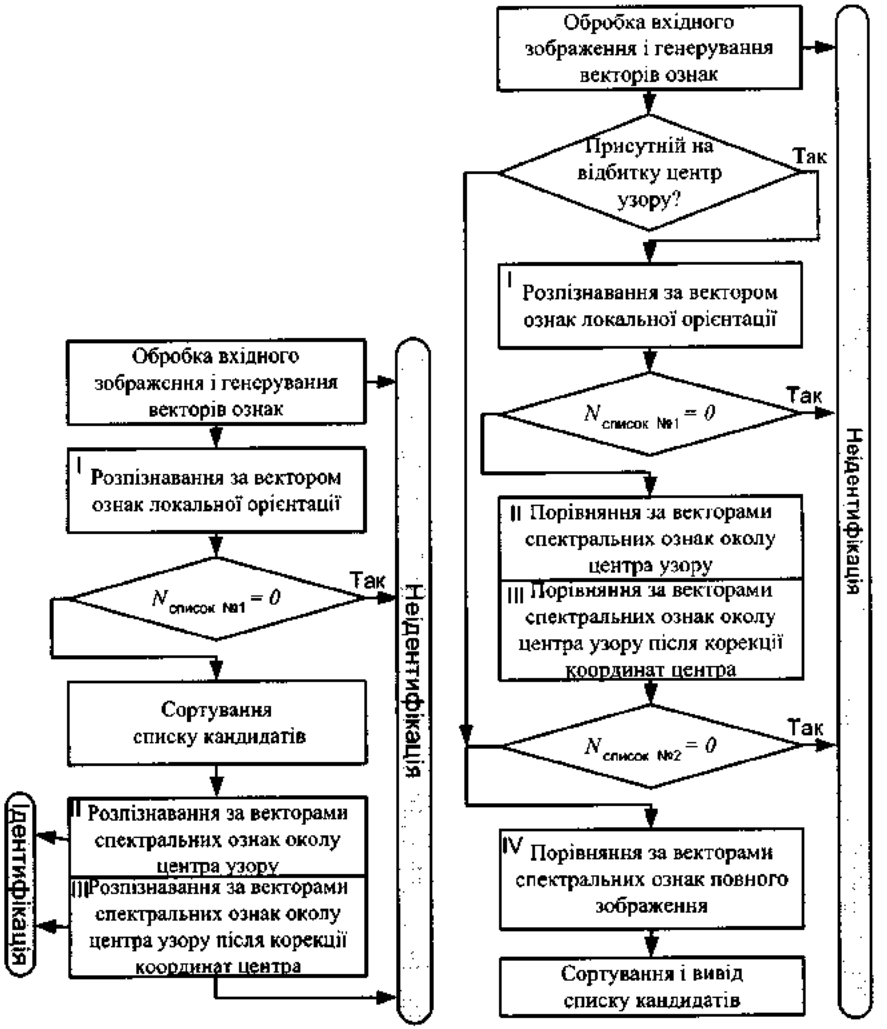


Рис.3.31. Блок-схеми ідентифікації для БІС (а) і АДІС (б).

центр узору присутній на вхідному відбитку, то здійснюється ідентифікація першими трьома етапами. Далі сформований список кандидатів подається на четвертий етап, де отримуємо додаткові значення $K_{пік}$ для кожного кандидата. Сортування в блоці виводу списку відбувається в порядку спадання суми $K_{пік} + K_{пік\ центр кор.}$, $K_{пік\ центр кор.}$ або $K_{пік}$ за вибором оператора. Наявність для кожного

кандидата інформації про його розташування відносно вхідного дає можливість проводити просторову нормалізацію вхідного зображення для візуального накладання двох зображень під час порівняння зображень оператором.

Така побудова ідентифікації дозволяє:

- зменшити час ідентифікації за рахунок поетапної ідентифікації й використання інформації з попереднього етапу для зменшення обчислень у наступному;
- налаштувати етапи (вибрати адаптивні пороги) таким чином, щоб кожен із них відповідав першому критерієві п.3.8., відтак, це не призводить до збільшення ІНН і забезпечує максимальне пришвидшення функціонування системи за другим критерієм;
- досягти інваріантності до повороту розробленого методу, незначно збільшивши обчислювальні затрати;
- уникнути впливу похибки визначення центра узору на результати ідентифікації.

3.9.4. Експериментальне визначення параметрів адаптивних порогів ідентифікації

Адаптивні пороги відіграють суттєвішу роль в АДІС, ніж у БІС. В БІС найважливішим є поріг ідентифікації на першому етапі, оскільки здебільшого список кандидатів після цього етапу складається з декількох відбитків, а кандидат, який є еталоном вхідного, розташовується на першому місці (рис. 3.32).

Задача визначення адаптивного порогу за статистичними залежностями еквівалентна задачі встановлення лінійної вирішуючої функції у теорії розпізнавання об'єктів. У нашому випадку вирішуюча функція поділяє двовимірний простір ознак (ознаками є якість і міра, для якої визначається адаптивний поріг) на дві області: ідентифікації та неідентифікації.

Залежності визначалися на БД із 5000-ми зображень відбитків із дактилокарт розміром 512×512 точок і 40 реальних слідів із карток (рис. 1.18).

Першою розглянемо залежність різниці $\overline{\Delta}_{орієнт.} - \overline{\Delta}_{орієнт.\min}$ для вхідного й еталонного зображень від якості $Q_{центр}$ (рис.3.33).

Як бачимо, зі зростанням якості різниця $\overline{\Delta}_{орієнт.} - \overline{\Delta}_{орієнт.\min}$ зменшується. Узявши дві точки, через які проходить пряма

$\left(\overline{\Delta}_{орієнт.\,пор.} - \overline{\Delta}_{орієнт.\min}\right)(Q_{центр})$ та прийнявши до уваги, що згідно обчислень за формулою (3.56) $\left(\overline{\Delta}_{орієнт.\,пор.} - \overline{\Delta}_{орієнт.\min}\right)(Q_{центр}) = a_{\Delta_{орієнт}} + \frac{b_{\Delta_{орієнт}}}{Q_{центр}}$, розраховуємо значення $a_{\Delta_{орієнт}}$ і $b_{\Delta_{орієнт.}}$. Поріг ідентифікації для першого етапу тоді становитиме

$$\overline{\Delta}_{орієнт.пор.}(Q_{центр}, \overline{\Delta}_{орієнт.\min}) = \overline{\Delta}_{орієнт.\min} + 5{,}2121 + \frac{2{,}6326 \cdot 10^{12}}{Q_{центр}}. \quad (3.80)$$

Адаптивні пороги для другого й третього етапів ідентифікації описуються лінійною залежністю, оскільки в цьому випадку не спостерігається залежність подібна до $\overline{\Delta}_{орієнт.пор.}(Q_{центр}, \overline{\Delta}_{орієнт.\min})$. Як і для обчислення параметрів порога (3.80) вибираються дві точки, за якими визначаються параметри (рис.3.34, 3.35).

Залежність на рис.3.35 вказує на більшу згрупованість точок, ніж на рис.3.34, що для розпізнавання має вагоме значення, бо дозволяє точніше розділити області ідентифікації і неідентифікації.

Пороги для другого та третього етапів ідентифікації опишуться такими формулами:

$$K_{поріг\ №1}(Q_{центр}) = 0{,}2956 - \frac{3{,}5702 \cdot 10^{10}}{Q_{центр}}, \quad (3.81)$$

$$K_{поріг\ №2}(Q_{центр}) = 0{,}4963 - \frac{1{,}0933 \cdot 10^{11}}{Q_{центр}}. \quad (3.82)$$

Представлені залежності вказують на те, що зі зменшенням якості зображень розкид значень мір подібності $K_{пік\ центр}$, $K_{пік\ центркор.}$ і різниці $\overline{\Delta}_{орієнт.}$ зростає. Пороги розраховані так, щоб врахувати цю закономірність, тож із погіршенням якості вхідного зображення час ідентифікації буде тривалішим. Це викликано тим, що більше кандидатів будуть ідентифікуватися, тобто буде збільшуватися ІНІ кожного етапу. Оскільки поріг T для видачі рішення про ідентифікацію біометричною системою є незмінним, то адаптація порогів не впливатиме на імовірнісні показники системи. Звідси, чим якісніше вхідне зображення, тим суттєвіший виграш у часі дасть застосування багатоетапної ідентифікації з адаптивними до якості відбитка порогами.

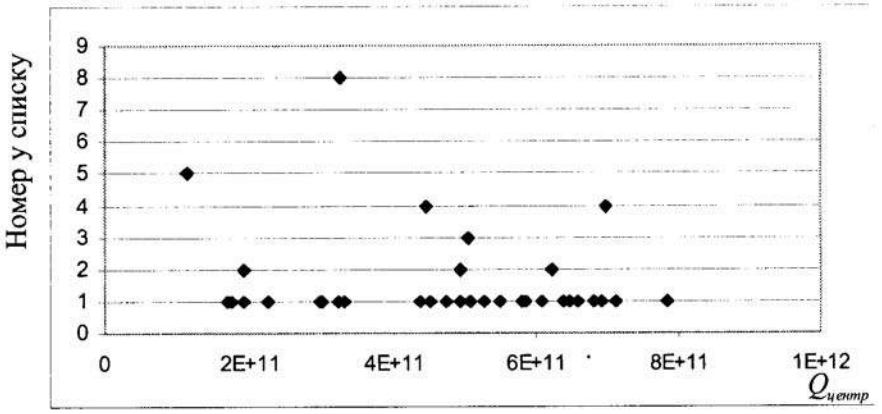


Рис.3.32. Залежність місця кандидата, який є еталоном, від якості вхідного зображення.

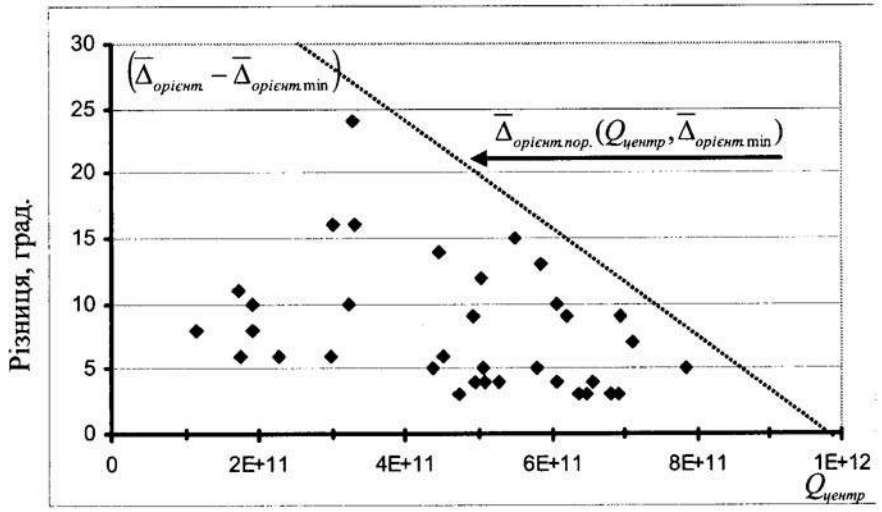


Рис.3.33. Експериментальна залежність значення $\overline{\Delta}_{орієнт.} - \overline{\Delta}_{орієнт.\min}$ від якості $Q_{центр}$.

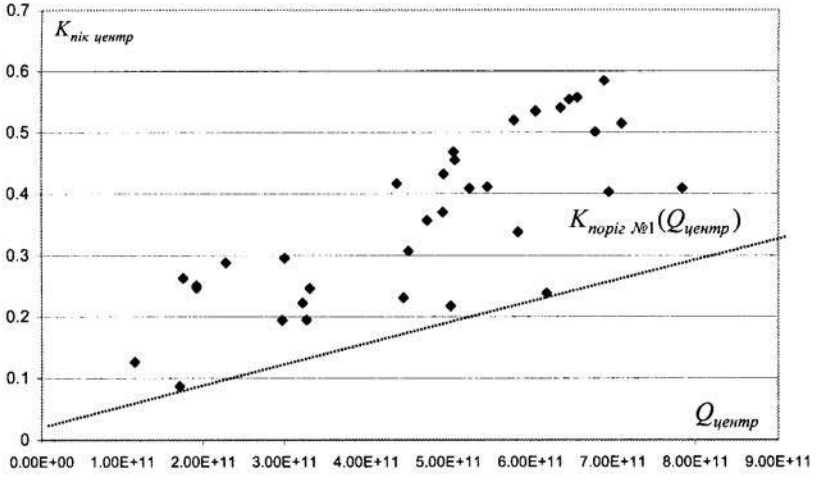


Рис.3.34. Експериментальна залежність значення $K_{пік\ центр}$ від якості $Q_{центр}$ після другого етапу ідентифікації.

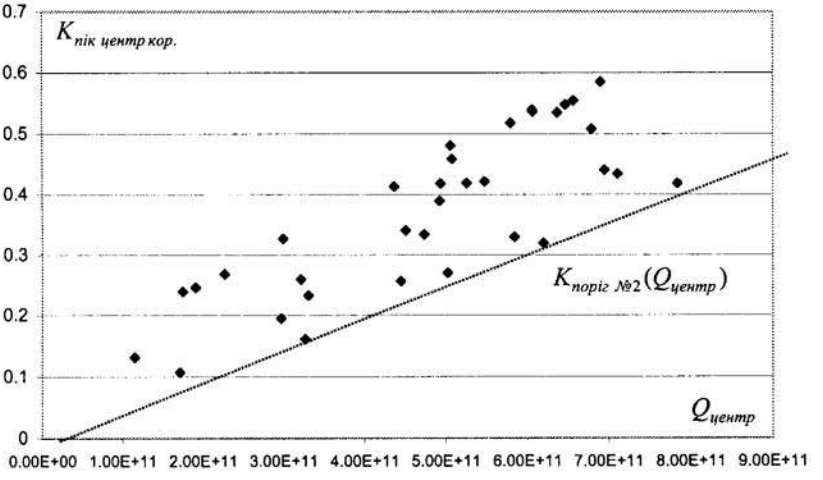


Рис.3.35. Експериментальна залежність значення $K_{пік\ центр\ кор.}$ від якості $Q_{центр}$ після третього етапу ідентифікації.

3.9.5. Результати тестування

Першими розглянемо часові показники роботи кожного етапу. Тестування проводилося на персональній електронно-обчислювальній машині з процесором Pentiun-III 800МГц. Усі програми виконані мовою програмування С++, у редакторі Microsoft Visual C++ 6.5 у середовищі Windows 2000.

Тестова база для БІС складається з 1000 зображень 256 градацій сірого (100 пальців із 10-ма відбитками кожного) розміром 400×300 точок. Оцифровка здійснювалася біосенсором фірми Testech. Тестова база для АДІС складається з 5000 еталонних зображень 256 градацій сірого, розміром 512×512 точок, оцифрованих із дактилокарт прикладною відеосистемою ELMO. Як вхідні зображення, котрі необхідно ідентифікувати, використовувалися 40 зображень слідів такого ж формату, отриманих із реальних карток слідів із місць злочинів.

Розглянемо часові параметри програм, виконаних за наведеними раніше блок-схемами. Попередня обробка для БІС, яка представлена блок-схемою на рис.3.19 а, проводиться за $\approx 0{,}6$ с, а для АДІС (рис.3.19 б) – ≈ 8 с. Середній час ідентифікації, без попередньої обробки, для БІС складає ≈ 1 с. Час ідентифікації першим етапом – $\approx 1{,}2$ мс, другим – ≈ 45 мс, третім – $\approx$200 мс, четвертим – $\approx$ 180мс. Для якісних вхідних зображень відбитків пальців перший етап ідентифікації видає список з одного кандидата, який відповідає еталонові вхідного. Наступним етапом проводиться обчислення міри подібності та ідентифікація, що займає від 52 до 244 мс. У випадку, коли вхідне зображення не матиме еталонного в БД, список після першого етапу буде більшим і час ідентифікації відповідно зросте. Це означає, що доступ до об'єкта користувачеві, який має такі права, буде наданий за < 2 с. Час неідентифікації буде більшим, а це додатково ускладнить наміри несанкціонованого доступу.

Характеристикою, яка описує роботу АДІС, є розподіл місць еталона в списку кандидатів, який відповідає вхідному зображенню. Така залежність представлена на рис. 3.36.

Розподіл (рис. 3.36) показує, що 67,5% ідентифікацій були проведені за списками, в яких еталонне зображення, що відповідає вхідному слідові, було розташоване на першому місці. В існуючих системах ідентифікація вважається успішною, якщо кандидат, який відповідає сліду, розміщений на перших 30 позиціях.

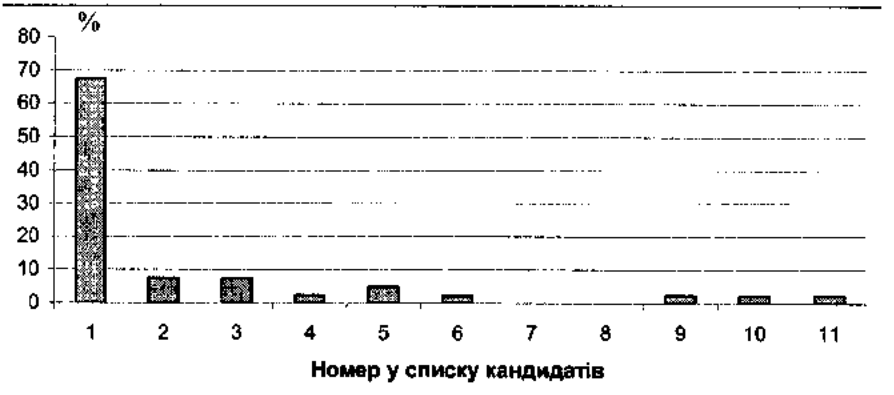
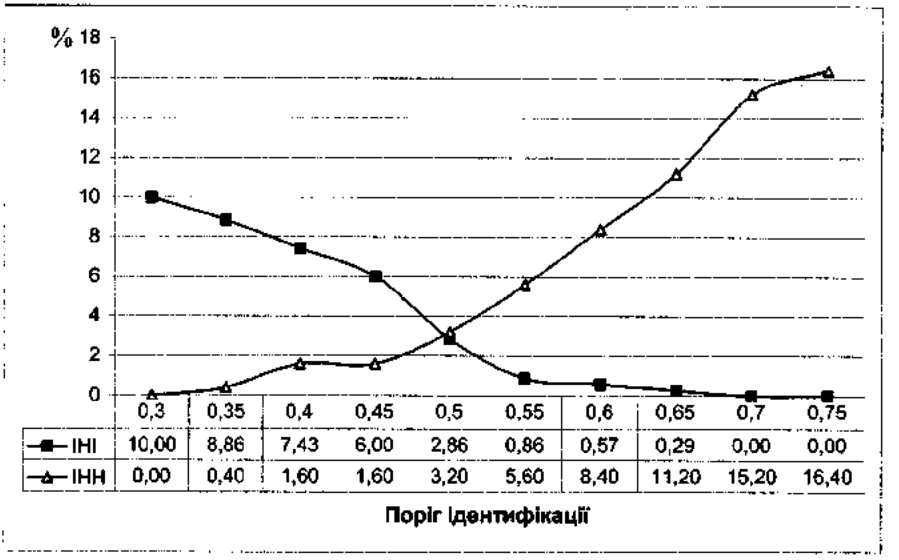


Рис.3.36. Розподіл місць еталонів слідів, що ідентифікуються в списку кандидатів.



	0,3	0,35	0,4	0,45	0,5	0,55	0,6	0,65	0,7	0,75
ІНІ	10,00	8,86	7,43	6,00	2,86	0,86	0,57	0,29	0,00	0,00
ІНН	0,00	0,40	1,60	1,60	3,20	5,60	8,40	11,20	15,20	16,40

Рис.3.37. Експериментально отримані імовірнісні характеристики БІС побудованої за розробленими блок-схемами.

Імовірнісні характеристики БІС, побудованої на основі розроблених блок-схем, представлені на рис. 3.37.

Експериментально встановлено, що при ІНН 15,2% досягається ІНІ 0%, що є кращим результатом і відповідає сучасним алгоритмам,

розглянутим у п.1.4.5 - 1.4.7. Але потрібно наголосити, що розмір області, за якою проводиться ідентифікація, рівний 100×100 точок. Для більшості відбитків із таким розміром інформативної області алгоритми, побудовані на особистих ознаках, видаватимуть повідомлення про малу кількість ознак для ідентифікації, не говорячи вже про саму ідентифікацію.

Порівняти отримані дані для АДІС з існуючими системами немає можливості, адже вони не розголошуються розробниками. В цьому випадку можемо лише наголошувати на тому, що система, побудована на основі розроблених ознак і методів, є повністю автоматизована (на відміну від "Дакто2000", "Сонда 7", в яких оператори повинні коректувати скелети), не вимагає наявності особистих ознак на відбитку (як в діючих системах), що дозволяє вести пошук за слідами малого розміру (чого не роблять існуючі АДІС).

РОЗДІЛ 4. БІОМЕТРИЧНИЙ ЗАХИСТ КЛЮЧІВ КРИПТОГРАФІЧНИХ АЛГОРИТМІВ

4.1. Біометричний екстрактор

На сьогоднішній день імовірнісні алгоритми та протоколи повністю змінили погляди на теорію складності, а у криптографії дозволили зробити те, що було нездійсненним за використання детермінованих алгоритмів. Імовірнісні алгоритми є швидшими, простішими та менш вимогливими до ресурсів, ніж відомі детерміновані алгоритми.

Імовірнісний алгоритм, окрім входу w, отримує випадкову двійкову послідовність $u \in \{0,1\}^l$, далі працює як звичайний детермінований алгоритм і результат роботи y подає на вихід. Довжина випадкової послідовності l залежить від довжини входу. Слід підкреслити, що вихід $y = y(w, u)$ імовірнісного алгоритму залежить не лише від входу, а й від випадкової послідовності. Випадкова послідовність вважається рівномірно розподіленою на $\{0,1\}^l$, тобто кожне u вибирається з імовірністю 2^{-l}.

Отже, очікуваним результатом роботи розглядуваних алгоритмів є дійсно випадкові біти, тобто бітова послідовність, біти у якій рівномірно розподілені та незалежні один від одного. Розглянемо методи отримання випадкових послідовностей бітів.

Перша група методів – це використання певного фізичного процесу. Прикладом є використання стабілітрона, на виході якого фіксуємо квантово-механічний шум; джерела радіоактивності; шуми мікрофонів та відеокамер; тощо. На жаль, деякі дослідження [184] вказують на нерівномірність розподілу вихідних бітових послідовностей із асиметріями, характерними для конкретного фізичного процесу.

Наступні методи – це використання так званих екстракторів [202] імовірнісних функцій, які описують процеси отримання потоку квазі-випадкових бітів із слабовипадкових джерел, тобто значеннями таких функцій є бітові послідовності, які жодним поліноміальним алгоритмом неможливо відрізнити від рівномірно розподілених бітових послідовностей такої ж довжини. Слабовипадкове джерело (термін запроваджений Цукерманом [265,266]) – це математична модель, яка описує об'єкти, що генерують послідовності довжиною n символів, $l < n$ із яких дійсно випадкові. Прикладами є:

- джерела на марковських ланцюгах: розподіл $\mathbf{P}[W]$ на $\{0,1\}^n$, а саме $w_1,\ldots, w_n$, отримується n - кроковим марковським ланцюгом із матрицею ймовірностей переходів $\boldsymbol{T}=(t_{ij})$, причому для l виконується умова

$$l/n < t_{ij} < 1-l/n; \tag{4.1}$$

- джерела на базі псевдовипадкових генераторів: на виході отримується розподіл $\mathbf{P}[W]$ на $\{0,1\}^n$ із наступною властивістю – для кожного $1\le i\le n$ і $b_1,\ldots, b_{i-1} \in \{0,1\}$ виконується умова

$$l/n \le P\left[w_i = 1 \middle| w_1 = b_1,\ldots,w_{i-1} = b_{i-1}\right] \le 1-l/n, \tag{4.2}$$

тобто кожен генерований біт є випадковим, навіть якщо відомі попередні біти (властивість непередбачуваності псевдовипадкових генераторів), уперше джерело розглядається у роботі [228] та більш ґрунтовно значно пізніше [116] уже як блочне джерело випадкових бітів;

- джерела із фіксацією бітів: генерується випадкова двійкова послідовність довжиною n біт, $n-l$ з яких залишаються незмінними, а l рівномірно розподілені та незалежні один від одного [117,120].

4.1.1. Екстрактор випадкових величин

Для подальшого формального опису екстрактора наведемо деякі визначення та нотації, які будуть надалі використовуватись.

Насамперед визначимо скінченний дискретний метричний простір $\boldsymbol{\Lambda}$ із метрикою ρ як функцією віддалі між його елементами $\rho : \boldsymbol{\Lambda}\times\boldsymbol{\Lambda} \to \mathbf{R}^+$, із властивостями тотожності ($\rho(x,y)=0, \Leftrightarrow x=y$) та трикутника ($\rho(x,y)\le\rho(x,z)+\rho(z,y), \quad \forall\, x,y,z \in \boldsymbol{\Lambda}$). Надалі розглядатиметься багатовимірний дискретний метричний простір у вигляді $\boldsymbol{\Lambda} = \boldsymbol{\mathcal{F}}^n$ для певного поля $\boldsymbol{\mathcal{F}}$. Для двійкового алфавіту $\boldsymbol{\Lambda} = \{0,1\}^n$.

Припустимо, що кожна точка простору відображається бінарною стрічкою, тоді довжина такої стрічки дорівнює $\log_2(\#\boldsymbol{\Lambda})$, де $\#\boldsymbol{\Lambda}$ – потужність простору.

Через U_d позначатимемо рівномірно розподілену випадкову величину на $\boldsymbol{\mathcal{F}}^d$, тобто $U_d \in_U \boldsymbol{\mathcal{F}}^d$. Через u – реалізацію випадкової величини U_d з рівномірним розподілом, тобто $U_d = u$, а через $X = x$ – реалізацію x деякої випадкової величини X. Для деякої функції f і випадкової величини W під $f(W)$ слід розуміти випадкову величину, яка отримується при застосуванні f до усіх $w \in W$.

Означення 4.1. **Статистична віддаль** [202,128,129,117] між розподілами ймовірностей випадкових величин W_1 та W_2 у просторі Λ – це сума:

$$D[W_1, W_2] = \sum_{w \in \Lambda} \left| P\{W_1 = w\} - P\{W_2 = w\} \right|,$$

де $P\{W\}$ – символ розподілу ймовірностей випадкової величини W.

Якщо $D[W_1, W_2] \le \varepsilon$, тоді говорять, що випадкові величини W_1 та W_2 є ε-близькими [190]. Говорять, що W_1 є ε-квазівипадковим, якщо W_1 є ε- близьким до випадкової величини рівномірного розподілу.

Означення 4.2. **Мінімальна ентропія** [116] розподілу ймовірностей $P\{W\}$ на $\mathcal{F}^n$ розраховується як

$$H_\infty(W) = \min_{w \in F^n} \log \frac{1}{P\{W = w\}}. \qquad (4.3)$$

Іншими словами, розподіл ймовірностей $P\{W\}$ має мінімальну ентропію більшу, ніж k, якщо ймовірність появи будь-якого w із $\mathcal{F}^n$ є меншою, ніж 2^{-k}.

Таке значення ентропії вперше введене криптограмами Кором та Гольдрайхом (Chor and Goldreich) [116] та часто застосовується у криптографії. На відміну від звичайної Шенонівської ентропії $H(W)$, яка оцінює величину невизначеності у середньому, мінімальна ентропія оцінює величину невизначеності у найгіршому випадку, тобто для деякої найімовірнішої вибірки. Слід підкреслити, що мінімальна ентропія є обмеженою зверху Шенонівською ентропією, тобто $H_\infty(W) \le H(W)$, і дорівнює їй, якщо випадкова величина W є рівномірно розподіленою.

Якщо випадкова величина W є залежною від іншої випадкової величини V, тоді говорять про середню мінімальну ентропію W за умови V:

$$\tilde{H}_\infty(W \mid V) = \log\left(\mathrm{E}_V \left\{ \min_{w \in F^n} \frac{1}{P\{W = w \mid V\}} \right\} \right) = \log\left(\mathrm{E}_V \left\{ 2^{H_\infty(W \mid V)} \right\} \right),$$

де $\mathrm{E}\{\}$ – символ математичного очікування.

Якщо V бітова послідовність довжиною l біт, тоді

$$\tilde{H}_\infty(W \mid V) \ge H_\infty(W) - l.$$

Таку ентропію ще називають залишковою ентропією випадкової величини W за умови, що відома випадкова велична V [105,147].

Означення 4.3. **(n, m, l, ε) - екстрактор** [202,228,265,266] – це імовірнісна функція

$$Ext:\{0,1\}^n \times \{0,1\}^d \to \{0,1\}^l, \qquad (4.4)$$

яка для будь-якої випадкової величини (слабовипадкового джерела) W визначеної на $\{0, 1\}^n$ з мінімальною ентропією $H_\infty(W) \le m$, видає випадкову величину $Ext(W, U_d)$, яка є ε-близькою до U_l.

У формулі (4.4) n – довжина джерела; m – поріг мінімальної ентропії; ε – помилка екстрактора; d – довжина паростка (визначення за Вербіцьким [15]).

Уведемо наступні властивості екстрактора:

коефіцієнт ентропії джерела – це відношення m/n;

коефіцієнт випадковості – це відношення l/m;

втрата ентропії – $\Delta H = m + d - l$, тобто вхідна мінімальна ентропія дорівнює $m + d$, а дана властивість вказує на кількість втраченої ентропії у процесі екстракції.

У роботі [238] вказані залежності між вхідними та вихідним параметрами розсіювача (disperser, аналог екстрактора):

$$d = \log(n - m) + 2\log(1 / \varepsilon) - O(1),$$
$$l = m + d - 2\log(1 / \varepsilon) + O(1),$$

тобто втрата ентропії екстрактора рівна $2\log(1 / \varepsilon) - O(1)$.

У якості екстрактора іноді використовуються попарно-незалежні хеш функції [147,106]. Показано, що для такої конструкції екстрактора $l = m + d - 2\log(1 / \varepsilon)$.

4.1.2. Біометричний екстрактор та біометричний ідентифікатор

Усі, без винятку, сучасні криптографічні алгоритми для захисту значних об'ємів конфіденційної інформації застосовують порівняно недовгі таємні стрічки даних – ключі. Ключ чи пара ключів – це послідовність незалежних один від одного та рівномірно розподілених бітів. Такі таємні стрічки генеруються детермінованими [104,232], а останнім часом і ймовірнісними алгоритмами. Оперуючи поняттям екстрактора автори роботи [131] описали ряд псевдовипадкових генераторів для створення ключів.

Після генерації ключ записується на деякому електронному носії і надалі служить використовується для шифрування та розшифрування. Як показано у першому розділі, безпосереднє використання біометричних даних у якості ключа у криптографії є неможливим через нечіткість та стабільність біометрії при кожному наступному зчитуванні. Саме тому описану вище математичну модель екстрактора необхідно розширити до криптографічного примітива, придатного для зв'язування попередньо згенерованих сильних криптографічних ключів

з нечіткими та нерівномірно розподіленими вхідними біометричними даними. Для цього створено біометричні екстрактор та ідентифікатор.

Означення 4.4. **($\mathcal{F}$, m, l, t, ε) - біометричний екстрактор** – це пара функцій $\langle FG, FR\rangle$ із такими властивостями:

FG – імовірнісна генеруюча функція, яка, отримуючи на вхід $W \in \mathcal{F}^n$ та $U_d \in_U \mathcal{F}^d$, видає таємну стрічку $S \in \mathcal{F}^l$ та відкриту стрічку $Q \in \mathcal{F}^*$, які для усіх випадкових величин $W \in \mathcal{F}^n$ із мінімальною ентропією $H_\infty(W) \geq m$ та двійки величин $\langle S, Q\rangle \leftarrow FG(W, U_d)$ задовольняють нерівності $\mathrm{D}[S, U_l] \leq \varepsilon$:

$$FG : \mathcal{F}^n \times \mathcal{F}^d \to \mathcal{F}^l \times \mathcal{F}^*;$$

FR – відновлююча функція, яка, отримуючи на вхід $W' \in \mathcal{F}^n$ та відкриту стрічку $Q \in \mathcal{F}^*$, видає стрічку $S' \in \mathcal{F}^l$, яка для усіх $W, W' \in \mathcal{F}^n$ із $\rho(W, W') \leq t$ та двійки величин $\langle S, Q\rangle \leftarrow FG(W, U_d)$ задовольняє умові $S' = S$:

$$FR : \mathcal{F}^n \times \mathcal{F}^* \to \mathcal{F}^l.$$

Залишкова ентропія біометричного екстрактора

$$\tilde{H}_\infty(W \mid Q) = l \geq m + d - 2\log(1/\varepsilon).$$

Біометричний екстрактор зводиться до "чіткого", якщо $t = 0$, $Q = U_d$.

Біометричний екстрактор вирішує проблему стабільності, а саме дозволяє поставити у відповідність до біометричних даних один або більше випадково вибраних ключів. Для вирішення проблеми нечіткості нами уперше введено поняття біометричного ідентифікатора. Біометричний ідентифікатор – це композиція функцій, яка відображає вхідні біометричні дані у певну структуру, нечутливу до визначеного рівня змін у біометричних даних.

Означення 4.5. **($\mathcal{F}$, m, m', t) - біометричний ідентифікатор** – це пара функцій $\langle FI, FC\rangle$ із наступними властивостями :

FI – імовірнісна ідентифікуюча функція, яка, отримуючи випадкову величину $W \in \mathcal{F}^n$ із мінімальною ентропією $H_\infty(W) \geq m$ та паросток $U_d \in_U \mathcal{F}^d$, видає величину $p \in \mathcal{F}^*$ – ідентифікатор, який задовольняє нерівності $\tilde{H}_\infty(W \mid p) \geq m'$, тобто втрата ентропії біометричного ідентифікатора за умови, що відомо p, $\Delta H = m - m'$:

$$FI : \mathcal{F}^n \times \mathcal{F}^d \to \mathcal{F}^*;$$

FC – коректуюча функція, яка, отримуючи на вхід $W' \in \mathcal{F}^n$ та результат від попередньої функції p, видає таке $W'' \in \mathcal{F}^n$, що для усіх

$p \leftarrow FI(W, U_d)$ та $\rho(W, W') \le t$ виконується умова $W'' = W$, тобто $FC(W', FI(W, U_d)) = W$:

$$FC : \mathcal{F}^n \times \mathcal{F}^* \to \mathcal{F}^n.$$

4.1.3. Біометричний екстрактор з біометричного ідентифікатора та чіткого екстрактора

Покажемо, що біометричний екстрактор – це складена конструкція, а саме, побудований з біометричного ідентифікатора та чіткого екстрактора. Перепишемо двійку функцій біометричного екстрактора наступним чином:

$FG(W, \langle U_{d1}, U_{d2}\rangle)$:
- розраховуємо $p \leftarrow FI(W, U_{d1})$ та $S \leftarrow Ext(W, U_{d2})$;
- виводимо $\langle S, Q\rangle$, де $Q \leftarrow \langle p, U_{d2}\rangle$.

$FR(W', \langle p, U_{d2}\rangle)$:
- відновлюємо $W \leftarrow FC(W', p)$;
- виводимо $S \leftarrow Ext(W, U_{d2})$.

Генеруюча функція FG отримує на вхід випадкову величину W деякого нерівномірного розподілу та двійку паростків $\langle U_{d1}, U_{d2}\rangle$ для роботи імовірнісних функцій. Функція FI створює ідентифікатор p вхідної величини W, а чіткий екстрактор видає таємну стрічку S, що застосовуватиметься у криптографічних алгоритмах у ролі ключа чи пароля. Цій стрічці ставиться у відповідність відкрита величина Q, яка використовуватиметься надалі функцією FR для відновлення таємної стрічки S.

На відміну від генеруючої функції, яка служитиме лише один раз для створення S та її ідентифікатора Q, відновлююча функція вживатиметься постійно для отримання із вхідних даних W', які є близькими у певному розумінні до W, таємної стрічки S. Саме міра близькості W' до W визначатиме конструкцію біометричного екстрактора.

4.2. Конструкції біометричного екстрактора

Досягнути нечутливості біометричного екстрактора до деякої кількості помилок можливо за допомогою кодів корекції помилок (ККП) у скінченному дискретному просторі $\mathcal{F}^n$.

Код $\mathbf{C}$ з параметрами $[n, k, d]$ – це підмножина $\{w_1, w_2, \dots, w_K\}$ простору $\mathcal{F}^n$, де $K = n^k$. Елементи $\mathbf{C}$ називають кодовими словами, а підмножину з усіх кодових слів – кодовою книгою. Функцію

$C : \mathcal{F}^k \to \mathcal{F}^n$ називають функцією кодування. Мінімальною віддаллю у коді **C** називають таке найменше $d > 0$, яке для усіх $i \neq j$ задовольняє умові $\rho(w_i, w_j) \geq d$. Поріг декодування у **C** – це таке найбільше $t > 0$, котре для усіх $w \in \mathcal{F}^n$ ставить у відповідність лише одне кодове слово $w_i \in \mathbf{C}$, для якого виконується умова $\rho(w_i, w) \leq t$. Тобто, якщо $\rho(w_i, w) \leq t$ і задана відповідна до C функція декодування D, тоді $C(D(w)) = w_i$. У випадку $\mathcal{F} \subseteq \mathbf{R}^+$ справедлива умова:

$$t = \lfloor (d-1)/2 \rfloor.$$

Уведемо у простір $\mathcal{F}^n$ операцію перестановки елементів $\mathbf{\Pi} = \{\pi_i : \mathcal{F}^n \to \mathcal{F}^n\}$ – сімейство взаємно однозначних відображень у $\mathcal{F}^n$ на себе, проіндексоване по i.

Π утворює групу, якщо визначена групова операція множення (композиції) $\circ$, відносно якої у **Π** існує одинична перестановка та обернена підстановка $\pi_i \circ \pi_i^{-1} = 1$.

Π володіє наступними властивостями:

- транзитивності, якщо для будь-якої пари $a, b \in \mathcal{F}^n$ існує таке $\pi_i \in \mathbf{\Pi}$, що $\pi_i(a) = b$;
- ізометрії, якщо для будь-якої пари $a, b \in \mathcal{F}^n$ та визначеної у $\mathcal{F}^n$ метрики ρ має місце $\rho(a, b) = \rho(\pi_i(a), \pi_i(b))$.

Прикладом сімейства перестановок, що володіє вказаними властивостями, є множина усіх зсувів $\pi_x(w) = w \oplus x$ у просторі з метрикою Хемінга (п.4.2.1).

Користуючись поняттям коду та перестановки, слід формально описати ядро будь-якої конструкції біометричного ідентифікатора.

Нехай на вхід FI подано $w \in \mathcal{F}^n$. Необхідно випадковим чином вибрати такі кодове слово $b \in \mathbf{C}$ та перестановку $\pi \in \mathbf{\Pi}$, що відповідають $\pi(w) = b$. На виході ідентифікуючої функції отримуємо $FI(w) = \pi$. Для відновлення w, якщо задано w' та ідентифікатор $p = \pi$, потрібно знайти найближче до $\pi(w')$ кодове слово b' та вивести $\pi^{-1}(b')$. Якщо $\rho(w, w') \leq t$, а отже, і $\rho(b, \pi(w')) \leq t$, тоді $b' = b$ та $w = \pi^{-1}(b')$.

4.2.1. Конструкція для віддалі Хемінга

Розглянемо конструкцію біометричного екстрактора у векторному просторі $\mathcal{F}^n = \{0, 1\}^n$, метрикою якого є віддаль Хемінга.

Нехай $C : \{0, 1\}^k \to \{0, 1\}^n$ двійковий ККП з параметрами $[n, k, d]$, де $d = 2t + 1$, та відповідною функцією декодування

$D: \{0,1\}^n \to \{0,1\}^k$. Для паростка $U_d \in_U \{0,1\}^k$ визначимо ідентифікуючу та коректуючу функції наступним чином:

$$p \leftarrow FI(w, U_d) = w \oplus C(U_d), \qquad w \leftarrow FC(w', p) = p \oplus C(D(w' \oplus p)),$$

де $\oplus$ – сума по модулю 2.

У разі лінійності коду **C** значення p відповідатиме синдрому вектора w, тобто $p = \text{synd}_C(w)$. Оскільки синдром лінійного коду із кодовою книгою з K елементів є бітовою послідовністю у $n-k$ біт, втрата ентропії біометричного ідентифікатора з кодовим зсувом становить $n-k$ біт.

Лема 4.1. Для будь-якого $[n, k, d]$ – коду **C** ідентифікуюча та коректуюча функції, що визначені вище, утворюють $(\mathcal{F}, m, m+k-n, t)$ – біометричний ідентифікатор.

Доведення. Нехай функція декодування D коректує до t помилок. Якщо $p = FI(w, U_d) = w \oplus C(U_d)$ та $\rho(w, w') \le t$, тоді $D(w' \oplus p) = U_d$, а $w = FC(w', p) = p \oplus C(D(w' \oplus p))$. Нехай A – сумісна випадкова величина (U_d, W). Для незалежних випадкових величин U_d та W виконується $H_\infty(A) = H_\infty(W) + H_\infty(U_d) = m + k$. Враховуючи, що $p \in \{0,1\}^n$, одержуємо $\widetilde{H}_\infty(W, U_d \mid p) \ge m + k - n$. Якщо задане p, тоді U_d та W взаємно однозначно обчислюються, тому попередній вираз записується як $\widetilde{H}_\infty(W \mid p) \ge m + k - n$.

Лему доведено.

У випадку, коли W є випадковою величиною з рівномірним розподілом, тобто $m = n$, $S = U_d$ та $FR(w', p) = D(w' \oplus p)$, отримується $(\mathcal{F}, m, l, t, 0)$ – біометричний екстрактор. Якщо W є рівномірно розподіленим, тоді рівномірно розподіленим та незалежним від U_d є p. Екстрактор саме такого виду запропонували автори роботи [164]. Але через те, що W – це біометричні дані, величина матиме нерівномірний розподіл. Отже, p викриває інформацію про U_d: $\widetilde{H}_\infty(U_d \mid p) < H_\infty U_d)$. Саме тому у конструкцію необхідно ввести чіткий екстрактор. У результаті отримується $(\Lambda, m, l, t, \varepsilon)$ – біометричний екстрактор згідно п. 4.1.3, де t – віддаль Хемінга, а $l = m + k - n - 2\log(1/\varepsilon)$.

4.2.2. Конструкція для різниці множин

Розглянемо колекцію усіх множин із потужністю s у просторі $\mathcal{F} = \{1, \ldots, n\}$. Віддаллю між двома множинами **A** та **B** у просторі $\mathcal{F}$ є кількість елементів, які належать **A**, але не належать **B**. Враховуючи, що множини мають однаковий розмір s, метрику визначають, як

половину симетричної різниці множин **A** та **B**, тобто $\rho(\mathbf{A}, \mathbf{B}) = 1/2\ |\mathbf{A}\Delta\mathbf{B}|$.

Множини **A** та **B** можна розглядати як характеристичні вектори простору $\mathcal{F}$ довжиною n з бінарною метрикою – віддалю Хемінга (враховуючи коефіцієнт ½) між бітовими послідовностями із s ненульовими бітами.

Надалі припускається, що n є значно більшим від s, і розглядатимуться два випадки:

1. *малий простір* $\mathcal{F}$ – $n = O(s^a)$, де $a \in \mathbf{R}^+$ деяка константа, алгоритми виконуватимуться у поліноміальному часі та вимагатимуть поліноміальних затрат пам'яті;
2. *великий простір* $\mathcal{F}$ – $n = O(a^s)$, де $a \in \mathbf{R}^+$ деяка константа, алгоритми виконуватимуться у суперполіноміальному часі та вимагатимуть суперполіноміальних затрат пам'яті;

а) Малий простір. Представлення множини у просторі $\mathcal{F}$ характеристичними векторами дозволяє застосувати методику, викладену у конструкції для віддалі Хемінга, зауваживши лише, що метрика у випадку різниці множин дорівнює половині віддалі Хемінга між характеристичними векторами.

За малого простору множини простору розглядаються як кодові слова коду сталою вагою. Після викладення цієї методики здійснимо порівняння обох конструкцій за допомогою саме віддалі Хемінга.

Нехай **C** є $[n, k, d]$ – код із кодовими словами сталої ваги s. Кожне кодове слово є характеристичним вектором множини у просторі $\mathcal{F}$. Розглянемо алгоритм реалізації біометричного ідентифікатора.

1. Вхід: множина $\mathbf{A} \subset \mathcal{F}$, $\#\mathbf{A} = s$, $\#\mathcal{F} = n$;
2. Вибрати випадковим чином $\mathbf{B} \subset \mathcal{F}$ таке, що $\mathbf{B} \subseteq \mathbf{C}$;
3. Вибрати випадковим чином перестановку $\pi : \mathcal{F} \to \mathbf{C}$ таку, що $\pi(\mathbf{A}) = \mathbf{B}$, тобто вибрати деяку відповідність між **A** та **B** і між $\mathcal{F} - \mathbf{A}$ та $\mathcal{F} - \mathbf{B}$;
4. Вихід: $FI(\mathbf{A}) = \pi$ (наприклад, список: $\pi(1), \ldots, \pi(n)$).

Лема 4.2. Нехай **C** – це $[n, k, d]$ код із сталою вагою. Тоді

1. якщо $d \geq 4t + 1$, для деякого $t > 0$, то існує алгоритм $FC()$, який $FC(\mathbf{A}', FI(\mathbf{A})) = \mathbf{A}$ для будь-яких множин **A** та **A′**, для яких виконується нерівність $\frac{1}{2}\ |\mathbf{A}\Delta\mathbf{A}'| \leq t$;
2. залишкова ентропія $\tilde{H}_\infty(\mathbf{A} \mid FI(\mathbf{A})) \geq H_\infty(\mathbf{A}) + k - \log\binom{n}{s}$.

Доведення.

1. Нехай задано випадкову перестановку π та множину $\mathbf{A}'$ з потужністю s, тоді можливо порахувати $\mathbf{B}' = \pi(\mathbf{A}')$. Оскільки π володіє властивістю транзитивності, перетин $\mathbf{B}' \cap \mathbf{B}$ матиме такий самий розмір, як і $\mathbf{A} \cap \mathbf{A}'$, тож віддаль Хемінга між характеристичними векторами $\mathbf{B}'$ та $\mathbf{B}$ є не більшою від $2t$. Через те, що код $\mathbf{C}$ має кодову віддаль $d \geq 4t + 1$, тобто здатен коректувати $2t$ помилок, найближчим кодовим словом до $\mathbf{B}'$ є саме $\mathbf{B} = \pi(\mathbf{A})$. Отже, $\mathbf{A} = \pi^{-1}(\mathbf{B}')$.

2. Нехай X – випадкова величина, що використовується у конструкції біометричного ідентифікатора.

Існує $s!$ варіантів відповідностей між $\mathbf{A}$ та $\mathbf{B}$ і $(n-s)!$ варіантів відповідностей між $\Lambda - \mathbf{A}$ та $\Lambda - \mathbf{B}$, тому мінімальна ентропія пари $(\mathbf{A}, X)$ рівна $H_\infty(\mathbf{A}) + \log(s!\,(n-s)!)$.

Існує $n!$ варіантів перестановок π у просторі Λ, тоді залишкова ентропія $(\mathbf{A}, X)$ за умови, що задано $FI(\mathbf{A})$, становитиме

$$\widetilde{H}_\infty(\mathbf{A}, X \mid FI(\mathbf{A})) \geq = H_\infty(\mathbf{A}) + \log(s!\,(n-s)!) - \log(n!) =$$

$$H_\infty(\mathbf{A}) + k - \log\binom{n}{s}.$$

Якщо задане $FI(\mathbf{A})$, то $\mathbf{A}$ та X взаємно однозначно визначаються, тому

$$\widetilde{H}_\infty(\mathbf{A}, X \mid FI(\mathbf{A})) = \widetilde{H}_\infty(\mathbf{A}, \mid FI(\mathbf{A})).$$

Лему доведено.

Отже, втрата ентропії біометричного ідентифікатора на базі кодів із постійною вагою рівна $\log\binom{n}{s} - k$.

б) Порівняння конструкції для віддалі Хемінга з конструкцією для різниці множин (малий простір). Із літератури по теорії інформації та кодуванню для будь-яких кодів вводяться такі характеристики:

- $M(n, d)$ – максимальна потужність кодової книги бінарного коду з довжиною кодового слова n і кодовою віддаллю d;
- $M(n, d, s)$ – максимальна потужність кодової книги бінарного коду з довжиною кодового слова n та вагою s, d – кодова віддаль.

Порівняємо методику з використанням перестановок із методикою, що застосовує віддаль Хемінга у конструкції для різниці множин. Для коректного порівняння необхідно прийняти, що кодова віддаль коду $d \geq 4t + 1$. Конструкція із кодовим зсувом завдяки

оптимальним кодам (кодам із максимальним упакуванням) забезпечує втрату ентропії на рівні $n - \log(M(n, d))$. Конструкція із вибором випадкової перестановки – $\log\binom{n}{s} - \log(M(n, d, s))$. Нерівність Бесальго-Еліаса (Bassalygo-Elias) [252] вказує, що втрата ентропії для схеми з випадковою перестановкою є обмеженою зверху втратою ентропії у схемі для віддалі Хемінга, тобто

$$M(n,d)\cdot 2^{-n} \le M(n,d,s)\cdot\binom{n}{s}^{-1}$$

або

$$n - \log M(n,d) \ge \log\binom{n}{s} - \log M(n,d,s).$$

Отже, для простору, в якості метрики якого використовується різниця множин, оптимальною є методика на основі випадкових перестановок.

в) Великий простір. Нехай $n = \#\mathcal{F}$ є степенем простого числа ($n = g^k$, де g просте число) і розглядатимемо поле $\mathcal{F} = \mathrm{GF}(n)$.

Необхідно створити алгоритм зв'язування (блокування) [8,10] секретних даних $M = \{m_0,\ldots, m_{k-1}\} \subset \mathcal{F}$ із множиною $W = \{w_1,\ldots, w_s\} \subset \mathcal{F}$, де k та s – параметри алгоритму. На виході алгоритму отримують набір кортежів $B_P \subseteq \mathcal{F}^r \times \mathcal{F}^r$ для деякого параметра безпеки алгоритму $s < r \le n$. Набір B_P містить у прихованій формі інформацію про M і готовий для безпечного зберігання та передавання відкритими каналами зв'язку. На вхід алгоритму розблокування подається B_P та множина $W' = \{w'_1,\ldots, w'_s\} \subset \mathcal{F}$. Якщо множина W є достатньо близькою до W', тоді на виході екстрактора отримуємо M, інакше – "null". Тобто $B_P = p = FI(W, U_d)$, відповідно $W = FC(W, B_P)$ та $M = S \leftarrow Ext(W, B_P)$.

В алгоритмі використаємо $\mathbf{C} - [s, k, d]$ код Ріда-Соломона (РСК). У літературі широко описана теорія цих кодів [4,182,222] та запропоновано цілий ряд швидких алгоритмів кодування/декодування [146,227,245].

У класичному застосуванні РСК M є повідомленням, яке потрібно передати по каналу з шумом. Повідомлення використовують для створення унікального полінома:

$$f(x) = m_0 + m_1 x + \ldots + m_{k-1} x^{k-1}. \qquad (4.5)$$

Кодове слово c утворюють за допомогою полінома. На вхід декодера подають спотворене шумом кодове слово c'. За алгоритмом декодування РСК відновлюють істинне кодове слово c, реконструюють поліном $f(x)$, а отже, і повідомлення, що передавалось каналом зв'язку.

Нас цікавить РСК з кодовими словами c довжиною s інформаційних символів, які є елементами поля $\mathcal{F}$. Кожне кодове слово отримуємо за допомогою унікального полінома $f(x)$ степеня $k-1$ над полем $\mathcal{F}$, тобто $c = \{c_1 = f(w_1), c_2 = f(w_2),\ldots, c_s = f(w_s)\}$, де $w_1,\ldots, w_s$ та $c_1,\ldots, c_s$ – елементи поля $\mathcal{F}$. Загальна кількість можливих кодових слів n^k. Для досягнення завадостійких властивостей необхідно, щоб $s > k$. Як показано у літературі [139], такий код формує лінійний код у полі $\mathcal{F}$ із мінімальною кодовою відстанню $d = s - k + 1$ та здатен коректувати до $t = \dfrac{s-k}{2}$ помилок.

Вхідними даними алгоритму зв'язування є секретні дані M довжиною k елементів та множина блокування $W = \{w_i\}^s_{i=1}$. Основною ідеєю є генерація кодового слова РСК відповідного до M. Перед початком роботи алгоритму вихідна множина кортежів B_P дорівнює порожній множині $\varnothing$. На першому етапі створюємо поліном $f(x)$ степеня $k-1$ з елементів M. Далі заповнюємо B_P s двійками елементів w_i та $c_i = f(w_i)$, де c_i – елементи кодового слова РСК.

Для досягнення криптографічної надійності алгоритму зв'язування на останньому етапі набір кортежів B_P доповнюємо $(r-s)$ двійками фіктивних елементів α_i та $\beta_i \neq f(\alpha_i)$. Елементи відповідають таким умовам:

1. елементи вибирають випадково;
2. елементи знаходяться у множинах, що задовольняють виразам

$$\{\alpha_i\}^r_{i=s+1} \not\subset \{w_i\}^s_{i=1},\ \{\beta_i\}^r_{i=s+1} \not\subset \{f(\alpha_i)\}^s_{i=1}. \qquad (4.6)$$

На рис.4.1 зображено блок-схему алгоритму блокування.

Блок-схему алгоритму розблокування зображено на рис.4.2. На вхід алгоритму подають набір B_P та множину розблокування $W' = \{w'_i\}^s_{i=1}$. На першому етапі необхідно із набору $B_P = \{(x_i, y_i)\}^r_{i=1}$ виділити вірні кортежі. Умовою відбору є близькість перших елементів кортежу елемента множини W', тобто x_i та w'_i. Результатом виділення є набір кортежів $B_P' = \{(w'_i, c'_i)\}^s_{i=1}$, другі елементи якого відповідають елементам кодового слова c'.

Оскільки множина W' містить більшість елементів W, але не рівна W, кодове слово c' не рівне початковому кодовому слову c, тому,

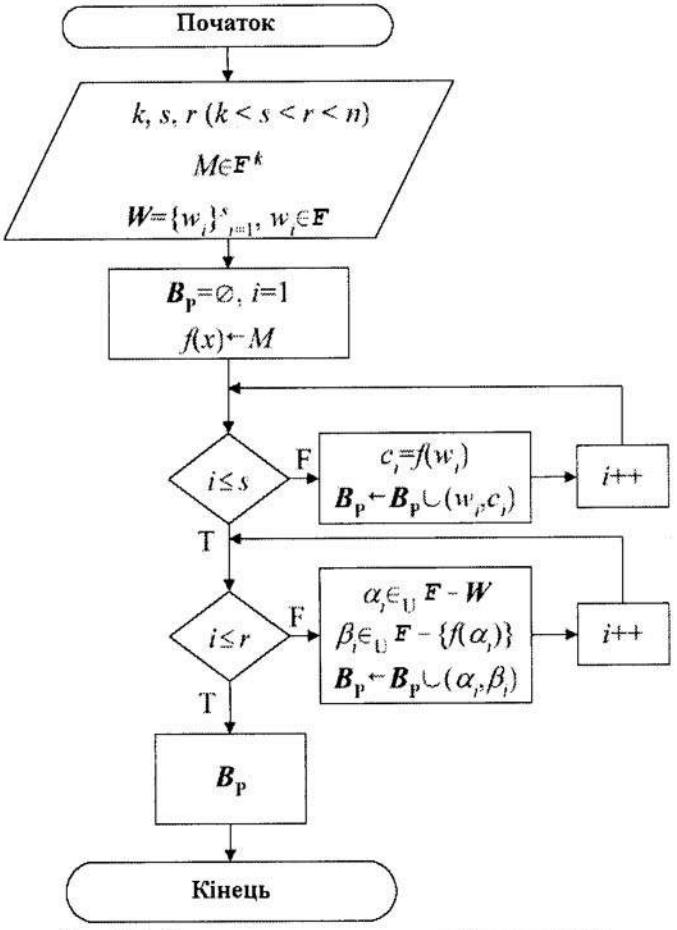


Рис.4.1. Блок - схема алгоритму блокування.

використовуючи набір кортежів B_P', необхідно здійснити інтерполяцію полінома степеня $k-1$ (на блок-схемі – *PolyInt*(B_P', k)). Результатом може бути або поліном $f(x)$, або "null".

На сьогодні відомо ряд методів інтерполяції. Кожен із методів характеризується мінімальною кількістю елементів τ, через які проходить поліном, для успішної його інтерполяції. Найпростішим методом є метод простого перебору [149]. Метод для реконструкції полінома використовує інтерполяцію Ньютона k точками із набору B_P'. Його перевагою є малі значення $\tau = k$, недоліком – значні затрати часу для повного перебору C^s_k варіантів. Найпотужнішими методами

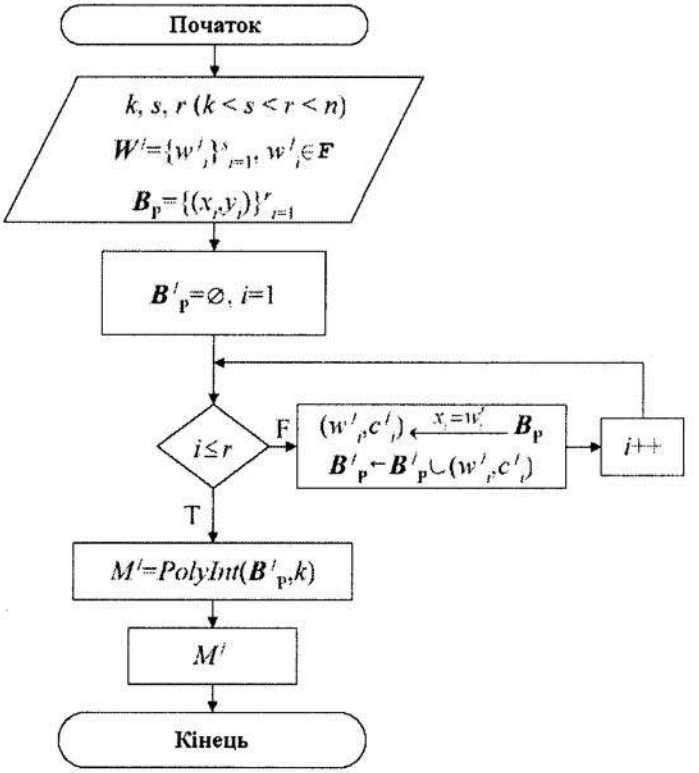


Рис.4.2. Блок-схема алгоритму розблокування.

реконструкції полінома є метод Берлекемпа-Месі ($\tau_{БМ} = \frac{s+k}{2}$) [227] та метод Судана ($\tau_C = \sqrt{ks}$) [146]. Перевагою останнього є менші значення τ ($\tau_C < \tau_{БМ}$), недоліком – складніша реалізація та менша швидкодія порівняно з методом Берлекемпа-Месі. Саме тому в алгоритмі розблокування використаємо метод Берлекемпа-Месі.

Метод інтерполяції накладає певні обмеження на множини $\boldsymbol{W}$ та $\boldsymbol{W}'$. Для успішного відновлення секретних даних M необхідно, щоб $\#(\boldsymbol{W} \cap \boldsymbol{W}') \geq \tau$.

Параметр r визначає, з одного боку, затрати пам'яті на зберігання та розповсюдження, а з іншого – надійність алгоритму. При $r = s$ набір кортежів B_P містить лише елементи множини блокування w_i та їхні відображення c_i, а тому однозначно вказує на використовуваний поліном $f(x)$. Зі збільшенням r утворюється множина фіктивних

поліномів, подібних до $f(x)$, а саме: степінь полінома – $k-1$; значення $f(x)$ збігаються з $B_{\mathbf{P}}$ у s точках. Інакше кажучи, що більше додано фіктивних точок, то більшою є імовірність того, що будь-які s із загальної кількості r лежать на поліномі степеня $k-1$, відмінному від $f(x)$. Отже, під час введення фіктивних елементів у $B_{\mathbf{P}}$ приховуються істинні елементи множини $\boldsymbol{W}$, а відтак, і поліном $f(x)$, що несе інформацію про секретні дані, тому алгоритм є надійним в обчислювальному сенсі, а рівень надійності пропорційний до загальної кількості поліномів.

Лема 4.3. Втрата ентропії $FI(\boldsymbol{W}, U_d)$ біометричного ідентифікатора є не більшою, ніж

$$2t\log n + \log\binom{n}{r} - \log\binom{n-s}{r-s}.$$

Доведення. Нехай U_d – випадкова величина, що використовується в алгоритмі ідентифікатора $FI(\boldsymbol{W})$. Очевидно, що максимальна степінь полінома $f(x)$ при збереженні коректуючих властивостей $k = s-2t-1$, тобто створення полінома вимагає $s-2t$ вибірок з $\mathcal{F}$, що відповідає n^{s-2t} способам вибору або кількості можливих кодових слів. Вибір фіктивних α_i можна здійснити $\binom{n-s}{r-s}$ способами, а $\beta_i - n^{r-s}$ способами. Мінімальна ентропія пари $\boldsymbol{W}$ та U_d рівна

$$H_\infty(\boldsymbol{W}, U_d) = H_\infty(\boldsymbol{W}) + \log(n^{s-2t}) + \log\binom{n-s}{r-s} + \log(n^{r-s})$$

або

$$H_\infty(\boldsymbol{W}, U_d) = H_\infty(\boldsymbol{W}) + (r-2t)\log n + \log\binom{n-s}{r-s}.$$

На виході алгоритму отримуємо набір кортежів $B_{\mathbf{P}}$ – кількість можливих варіантів $\binom{n}{r} \times n^r$. Отже, залишкова ентропія

$$\tilde{H}_\infty(\boldsymbol{W}, U_d \mid FI(\boldsymbol{W})) = H_\infty(\boldsymbol{W}) + (r-2t)\log n + \log\binom{n-s}{r-s} - \log\left(\binom{n}{r} n^r\right),$$

$$\tilde{H}_\infty(\boldsymbol{W}, U_d \mid FI(\boldsymbol{W})) = H_\infty(\boldsymbol{W}) - 2t\log n - \log\binom{n}{r} + \log\binom{n-s}{r-s}. \quad (4.7)$$

Враховуючи, що U_d однозначно визначається, якщо задані $\boldsymbol{W}$ та $FI(\boldsymbol{W})$, наступні ентропії рівні:

$$\widetilde{H}_{\infty}(\boldsymbol{W}, U_d \mid FI(\boldsymbol{W})) = \widetilde{H}_{\infty}(\boldsymbol{W} \mid FI(\boldsymbol{W})).$$

Лему доведено.

Зауваження. Використавши заміну

$$\binom{n}{r}\binom{r}{s} = \binom{n}{s}\binom{n-s}{r-s},$$

втрату ентропії перепишемо наступним чином:

$$2t\log n - \log\binom{r}{s} + \log\binom{n}{s}.$$

Далі, через те, що ентропія $H_{\infty}(\boldsymbol{W})$ є не більшою за $\log\binom{n}{s}$, залишкова ентропія обмежена зверху значенням

$$\log\binom{r}{s} - 2t\log n\ ,$$

тобто для збільшення останньої необхідно збільшувати r.

4.2.3. Оцінка верхньої межі втрати ентропії біометричного ідентифікатора та біометричного екстрактора

Розглянемо код $\mathbf{C} - [n, k, d]$, визначений у дискретному просторі $\boldsymbol{\mathcal{F}}^n$. Код має такі властивості:

- K – потужність кодової книги, $K = \#\mathbf{C}$;
- d – мінімальна віддаль між кодовими словами;
- t – максимальна кількість помилок, які здатен коректувати код;
- $K(n, t)$ – максимальне K, для якого існує $\mathbf{C}$;
- $K(n, t, m)$ – максимальне K, для якого всі кодові слова коду $\mathbf{C}$ належать множині $\boldsymbol{M} \subseteq \boldsymbol{\mathcal{F}}^n$ з потужністю $\#\boldsymbol{M} = 2^m$;
- $L(n, t, m) = \log(\min_{|M|=2^m} K(n,t,m))$ – у випадку, коли $m = n$, тобто

$$L(n, t, m) = \log K(n, t).$$

Точне визначення $K(n, t)$ та $K(n, t, m)$ для заданого коду $\mathbf{C}$ є головною проблемою у теорії кодування. Вважатимемо, що вони визначені, та дамо верхню оцінку залишкової ентропії біометричного ідентифікатора та біометричного екстрактора.

Лема 4.4. Залишкова ентропія (Λ, m, m', t) - біометричного ідентифікатора є обмеженою зверху $m' \le L(n, t, m)$.

Доведення. Нехай задані $FI()$, $FC()$, множина $\boldsymbol{M} \subseteq \Lambda$ з потужністю $\#\boldsymbol{M} = 2^m$ та випадкова величина з рівномірним розподілом W.

Згідно з визначенням біометричного ідентифікатора $\widetilde{H}_{\infty}(W \mid FI(W)) \ge m'$. Зокрема, мусить існувати таке v, для якого $\widetilde{H}_{\infty}(W \mid FI(W) = v) \ge m'$, а це говорить про те, що за умови існування $FI(W) = v$ існує щонайменше $2^{m'}$ значень величини W (назвемо цю множину $\boldsymbol{T}$) у множині $\boldsymbol{M}$, які задовольняють умову $FI(W) = v$.

Далі стверджуватимемо, що усі $2^{m'}$ величини W утворюють ККП із порогом декодування t. У протилежному випадку знайшлося б таке $w' \in \Lambda$, для якого $\rho(w_0, w') \le t$ та $\rho(w_1, w') \le t$, де $w_0, w_1 \in \boldsymbol{T}$ та $w_0 \ne w_1$. Тобто функція $FC(w', v)$ могла б видати або w_0, або w_1, що є неможливим для детермінованої функції $FC()$. Отже, множина $\boldsymbol{T}$ насправді формує у множині $\boldsymbol{M}$ $(n, 2^{m'}, d)$ – код, де $d = 2t + 1$. Із цього факту витікає, що $m' \le L(n, t, m)$.

Лему доведено.

Лема 4.5. Залишкова ентропія (Λ, m, l, t, ε) - біометричного екстрактора є обмеженою зверху $l \le L(n, t, m) - \log(1 - \varepsilon)$.

Доведення. Нехай задані $FG()$, $FR()$, множина $\boldsymbol{M} \subseteq \Lambda$ з потужністю $\#\boldsymbol{M} = 2^m$ та випадкова величина з рівномірним розподілом W.

Згідно з визначенням біометричного екстрактора $D[\langle S, Q\rangle, \langle U_d\, Q\rangle] \le \varepsilon$. Тоді знайдеться таке $q \leftarrow Q$, за умови існування якого величина S є ε-близькою до U_d, тобто існуватиме щонайменше $(1 - \varepsilon)\, 2^l$ реалізацій s величини S (назвемо цю множину $\boldsymbol{T}$) у множині $\{0, 1\}^l$, які можуть бути видані функцією $FG()$ за умови, що $q \leftarrow Q$.

Введемо таке відображення $\boldsymbol{C}$, що кожному $s \in \boldsymbol{T}$ ставить у відповідність певне значення $w \in \boldsymbol{M}$.

Далі стверджуватимемо, що $\mathbf{C}$ утворює ККП із порогом декодування t. У протилежному випадку знайшлося б таке $w' \in \Lambda$, для якого $\rho(\boldsymbol{C}(s_0), w') \le t$ та $\rho(\boldsymbol{C}(s_1), w') \le t$, де $s_0, s_1 \in \boldsymbol{T}$ та $s_0 \ne s_1$. Тобто функція $FR(w', q)$ могла б видати або s_0, або s_1, що є неможливим для детермінованої функції $FR()$. Отже, відображення $\boldsymbol{C}$ насправді формує у множині $\boldsymbol{M}$ $(n, 2^{l + \log(1 - \varepsilon)}, d)$ – код, де $d = 2t + 1$. Із цього факту витікає, що $l \le L(n, t, m) - \log(1 - \varepsilon)$.

Лему доведено.

Зауваження. Слід наголосити на тому, що поки $\varepsilon < ½$, виконується нерівність $0 < -\log(1 - \varepsilon) < 1$. Тобто верхні оцінки залишкової ентропії біометричного екстрактора та біометричного ідентифікатора відрізняються менш ніж на один біт.

4.3. Дактилоскопічний захист криптографічних ключів

Вище було обґрунтовано необхідність впровадження систем захисту криптографічних ключів, робота яких базується на застосуванні біометрії – набору індивідуальних ознак, властивих кожному індивіду, та відходу від класичних парольних систем захисту.

Змоделюємо роботу сучасної клієнт-серверної комп'ютерної системи з підсистемою дактилоскопічного захисту ключів на базі біометричного екстрактора запропонованого вище. Для цього у структурній схемі на рис. 1.37 замінимо блок парольного захисту ключів на блок дактилоскопічного захисту ключів, як зображено на рис. 4.3.

Протокол процесу авторизації виглядатиме так.

1. Клієнт відсилає запит на взаємодію до сервера;
2. На блок криптографічної обробки подаються:
   а) набір ознак із блоку виявлення та аналізу ознак і
   б) збережений на сервері у процесі реєстрації ідентифікатор клієнта;
3. Біометричний ідентифікатор, опрацьовуючи вхідні дані, може видати на вихід:
   а) відновлений "опорний" набір ознак або
   б) "null" – відмову у продовжені процесу авторизації;
4. Успіх на попередньому кроці забезпечує подачу до екстрактора набору ознак, із якого відновлюється криптографічний ключ (або пароль);
5. Відновлений ключ перед передачею каналами зв'язку хешується односторонньою функцією;
6. На стороні сервера здійснюється порівняння хешу отриманого від клієнта, із записаним на сервері хешем.
7. Успіх порівняння ініціює процес обміну інформацією від бази даних до клієнта.

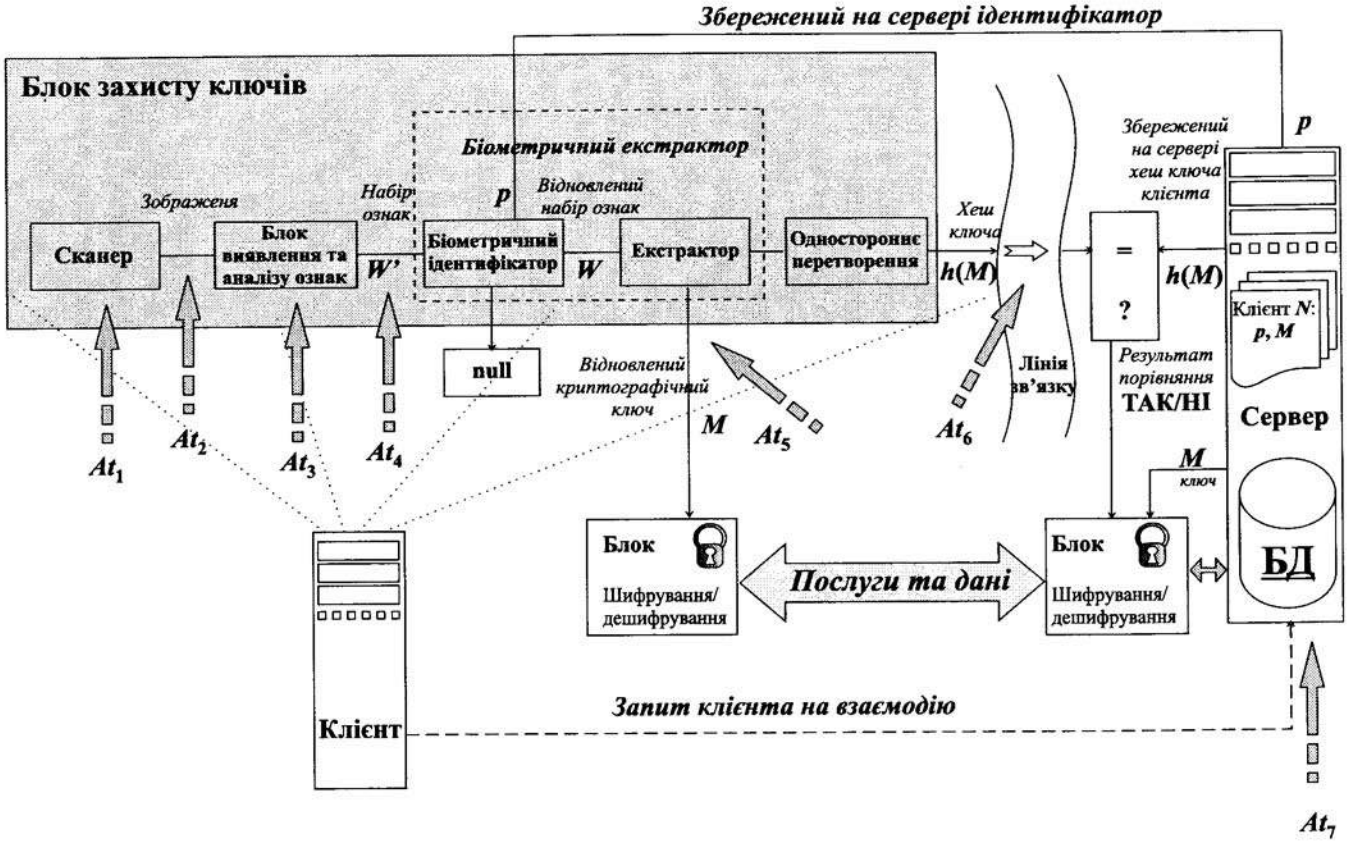


Рис.4.3. Клієнт-серверна система з блоком біометричного захисту ключів.

4.3.1. Аналіз криптографічної стійкості

Необхідно оцінити рівень надійності системи та сформулювати мінімальні вимоги для забезпечення достатнього захисту.

Проведемо попередню оцінку шляхів впливу на процес прийняття рішення про ідентифікацію користувача у системі. На рис.4.3 вказано можливі різновиди атаки (At_1, …, At_7).

Усього виділяють сім можливих:

At_1 – на сканер подається фальсифікований об'єкт ідентифікації (муляж відбитка пальця, копія підпису, маска обличчя);

At_2 – на вхід системи подається раніше записаний біометричний сигнал (копія зображення пальця, записаний голос);

At_3 – вплив на процес формування ознак (наприклад, за допомогою вірусів змінюється нормальний хід роботи програми);

At_4 – вплив на вхід біометричного екстрактора (наприклад, заміна всього представлення ознак певним штучно синтезованим);

At_5 – вплив на процес ідентифікації множини ознак та екстракції ключа;

At_6 – атака на канал передачі до блоку порівняння;

At_7 – фальсифікація зразків збережених на сервері для порівняння.

Проаналізуємо варіанти атак та виділимо найімовірніші. Атака At_1 нівелюється застосуванням інтелектуальних сканерів, що дозволяють зафіксувати факт використання муляжів відбитків (вимірювання температури, провідності, пульсу). Атака At_2 при невідомому вхідному зображенні є обчислювально нездійсненною (неможливо зробити тотальний перебір декількох десятків тисяч пікселів зображення).

Можливість атаки At_3 слід вивчати з точки зору вірусології, тому тут не розглядають.

Захист від атаки At_6 забезпечують гібридні криптографічні системи захисту конфіденційної інформації.

Випадок атаки At_7 потрібно досліджувати для кожного виду СУБД окремо. Захист здійснюється як внутрішніми засобами мови SQL, так і додатковими: шифруванням, створенням специфічних політик та прав доступу тощо, а також задіянням сучасних мережевих операційних систем.

У подальшому розглянемо атаки At_4 і At_5 та формально оцінимо стійкість системи дактилоскопічного захисту криптографічних ключів.

а) Аналіз атаки на процес ідентифікації множини ознак. Для аналізу атаки на вхід біометричного екстрактора At_4 приймемо наступне [11]:

1. система використовує координати особистих ознак папілярних ліній узору;

2. розмір зісканованого зображення

$$I = 322 \text{ пікселів} \times 255 \text{ пікселів};$$

3. мінімальна віддаль між ознаками

$$L = 10 \text{ пікселів};$$

4. загальна кількість можливих місць положення особистих ознак

$$Q = I / L^2 = 822;$$

5. мінімальна кількість ознак, яка необхідна для успішного розблокування ключа $\tau \geq \dfrac{s+k}{2}$ (для методу Берлекемпа-Месі);

6. кількість можливих ознак на відбитку N – залежно від якості відбитку від 10…40 (якісний відбиток) і до 100 (неякісний відбиток з великою кількістю фіктивних ознак).

Значення 2, 3 отримані із стандартного сканера відбитків пальців, представленого на ринку (≈ 505 dpi).

Теорема 4.1. Для вхідної множини особистих ознак W з параметрами Q і N та параметра біометричного екстрактора τ мінімальна ентропія W

$$H_\infty(W) = -\log_2\left(\frac{e^{-\frac{N^2}{Q-N+1}}}{\sqrt{2\pi\tau}}\left(\frac{eN^2}{(Q-N+1)\tau}\right)^\tau\right).$$

Доведення. Для проведення атаки At_4 необхідно синтезувати набір ознак, який відповідає набору ознак на оригінальному відбитку. Припустимо, що оригінальний відбиток має $N = 40$ ознак, кожна ознака може займати одну із Q можливих позицій. Тоді ймовірність того, що перша випадково синтезована ознака співпадатиме у місцеположенні з ознакою оригінального відбитка буде

$$p_1 = \frac{N}{Q}.$$

Після синтезування $(j-1)$ ознак ймовірність того, що j-та ознака співпадатиме (вважаючи, що попередні не співпали)

$$p_j \leq \frac{N}{Q-j+1}.$$

А синтезувавши повний набір ознак з N ознаками, можна припустити, що кожна ознака матиме ймовірність співпадіння

$$P_1 \le \frac{N}{Q-N+1}. \tag{4.8}$$

Випадкова величина співпадіння z ознак із N синтезованих із z ознаками в оригінальному відбитку матиме біноміальний розподіл:

$$p_{ЗАГ} = \binom{N}{z} P_1^z (1-P_1)^{N-z}, \text{ де } \binom{N}{z} = \frac{N!}{z!(N-z)!}.$$

Для розблокування ключа необхідним є співпадіння τ або більшої кількості ознак, тобто

$$P_{РОЗБЛОК} = \sum_{z=\tau}^{N} \binom{N}{z} P_1^z (1-P_1)^{N-z}. \tag{4.9}$$

Враховуючи, що $P_1 << 1$, застосуємо до виразу (4.9) теорему Пуассона:

$$P_{РОЗБЛОК} = \sum_{z=\tau}^{N} e^{-NP_1} \frac{(NP_1)^z}{z!}. \tag{4.10}$$

Отриманий ряд (4.10) оцінюється своїм першим членом. Кожен наступний член у 10…20 раз менший ніж, попередній. Тобто, відкинувши члени ряду починаючи з другого, можливо з точністю до порядку оцінити величину $P_{РОЗБЛОК}$:

$$P_{РОЗБЛОК} = e^{-NP_1} \frac{(NP_1)^\tau}{\tau!}. \tag{4.11}$$

У формулі (4.11) застосуємо до факторіала апроксимацію Стірлінга:

$$P_{РОЗБЛОК} = e^{-NP_1} \frac{(NP_1)^\tau}{\sqrt{2\pi\tau}\, e^{-\tau}\tau^\tau} = \frac{e^{-NP_1}}{\sqrt{(2\pi\tau)}} \left(\frac{eNP_1}{\tau}\right)^\tau. \tag{4.12}$$

Мінімальне значення $P_{РОЗБЛОК}$ досягається при максимальному P_1, тобто нерівність (4.8) перетворюється на рівність. Використавши формулу (4.3), отримаємо значення мінімальної ентропії

$$H_\infty(W) = -\log_2(P_{РОЗБЛОК})$$

або, підставивши вирази для $P_{РОЗБЛОК}$ та P_1, необхідний результат.

Теорему доведено.

На рис.4.4 зображено залежність ентропії від τ кількості ознак, необхідних для прийняття рішення про верифікацію особи. Рисунок

показує, що при збільшенні τ зростає стійкість системи, що є аналогічним видовженню пароля у парольних системах.

Аналіз формули (4.12) дає підставу для двох важливих висновків.

Перший: отримуємо підвищення стійкості при збільшені роздільної здатності зображення (збільшення I, відповідно зменшення L). Цей фактор безпосередньо впливає на ймовірність співпадіння окремої ознаки P_1 (4.8).

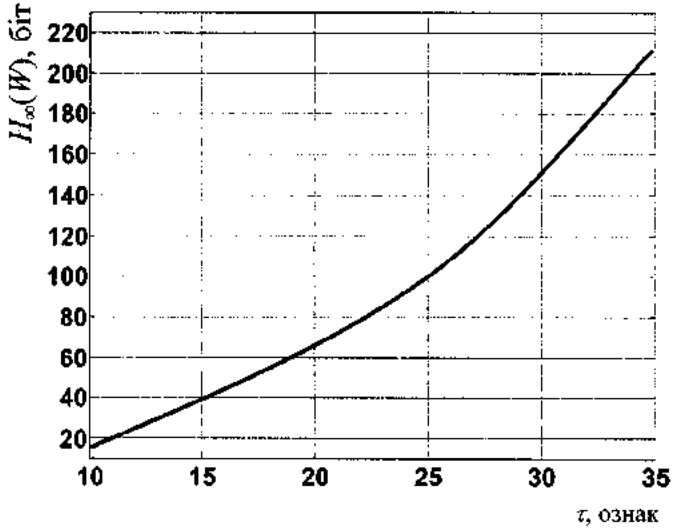


Рис. 4.4. Залежність ентропії вхідних біометричних даних від мінімальної кількості ознак, необхідної для успішного розблокування ключа τ (для N =45).

У системі τ = 25, $H_\infty(W)$ = 100 біт, що відповідає 12 символьному випадковому паролю, який може складатися із усіх можливих ASCII символів.

Другим важливим висновком є суттєва залежність стійкості від загальної кількості ознак на оригінальному відбитку пальця N. Така залежність зображена на рис. 4.5.

Для збільшення рівня захисту N мусить бути якомога меншим. Тобто стійкість системи при використанні відбитків високої якості буде значно вищою, ніж при застосуванні відбитків поганої якості з великою кількістю фіктивних ознак. Згідно з рис. 4.5 при τ=25, N=35…50 отримуємо $H_\infty(W)$ = 155…70 біт.

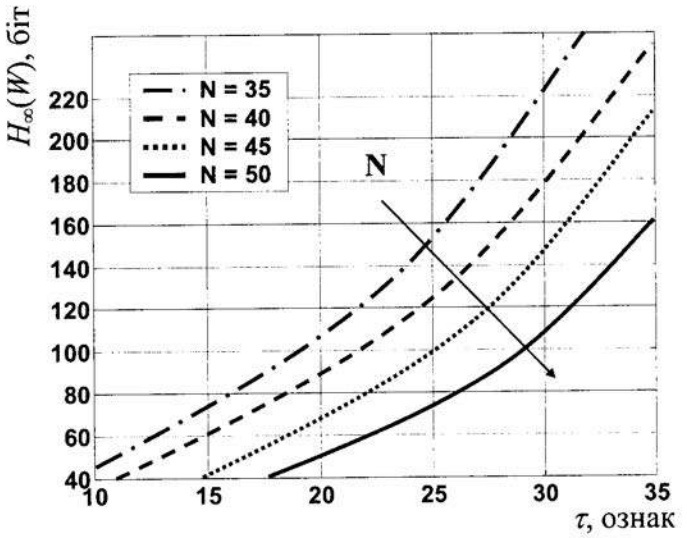


Рис. 4.5. Залежність ентропії від τ та загальної кількості ознак на відбитку пальця N.

Вираз для $H_\infty(W)$ дозволяє розрахувати значення залишкової ентропії біометричного екстрактора (4.7).

б) Стійкість біометричного екстрактора. Для аналізу стійкості системи до атаки At_5 на біометричний екстрактор був запропонований алгоритм захисту ключа $M = \{m_0, \ldots, m_{k-1}\} \subset \boldsymbol{F}$ за допомогою постійно змінних наборів даних. В алгоритмі секретний ключ, який необхідно захистити, перетворюємо у коефіцієнти полінома $\boldsymbol{f}(x)$ степені $k-1$ над полем $\boldsymbol{F}$:

$$\boldsymbol{f}(x) = m_1 + m_1 x + \ldots + m_k x^{k-1}.$$

Набір даних $\boldsymbol{W} = \{w_1, \ldots, w_s\} \subset \boldsymbol{F}$ використовується для захисту (блокування) $\boldsymbol{f}(x)$, при цьому $s > k$. На виході алгоритму блокування отримується набір кортежів $B_{\mathbf{P}}$, який складається з s пар $\{w_i, \boldsymbol{f}(w_i)\}$ та $r - s$ пар фіктивних точок $\{\alpha_i, \beta_i\}$ із $\boldsymbol{F}$, які задовольняють умовам $\boldsymbol{f}(\alpha_i) \neq \beta_i$.

Для розкриття системи, яка використовує $B_{\mathbf{P}}$, атакуючій стороні потрібно виділити з такого набору точки, що лежать на поліномі $\boldsymbol{f}(x)$, власне, відновити секретний ключ. Очевидно, що чим більшим є r, тим більшою є кількість подібних до $\boldsymbol{f}(x)$ фіктивних поліномів, а отже, і стійкість системи до розкриття.

Легальному користувачеві системи необхідно і достатньо пред'явити щонайменше $\tau \geq k$ істинних точок, щоб успішно інтерполювати прихований поліном. Іншими словами, для розблокування надається набір $W' \subset \mathcal{F}$, який містить лише частину елементів W, тобто потужність різниці двох множин особистих ознак $\#(W - W') = t$.

Необхідно реалізувати алгоритм, використовуючи в якості множин блокування та розблокування дактилоскопічні дані людини. У цьому випадку набором блокування є набір координат пікселів, які відповідають місцеположенню ознак на відбитку пальця, тому найкращим вибором є поле $\mathcal{F} = \mathrm{GF}(n)$, де $n = g^2$, а g – просте число.

Задача оцінки стійкості системи до атаки на вихід біометричного екстрактора зводиться до оцінки складності інтерполяції полінома $f(x)$ степеня $k - 1$ з набору точок B_P потужністю r, мінімум τ з яких лежать на поліномі. Існує два варіанти вирішення задачі:

1. методом тотального перебору, а саме, вибіркою по k точок із r можливих, намагаємося здійснити інтерполяцію Ньютона;
2. шляхом використання методу Берлекемпа-Месі декодування РСК довжиною $s = k + 2t$, де $s > \tau \geq k + t$, а t – віддаль між W' та W, тобто кількість невідповідних ознак у W' по відношенню до W.

Обчислювальну складність алгоритму розглядаємо у двох контекстах: складність розблокування легітимним користувачем з відповідним відбитком пальця необхідно мінімізувати; складність розблокування нелегітимним користувачем, який намагається зламати B_P, необхідно максимізувати.

Для першого випадку доведемо наступну теорему.

Теорема 4.2. Обчислювальна складність розблокування B_P методом тотального перебору:

$$C_{NI}(f(x)) = \frac{r!\,t!}{(r-k)!\,(k+t)!}. \qquad (4.13)$$

Доведення. У методі тотального перебору потрібно знайти набори з k точок, за допомогою яких інтерполюється поліном $f(x)$. Кількість наборів рівна кількості розміщень:

$$A_r^k = \frac{r!}{(r-k)!}.$$

Істинним набором може бути будь-який із

$$A_{k+t}^k = \frac{(k+t)!}{(k+t-k)!} = \frac{(k+t)!}{(t)!}$$

наборів, тому що будь-якими k точками із вірних $\tau = k + t$ однозначно здійснюється інтерполяція полінома степеня $k-1$ у формі Ньютона чи Лагранжа. Частка обох величин дає кількість спроб, необхідних для знаходження вірного полінома (4.13).

Теорему доведено.

Для проведення атаки на біометричний екстрактор із параметрами $r = 300$, $k = 16$, $t = 8$ нелегальному користувачу прийдеться виконати $C_{NI} = 2^{67}$ перевірок.

Для легітимного користувача, після перетину $B_{\mathbf{P}}$ з множиною розблокування користувача $\boldsymbol{W}'$, значення нехай $r = 30$ точок, тоді $C_{NI} = 2^8$.

Останній приклад показує, що метод тотального перебору є далеко не ідеальним для легітимного користувача.

Іншим методом є застосування РСК.

Теорема 4.3. Обчислювальна складність розблокування $B_{\mathbf{P}}$ з використанням РСК:

$$C_{RSC}(f(x)) = \frac{r!}{s!}\left(\sum_{i=\tau}^{s}\frac{(r-i)!}{(s-i)!}\right)^{-1}.$$

Доведення. Подібно до C_{NI} необхідно вибирати кодове слово довжини s та намагатись розблокувати $B_{\mathbf{P}}$. Таких кодових слів є

$$A_r^s = \frac{r!}{(r-s)!}.$$

Кількість вірних кодових слів визначимо наступним чином. Відомо, що для успішної реконструкції полінома степеня $k-1$ методом Берлекемпа-Месі необхідно $\tau \geq \frac{s+k}{2}$ вірних елементів, тоді фіктивних елементів у $\boldsymbol{W}'$ є $s - \tau$. Нехай ми маємо i дійсних елементів ($\tau \leq i \leq s$), тоді існує

$$A_{r-i}^{s-i} = \frac{(r-i)!}{(r-i-s+i)!} = \frac{(r-i)!}{(r-s)!}$$

способів вибрати фіктивні елементи та

$$A_s^i = \frac{s!}{(s-i)!}$$

способів вибрати дійсні елементи.

Кількість вірних кодових слів визначається як

$$\sum_{i=\tau}^{s} A_s^i A_{r-i}^{s-i}.$$

Кінцевий результат – це частка від ділення обох вищенаведених результатів:

$$C_{RSC}(f(x)) = \frac{r!}{(r-s)!}\left(\sum_{i=\tau}^{s}\left(\frac{s!}{(s-i)!}\right)\left(\frac{(r-i)!}{(r-s)!}\right)\right)^{-1},$$

$$C_{RSC}(f(x)) = \frac{r!}{s!}\left(\sum_{i=\tau}^{s}\frac{(r-i)!}{(s-i)!}\right)^{-1}.$$

Теорему доведено.

Наслідок 4.1. Нехай $s = k$, тоді $C_{NI} = C_{RSC}$:

$$C_{RSC}(f(x)) = \frac{r!}{k!}\left(\sum_{i=k}^{k}\frac{(r-i)!}{(k-i)!}\right)^{-1} = \frac{r!}{k!(r-k)!} = \binom{r}{k},$$

$$C_{NI}(f(x)) = \frac{r!\,0!}{(r-k)!(k+0)!} = \frac{r!}{(r-k)!\,k!} = \binom{r}{k}.$$

Наслідок 4.2. Нехай $r >> \tau$, тоді $C_{BF} \le C_{RS}$ для усіх s.

Для доведення нерівності необхідно розкрити суму у виразі для C_{RS} та проаналізувати члени ряду, внесок яких у результат є найбільшим:

$$C_{RSC}(f(x)) = \frac{r!}{s!}\left(\sum_{i=\tau}^{s}\frac{(r-i)!}{(s-i)!}\right)^{-1},$$

$$C_{RSC}(f(x)) = \frac{r!}{s!}\left(\frac{(r-\tau)!}{(s-\tau)!} + \cdots\right)^{-1},$$

$$C_{RSC}(f(x)) = \binom{r}{s}\left(\frac{(r-\tau)!}{(s-\tau)!(r-s)!} + \frac{(r-\tau)!}{(s-\tau-1)!(r-s+1)!} + \ldots\right)^{-1}.$$

У сумі розглядатимемо лише перший член, тому що кожен наступний у r раз менший за попередній. Враховуючи, що $\tau \ge \frac{s+k}{2}$, C_{RSC} можливо оцінити наступним чином

$$\frac{r!}{(r-s)!}\left(\frac{s!(r-\tau)!}{t!(r-s)!}\right)^{-1}.$$

Очевидно, що для мінімізації складності необхідно у попередньому виразі зменшувати чисельник та збільшувати знаменник, але це вимоги, що суперечать одна одній. Та проаналізувавши чисельник виявляємо, що його внесок у результат у r^{τ} раз більший, ніж знаменника, а для усіх $s \geq k$ виконується нерівність

$$\frac{r!}{(r-k)!} \geq \frac{r!\,t!}{(r-k)!\,(k+t)!},$$

тобто $C_{NI} \leq C_{RSC}$.

Рис.4.6 – 4.8 ілюструють обчислювальну складність C_{RSC} як функцію від довжини кодового слова РСК s для випадків:

а) у атакуючої сторони немає жодної інформації про відбиток пальця;

б) у атакуючої сторони є часткова інформація про відбиток пальця;

в) обчислювальна складність легітимного користувача.

Додатково на рисунках для порівняння зображено обчислювальну складність C_{NI}.

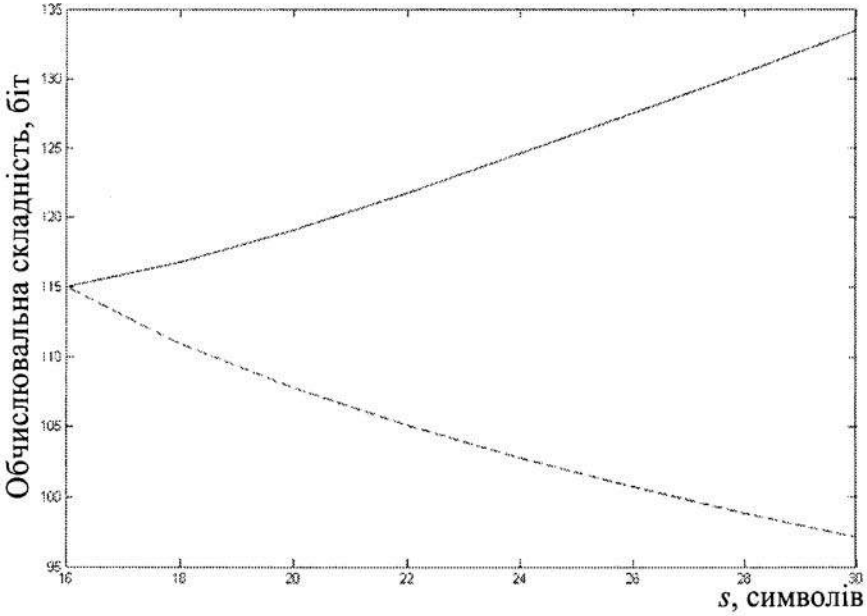


Рис.4.6. Двійковий логарифм від обчислювальної складності C_{RSC} як функція від довжини кодового слова: $r = 1000$, $k = 16$ (штриховою лінією зображено двійковий логарифм від C_{NI}).

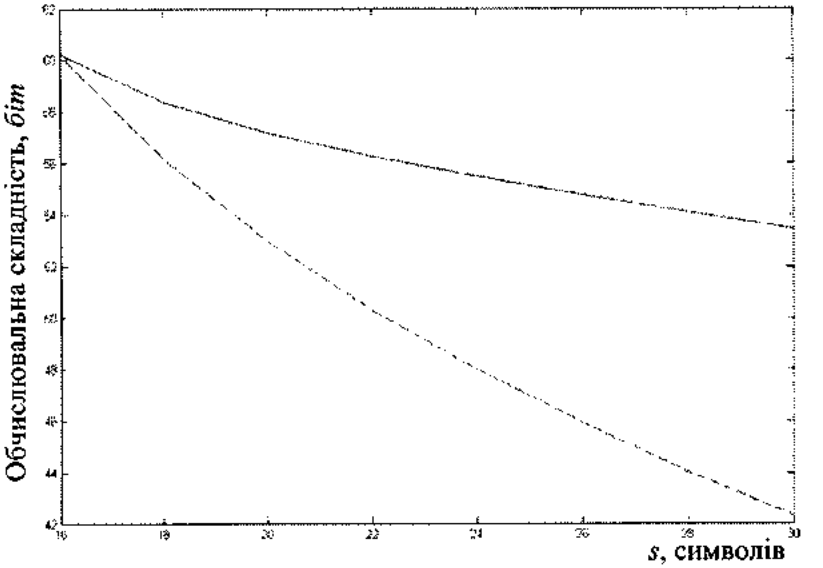


Рис.4.7. Двійковий логарифм від обчислювальної складності C_{RSC} як функція від довжини кодового слова: r=100, k = 16 (штриховою лінією зображено двійковий логарифм від C_{NI}).

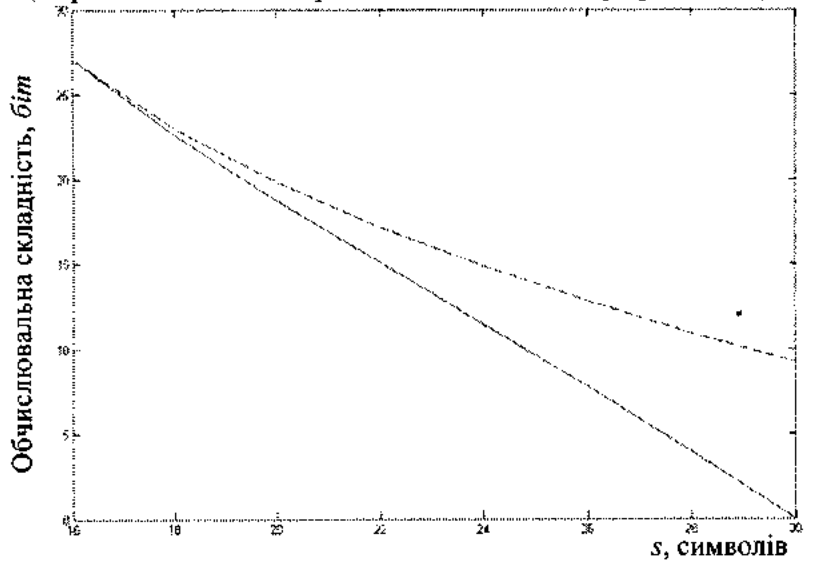


Рис.4.8. Двійковий логарифм від обчислювальної складності C_{RSC} як функція від довжини кодового слова: r = 30, k = 16 (штриховою лінією зображено двійковий логарифм від C_{NI}).

Залежно від відношення r до s оптимальним може бути як і метод тотального перебору, так і метод із залученням РСК. Але легітимний користувач за допомогою кодів розблокує B_P за 1 або 2 спроби, а для нелегітимного у найкращому випадку залишається вдатися до тотального перебору. Вибір фіктивних точок у методі здійснюється таким чином, щоб змусити атакуючу сторону розглядати всі точки B_P.

Якщо ж нелегітимний користувач зможе відкинути частину фіктивних точок, орієнтуючись на найбільш імовірні місцеположення особистих ознак на відбитку пальця, то це лише незначно зменшить обчислювальну складність.

Численні дослідження [207,230] вказують на те, що ймовірність того, що дві людини матимуть однакові відбитки пальців, наближено дорівнює 10^{-80} або – $\log(10^{-80}) \approx 265$ біт ентропії. Це, з одного боку вказує на надійність методу в обчислювальному сенсі щодо атаки з найбільш імовірними відбитками пальців, але з іншого – теоретичну межу надійності розглядуваного методу. Тобто незалежно від використовуваних параметрів більшого рівня надійності досягнути не вдасться.

4.3.2. Аналіз імовірнісних характеристик

Біометричний екстрактор, по своїй суті, здійснює ідентифікацію користувача системи з криптографічним захистом інформаційного обміну. У першому розділі було зауважено, що найважливішим параметром систем ідентифікації є імовірність неправильної неідентифікації (FRR) $P_{нн}$, яка характеризує кількість спроб санкціонованого доступу користувача під час ідентифікації системою. Для оцінки $P_{нн}$ необхідно ґрунтовно проаналізувати алгоритми блокування та розблокування ключів (рис. 4.7 та рис. 4.8)

а) Створення множини блокування. Блок виявлення та аналізу ознак (рис. 4.9) розглядатиметься як чорна скринька, на виході якої отримується нормалізований вектор основних візуальних ознак. Кожен вектор ознак пальця містить деяку фіксовану кількість мінуцій $t_i=(x_i, y_i) \in T$ [80]. Але відомо, що під час послідовних зчитувань біометрії пальця у зображенні з'являються геометричні спотворення, тобто $t_i'=(x_i+\xi_{xi}, y_i+\xi_{yi})$, де ξ_{xi} , ξ_{yi} – шум розташування ознак, що виникає внаслідок спотворень по осях x та y відповідно.

Для оцінки розподілу розташування особистих ознак проведено експеримент (п. 4.4.2), у якому у декількох послідовних зчитуваннях одного і того ж пальця виділялися ознаки та розраховувались

математичні очікування та дисперсії. На основі отриманих результатів досліджень розроблено наступний алгоритм відбору ознак для створення множини блокування W.

Вхідними даними алгоритму є N наборів особистих ознак $v_1,\ldots v_N$, які відповідають N скануванням пальця користувача. Набори корелюються використовуючи поріг відстані $\sigma_S = \mu + \sigma$ пікселів та поріг кратності T.

1. Нехай **A** – це множина центрів ваги набору точок, що корелюються відповідно σ_S, з певним значенням кратності T;
2. Для кожної множини v_i;
3. Для кожної ознаки $t_j \in v_i$;
4. Знайти такий елемент $a_k \in \mathbf{A}$, для якого виконується $\boldsymbol{min}(|\, a_k - t_j \,|) < \sigma_S$;
5. Якщо елементів декілька, то вибрати елемент із найменшим T;
6. Якщо елемент знайдено, то перерахувати центр ваги та збільшити кратність;
7. Інакше створити новий елемент у **A** з кратністю одиниця;
8. $W = \{a \in \mathbf{A}: T(a) > T\}$.

Ознаки, що з'явились T або менше раз, вважаються шумом та відкидаються. Такі ознаки найчастіше з'являються на краю пальця.

Отриману множину W разом із її відображенням $f: W \to \mathcal{F}$ записуємо у формі кортежів у B_P.

б) Створення множини фіктивних ознак. Наступним етапом є формування множини фіктивних ознак та заповнення ними B_P. Такі ознаки не можуть розташовуватися ближче, ніж за L пікселів до реальних ознак. Величина L є параметром алгоритму зв'язування, для якого виконується $L > 2\,\sigma_S$. Очевидно, що фіктивні ознаки теж не повинні розміщатись на відстані меншій L одна від одної. Інакше атакуюча сторона відразу відкине ці елементи як фіктивні.

Лема 4.6. Нехай віддаль між ознаками є більшою L, тоді загальна кількість елементів r з густиною упакування ρ є не більшою $\dfrac{4\rho g^2}{L^2\pi}$.

Доведення. У даному випадку необхідно у прямокутник площею g^2 упакувати круги площею $\left(\dfrac{L}{2}\right)^2\pi$. Кількість таких кругів

$$r \le \rho\left(\frac{g^2}{(L/2)^2\pi}\right) = \frac{4\rho g^2}{\pi L^2}.$$

Оптимальне упакування досягається за використання гексагональної решітки. Тоді

$$\rho = \frac{\pi(L/2)^2}{6(L/2)^2 tg(\pi/6)} = \frac{\pi\sqrt{3}}{6} \approx 0.91.$$

На жаль, розташування елементів із такою густиною веде до миттєвого виявлення реальних елементів, які не відповідають розташуванню у гексагональній решітці. Тому фіктивні елементи необхідно розміщати випадковим чином на віддалі більшій L. Це веде до зменшення густини упакування до $\rho \approx 0{,}45$. Інша техніка упакування, запропонована у роботі [158], дозволяє досягнути $\rho \approx 0{,}75$. Але ця техніка не забезпечує достатньої випадковості розташування та не тестувалася для двовимірного випадку.

Створена множина фіктивних ознак об'єднується із множиною блокування згідно умов (4.6), утворюючи набір кортежів $B_{\text{Р}}$, який зберігається на сервері (рис. 4.9) у вигляді ідентифікатора p разом з іншою інформацією користувача.

Для здійснення захищеного обміну даними користувачеві необхідно розблокувати $B_{\text{Р}}$.

в) Імовірність неправильної неідентифікації біометричного екстрактора. Множину розблокування $\boldsymbol{W}'$ потужністю s створюємо з набору особистих ознак одного відбитка пальця користувача. Для кожної ознаки потрібно знайти найближчу у $B_{\text{Р}}$ ознаку, використовуючи поріг віддалі σ_S.

Існує імовірність того, що деякі з ознак будуть ближчими до фіктивних, ніж до істинних ознак, а для розблокування прихованого криптографічного ключа необхідно мінімум k (інтерполяція полінома у формі Ньютона) або $\tau \geq \dfrac{k+s}{2}$ (декодування кодового слова РСК методом Берлекемпа-Месі) дійсних ознак у $\boldsymbol{W}'$. За умови невиконання цих умов біометричний екстрактор поверне "null" (рис. 4.3).

Для реальної оцінки імовірності неправильної неідентифікації доведемо наступні лему та теорему.

Лема 4.7. Імовірність невиявлення (неправильної неідентифікації) однієї ознаки, яка знаходиться на віддалі не меншій L від усіх інших ознак, можна оцінити як

$$P_{\text{нн1}} \geq \exp\left(-\frac{\rho g^2}{2r\pi\sigma_S^2}\right). \qquad (4.14)$$

Доведення. Нехай розташування особистих ознак відповідає круговому нормальному розподілу. Використаємо полярну систему координат. Імовірність успішного виявлення (правильної неідентифікації) однієї ознаки, розміщеної на віддалі не меншій L від усіх інших ознак, становитиме

$$P_{пн1} \le \int_0^{L/2} \frac{R}{\sigma_S^2} e^{-R^2/2\sigma_S^2}\, dR .$$

Після інтегрування

$$P_{пн1} \le 1 - \exp\left(\frac{-L^2}{8\sigma_S^2}\right).$$

Лему 4.6 перепишемо наступним чином:

$$L^2 \le \frac{4\rho g^2}{\pi r}.$$

Оскільки відомо, що

$$P_{нн1} = 1 - P_{пн1},$$

отримаємо бажаний результат.

Лему доведено.

Теорема 4.4. Імовірність неправильної неідентифікації біометричного екстрактора є не меншою:

$$P_{нн} \ge \sum_{i=k}^{\tau} e^{-\tau e^{-\frac{\rho g^2}{2\pi r\sigma_S^2}}} \frac{\left(\tau e^{-\frac{\rho g^2}{2\pi r\sigma_S^2}}\right)^i}{i!}.$$

Доведення. Результату досягаємо використовуючи дві попередні леми.

Алгоритм інтерполяції полінома степеня $k-1$ є толерантним до певної кількості помилок. Необхідною умовою є виявлення від k до τ істинних точок, де $\tau \ge k$, тобто

$$P_{нн} \ge \sum_{i=k}^{\tau} \binom{\tau}{i} \left(P_{нн1}\right)^i \left(1 - P_{нн1}\right)^{\tau - i}.$$

Подібно до формули (4.9) застосуємо теорему Пуассона:

$$P_{нн} \ge \sum_{i=k}^{\tau} e^{-\tau P_{нн1}} \frac{\left(\tau P_{нн1}\right)^i}{i!},$$

де $P_{нн1}$ визначається виразом (4.14).

Теорему доведено.

На рис.4.9 зображено імовірність неправильної неідентифікації як функцію від розміру r бінарного об'єкта B_P для різних об'ємів приховуваної ключової інформації.

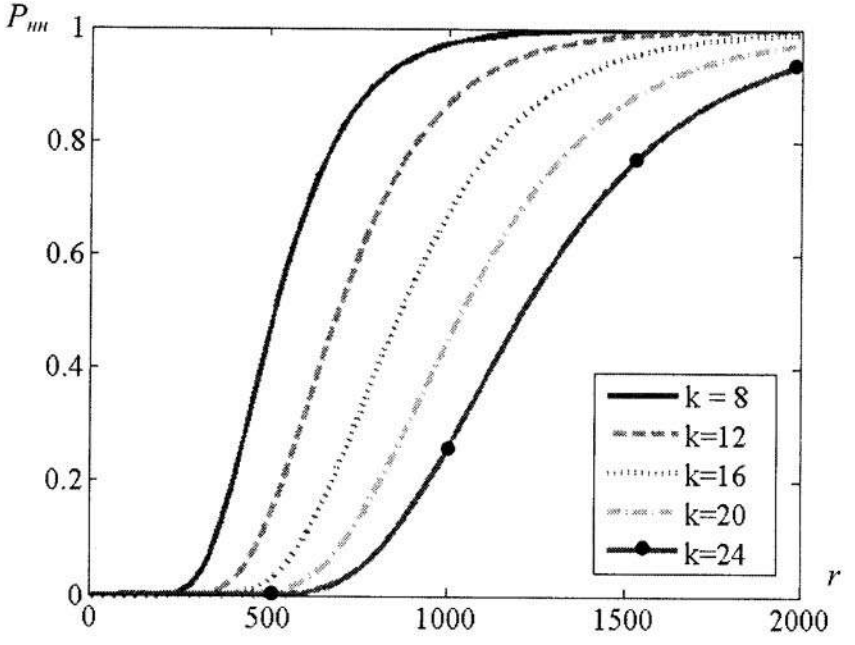


Рис.4.9. Імовірність неправильної неідентифікації як функція від r для різних k. Параметри: $\sigma_S^2 = 10$; $g = 251$; $t = 10$.

4.4. Особливості реалізації зв'язування криптографічних ключів з дактилоскопічними даними

4.4.1. Генерація ключа

Для успішної реалізації методів блокування, запропонованих вище, необхідно створити алгоритм генерації випадкових послідовностей для використання у якості ключів [9].

Заради гарантованої таємності ключа він повинен бути дійсно випадковим, а повний перебір усіх можливих послідовностей такої ж довжини фізично неможливим. Поява кожної з послідовностей заданої

довжини мусить бути рівноймовірною. Це можливо лише в одному випадку. Розподіл відповідної випадкової величини повинен бути рівномірним, не мати жодних асиметрій, кореляцій чи зміщень.

Недоліком існуючих програмних генераторів випадкових чисел (ГВЧ) є генерація випадкової послідовності детермінованим алгоритмом, тобто подача ідентичних даних у різні моменти часу на вхід алгоритму приведе до того самого результату. Комп'ютер може знаходитися лише в обмеженій кількості станів, і отриманий результат буде строго визначатися вхідними даними і поточним станом комп'ютера. Такі ГВЧ прийнято називати генераторами псевдовипадкових чисел.

Ефективним вирішенням проблеми є внесення "випадковості" в алгоритм генерації програмного ГВЧ безпосередньо користувачем. Це відбувається при натисканні на клавішу клавіатури чи мишки або при русі мишкою. Далі сам процес генерації здійснює алгоритм, який фіксує:

- покази системного таймера;
- час, який пройшов між натисканнями клавіш;
- вміст буферів вводу/виводу;
- стан операційної системи чи мережі і т.д.

Створено програмний недетермінований ГВЧ, (рис. 4.10), робота якого базується на фіксації мілісекунди поточного системного часу у момент натискання клавіші мишки по рухомому об'єкту (ключ) , котрий випадковим чином переміщується по вікну. Доведено, що отриманий розподіл випадкової величини відповідає дискретному рівномірному на відрізку [0,9].

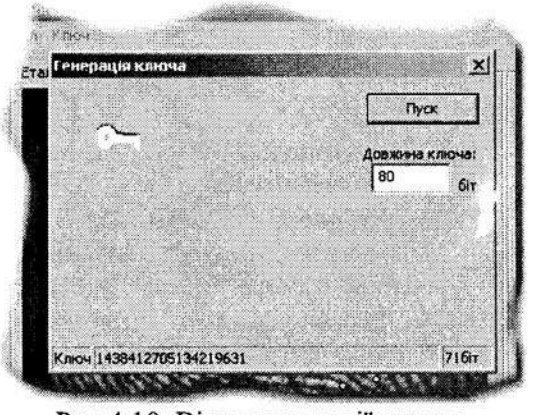


Рис.4.10. Вікно генерації ключа.

При генерації випадкової послідовності у якості одного знака береться одна мілісекунда. Приймається, що мілісекунда вибирається випадково і рівномірно з множини чисел {0, 9}.

Для доведення рівномірності отриманого розподілу необхідно привести певний теоретичний матеріал.

Програмні ГВЧ, з точки зору теорії інформації [233], можна розглядати як дискретне джерело повідомлень, яке у кожен момент часу випадковим чином приймає один із множини можливих станів u_1, u_2, ..., u_N, де N – об'єм алфавіту джерела. Окремі стани джерела можуть вибиратися частіше, інші рідше. Прийнято описувати джерело дискретним ансамблем U, тобто повною сукупністю станів із імовірностями їх появи, які у сумі складають одиницю:

$$U = \begin{pmatrix} u_1 & u_2 & \dots & u_i & \dots & u_N \\ P(u_1) & P(u_2) & \dots & P(u_i) & \dots & P(u_N) \end{pmatrix}, \qquad \sum_{i=1}^{N} P(u_i) = 1,$$

де $P(u_i)$ – імовірність вибору стану u_i джерелом повідомлень.

Числовою характеристикою джерела повідомлення є ентропія

$$H(U) = \sum_{i=1}^{N} P(u_i) \cdot \log\left(\frac{1}{P(u_i)}\right). \qquad (4.15)$$

Що більшою є ентропія джерела, то більшою є невизначеність повідомлень, які генеруються. Максимальне значення ентропії досягається при однаковій імовірності вибору кожного із символів алфавіту $P(u_i)=1/N$ для усіх i

$$H(U) = \log(N). \qquad (4.16)$$

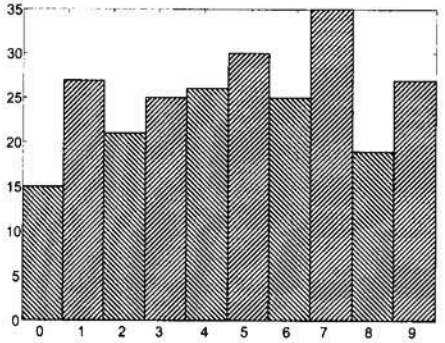
Також для дискретного рівномірного розподілу над {0, 1, ... N-1} відомі наступні значення перших двох моментів: математичного очікування – $\mu = \frac{N-1}{2}$, дисперсії – $\sigma^2 = \frac{N^2-1}{12}$; та двох коефіцієнтів: коефіцієнта асиметрії – $\gamma_1 = 0$, ексцесу – $\gamma_2 < 0$, які повністю характеризують відповідний розподіл [14].

Для випадку {0, 1, ... 9} отримуємо: $\mu = 4{,}5$; $\sigma^2 = 8{,}25$; $\gamma_2 = -1{,}243$. Теоретичне значення для ентропії $H_{\text{теор}}(U) = 3{,}3219$.

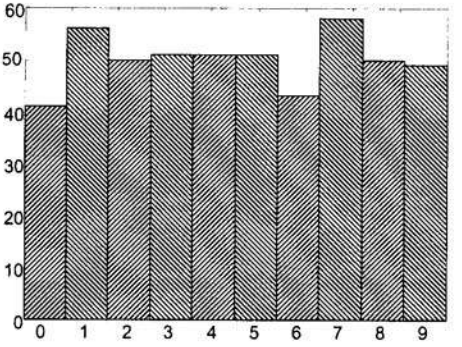
Проводились експерименти для послідовностей з довжинами, необхідними для утворення ключів згідно таблиць з п. 1.5. Для кожного експерименту розраховувались відповідні моменти та коефіцієнти, а також величина ентропії за формулою (4.15). Отримані значення порівнювалися з теоретичними.

Отримані гістограми та графіки для "найгіршого" випадку наведені на рис.4.11. Характеристики цього розподілу такі:

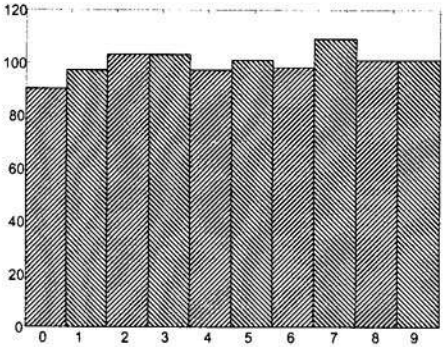
Серія	Довжина послідовності	μ	σ^2	γ_1	γ_2	$H_{пр}$, біт	$H_{пр}/H_{теор}$, %
1	250	4,6721	7,5049	-0,0327	-1,1367	3,2880	98,98
2	500	4,5663	8,0643	-0,0206	-1,2326	3,3151	99,79
3	1000	4,5634	8,1148	-0,0122	-1,2198	3,3203	99,95
4	3000	4,5152	8,2271	-0,0031	-1,2199	3,3216	99,99
5	*Теоретичні значення*	4,5	8,25	0	-1,2243	3,3219	100



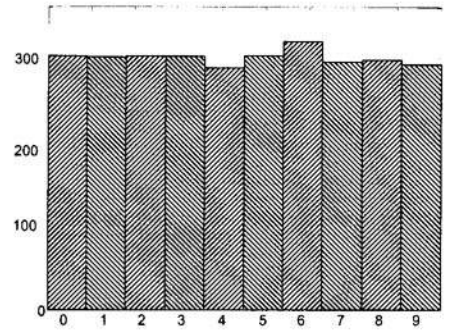
а) N=250; μ=4,672; σ^2=7,5049; $H_{пр}/H_{теор}$=98,98 %



б) N=500; μ=4,566; σ^2=8,063; $H_{пр}/H_{теор}$ = 99,79 %



в) N=1000; μ=4,563; σ^2=8,1148; $H_{пр}/H_{теор}$=99,95 %



г) N=3000; μ=4,5152; σ^2=8,217; $H_{пр}/H_{теор}$=99,99%

Рис.4.11. Гістограми випадкових послідовностей:
а) – 250 символів; б) – 500 символів; в) – 1000 символів;
г) – 3000 символів.

4.4.2. Створення множини блокування

Для оцінки розташування особистих ознак проведено експеримент, у якому у декількох послідовних зчитуваннях одного і того ж пальця виділялися ознаки, оцінювалася їхня кількість на окремому відбитку та кількість співпадаючих ознак, розраховувались математичні очікування та дисперсії.

Для експерименту використовувалася база з 10 000 зображень, отриманих із ≈ 1000 різних пальців світловипромінюючим сенсором фірми Testech Inc з роздільною здатністю 505 dpi (матриця 322 × 255 пікселів).

У таблиці 4.1 наведено статистику кількості особистих ознак на відбитку пальця. Для експериментів створено інформаційну систему (рис. 4.12), за допомогою якої порівнювалися відбитки одного і того ж пальця та оцінювалась кількість ознак, що співпали.

Критерієм співпадіння було вибрано віддаль між особистими ознаками. Результати розбито на дві групи: до вирівнювання зображення та після вирівнювання зображення, які, додатково, розбиті ще на три підгрупи залежно від віддалі між ознаками:

- мінімальна – найменша віддаль між відповідними особистими ознаками на різних зображеннях одного пальця, характерна для центру зображення;
- максимальна – найбільша віддаль, яка є типовою для ознак на краю зображення;
- середня – найбільш імовірна віддаль, характерна для усього зображення в цілому, за винятком згаданих випадків.

Таблиця.4.1. Статистика кількості ознак (база з 10 000 зображень)

Набір особистих ознак	Математичне очікування кількості ознак	Середньо-квадратичне відхилення кількості особистих ознак
На відбитку	41,7	11,8
Ті, що співпали з ознаками на еталонному відбитку	37,9	11,9
З'явилось нових або зникло з еталонного	4,1	5,0

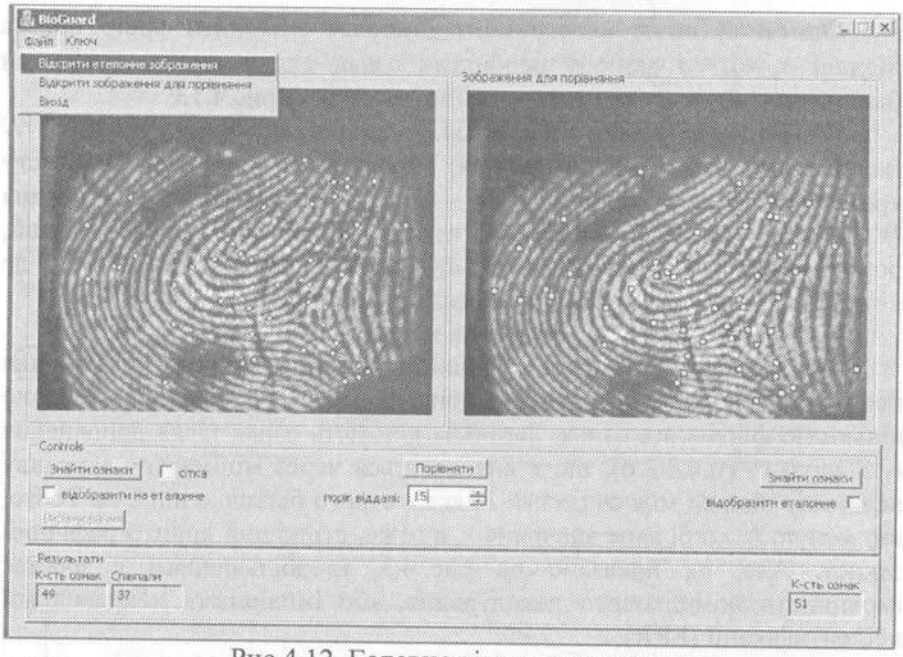


Рис.4.12. Головне вікно програми.

Дані з та без вирівнювання, наведені у наступній таблиці (використано набори з $N = 10$ відбитків):

Віддаль, пікселі		Математичне очікування	Середньо квадратичне відхилення
Без вирівнювання	Мінімальна	33,7	30,3
	Середня	42,1	35,1
	Максимальна	52,1	37,2
З вирівнюванням	Мінімальна	0	1,9
	Середня	3,5	2,3
	Максимальна	12,4	6,7

Згідно алгоритму, запропонованого у п.4.3.2 а, необхідно із N вхідних наборів особистих ознак створити множину зв'язування (блокування) W таємного криптографічного ключа M. Як правило, цей процес відбувається під час реєстрації нового користувача системи захисту або при зміні ключа існуючого користувача.

Описаний вище експеримент дозволяє здійснити вибір порога віддалі $\sigma_S = \mu + \sigma$ відбору особистих ознак для створення множини блокування. Блок-схему алгоритму зображено на рис.4.13.

На вхід алгоритму подаються набори v_i особистих ознак із N послідовних сканувань пальця користувача системи захисту криптографічних ключів. На виході отримується множина $\boldsymbol{W} = \{w_1,\ldots, w_s\}$. Кожен елемент w_i є центром ваги групи мінуцій, розташованих на віддалі меншій σ_S одна від одної, із наборів v_i , де $i = 1\ldots N$. Додатковою умовою є поріг кратності T.

Робота алгоритму відображена на рис.4.14 - 4.16.

Для досягнення криптографічної надійності алгоритму зв'язування необхідно множину реальних особистих ознак $\boldsymbol{W}$ доповнити певною кількістю фіктивних ознак. Загальна кількість ознак після доповнення r. З'ясовано (п.4.3.2 б), що r визначається через мінімальну можливу величину віддалі між ознаками L, яка є строго більшою від $2\,\sigma_S$. Тобто, що менше L, то більше значення r, а отже, стійкіший криптографічний захист. Але, як показано на рис. 4.3, із збільшенням r зростає імовірність помилкового декодування, або імовірність неправильної неідентифікації (FRR).

З іншого боку кількість та розташування фіктивних ознак обмежені розміщенням дійсних особистих ознак та середньоквадратичним відхиленням положення ознак (табл. 4.2).

Для множини блокування (рис. 4.16), із використанням порога віддалі $\sigma_S = 5{,}8$ пікселів, утворено маску (рис. 4.17), в межах якої розташовувати фіктивні ознаки заборонено.

Встановлено (п. 4.3.2 б), що найоптимальнішою є випадкова техніка доповнення (упакування) множини блокування, для якої $\rho \approx 0{,}45$. Результат роботи алгоритму заповнення фіктивними ознаками зображений на рис. 4.18.

4.4.3. Блокування криптографічного ключа

Для ефективної роботи алгоритму блокування криптографічних ключів, блок-схему якого представлено на рис. 4.1, потрібно визначити параметри k, s, n, r.

Насамперед необхідно створити поліном (4.5) із секретної ключової послідовності, яка захищається алгоритмом. Коефіцієнтами полінома є елементи деякого скінченого поля $\mathcal{F} = \mathrm{GF}(n)$.

Для коректної роботи алгоритмів декодування коду Ріда-Соломона слід використати поле з $n = g^z$ елементів, де g – просте число.

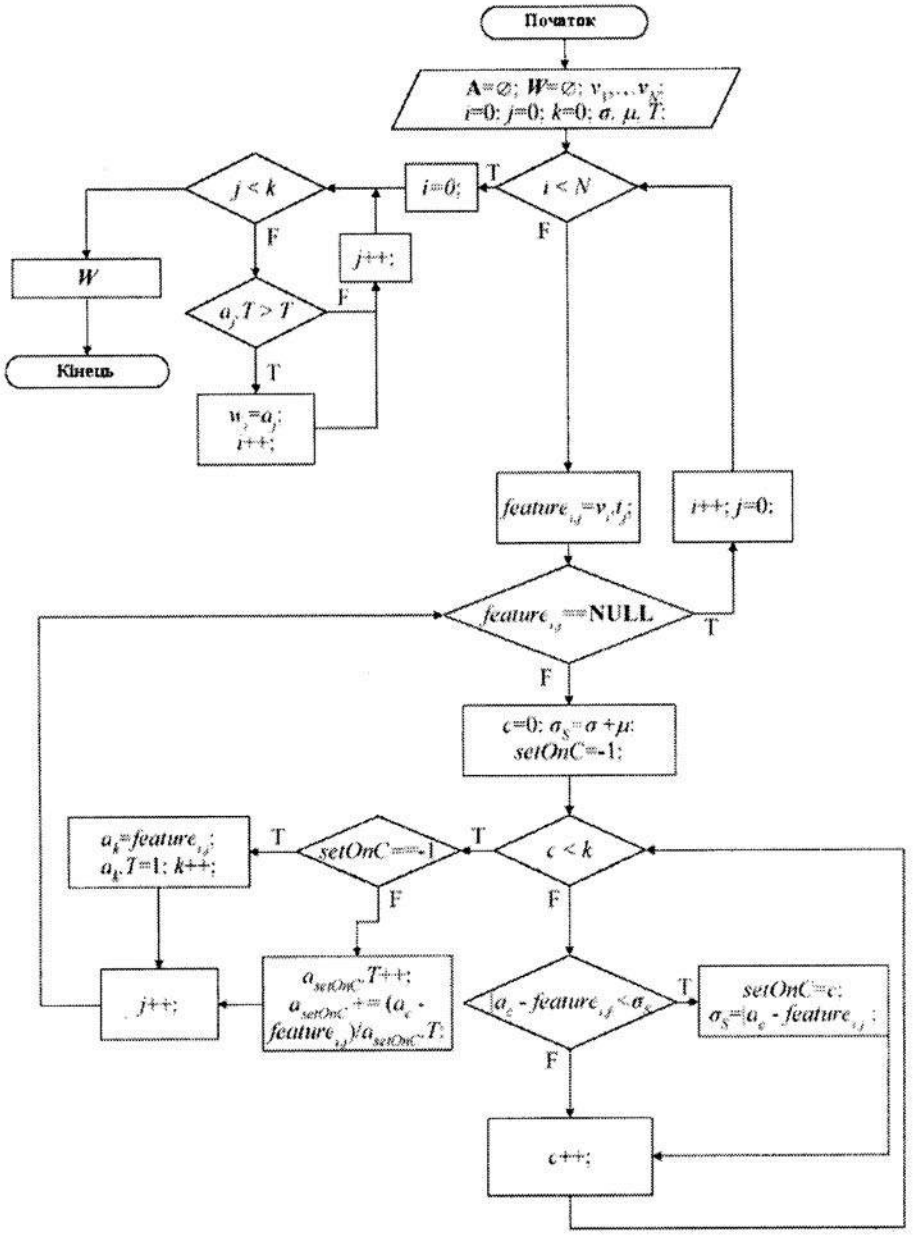


Рис.4.13. Блок-схема алгоритму створення множини блокування із N наборів особистих ознак.

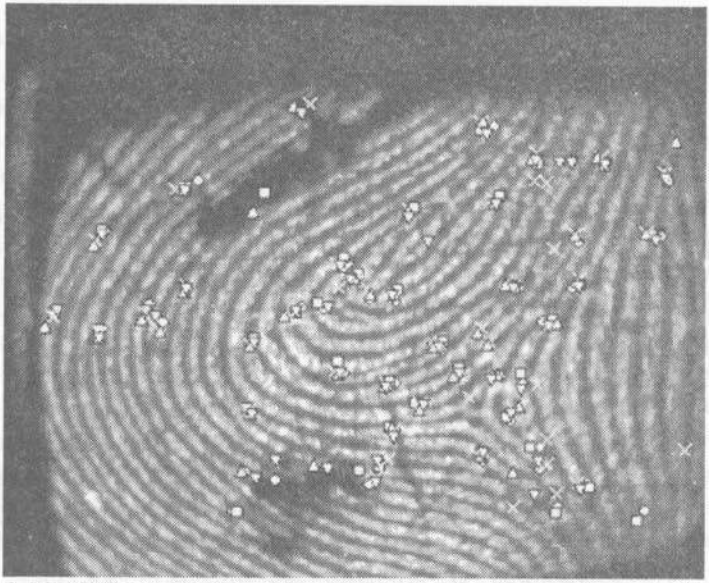


Рис. 4.14. Набори ознак, які подаються на вхід алгоритму. $N = 5$. (символи ○, □, ×, △, ▽ – відповідають ознакам із одного набору).

Рис. 4.15. Найімовірніші регіони положення особистих ознак конкретного відбитка пальця (45 регіонів) для порогу кратності $T = 3$.

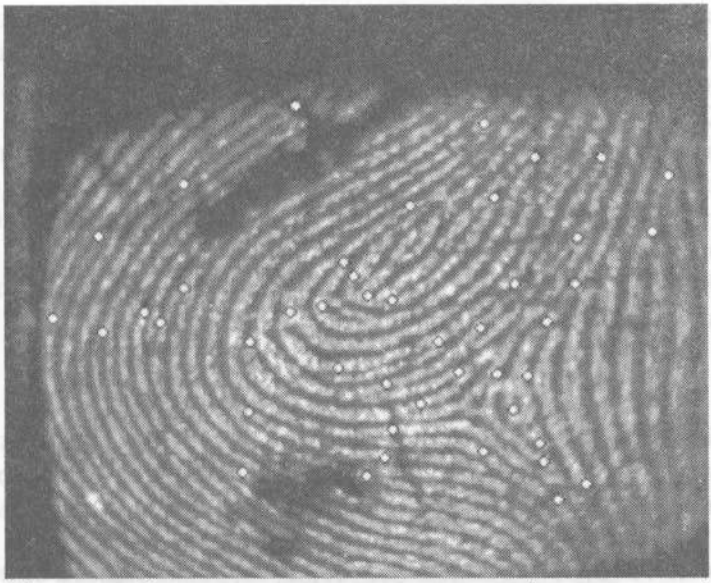


Рис. 4.16. Множина блокування, отримана на виході алгоритму відбору особистих ознак.

Водночас полем для алгоритму блокування є множина пікселів зображення відбитка пальця.

При проведенні експерименту, описаного у п. 4.4.2, було помічено, що з усієї площі сканування 322 × 255 пікселів ефективною, тобто такою, на яку припадає основна частина зображення (≈ 98%), є область у 280 × 249 пікселів. Такий висновок дає можливість вибору простого числа.

Найближчим до вищенаведених значень є область площею 251 × 251 піксель, що утворює поле $\mathcal{F} = \mathrm{GF}(251^2)$.

Довжина полінома, значення k, визначатиметься довжиною криптографічного ключа. Кожен із елементів поля $\mathrm{GF}(251^2)$ несе по 16 біт інформації. Так, для сучасного симетричного криптоалгоритму AES потрібен ключ довжиною 256 біт, що відповідає 16 - ти коефіцієнтам полінома, або поліному 15 степені.

Для утворення полінома (4.5) необхідно насамперед згенерувати 256 біт ключа за допомогою алгоритму, запропонованого у п.4.4.1. Далі поділити отриману послідовність на групи по 16 біт. Кожна така група є елементом поля $\mathrm{GF}(251^2)$ і відповідним коефіцієнтом m_i поліному $f(x)$.

Для перетворення координат положення дійсних і фіктивних особистих ознак у елементи поля доцільно використовувати 16-бітові

цілі числа, молодших вісім біт якого відповідають координаті x, а старші – y. Наприклад, мінуції з координатами (2, 3) відповідатиме елемент поля 514, або у двійковій системі числення – 0000 0010 0000 0010.

Згідно блок-схеми (рис. 4.1) до множини блокування, записаної як елементи поля, необхідно застосувати поліном $f(x)$. Отримані двійки вносяться у набір кортежів $B_{\mathbf{P}}$, який готовий для безпечного зберігання на сервері та передавання відкритими каналами зв'язку.

Оцінимо потужність набору $B_{\mathbf{P}}$ для параметрів $L > 2\,\sigma_S$; $L = 12$ пікселів; $\rho \approx 0{,}45$; $g = 251$:

$$r = \frac{4\rho g^2}{\pi L^2} \approx 300. \qquad (4.17)$$

Різниця між теоретичним значенням (4.17) і значенням, отриманим у результаті роботи алгоритму внесення фіктивних ознак (рис. 4.18), спричинена зменшенням області зображення, що опрацьовується.

4.4.4. Розблокування криптографічного ключа та оцінка ефективності

Для розблокування криптографічного ключа із $B_{\mathbf{P}}$ користувач надає множину особистих ознак, утворюючи множину розблокування $\boldsymbol{W}' = \{w'_1, \ldots, w'_r\}$, за допомогою якої у $B_{\mathbf{P}}$, згідно алгоритму розблокування (рис. 4.2), виділяється набір найближчих (з порогом віддалі σ_S) ознак $B_{\mathbf{P}}'$ потужністю r, де $r \approx s$ для легального користувача і $r >> s$ – для нелегального користувача. На рис. 4.19 всього ознак – $r = 47$, довжина кодового слова – $s = 45$, співпало – $\tau = 35$. Для значення $k = 16$ мінімально можливе число $\tau = \frac{s+k}{2} = \frac{45+16}{2} = 31$. Використовуючи подібний підхід, оцінимо ефективність алгоритму розблокування як залежність від кількості вірних ознак.

Помічаємо: що більшим є r, то складніше розблокування для нелегального користувача, але і зростає також складність для дійсного користувача (рис. 4.20, $k = 16$, $s = 45$). Для ефективної роботи екстрактора необхідно вибрати таке найбільше s, для якого складність розблокування легального користувача є мінімальною, тобто s повинно бути якомога ближчим до r, що досягається шляхом зменшення кратності T в алгоритмі утворення множини блокування (рис. 4.13).

Іншим важливим параметром, який впливає на ефективність алгоритму, є k. Рис. 4.21 ілюструє складність проведення атаки як

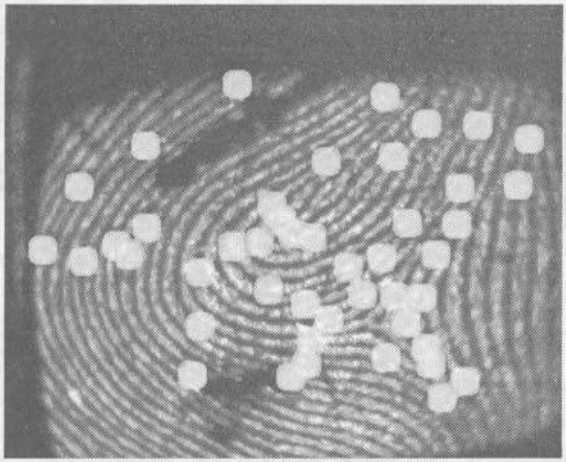


Рис. 4.17. Маска фіктивних ознак.

Рис. 4.18. Результат роботи алгоритму внесення фіктивних ознак у множину блокування ($r = 313$).

функцію від k та кількості істинних точок, а рис. 4.22 – імовірність неправильної неідентифікації як функцію від k.

Наведені залежності вказують на зменшення стійкості біометричного екстрактора та підвищення імовірності неправильної неідентифікації при збільшенні завадостійкості РСК, тобто можливостей корекції нечіткості вхідних біометричних даних.

Зростання стійкості зафіксоване при видовженні ключа k, що пояснюється збільшенням залишкової ентропії біометричного

Рис. 4.19. Множина блокування ○, із накладеною на неї множиною розблокування □. Дійсні ознаки виділено кругами з радіусом $\sigma_S = 6$.

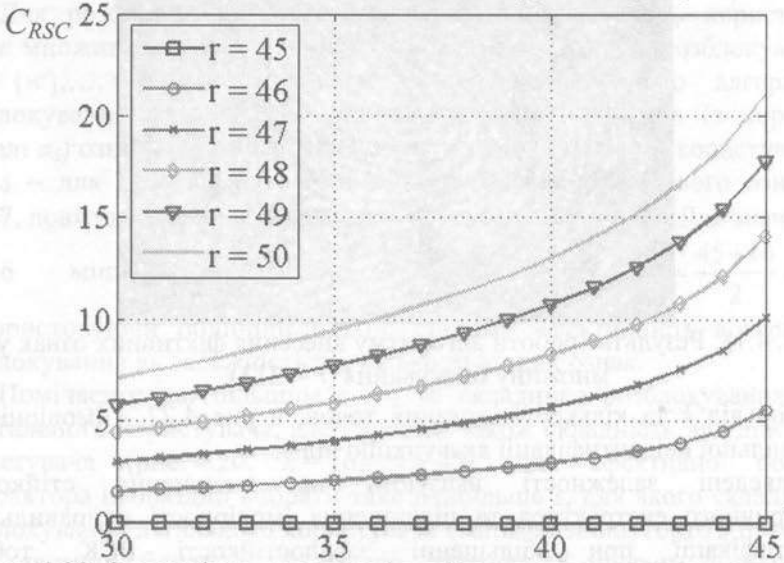


Рис. 4.20. Залежність складності розблокування методом коду Ріда-Соломона від кількості істинних ознак τ та загальної кількості ознак на відбитку r, який подано для розблокування.

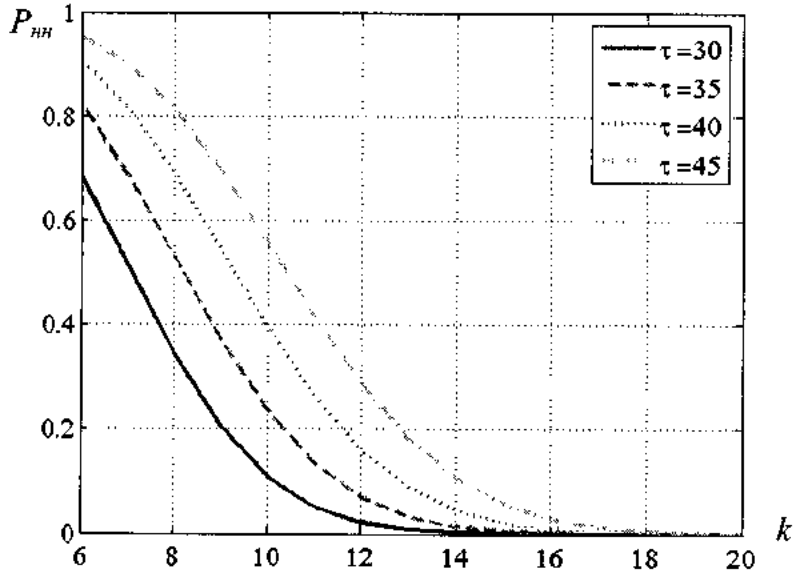


Рис. 4.21. Залежність імовірності неправильної неідентифікації від k та τ.

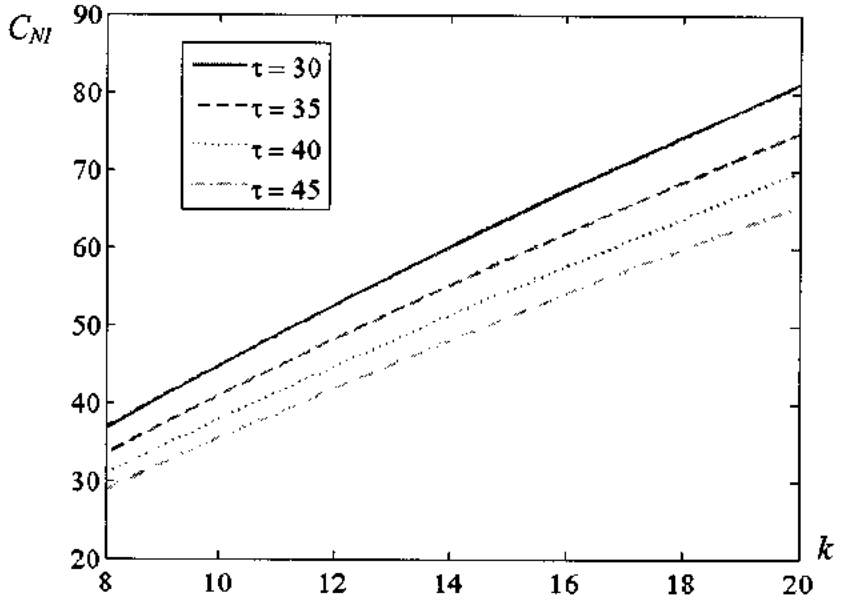


Рис. 4.22. Залежність складності проведення брутальної атаки від k та τ.

екстрактора за рахунок збільшення ентропії приховуваного у B_P криптографічного ключа.

Як встановлено у п. 4.3.1, для легітимного користувача найкращим методом реконструкції прихованого полінома є функція декодування РСК. Найефективнішим способом є метод Берлекемпа-Месі, який дозволяє зменшити складність розблокування криптографічного ключа для легального користувача на 3 - 4 порядки.

ЛІТЕРАТУРА

1 Аністратенко В.В., Коваль О.І., Косаревич Р.Я., Русин Б.П. Особливості побудови АДІС "УкрДакто"//Криміналістичний вісник. – К.: ЛАТСТАР, 2000. – С.27-32.

2 Астафьева Н.М. Вейвлет-анализ: Основы теории и примеры применения //Успехи физических наук. – 1996. – т.166. – № 11. – С.1145-1170.

3 Баскаков С.И. Радиотехнические цепи и сигналы. – М.: Высш. шк., 1988.- 448 с.

4 Берлекэмп Э. Алгебраическая теория кодирования. – М.: Мир, 1971. – 480 с.

5 Блум Ф., Лейзерсон А., Хофстедтер Л. Мозг, разум и поведение. – М.: Мир, 1988. – 193 с.

6 Бондарко Л.В., Загоруйко Н.Г., Кожевников В.А. и др. Модель восприятия речи человеком. -- Новосибирск: Наука, 1968. – 60 с.

7 Бронштейн И.Н., Семендяев К.А. Справочник по математике / Пер. с англ. - М.: Наука, 1964. – 321 с.

8 Варецький Я.Ю. Алгоритм біометричного блокування ключів для криптографічних систем // Відбір і обробка інформації. – Львів: НАН України. Фізико-механічний інститут ім. Г.В. Карпенка. – 2005. – № 98. – С.111-115.

9 Варецький Я.Ю. Реалізація криптографічного генератора випадкових чисел // Відбір і обробка інформації. – Львів: НАН України. Фізико-механічний інститут ім. Г.В. Карпенка. – 2003. – № 95. – С.145-148.

10 Варецький Я.Ю., Русин Б.П. Дактилоскопічне блокування ключів для криптографічних систем // Збірник наукових праць ІПМЕ НАН України. – Київ. – 2005. – № 31. – С.28-36.

11 Варецький Я.Ю., Русин Б.П., Чорній А.М. Аналіз стійкості дактилоскопічної біометричної системи верифікації // Збірник наукових праць ІПМЕ НАН України. – Київ. – 2004 – № 26 – С. 81-88.

12 Василенко Г.И., Цибулькин Л.М. Голографические распознающие устройства. – М.: Радио и связь, 1985. – 312 с.

13 Вемян Г.В. Качество телефонной передачи и его оценка. – М.: Связь, 1970. – 224 с.

14 Венцель Е.С. Теория вероятностей. – М.: Наука, 1969.– 367 с.

15 Вербіцький О.В. Вступ до криптології. – Львів: Видавництво науково-технічної літератури, 1998. – 248 с.

16 Винцюк Т.К. Анализ, распознавание и интерпретация речевых сигналов. – Киев: Наук. думка, 1987. – 264 с.

17 Винцюк Т.К. ИКДП - метод пофонемного распознавания и смысловой интерпретации речи многих дикторов // Распознавание и синтез звуковых сигналов: Сб. науч. тр. - Киев: Ин-т кибернетики АН УССР, 1987. – С. 4-16.

18 Винцюк Т.К. Организация вычислений при распознавании больших словарей //Автоматическое распознавание и синтез речевых сигналов: Сб. науч. тр. – Киев: Ин-т кибернетики АН УССР, 1989. – С. 4-12.

19 Винцюк Т.К. Сравнение ИКДП - и НММ - методов распознавания речи // Методы и средства информатики речи: Сб. науч. тр. – Киев: Ин-т кибернетики АН УССР, 1991. – С. 4-9.

20 Винцюк Т.К. Сравнительный теоретический анализ ИКДП - и НММ - методов распознавания речи // Автоматическое распознавание слуховых образов: Тез. докл. 15-го Всесоюз. семинара (АРСО - 15), Таллинн, 13-17 марта 1989 г. – Таллинн: ИК АН ЭССР,1989. – С. 18-24.

21 Вінцюк Т.К. Багатозначна смислова інтерпретація усномовного сигналу // Оброблення сигналів і зображень та розпізнавання образів: Праці 4 - ї Всеукр. міжнар. конференції,Київ, 19 - 23 жовтня 1998 р. – Київ, 1998. – С. 63-68.

22 Вінцюк Т.К. Генеративна модель образного комп'ютера // Оброблення сигналів і зображень та розпізнавання образів: Праці 6 - ї Всеукр. міжнар. конференції, Київ, 8-12 жовтня 2002 р. – Київ, 2002. – С. 7-14.

23 Вінцюк Т., Сажок М., Людовик Т. Сєлюх Р. Автоматичний озвучував українських текстів на основі фонемно - трифонної моделі з використанням природного мовного сигналу // Оброблення сигналів і зображень та розпізнавання образів: Праці 6-ї Всеукр. міжнар. конференції, Київ, 8-12 жовтня 2002 р. – Київ, 2002. – С. 79-84.

24 Вінцюк Т.К. Узагальнене автоматичне фонетичне транскрибування усномовного сигналу // Оброблення сигналів і зображень та розпізнавання образів: Праці 5-ї Всеукр. міжнар. конференції, Київ, 27 листопада - 1 грудня 2000 р. – Київ, 2000. – С. 95-98.

25 Вінцюк Т.К. Інтелектуальні усномовні інформаційні технології та системи //Оброблення сигналів і зображень та розпізнавання образів: Праці 3-ї Всеукр. міжнар. конференції, Київ, 26-30 листопада 1996р.– Київ, 1996. – С. 117-120.

26 Витерби А.Д., Омура Дж.К. Принципы цифровой связи и кодирования / Пер. с англ.; под ред. К.Ш. Зиганчирова. – М.: Радио и связь, 1982. – 536 с.

27 Галаган В.І., Петряєв С.Ю. Перспективи та проблеми впровадження в експертну практику органів внутрішніх справ України автоматизованих дактилоскопічних ідентифікаційних систем // Криміналістичний вісник. – К.: ЛАТСТАР, 2000. – С.21-26.

28 Галунов В.И. Бионическая модель системы распознавания речи // Исследование моделей речеобразования и речевосприятия. – Л., Науч. совет по комплекс пробл. физиологии человека и животных АН СССР, 1981. - С. 36-51.

29 Голд Б., Рэйдер Ч. Цифровая обработка сигналов / Пер. с англ. – М.: Сов. радио, 1973. – 368 с.

30 Горбань І.І., Клименко А.В. Робастні алгоритми верифікації особи за голосом, що призначені для роботи в умовах сильних завад та спотворень мовних повідомлень // Оброблення сигналів і зображень та розпізнавання образів: Праці 4-ї Всеукр. міжнар.конференції, Київ, 19 - 23 жовтня 1998 р. – Київ, 1998. – С. 69-70.

31 Горелик Л.А., Скрипник В.А. Некоторые аспекты построения систем распознавания. – М.: Сов. радио, 1974. – 224 с.

32 ГОСТ 28147-89. Система обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М. Госстандарт СССР

33 Гусєєв К., Новосельський О. Гомоморфне оброблення мови з використанням зменшеного часового вікна // Оброблення сигналів і зображень та розпізнавання образів: Праці 3-ї Всеукр. міжнар. конференції, Київ, 26 30 листопада 1996 р. – Київ, 1996. – С. 123-124.

34 Дактилоскопическая экспертиза: современное состояние и перспективы развития. – Красноярск: Министерство внутренних дел, 199[illegible]. – 416 с.

35 Дремин И.Л. и др. Вейвлеты и их использование // Успехи физических наук. – 2001. – т.171, № 5. – С. 465-501.

36 Дубовий О.П., Лукашенко В.Я., Рибалко Я.В., Тимошенко П.Ю., Чорнобай Л.М. Криміналістичне дослідження слідів рук. / Під ред. Я.Ю. Кондратьєва. – К.: Атіка, 2000. – 188 с.

37 Дьяконов В. Вейвлеты: от теории к практике. – М.: Солон-Р, 2002. – 448 с.

38 Дьяконов В., MATLAB Обработка сигналов и изображений: Специальный справочник. – СПб.: Питер, 2002. – 608 с.

39 Илюшин А.Д. Теория и применение вейвлет-анализа. – http://atm563.phus.msu.su/Ilyushin/index.htm.

40 Капустій Б.О., Русин Б.П., Таянов В.А. Нові підходи до параметричного синтезу алгоритмів розпізнавання // Радиоэлектроника и информатика. – 2005. – № 3. – С. 122-128.

41 Капустій Б.О., Русин Б.П., Таянов В.А. Системи розпізнавання образів з малими базами даних. – Львів: Сполом, 2006. – 152с.

42 Капустий Б.Е., Русын Б.П., Таянов В.А. Новый подход к определению вероятности правильного распознавания объектов множеств // Управляющие системы и машины. – 2005. – №2. – С. 8-13.

43 Киедзи А. и др. Прикладные нечеткие системы / Под ред. Т.Тэрано и др. – М: Мир, 1993. – 368 с.

44 Келані Ф. Дослідження характеристик мовного сигналу в задачах розпізнавання // Комп'ютерні системи та мережі. – Національний університет "Львівська Політехніка". – 2004. – Вісник № 523. – С.140-144.

45 Келані Ф. Особливість компресії мовних сигналів на основі використання ортогональних перетворень // Відбір і обробка інформації. – Львів: НАН України. Фізико-Механічний інститут ім. Г.В. Карпенка. – 2004. – № 20(96). – С. 137-142.

46 Косаревич Р.Я., Ісаєв І.Ю., Русин Б.П. Визначення періоду папілярного відбитка на зображенні на основі побудови функціоналів математичного сподівання // Оброблення сигналів і зображень та розпізнавання образів: Праці 5-ї Всеукр. міжнар. конференції, Київ, 27 листопада - 1 грудня 2000 р. – Київ, 2000. – С. 275-278.

47 Косаревич Р.Я., Русин Б.П. Виділення папілярних ліній на багатоградаційних зображеннях дактилоскопічних об'єктів за допомогою профілів // Відбір і обробка інформації. – Львів: НАН України. Фізико-Механічний інститут ім. Г.В. Карпенка. – 2000. – №14 (90). – С. 121-124.

48 Косаревич Р.Я., Русин Б.П. Використання дуальності ознак папілярних відбитків при покращенні дактилоскопічних зображень // Інформаційні технології та системи. – 2003. – том.1-2. – С. 115-117.

49 Косаревич Р.Я., Русин Б.П. Опис та розпізнавання зображень папілярних відбитків на основі елементів поля напрямків // Комп'ютерна інженерія та інформаційні технології. – Національний університет "Львівська Політехніка". – 2001. – Вісник № 433. – С. 79-84.

50 Кофман А. Введение в теорию нечетких множеств. – М.: Радио и связь, 1982. – 432 с.

51 Крак Ю., Вінцюк Т., Кириченко М., Гаращенко Ф., Бармак О. Розробка комп'ютерних технологій моделювання та керування візуальними образами людського обличчя при синтезі мовлення // Оброблення сигналів і зображень та розпізнавання образів: Праці 6-ї Всеукр. міжнар. конференції, Київ, 8-12 жовтня 2002 р. – Київ, 2002. – С. 23-26.

52 Лобур М. В., Лисак Ю. В., Келані Ф. Використання пакетних вейвлетів для визначення ознак розпізнавання мовних сигналів // Моделювання та інформаційні технології. – Київ, 2005. – Випуск 31. – С. 41-46.

53 Лобур М.В., Келані Ф. Аналіз методів компресії мовних сигналів // Радіоелектроніка та телекомунікації. – Національний університет "Львівська Політехніка". – 2004. – Вісник № 508. – С. 42-45.

54 Магєра В.М., Горбань І.І., Лєвий С.В. Автоматизація криміналістичних досліджень мовленнєвих сигналів // Оброблення сигналів і зображень та розпізнавання образів: Праці 5-ї Всеукр. міжнар. конференції, Київ, 27 листопада - 1 грудня 2000 р. – Київ, 2000. – С. 107-110.

55 Маркел Дж., Грей А.Х. Линейное предсказание речи / Пер. с англ.; под ред. Ю.Н. Прохорова, В.С. Звездина. – М.: Связь, 1980. – 308 с.

56 Марпл С. Л. Цифровой спектральный анализ и его приложение / Пер. с англ. – М.: Мир, 1990. – 547 с.

57 Мельник А.А., Молдовян Н.А., Гуц Н.Д., Изотов Б.В., Коркишко Т.А. Реализация скоростного шифра на основе управляемых перестановок // Вопросы защиты информации. – М.: Гос. унитарное предприятие "Всероссийский научно-исследовательский институт межотраслевой информации-федеральный информационно-аналитический центр оборонной промышленности". – 2001. №2 – С. 44-53.

58 Молдовян А.А. и др. Криптография: скоростные шифры. – СПб.: БХВ-Петербург, 2002. – 496 с.

59 Назаров М.В., Прохоров Ю.Н. Методы цифровой обработки и передачи речевых сигналов. – М.: Радио и связь, 1985. – 176 с.

60 Орищенко В. И. и др. Сжатие данных в системах сбора и передачи информации. – М.: Радио и связь, 1995. – 185 с.

61 Остап В.П. Кореляційний метод порівняння дактилоскопічних зображень за спектральними ознаками // Радіоелектроніка та телекомунікації. –Національний університет "Львівська політехніка". – 2002. –Вісник №440. – С. 155-162.

62 Охрименко В. Дактилоскопия и типы датчиков отпечатка пальца // Электронные компоненты и системы. – 2002. – №8. – С. 8-14.

63 Охрименко В. Методы и средства биомстрической идентификации // Электронные компоненты и системы. – 2002. – №8. – С. 3-7.

64 Петухов А.П. Введение в теорию базисов всплесков. – СПб.: Изд-во СПбГТУ, 1999. – 132 с.

65 Пилипенко В. Моделювання перекладу усномовних слів // Оброблення сигналів і зображень та розпізнавання образів: Праці 4-ї Всеукр. міжнар. конференції, Київ, 19-23 жовтня 1998 р. – Київ, 1998. – С. 73-74.

66 Пресняков И.Н., Омельченко С.В. Автоматическое распознавание раздельных слов и фонем речи // Радиоэлектроника и информатика. – 2003. – №2. – С.41 - 47.

67 Пресняков И.Н., Омельченко С.В. Распознавание фонем речи // Радиоелектроника и информатика. – 2004. – №3. – С. 59-63.

68 Претт У. Методы передачи изображений. Сокращение избыточности / Пер. с англ. – М.: Радио и связь, 1983. – 264 с.

69 Претт У. Цифровая обработка изображений / Пер. с англ. – М.:Мир, 1982. – т.2. – 480 с.

70 Прохоров Ю. Статистические модели и рекуррентное представление радиосигналов – М.: Радио и связь, 1984. – 237 с.

71 Путятин Е.П., Аверин С.И. Обработка изображений в робототехнике. – М.: Машиностроение, 1990. – 320 с.

72 Пятышев Е.Н., Лурье М.С. Микротехнологии и микроэлектромеханические системы – новое научно-техническое направление // Научно-технический вестник СПбГТУ. – 1999. – № 3. – С. 101-112.

73 Рабинер Л.Р., Шафер Р.В. Цифровая обработка речевых сигналов / Пер. с англ.; под ред. М.В. Назарова, Ю.Н. Прохорова. – М.: Радио и связь, 1981. – 495 с.

74 Рамишвили Г.С. Автоматическое опознавание говорящего по голосу. – М.: Радио и связь, 1981. – 224 с.

75 Рамишвили Г.С. Речевой сигнал и индивидуальность голоса. – Тбилиси: МЕЦНИЕРЕБА, 1976. – 183 с.

76 Рашкевич Ю.М. Аналіз методів часового масштабування мовних сигналів // Оброблення сигналів і зображень та розпізнавання образів: Праці 3-ї Всеукр. міжнар. конференції, Київ, 26-30 листопада 1996 р. – Київ, 1996. – С. 129-131.

77 Рашкевич Ю.М. Перетворення часового масштабу мовних сигналів. – Львів: Академічний експрес, 1997. – 143 с.

78 Рашкевич Ю., Марцинишин Р., Шпак З. Особливості зміни тем поральної структури мовних сигналів в різних темпах мовлення // Оброблення сигналів і зображень та розпізнавання образів: Праці 3-ї Всеукр. міжнар. конференції, Київ, 26 - 30 листопада 1996 р. – Київ, 1996. – С. 131-132.

79 Рашкевич Ю., Ткаченко Р., Шпак З. Часова трансформація мовних сигналів на основі нейронних мереж // Оброблення сигналів і зображень та розпізнавання образів: Праці 4-ї Всеукр. міжнар. конференції, Київ, 19-23 жовтня 1998 р. – Київ, 1998. – С. 75-76.

80 Русин Б., Остап В. Вибір інформативних ознак зображень відбитків пальців при розпізнаванні // Радіотехніка та телекомунікації. – Нацыональний уныверситет "Львівська політехніка". – 2000. – Вісник №399. – С. 56-64.

81 Русин Б., Остап В. Попередня фільтрація при розпізнаванні зображень // Комп'ютерні технології друкарства. – Львів: Українська академія друкарства. – 2000. – №4. – С. 295-300.

82 Русин Б.П., Остап В.П., Остап О.П. Спосіб розпізнавання зображень // Пат. 39442 А Україна, МКИ G 06 K 9/68. – Опубл. 15.06.2001; Бюл. №5. – С. 147-148.

83 Русин Б.П. Системи синтезу, обробки та розпізнавання складно структурованих зображень. – Львів: Вертикаль, 1997. – 264 с.

84 Русин Б.П., Кисіль Б.В., Фатхи Р. Система розпізнавання зображень на основі опорних точок алгебраїчними методами, що грунтуються на обчисленні оцінок // Радіоелектроніка та телекомунікації. – Національний університет "Львівська Політехніка". – 2004. – Вісник № 508. – С. 127-131.

85 Русин Б.П., Прудиус І.Н., Остап В.П. Спотворення й алгоритм попередньої обробки дактилоскопічних зображень // Відбір і обробка інформації. – Львів: НАН України. Фізико-механічний інститут ім. Г.В.Карпенка. – 2002. – №92. – С. 87-91.

86 Свириденко В. А. Анализ систем со сжатием данных. - М.: Связь, 1977. - 184 с.

87 Свириденко В.А. Передача сообщений с повышенной информативностью. – М.: Радио и связь, 1983. – 63 с.

88 Секунов Н. Обработка звука на PC. – СПб.: БХВ-Петербург, 2001 – 1248 с.

89 Техническое зрение роботов / Пер. с англ.; под ред. А. Пью – М.: Машиностроение, 1987. – 320 с.

90 Ту Дж., Гонсалес Р. Принципы распознавания образов / Пер. с англ. – М.: Мир, 1978. – 411с.

91 Фокина А.А. Зависимость частоты встречаемости деталей папиллярного узора от величины участка ладонной поверхности и его локализации // Криминалистика и судебная экспертиза. – 1976. – №13. – С. 57-64.

92 Френкс Л. Теория сигналов. – М.: Сов. радио, 1974. – 373 с.

93 Шеннон К. Теория связи в секретных системах // Работы по теории информации и кибернетике. – М.: Изд-во иностранной литературы, 1963. – С. 333-402.

94 Шлезингер М.И. Математические средства обработки изображении. – Киев: Наукова думка, 1989. – 196 с.

95 Шорошев В.В., Ильницкий А.Е. К вопросу решения проблемы экспертной оценки безопасности информации в компьютерных системах // Бизнес и безопасность. – 2001. – №1. – С. 62-64.

96 Шпак З., Рашкевич Ю. Аналіз темпоральних перетворень мовних елементів для задач часового масштабування голосових повідомлень // Оброблення сигналів і зображень та розпізнавання образів: Праці 6-ї Всеукр. міжнар. конференції, Київ, 8-12 жовтня 2002р. – Київ, 2002. – С. 97-100.

97 Юхименко О. Моделі фонем. Оцінка ефективності моделей // Обробка сигналів і зображень та розпізнавання образів: Праці 2-ї Всеукр. міжнар. конференції, Київ, 20-24 грудня 1994 р. – Київ, 1994. – С. 133-138.

98 Юхименко О. Методи розв'язання задачі навчання розпізнаванню сигналів мовлення на основі використання моделей фонем різної складності // Обробка сигналів і зображень та розпізнавання образів: Праці 2-ї Всеукр. міжнар. конференції, Київ, 20-24 грудня 1994 р. – Київ, 1994. – С. 139-142.

99 Al-Khaiyat M., Kamangar F. Planar Curve Representation and Matching // Proc. Ninth British Machine Vision Conference. – Southampton (UK). – 1998. – P. 174-184.

100 Asker M., Gerez B., Gerez S. Directional Field Computation for Fingerprints Based on the Principal Component Analysis of Local Gradients // Proc. Conf. Program for Research in Integrated Systems and Circuits (ProRISC2000). – Veldhoven (Netherlands). – 2000. – P. 215-222.

101 Bazen A.M., Gerez S.H. Segmentation of Fingerprint Images // Proc. Conf. Program for Research in Integrated Systems and Circuits (ProRISC2001). Workshop on Circuits, Systems and Signal Processing. – Veldhoven (Netherlands). – 2001. – P. 276-280.

102 Bazen A.M., Otterlo van M., Poel M., Gerez S.H. A Reinforcement Learning Agent for Minutiae Extraction from Fingerprints // Proc. Belgian-Dutch Conference on Artificial Intelligence (BNAIC'01). – Amsterdam (Belgium). – 2001. – P. 329–336.

103 Bazen A.M., Verwaaijen G.T.B., Gerez S.H., Veelenturf L.P.J., Zwaag B.J. A Correlation-Based Fingerprint Verification System // Proc. Conf. Program for Research in Integrated Systems and Circuits (ProRISC2000), Workshop on Circuits, Systems and Signal Processing. – Veldhoven (Netherlands). – 2000. – P. 102-108.

104 Beauchemin R., Brassard G., Crepeau C., Goutier C., Pomerance C. The Generation of Random Numbers that are Probably Prime // Journal of Cryptology. – 1988. – Vol.1, №1. – P. 53-64.

105 Bennett C., Brassard G., Cr'epeau C., Maurer U. Generalized Privacy Amplification // IEEE Transactions on Information Theory. – 1995. – Vol.6, № 41. – P. 1915-1923.

106 Bennett C., Brassard G., Robert J. Privacy Amplification by Public Discussion // SIAM Journal on Computing. – 1988.– Vol.2, №17. – P. 210 - 229.

107 Blakley G.R., Borosh I. Rivest-Shamir-Adleman Public Key Cryptosystems Do Not Always Conceal Messages // Computers and Mathematics with Applications. – 1979.– Vol.5, №3. – P. 169-178.

108 Boer J., Bazen A.M. Gerez S.H. Indexing Fingerprint Databases Based on Multiple Features // Proc. Conf. Program for Research in Integrated Systems and Circuits (ProRISC2000), Workshop on Circuits, Systems and Signal Processing. – Veldhoven (Netherlands). – 2000. – P. 32-37.

109 Burge M., Burger W. Ear Recognition // Biometrics: Personal Identification in Networked Society. – Kluwer: Kluwer Academic Publishing, 1998. – P. 273-286.

110 Buse R., Liu Z.Q., Caelli T. Using Gabor filters to measure the physical parameters of lines // Pattern Recognition. – 1996. – Vol.29, №4. – P.615-625.

111 Campbell Jr.J. Speaker recognition: A tutorial // Proc. of IEEE. – 1997. – Vol.85, №9. – P. 1437-1462.

112 Candela G.T., Chellappa R. Comparative Performance of Classification Methods for Fingerprints: Tech. Report TR 5163 / National Institute of standards and Technology. – Gaitherburg, 1993. – 41p.

113 Chapel C. Fingerprinting – A Manual of Identification. – New York: Coward McCann, 1971. – 55 p.

114 Chaum D., Schaumuller-Bichel J. Smart Card 2000. – North Holland: Elsevier Science Publishers, 1989. – 130 p.

115 Chen S., Ratha N., Karu K., Jain A. K. A real-time matching system for large fingerprint database // IEEE Trans. Pattern Anal. and Machine Intell. – 1996. – Vol.18, №8. – P.799–813.

116 Chor B., Goldreich O. Unbiased bits from sources of weak randomness and probabilistic communication complexity // SIAM Journal on Computing, Special issue on cryptography. – 1988. – Vol.2, №17. – P. 230-261.

117 Chor B., Goldreich O., Hastad J., Friedman J., Rudich S., Smolensky R. The bit extraction problem or t-resilient functions // Proc. of 26th Annual IEEE Symposium on Foundations of Computer Science. – 1985. – P. 156-182

118 Coetzee L. Fingerprint recognition: Master diploma. – Pretonia, 1992. – 71 p.

119 Coetzee L., Botha E.C. Fingerprint recognition in low quality images // Pattern Recognition. – 1993. – Vol.26, №10. – P. 1441-1460.

120 Cohen A., Wigderson A. Dispersers, deterministic amplification, and weak random sources // Proc. of the 30th Annual IEEE Symposium on Foundations of Computer Science. – 1989. – P. 234-266.

121 Connell A. An analysis of NewDES: A modified Version of DES // Cryptologia. – Vol. 14, №3. – 1990. – P.217-223.

122 Cowger J. Friction Ridge Skin: Comparison and Identification of Fingerprints. – New York: Elsevier, 1983. – 245 p.

123 Cummins H., Mildo C. Finger Prints, Palms and Soles. – New York: Dover Publication Inc., 1961. – 319 p.

124 Daemen J., Rijmen V. AES Proposal: Rijndael // First Advanced Encryption Standard (AES) Conference. – Ventura, CA., 1998. – P. 5-36.

125 Daugman J.G. High confidence visual recognition of persons by a test of statistical independence // IEEE Trans. Pattern Anal. and Machine Intell. – 1993. – Vol.15, № 1– P. 1148–1161.

126 Davida G.I., Frankel Y., Matt B.J. On enabling secure applications through off-line biometric identification // Proc. IEEE Symp. Privacy and Security. – 1998. – P. 148-157.

127 Davida G.I., Frankel Y., Matt B.J., Peralta R. On the relation of error correction and cryptography to an offline biometric based identification scheme // Proc. Workshop Coding and Cryptography (WCC'99). – 1999. – P. 129–138.

128 Davies S. G. Touching big brother: How biometric technology will fuse flesh and machine // Information Technology & People. – 1994. – Vol.7, №4. – P. 60-69.

129 Derakhshani R., Schuckers S., Hornak L., O'Goman L. Determination of vitality from a non-invasive biomedical measurement for use in fingerprint scanners // Pattern Recognition. – 2003. – Vol.36, №1. – P. 383-396.

130 Diffie W., Strawczynski L., O'Higgins B., Steer D. An ISDN Secure Telephone Unit // Proceedings of the National Telecommunications Forum. – 1987. – Vol.41, №1. – P. 473-477.

131 Dodis Y., Elbaz A., Oliveira R. Improved Randomness Extraction from Two Independent Sources // Proc. of RANDOM-APPROX. – 2003. – P. 252-263.

132 Donahue M.J., Rokhlin S.I. On the use of Level Curves in Image Analysis // Image Understanding. – 1993. – Vol.57, №2. – P. 185-203.

133 ElGamal T. A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms // Advances in Cryptology: Proc. of CRYPTO 84. – Springer Verlag, 1985. – P. 1-18.

134 Ellison C. , Hall C., Milbert R., Schneier B. Protecting keys with personal entropy // Future Generation Computer Systems. – 2000. – Vol.16. – P. 311 – 318.

135 Emyrodlu Y. Fingerprint Image: Enhancement and Recognition PhD thesis. – Hertfordshire (Turkey). – 1997. – 179 p.

136 Fielding K.H., Horner J.L., Makekau C.K. Optical fingerprint identification by binary joint transform correlator // Optical Engineering. – 1991. – Vol.30, №12. – P. 1958-1961.

137 FIPS 46, "Data Encryption Standard", Federal Information Processing Standard (FIPS), Publication 46. – National Bureau of Standards, U.S. Department of Commerce. – Washington D.C.

138 Galton F. Finger Prints. – New York: Da Capo Press, 1961. – 412 p.

139 Gao S. A new algorithm for decoding reed-solomon codes // Future Generation Computer Systems. – 2002. – Vol.13. – P. 52-63.

140 Gardiner C.W. Distributed Public Key Certificate Management // Proc. of the Privacy and Security Research Group, Workshop on Network and Distributed System Security. – The Internet Society, 1993. – P. 69-73.

141 Garon G., OuterBridge R. DES Watch: An Examination pf the Sufficiency of the Data Encryption Standard for Financial Institution Information Security in the 1990's // Cryptologia. – 1991. – Vol. 15, №3. – P. 177-193.

142 Gaussian Scale-Space Theory / Sporring J., Nielsen M., Florack L. and eds. – Copenhagen: Kluwer, 1996. – 306 p.

143 Golfarelli M., Maio D., Maltoni D. On The Error-Reject tradeoff in Biometric Verification Systems // IEEE Trans. on Pattern Anal. and Machine Intell. – 1997. – Vol.19, №7. – P. 786-796.

144 Grycewicz T.J. Fingerprint recognition using binary nonlinear joint transform correlators // Optoelectronic Devices and Systems for Processing. – 1996. – Vol. CR65. – P. 27-56.

145 Guideline for The Use of Advanced Authentication Technology Alternatives: FIPS PUB 190 / USA National Institute of Standards and Technology, 1994.

146 Guruswami V., Sudan M. Improved decoding of reed-solomon and algebraic-geometric codes // Proc. of FOCS '98. – 1998. – P. 28-39.

147 Hastad J., Impagliazzo R., Levin L., Luby M. A Pseudorandom generator from any one-way function // Proc. of 21st ACM Symp. on Theory of Computing. – 1989. – P. 121-143.

148 Hendessi E., Arcf M.R. A successful attack against the DES // Proc. Third Canadian Workshop on Information Theory and Applications. – 1994. – P. 78-90.

149 Hildebrand F. B. Introduction to Numerical Analysis. – McGraw-Hill.,1956. – 560 p.

150 Hong L. Algebraic feature extraction of image for recognition // Pattern Recognition. 1991. – Vol.24, №2. – P. 211-219.
151 Hong L. Automatic Personal Identification Using Fingerprints Phd Thesis. – Michigan State University. – 1998. – 227 p.
152 Hong L., Jain A. K., Pankanti S. Can Multibiometrics Improve Performance? // Proc. of Workshop on Automatic Identification Advanced Technologies (AutoID'99). – Morristown (USA). – 1999. – P. 59-64.
153 Hong L., Jain A. K., Pankanti S., Bolle R. Fingerprint Enhancement // Proc. IEEE Workshop on Applications of Computer Vision. – Sarasota (USA, FL). – 1996. – P. 202-207.
154 Hong L., Wan Y., Jain A. Fingerprint Image Enhancement: Algorithm and Performance Evaluation // IEEE Trans. Pattern Anal. and Machine Intell. – 1998. – Vol.20, №8. – P. 777-789.
155 Hrechak A.K., McHugh J.A. Automated fingerprint recognition using structural matching // Pattern Recognition. – 1990. – Vol.23, №8. – P. 893-904.
156 Ikonomopoulos A., Unser M. A Directional Filtering Approach to Texture Discrimination // Proc. of the Seventh International Conference on pattern Recognition. – Montreal (Canada). – 1984. – P. 87-89.
157 Isenor D.K., Zaky S.G. Fingerprint identification using Graph matching // Pattern Recognition. – 1986. – Vol.19, №2. – P. 113-122.
158 Jaeger H., Nagel S. Physics of granular states // Science. – 1992. – №255. – P.1524.
159 Jain A., Hong L., Bolle R. On-Line Fingerprint Verification // IEEE Trans. Pattern Anal. and Machine Intell. – 1997. – Vol.19, №4. – P. 302-314.
160 Jain A., Pankanti S. Automated Fingerprint Identification and Imaging Systems // Advances in Fingerprint Technology. – New York.: Elsevier Science, 2001. – 456 p.
161 Jain A.K., Prabhakar S., Chen S. Combining multiple matchers for a high security fingerprint verification system // Pattern recognition letters. – 1999. – Vol.20. – P. 1371-1379.
162 Jain A.K., Prabhakar S., Hong L., Pankanti S. Filterbank-based fingerprint matching. // IEEE Transactions on Image Processing. – 2000. – Vol.9, №5. – P.846–859.
163 Javidi B., Horner J.L. Optical pattern recognition for validation and security verification // Optical Engineering. – 1994. – Vol.33, №6. – P. 1752-1756.
164 Juels A., Wattenberg M. A fuzzy commitment scheme // Proc. 6th ACM Conf. Computer and Communications Security. – 1999. – P. 28-36.
165 Kao Yu-Hung, Hetsch L., Rajaserarau P.K. Speaker Recognition over Telephone Channels // Modern Methods in Speech Processing / Ed: R.Ramachandran, R.Mamoone. – 1995. – ch.13. – P. 299-321.
166 Kawagoe M., Tojo A. Fingerprint Pattern Classification // Pattern Recognition. – 1984. – Vol.17, №3. – P. 295-303.

167 Klein D.V. Foiling the Cracker: A Survey of, and Implications to, Password Security // Proc. of the USENIX, UNIX Security Workshop. – 1990. – P. 5-14.

168 Kobayashi Y., Toyoda H., Mukohzaka N., Yoshida N., Hara T. Fingerprint Identification by an Optical Joint Transform Correlation System // Optical Review. – 1996. – Vol.3, №6A. – P. 403-405.

169 Lacy J.B., Mitchell D.P., Schell W.M. CryptoLib: Cryptography in Software // UNIX Security Symposium Proceedings. – USENIX Association, 1993. – P. 1-17.

170 Lai X., Massey J.L. A proposal for a New Block Encryption Standard // Proc. Advances in Cryptology. – EUROCRYPT-90. – New York: Springer-Verlag, 1991. – P. 389-404.

171 Le V. T., Cheung Y. K., Nguyen H. M. A Fingerprint Recognizer Using Fuzzy Evolutionary Programming // Proc. of the 34th Annual Hawaii International Conf. on System Sciences (HICSS-34). – Maui (Hawaii). – 2001. – P. 56-61.

172 Lee H. C., Gaensslen R. E. Advances in Fingerprint technology. – New York: Elsevier, 1991. – 296 p.

173 Lenstra A.K., Lenstra H.W. The number field sieve. The development of the number field sieve // Lecture Notes in Math. – Berlin: Springer-Verlag, 1993. – vol. 1554. – pp. 11-42

174 Lenstra A.K., Lenstra H.W., Manasse Jr., M.S., Pollard J.M. The Number Field Sieve // Proc. of the 22-nd ACM Symposium on the Theory of Computing. – 1990. – P. 574-672.

175 Leung M.T., Engeler W.E., Frank P. Fingerprint Image Processing Using Neural Network // Proc. 10th conf. on Computer and Communication Systems. – Hong Kong (Chine). – 1990. – P. 582-586.

176 Li J., Testorf M., Fiddy M. A. Fourier properties of fingerprints // Proc. SPIE. – 1998. – Vol.3575. – P. 201-210.

177 Linn J. Privacy Enhancement for Internet Electronic Mail: Part III Algorithms, Modes, and Identifiers // RFC 1115 – Aug, 1989. – 25 p.

178 Linnartz J.-P., Tuyls P. New shielding functions to enhance privacy and prevent misuse of biometric templates // Proc. of 4th Int. Conf. Audio- And Video-Based Biometric Person Authentication. – 2003. – P. 393–402.

179 Mallat S.A. Theory for multiresolution signal decomposition: the wavelet representation // IEEE Trans. Pattern Anal. and Machine Intell. – 1989. – Vol.11, №7. – P. 674-693.

180 Manber U. A simple scheme to make passwords based on one-way functions much harder to crack // Computers & Security. – 1996. – Vol.15, №2. – P. 171-176.

181 Mario D., Maltoni D. Direct gray-scale minutia detection in fingerprints // IEEE Trans. Pattern Analysis and Machine Intell. – 1997. – Vol.19, №1. – P. 27-39.

182 Massey J.L. Shift register synthesis and BCH decoding // IEEE Trans. on Information Theory. –1969. – Vol.15, №1. – P. 122-127

183 Matyas V.Jr., Riha Z. Biometric Authentication Systems. – FI MU, 2000. – 46 p.

184 Maurer U.M. A universal statistical test for random bit generators // Proc. of CRYPTO 90. – Springer-Verlag, 1991. – P. 409-420.

185 McMahon P. SESAME V2 Public Key and Authorization Extensions to Kerberos // Proc. of the Internet Society, Symposium on Network and Distributed Systems Security. – IEEE Computer Society Press, 1995. – P. 114-131.

186 Mehtre B.M., Chatterjee B. Segmentation of fingerprint images – a composite method // Pattern Recognition. – 1989. – Vol.22, №4. – P. 381-385.

187 Mehtre B.M. Fingerprint Image Analysis for Automatic Identification // Machine Vision and Applications. – 1993. – Vol.6, №2-3. – P. 124-139.

188 Mehtre B.M., Murthy N. N., Kapoor S. Segmentation of Fingerprint Images using the Directional Image // Pattern Recognition. – 1987. – Vol.20, №4. – P. 429-435.

189 Menzes A.J., Van Oorschot P., Vanstone Scott. A. Handbook of applied cryptography. – NY.: CRC Press, 1996. – 780 p.

190 Micciancio D., Goldwasser S. Complexity of Lattice Problems: A Cryptographic Perspective. – Boston, Massachussetts: Kluwer Academic Publishers, 2002. – 356 p.

191 Moayer B., Fu K. A Tree System Approach for Fingerprint Pattern Recognition. // IEEE Trans. Pattern Anal. Machine Intell. – 1986. – Vol.8, №3. – P. 376-388.

192 Moenssens A. Fingerprint Techniques. – London: Chilton Book Company, 1971. – 29 p.

193 Monrose F., Reiter M. K., Li Q., Lopresti D. P., Shih C. Toward speech-generated cryptographic keys on resource constrained devices // Proc. of 11th USENIX Security Symp. – 2002. – P. 283–296.

194 Monrose F., Reiter M. K., Li Q., Wetzel S. Cryptographic key generation from voice // Proc. of IEEE Symp. Security and Privacy. – 2001 – P.202-213.

195 Monrose F., Reiter M. K., Li Q., Wetzel S. Using voice to generate cryptographic keys // Proc. of A Speaker Odyssey, Speaker Recognition Workshop. – 2001.l – P. 237–242.

196 Monrose F., Reiter M. K., Wetzel S. Password hardening based on keystroke dynamics // Proc. 6th ACM Conf. Computer and Communications Security. – 1999. – P. 73–82.

197 Monrose F., Rubin A. Authentication via keystroke dynamics // Proc. of the 4th ACM Conf. on Computer and Communications Security. – 1997. – P. 48-56.

198 Montgomery R.L. Speeding the Pollard and Elliptic Curve Methods of Factorization // Mathematics of Computation. – 1987. – Vol.48, №177. – P. 243-264.

199 Montgomery R.L., Silverman R. An FFT Extension to the p-1 Factoring Algorithm // Mathematics of Computation. – 1990. – Vol. 54, №190. – P. 839-854.

200 Navarro R., Tabernero A., Cristobal G. Image representation with Gabor wavelets and its applications // Advances in Imaging and Electron Physics. – New York: Academic Press, 1996. – 84 p.

201 Newham E. The Biometric Report. – New York: SJB Services, 1995. – 321p.

202 Nisan N., Zuckerman D. Randomness is linear in space // Journal of Computer and System Sciences. – 1996. – Vol.1, № 52. – P. 43–52

203 Noh S., Pae K., Lee C., Kim J. Multiresolution independent component analysis for iris identification // The 2002 International Technical Conference on Circuits/Systems, Computers and Communications. – Phuket (Thailand). – 2002. P. 86-103.

204 O'Gorman L., Nickerson J. V. An approach to fingerprint filter design // Pattern Recognition. – 1989. – Vol.22, №1. – P. 29-38.

205 Odlyzko A.M. The future of integer factorization // Advances in Cryptology: Proceedings of EUROCRYPT 84. – New York: Springer-Verlag, 1985. – P. 224-314.

206 O'Higgins B., Diffie W., Strawczynski L., De Hoog R. Encryption and ISDN a Natural Fit // Proceedings of the International Switching Symposium. – 1987. – P. 863-869.

207 Osterberg J., Parthasarathy T., Raghavan T., Sclove S. Development of a mathematical formula for the calculation of fingerprint probabilities based on individual characteristics // Journal of the American Statistical Association. – 1977. – №72. – P. 772-778.

208 Pal N.R., Pal S.K. A review on image segmentation techniques // Pattern Recognition. – 1993. – Vol.26, №9. – P. 1277-1294.

209 Pankanti S., Prabhakar S., Jain A. On the Individuality of Fingerprints // IEEE Trans. Pattern Anal. and Machine Intell. – 2002. – Vol.24, №8. – P. 1010-1025.

210 Patterson W. Mathematical Cryptology for Computer Scientists and Mathematicians. – Totowa, N.J.: Rowman & Littlefield, 1987. – 150 p.

211 Pavlidis T. Structural Pattern recognition. – New York: Springer-Verlag, 1980. – 302 p.

212 Pfieeger C.R. Security in Computing – Englewood Cliffs, N.J.: Prentice-Hall, 1989. – 56 p.

213 Pinkas D., Parker T., Kaijser R. SESAME: An Introduction Issue 1.2 – Bull, JCL, and SNI, 1993. – 68 p.

214 Pomerance C. The Quadratic Sieve Factoring Algorithm // Advances in Cryptology: Proc. of EUROCRYPT 84. – New York: Springer-Verlag, 1985. – P.169-182.

215 Pomerance C., Smith J.W., Tuler R. A Pipe-Line Architecture for Factoring Large Integers with the Quadratic Sieve Algorithm // SIAM Journal on Computing. – 1988. – Vol.17, №2. – P. 387-403.

216 Prabhakar S. Fingerprint Classification and Matching Using a Filterbank: PhD Thesis. – Michigan. – 2001. – 240 p.

217 Qinghan X., Raafat H. Combining statistical and structural information for fingerprint image processing, classification and identification // Pattern Recognition: Architectures, Algorithms and Applications. – New York: World Scientific Series in Computer Science, 1991. – P. 335-354.

218 Quisquater J.-J., Desmedt Y.G. Chinese lotto as an exhaustive code-breaking machine // Computer. – 1991. – Vol. 24, №11. – P. 14-22.

219 Ratha N.K., Chen S., Jain A. Adaptive Flow Orientation-Based Feature Extraction in Fingerprint Images // Pattern Recognition. – 1995. – Vol.28, №11. – P. 1657-1672.

220 Ratha N., Connell J., Bolle R. Enhancing security and privacy in biometrics-based authentication systems // IBM System Journal. –2001. – Vol. 40, №3. – P. 614–634.

221 Ravishankar Rao A. A Taxonomy for Texture Description and Identification. – New York: Springer-Verlag, 1990. – 331 p.

222 Reed I. S., Solomon G. Polynomial codes over certain finite fields // SIAM Journal Appl. Math. – 1960. – №8. – P. 300-304.

223 Rivest R. The RC5 encryption algorithm / B. Preneel, Ed // Proc. Fast Software Encryption, Second International Workshop (LNCS 1008). – 1995. – P. 86-96.

224 Rivest R., Robshaw M., Sidney R., Yin Y. The RC6 Block Cipher // First Advanced Encryption Standard (AES) Conference. – Ventura, CA., 1998. – 20 p.

225 Rivest R., Shamir A., Adleman L. A method for obtaining digital signatures and public-key cryptosystems // Proc. of communications of the ACM. – 1978. – Vol. 21, №2. – P. 120-126.

226 Rusyn B.P., Kapustiy B.O., Tayanov V.A. Features of statistical detection methods application to the recognition tasks // Journal of Automation and Information Sciences. – 2005. – №1. –P. 107-114.

227 Sakata S., Jensen H. E., Haholdt T. Generalized Berlekamp-Massey Decoding of Algebraic-Geometric Codes up to Half the Feng-Rao Bound // IEEE Transactions on Information Theory. – 1995. – Vol.41, №6. – P. 1762-1768

228 Santha M., Vazirani U. V. Generating quasi-random sequences from semi-random sources // Journal of Computer and System Sciences. – 1986. – №33. – P. 75-87.

229 Saviers K. Friction skin characteristics: A study and comparison of proposed standards. – Garden Grove: California Police Department, 1987. – 93 p.

230 Sclove S. The occurrence of fingerprint characteristics as a two-dimensional process // Journal of the American Statistical Association. – 1979. – №74. – P. 588-595.

231 Seal C., Gifford M., McCartney D. Iris recognition for user validation // British Telecommunications Engineering Journal. – 1997. – Vol.16, №7. – P. 113-117.

232 Shamir A. On the Generation of Cryptographically Strong Pseudo-Random Sequences // ACM Transactions on Computer Systems. – 1983. – Vol.1, №1. – P. 38-44.

233 Shannon C.E. A Mathematical Theory of Communication // Bell System Technical Journal. – 1948. – Vol.27, №4. – P. 379-423; 623-656.

234 Sherlock B.G., Monroe D.M., Millard K. Algorithm for enhancing fingerprint images // Electronics letters. – 1992. – Vol.28, №18. – P. 1720-1721.

235 Sherlock B.G., Monroe D.M., Millard K. Fingerprint Enhancement by Directional Fourier filtering // IEEE Proc. Vision, Image and Signal Processing. – 1994. – №141. – P. 87-94.

236 Sherstinsky A., Picard R. Restoration and Enhancement of Fingerprint Images Using M-lattice – A novel Non-linear Dynamical System // Proc. 13th International Conf. on Pattern Recognition. – Jerusalem (Israel). – 1994. - Vol.2. – P. 195-200.

237 Shneier B. Description of new variable-length key, 64-bit block cipher (Blowfish) // Proc. Fast Software Encryption, Second International Workshop (LNCS 809). – 1994. – P. 191-204.

238 Sipser M.. Expanders, randomness, or time versus space // Journal of Computer and System Sciences. – 1988. – Vol.1, № 36. – P. 388 - 405.

239 Soutar C., Roberge D., Stojanov S.A., Gilroy R., Vijaya Kumar B.V.K. Biometric encryption // ICSA Guide to Cryptography / R.K. Nichols. – Ed New York: McGraw-Hill, 1999. – 480 p.

240 Soutar C., Roberge D., Stojanov S.A., Gilroy R., Vijaya Kumar B.V.K. Biometric encryption using image processing // Proc. SPIE, Optical Security and Counterfeit Deterrence Techniques II. – 1998. – Vol.3314. – P. 178-188.

241 Soutar C., Roberge D., Stojanov S.A., Gilroy R., Vijaya Kumar B.V.K. Biometric encryption-enrollment and verification procedures // Proc. SPIE, Optical Pattern Recognition IX. – 1998. – Vol.3386. – P. 24-35.

242 Speech Understanding systems // Summary of results of the five-year effort at Carnegie-Mellon University, Department of Computer Science. –Pittsburg, 1977. – 175 p.

243 Stanley C. Are fingerprints a genetic marker for handedness? // Behavior Genetics. – 1994. – Vol.24, №2. – P. 141.

244 Stosz J.D., Alyea L.A. Automated system for fingerprint authentication using pores and ridge structure // Proc. of SPIE, Automatic Systems for the Identification and Inspection of Humans. – San Diego. – 1994. - Vol.2277. – P. 210-223.

245 Sudan M. Decoding of Reed-Solomon codes beyond the error correction bound // Journal of Complexity. – 1997. – Vol.13. – P. 180-193.
246 Szekely E.N., Szekely V. Image recognition problems of fingerprint identification // Microprocessors and Microsystems. – 1993. – Vol.17, №4. – P. 215.
247 The Science of Fingerprints: Classification and Uses. - Washington: (U.S.) Government Printing Office, 1998. – 214 p.
248 The transforms and applications handbook / Editor-in-chief, A. Poularikas. – Boca Raton (USA): CRC Press, 1996. – 1120 p.
249 Tisse C., Martin L., Torres L., Robert M. Person identification technique using human iris recognition // 15th International Conf. on Vision Interface. – Canada, 2002. – P. 294-299
250 Turk M., Pentland A. Eigenfaces for recognition // Journal of Cognitive Neuroscience. – 1991. – Vol.3, №1. – P. 71-86.
251 Valentin D., Abdi H., O'Toole A. J., Cottrell G. Connectionist models of face processing: A survey // Pattern Recognition. – 1994. – Vol.27, №9. – P. 1209-1230.
252 Van Lint J.H. Introduction to Coding Theory. – New-Jork: Springer-Verlag, 1992 – 183 p.
253 Verbitskiy E., Tuyls P., Denteneer D., Linnartz J.P. Reliable biometric authentication with privacy protection // Proc. of SPIE Biometric Technology for Human Identification Conf. – Orlando, FL. – 2004. P. 125-131.
254 Verma M. R., Majumdar A. K., Chatterjee B. Edge detection in fingerprints // Pattern Recognition. – 1987. – Vol.20, №5. – P. 513-523.
255 Weber D.M. A Cost Effective Fingerprint Verification Algorithm for Commercial Applications // Proc. of the IEEE South African Symposium on Communication and Signal Processing. – 1992. – P. 99-104.
256 White S.R. Convert distributed processing with computer viruses // Proc. of Advances in Cryptology (CRYPTO '89). – 1990. – P. 616-619.
257 Wildes R. Iris recognition: an emerging biometric technology // Proc. of the IEEE. – 1997. – Vol. 85, №9. – P. 1348-1363
258 Williams H.C. A Modification of the RSA Public-Key Encryption Procedure // IEEE Transactions on Information Theory. – 1980. – Vol. IT-26, №6. – P. 726-729.
259 Wilson C.L., Watson C.I., Paek E.G. Combined Optical and Neural Network Fingerprint Matching // Proc. International Conf. Optical Pattern Recognition VIII. – 1997. – Vol.3073. – P. 373-382.
260 Winer M.J. Efficient DES Key Search // School of Computer Science (TR-244). –Carleton. – 1994. – P. 6-8
261 Xiao Q., Raafat H. Fingerprint image postprocessing: a combined statistical and structural approach // Pattern Recognition. – 1991. – Vol.24, №10. – P. 985-992.
262 Zhang J., Yan Y., Lades M. Face recognition: Eigenface, elastic matching, and neural nets // Proc. of IEEE. – 1997. – Vol.85, №9. – P. 1423-1436.

263 Zhu Y., Tan T., Wang Y. Biometric personal identification based on iris patterns // Proc. of the 15th International Conference on Pattern Recognition. – Spain. – 2000. – Vol.2. – P. 2801-2804.

264 Zimmermann P. The Official PGP User's Guide. – Boston: MIT Press, 1995. – 250 p.

265 Zuckerman D. General weak random sources // Proc. of 31-st Annual Symposium on Foundations of Computer Science. – 1990. – Vol.2. – P. 534-543.

266 Zuckerman D. Simulating BPP using a general weak random source // Algorithmica. – 1996. – Vol.4, №16. – P. 367-391.

М о н о г р а ф і я

Русин Богдан Павлович
Варецький Ярема Юрійович

БІОМЕТРИЧНА АУТЕНТИФІКАЦІЯ ТА КРИПТОГРАФІЧНИЙ ЗАХИСТ

Р е ц е н з е н т и: д.т.н., проф. Дідковський В.С.
д.т.н., проф. Рибальський О.В.

Затверджено до друку вченою радою
ФМІ ім.Г.В.Карпенка НАН України

Редактор Р.Р.Кокотайло

Підписано до друку 25.10.06. Формат60х84/16
Папір офсетний. Гарнітура "Times".
Умовн. друк. арк. 16,80.
Зам. № 57
Наклад 300 примірників.

Видавництво "Коло"

Видруковано видавництвом "Коло"

Русин Богдан Павлович

Професор, доктор технічних наук, завідувач відділу "Методів та систем обробки, аналізу та ідентифікації зображень" Фізико-механічного інституту ім. Г.В. Карпенка НАН України.
Автор понад 220 наукових праць, в тому числі 10 монографій, 80 статей, 20 авторських свідоцтв і патентів.
Напрямки наукових досліджень пов'язані з обробкою та розпізнаванням зображень, 3-D реконструкцією, методами компресії, біометричною ідентифікацією , криптографічним захистом та цифровою обробкою сигналів.

Варецький Ярема Юрійович

Кандидат технічних наук, молодший науковий співробітник відділу "Методів та систем обробки, аналізу та ідентифікації зображень" Фізико-механічного інституту ім. Г.В. Карпенка НАН України.
Автор 20 наукових праць, в тому числі 7 статей, 1 патенту.
Напрямки наукових досліджень пов'язані з обробкою та розпізнаванням зображень, криптографічним захистом, біометричною ідентифікацією, 3-D реконструкцією та обчислювальною геометрією.