

Міністерство освіти і науки України
Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Спеціальність 125 «Кібербезпека»

Освітня програма «Безпека інформаційних та комунікаційних систем»

«Допущено до захисту»

Зав.кафедрою БІСТ

Сергій РАССОМАХІН



«02» 12 2022 р.

Пояснювальна записка

до кваліфікаційної роботи магістра

на тему: «Реалізація та аналіз алгоритму верифікації відбитків пальців на основі метрики циліндр-кодів»

оцінка « »

Голова ЕК

Доценко С.І. _____

Керівник проф. Рассомахін С.Г. 

Рецензент проф. Краснобаєв В.А. 

Виконавець : студент(ка) групи КБ-61

Панченко Н.В. 

Харків – 2022

РЕФЕРАТ

Кваліфікаційна робота магістра, 60 сторінок, кількість рисунків – 23, кількість використаних джерел – 22.

Робота складається зі вступу, 3 розділів, висновків, переліку використаних джерел.

Об'єкт дослідження: математична метрика системи верифікації відбитка пальця на основі циліндр-кодів.

Предмет досліджень: алгоритм математичної моделі системи верифікації відбитків пальців на основі циліндр-кодів.

Мета досліджень: проаналізувати математичну модель системи верифікації відбитків пальців на основі, дослідити та представити практичну реалізацію алгоритму циліндр-кодів.

Актуальність проведення дослідження полягає у поглибленому дослідженні алгоритму циліндр-кодів для його подальшого розширення та використання.

У першому розділі розглянуто біометричні дані людини, відбиток пальця та оглянуто способи ідентифікації людини за відбитком пальця.

У другому розділі було розглянуто та проаналізовано математичну метрику верифікації відбитків пальців на основі циліндр-кодів, її кроки реалізації та результати порівняння зі схожими алгоритмами.

У третьому розділі було описано практичну реалізацію частини алгоритму системи верифікації відбитків пальців на основі циліндр-кодів.

У ході даної роботи було розглянуто принципи біометричної верифікації людини, дані про будову відбитка пальця людини, досліджено принципи побудови алгоритму верифікації за допомогою циліндр-кодів, описано експериментальну оцінку алгоритму, представлено алгоритму у двійковому вигляді, а також описано його практичну реалізацію.

У результаті проведеної роботи було зроблено висновки щодо застосування та ефективності метрики системи верифікації відбитків пальців на основі циліндр-кодів, її перспективності у майбутньому, розширенні, рекомендації щодо подальшого удосконалення та застосування алгоритму.

Ключові слова: БІОМЕТРІЯ, АВТЕНТИФІКАЦІЯ, ВІДБИТОК ПАЛЬЦЯ, ЦИЛІНДР-КОД, МІНУЦІЯ, ЛОКАЛЬНІ ОЗНАКИ, БІТОВО-ОРІЄНТОВАНИЙ.

ABSTRACT

Qualifying work of a master, 60 pages, 23 figures, 23 references.

The work consist of the introduction, 3 sections, conclusion, list of references.

The object of the study is the mathematical metric of the fingerprint verification system based on cylinder codes.

The subject of the study is the algorithm of the mathematical model of the fingerprint verification system based on cylinder codes.

The purpose of the study: to analyze the mathematical system of the fingerprint verification model on the basis, to investigate and present the practical implementation of the cylinder code algorithm.

The relevance of the research is revealed in the in-depth study of the cylinder code algorithm for its further expansion and use.

The first chapter considers researches about the biometric data of a person, a fingerprint, and ways of identifying a person based on a fingerprint.

The second chapter considers an analysis of the the mathematical metric of fingerprint verification based on cylinder codes, it's implementation steps and the results of comparison with similar algorithms were considered.

The third chapter describes the practical implementation of a part of the algorithm of the fingerprint verification system based on cylinder codes.

In the course of this work, the principles of biometric verification of a person, data on the structure of a human fingerprint, the principles of building a verification algorithm using

cylinder codes were studied, the experimental evaluation of the algorithm was described, the algorithm was presented in binary form, and its practical implementation was also described.

As a result of the work, conclusions were drawn regarding the application and effectiveness of the metric of the fingerprint verification system based on cylinder codes, its prospects in the future, expansion, recommendations for further improvement and application of the algorithm.

Keywords: BIOMETRICS, AUTHENTICATION, FINGERPRINT, CYLINDER CODE, MINUTIA, LOCAL SIGNS, BIT-ORIENTED.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ.....	8
ВСТУП.....	9
1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО БІОМЕТРИЧНУ ВЕРИФІКАЦІЮ	11
1.1 Принципи верифікації за біометричними даними людини	11
1.2 Дані про відбиток пальця людини.....	14
1.3 Інформаційні ознаки відбитків пальців	22
1.4 Огляд біометричної ідентифікація за відбитком пальця.....	25
2 АЛГОРИТМ ВЕРИФІКАЦІЇ ВІДБИТКІВ ПАЛЬЦІВ ЦИЛІНДР-КОДІВ.....	30
2.1 Дослідження принципів побудови системи циліндр-кодів	30
2.2 Опис етапів алгоритму циліндр-кодів.....	33
2.3 Розгляд локальних структур алгоритму	37
2.3.1 Побудова циліндра конкретної мінущі.....	37
2.3.2 Створення набору циліндрів	42
2.3.3 Визначення схожості між двома циліндрами.....	44
2.3.4 Двійкова (bit-based) реалізація.....	47
2.4 Глобальна оцінка результату	48
2.4.1 Сортування за локальною подібністю	49
2.4.2 Дослідження локальної подібності	49
2.5 Експериментальна оцінка алгоритму	52
3 ОПИС ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ АЛГОРИТМУ	56

ВИСНОВКИ.....	61
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	63

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

CDEFFS	–	Committee to Define an Extended Fingerprint Feature Set.
DPI	–	Dots per inch.
EER	–	Equal Error Rate.
FAR	–	False acceptance ratio.
FNMR	–	False non-match rate.
FRR	–	False Reject Rate.
FTIR	–	Fourier-transform infrared spectroscopy.
FVC	–	Fingerprint Verification Competition.
ID	–	Identifier.
IEC	–	International Electrotechnical Commission.
IEEE	–	Institute of Electrical and Electronics Engineers.
ISO	–	International Organization for Standardization.
MCC	–	Minutia Cylinder-Code.
MC	–	Множина сусідства.
ЦК	–	Циліндр-коди.
2D	–	Two-dimensional.
3D	–	Three-dimensional.

ВСТУП

За довгі роки стрімкого розвитку інформаційних систем біометричної ідентифікації особи, що контролюють доступ користувачів до конфіденційної інформації, завдання безпечної біометричної автентифікації є ключовим для безлічі систем захисту. У якості біометричного ідентифікатора використовуються радужна оболонка ока людини, голос, почерк, відбитки пальців. Біометричні дані в хмарних сховищах, локальних пристроях, базах даних та інформаційних системах дедалі поширюються, інфраструктура розвивається, щоб забезпечити максимально якісні технології для користувача. Окрім цього, важливим є захист передачі біометричних даних від підробок, їх зберігання, тому повинні забезпечуватися розробка та створення біометричних систем автентифікації, шифрування та цифрового підпису в інформаційних системах.

Так як створюються єдині міжнародні стандарти, то використання пристроїв із біометричною автентифікацією систем поширюється, наприклад у службах паспортного контролю, ID-картках, смартфонах та інших засобах. У деяких країнах використання таких методів у системах соціальних виплат значно зменшило ризики несанкціонованих виплат, таким чином попередили фінансові збитки держав. Щодо українського ринку, системи біометричної ідентифікації за відбитками пальців є зручними у користуванні, і контролюють доступ до комп'ютерних мереж, інформаційних, банківських систем, і є досить ефективними.

Метою даної роботи є аналіз методу верифікації відбитків пальців на основі циліндр-кодів, дослідження методів і засобів для біометричної автентифікації, аналіз переваг і недоліків методу, опис практичної реалізації фрагментів алгоритму верифікації на основі циліндр-кодів і її аналіз. Повноцінна програмна реалізація у подальшому може використовуватися для того, щоб удосконалити систему

біометричної верифікації та захищеності даних у галузі інформаційної безпеки. Подальші напрямки розвитку і алгоритму пов'язані із розширенням його програмних частин та удосконаленням відповідно до міжнародних стандартів захисту інформації, наприклад, ISO 27001. Повинно бути проведено повний аналіз та оцінка ризиків його роботи, перспектив, розширень.

1 ТЕОРЕТИЧНІ ВІДОМОСТІ ПРО БІОМЕТРИЧНУ ВЕРИФІКАЦІЮ

1.1 Принципи верифікації за біометричними даними людини

Автентифікація – це процедура доведення того факту, що користувач інформації в даній системі дійсно належить саме тому ідентифікатору, який йому було пред'явлено.

Якщо розглядати термін з точки зору інформаційної безпеки, то автентифікація є частиною процедури, коли відбувається надання доступу до роботи в інформаційній системі, яка відбувається після ідентифікації користувача системи, але перед авторизацією.

Ідентифікація – процес розпізнавання користувача в системі за допомогою визначеного ідентифікатора чи іншої інформації про нього, порівняння всіх вхідних параметрів із тими, що записані у системи чи базі даних зареєстрованих користувачів.

Для того, щоб відбулася біометрична автентифікація алгоритму суб'єкта, він має дослідити одну чи декілька поведінкових або фізіологічних характеристик. До поведінкових відносяться підпис суб'єкта, клавіатурний почерк, голос, до фізіологічних – відбиток пальця, райдужна оболонка ока, сітківка ока, риси обличчя тощо. Біометричний метод автентифікації зазвичай використовують у критично важливих установках або системах, що мають спеціальне обладнання.

Як працює алгоритм автентифікації:

- 1) За допомогою біометричного зчитувача відбувається зчитування даних користувача;

- 2) Дані, що було зчитано, відправляються на сервер для подальшого порівняння з еталонними даними, які збережені в базі даних системи;

3) Якщо дані збігаються з еталонними, автентифікація вважається успішною, і доступ до системи буде надано, при умові, якщо дані збігаються з еталонними; у протилежному випадку – система повертається до кроку 1.

На сьогоднішній день, у наслідок стрімкого розвитку інформаційних технологій, вигадано дуже багато систем біометричної ідентифікації, що мають різні способи роботи та свою стійкість до злому. Ці біометричні системи у свою чергу використовують дані різних типів, до них відносяться: відбитки пальців, геометрія руки, особи, райдужна оболонка ока, сітківка ока, голос, почерк, термограма особи, геометрична карта судин долоні, мова, голос. Біометричні системи можуть використовувати як один різновид біометричних даних людини, так і складатися з декількох їх типів одночасно. У залежності від методу, на якому базується побудова функціонування системи, вона має свої певні переваги і недоліки. Для того, щоб проаналізувати біометричну систему, потрібно ознайомитися з їх характеристиками, до яких відносяться швидкість роботи алгоритму, обчислень та процесу ідентифікації, зручність даної процедури для користувача, вірогідність виникнення помилок різного роду, громіздкість обчислень, коштовність обладнання, що необхідне.

Впродовж останніх років біометричні методи, що ґрунтуються на розпізнаванні відбитків пальців людини, стрімко набирають популярності та залишаються найперспективнішими серед інших біометричних методів. На думку дослідників, даний метод автентифікації є номером один на корпоративному ринку, і в найближчому майбутньому за лідерство технології зможе поборотися тільки метод, оснований на розпізнаванні райдужної оболонки ока.

Частіше за все протоколи автентифікації можуть бути схильні до наступних видів атак:

- а) Видавання себе за іншу особу – коли одна особа, схожа на правдиву, видає себе за неї;

- b) Атака відтворення або повторне відтворення – попередні облікові дані передаються повторно будь-яким користувачем;
- c) Розмежування атак (Interleaving attack) – зміна даних, які проходять через атаку;
- d) Рефлексивна атака – різновид можливої атаки, при якій зловмисник повертає захоплену інформацію у межах цього сенсу;
- e) Примусова затримка – атака, при якій зловмисник запам'ятовує певну інформацію та пересилає її через певний проміжок часу;
- f) Виділена текстова атака або атака виділенням тексту – перехоплення трафіку зловмисником та спроби отримати інформація з клавіатури.

Під терміном протоколу автентифікації слід розуміти категорію криптографічних протоколів, що забезпечують надійну автентифікацію особи.

У інформаційно-комунікаційних системах існують декілька технологій автентифікації та ідентифікації користувачів, які, в свою чергу, мають свої переваги та недоліки.

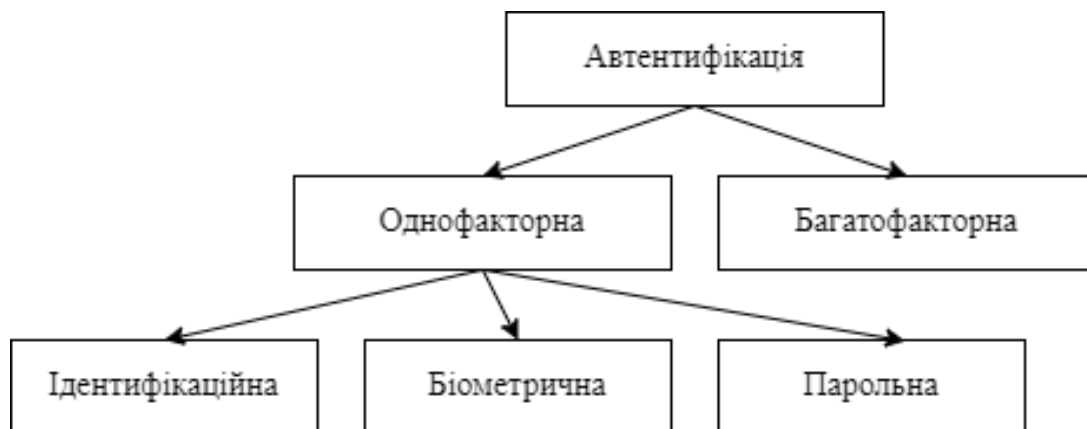


Рисунок 1.1 - Схема технологій автентифікації

Дані технології використовуються в різного виду комп'ютерних системах. Але, зазвичай, чітко визначеного випадку, при якому потрібно використовувати той чи

інший вид, не існує. Через це, як розробники програмного забезпечення, так і їх користувачі, самі обирають метод автентифікації, що буде використовуватися у інформаційно-комунікаційних системах.

1.2 Дані про відбиток пальця людини

Відбиток пальця – це слід, який залишає шкіра, а саме – папілярні лінії або візерунки пальця людини при їх контакті з поверхнею. Їх легко відобразити на рівних поверхнях (скло, метал, шліфований камінь тощо), можна зробити, використовуючи чорнила або інші матеріали для чіткого перенесення папілярних ліній.

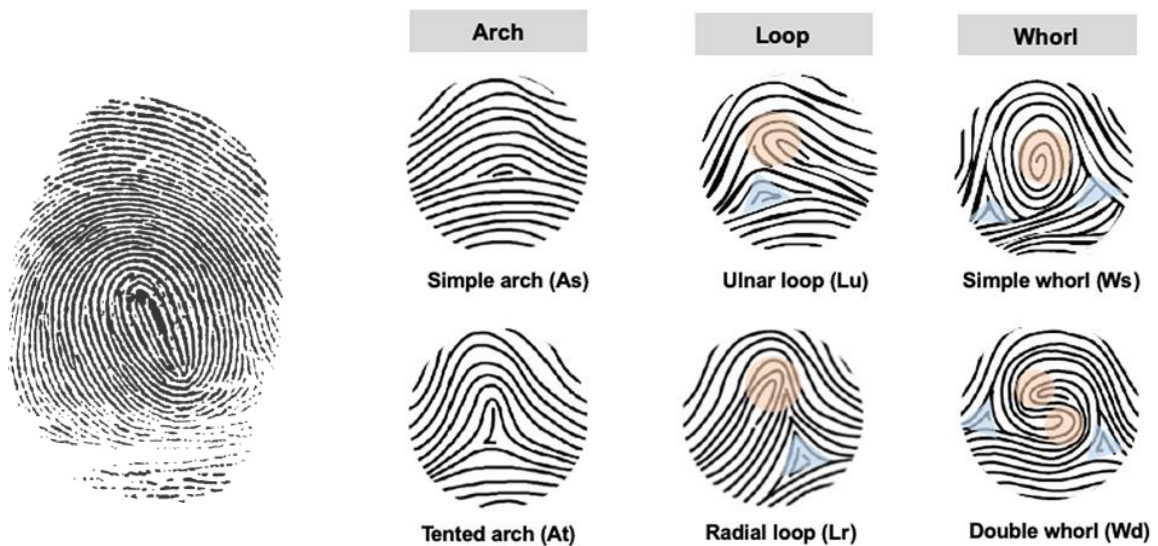


Рисунок 1.2 – Типи візерунків відбитка [1]

Дактилоскопія – розділ у криміналістиці, який займається ідентифікацією папілярних ліній відбитків пальців людини, заснований на унікальності візерунка шкіри. Ідею про незмінність папілярних ліній поверхонь долонь людини вперше висунув англієць Вільям Джеймс Гершель у 1877 році, який довгий час досліджував дане питання. Даний метод набув широкого використання у цілому світі.

Існує декілька різновидів відбитків пальців:

1) Екземплярні. Це відбитки пальців, які були зібрані у людини добровільно для того, щоб дозволити вхід у систему, або недобровільно унаслідок підозри у скоєнні злочину. У такому випадку робиться чіткий збір відбитків кожного пальця унаслідок його відтиску від одного краю до іншого, та прості відтиски кожного окремого з десяти пальців. Такого роду відбитки збираються за допомогою електронних сканерів, чорнил та аркушів паперу, або інших засобів;

2) Латентні (приховані) відтиски пальців означають у сучасному застосуванні судової експертизи так звані невидимі відбитки, тобто випадкові відбитки папілярних узорів шкіри на поверхні. На момент утворення вони можуть бути видимі або невидимі. Дані відбитки можуть бути зроблені на основі поту, мастила, фарби, крові, бруду та інших способів. Такого роду невидимі відбитки можна візуалізувати за допомогою різного характеру методик обробки, це можуть бути електронні, хімічні або фізичні методики. Латентні відбитки можуть відображати не повну частину області папілярних ліній відбитка пальця, і можуть бути не чіткими, розтертими або змазаними, зсунутими чи викривленими, і можуть накладатися на інші сліди відбитка пальця. Через такі недоліки складним буде процес здійснення їх порівняння, що призведе до певної кількості помилок, адже у випадку контрольованого збору відбитки є значно чіткими, містять у собі більше змісту про їх справжню структуру, деталі візерунків ліній та деформацій (вигинів) пальця, його форму;

3) Патентні (явні). Патентними відбитками пальця називають витиски папілярних ліній у наслідок перенесення чужорідного характеру речовини з пальця на поверхню, але вони є очевидними і їх видно неозброєним оком. Такі відбитки зазвичай не обробляють для отримання більш чіткого зображення, як у випадку із латентними відбитками. Також залишаються на поверхні такими речовинами як бруд, фарба тощо;

4) Пластичні;

5) Електронний запис;

6) Відбитки стоп.

Отримання зображення відбитка пальця є дуже важливим етапом в автоматизованій системі автентифікації за відбитком пальця, оскільки він визначає остаточну якість зображення відбитка, що має значний вплив на загальну працездатність системи. На ринку існують різні види зчитувачів відбитків пальців, але основна ідея кожного з них полягає у вимірюванні фізичної різниці між хребтами та долинами.

Усі існуючі методи можна об'єднати у дві групи: твердотілі сканери відбитків пальців та оптичні сканери. Процедура захоплення відбитка пальця сенсором складається з прокручування або дотику пальцем до чутливої області, і в залежності від фізичного принципу використання (оптичний, ультразвуковий, ємнісний або тепловий) записується різниця. Еластична шкіра деформується, коли палець стосується поверхні або прокочується нею. Величина та напрямок прикладеного користувачем тиску, стан шкіри та неправильна проекція тривимірного об'єкта(пальця) на двовірну площину вносять спотворення, шум та невідповідність у результуюче зображення відбитка пальця. Ці проблеми призводять до непослідовних, нерівномірних опуклостей на зображенні. Таким чином, під час отримання кожного зображення результат завантаження відрізняється та не може контролюватись. Щоразу, коли палець поміщається на сенсорну пластину, уявлення однієї й тієї ж відбитка змінюється, що підвищує складність зіставлення відбитків пальців і знижує продуктивність системи, що обмежує широке використання цієї біометричної технології.

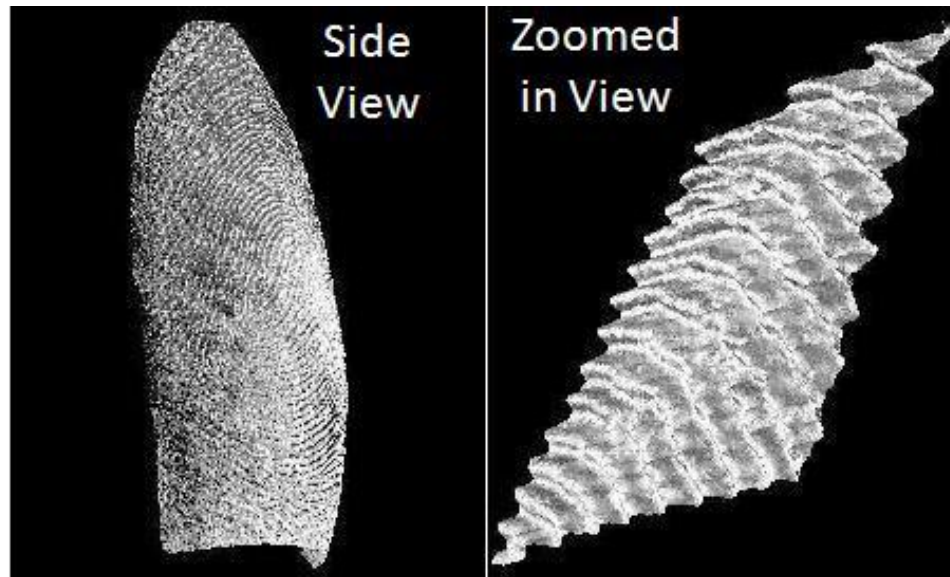


Рисунок 1.3 – 3D відбиток пальця [2]

Для того, щоб позбутися цих проблем, з 2010 року розробляються 3D-сканери відбитків пальців, які є безконтактними. Такі сканери мають в основі використання цифровий підхід до аналогової обробки натискання або повороту пальця, у процесі збору інформації. Можна відобразити відбиток пальця з роздільною здатністю, достатньою для запису всіх необхідних деталей, якщо змодельовати відстань між сусідніми точками.



Рисунок 1.4 – Сканери відбитків пальців [3] [4]

Існують різні методи зняття відбитків пальців, більша частина інструментів і електронних технологій для цього розробляється. Найпоширенішими з них є оптичний, ємнісний, радіо, мікроелектромеханічний та температурний методи.

Оптичний метод. Даний метод оснований на технологіях, які функціонують як цифрова камера. Відбиток паля людини повинен розміщуватися на поверхні зі скла, при цьому вона повинна мати особливе освітлення.

Усе, що необхідно для даного методу, – це оптична лінза, яка може знаходитися близько до предмету зйомки. Картинка, яка повинна бути отримана, створюється за допомогою сучасної матриці, при цьому використовуються інші технології. Після цього з цих всіх даних утворюється чорно-біле зображення із відтінками сірого кольору (частіше за все 2-16 переглядів є задовільною кількістю). Одним з недоліків даного способу є те, що відбитки пальців можуть залишатися на скляній поверхні, де раніше до цього був поміщений палець, та привертати увагу, що може надати змогу зловмисникові незаконного доступу до даних. Другим недоліком можна вважати складність розпізнавання справжнього відбитка пальця за якісно підготовленим підробленим відбитком.

Існує декілька різновидів оптичних відбитків пальців, опис яких наведено далі. Метод оптичного відбивання. Основою даного методу є фізичний ефект, що оснований на порушенні повного внутрішнього відбиття. При попаданні світла на границю двох середовищ, світлова енергія розподіляється на дві окремі частини, при цьому перша віддзеркалюється від границі, друга потрапляє через границю до іншого середовища. На те, яким у результаті буде співвідношення енергії, що відбилася, має вплив кут, під яким падає світло. Світлова енергія, що буде відбиватися від інтерфейсу, повинна мати певне значення цього самого кута. Дане явище має назву - тотальне внутрішнє відображення, і даний метод часто застосовується в оптичних сканерах FTIR.

У випадку, якщо відбувається контакт між поверхнею пальця із більшою щільністю і об'єктом з меншою щільністю, то частина світла буде потрапляти скрізь дану границю у точці повного внутрішнього відбиття. Отже, від границі відбувається відбиття тільки тих променів світла, що потрапили до певних точок повного

внутрішнього відбиття, по відношенню до яких не використовувався папілярний малюнок пальця.

Для отримання зображення відбитка пальця застосовується матриця спеціального призначення.

Недоліки способу:

- 1) Вірогідність помилкового підкріплення у випадку помилкового всмоктування;
- 2) Має чутливість до бруду.

Зчитувачі, які застосовуються в технології оптичної передачі даних, можна представити у вигляді волоконно-оптичного масиву, складовими якого є всі вихідні хвилеводи, що мають з'єднання до фотодатчиків.

Усі датчики є чутливими, через що є змога виявити залишкове світло, яке проходить через палець користувача у точці його контакту з поверхнею матриці. Малюнок повного відбитка формується згідно з даними, що було зчитано з кожного окремого фотодатчика.

Даний спосіб має безліч інших переваг, а саме:

- 1) Велика надійність при зчитуванні;
- 2) Стійкість до підміни даних.

Суттєвим недоліком даного методу є його складна реалізація.

При роботі оптичного безконтактного методу застосовуються оптичні контактні сканери, що не потребують повного запису на поверхню камери приладу. Палець поміщують у спеціальні відсіки, невелика кількість світлодіодів направляють світло на його поверхню під різними кутами, при цьому в центрі приладу знаходиться лінза, завдяки якій відбувається збір даних та їх подальша передача на спеціальну камеру, яка оцифровує інформацію.

Ємнісний метод. Це метод, що заснований на тому, що поверхня відбитка пальця людини опиняється на пристрої, що складається з матриці елементів, що мають схильність до електричного заряджання. Через те, що опуклості та поглиблення відбитка пальця є з різною електропровідністю, змінним є вміст елементів матриці. Завдяки цьому процесу є змога визначити точки опуклостей і поглиблень та скласти шаблон цифрового друку. Даний метод залишається одним із найбільш популярних, е дивлячись на те, що дана технологія розпізнавання відбитків пальців має деякі недоліки, а саме: чутливість пристрою до електростатичних розрядів та різного характеру блукаючих електричних полів.

Радіо метод. Розглянемо ситуацію, коли радіохвилі з низькою щільністю розміщуються на поверхні пальця. У цьому випадку є змога дізнатися місце розміщення опуклостей і поглиблень шкіри, використовуючи при цьому прилад з правильним налаштуванням елементів антени. Це можливо при умові, щоб поверхня відбитка пальця буде торкатися датчика, певна ділянка якого випромінює радіохвилі. Даний метод також базується на фізіологічних характеристиках шкіри, і через це існує дуже невелика вірогідність отримати несанкціонований доступ за допомогою несправжнього відбитка пальця. До недоліків даної технології можна віднести те, необхідною умовою є обережність при піднесенні пальця до приладу, випромінююча частина якого з часом може підвищувати температуру, що впливає на комфорт його використання.

Нажимний метод. Для того, щоб отримати певну інформацію про відбитки пальців, можна застосовувати пристрої із п'єзоелектричною матрицею, яка є чутливою до напруги. Дані технології мають і недоліки, до яких можна віднести низьку чутливість батарейок, складність процесу знаходження відмінностей між відбитком пальця користувача та підробленого, а також ймовірність пошкодження у наслідок надмірного застосування сили тощо. Однак слід зазначити, що деякі

виробники біометричних пристроїв займаються виготовленням пристроїв, що засновані на даній технології.

Мікроелектромеханічний метод. Застосування технологій даного типу на даний момент розвиваються та досліджуються, при цьому інтегруються для аналізу їх ефективності. Даний метод працює за тим самим принципом, фіксуючи положення подушечок пальців і вдавнення за допомогою спеціального мікроелектромеханічного масиву датчиків.

Температурний метод. Даний спосіб базується на тому, чи є змога у піроелектричних елементів виробляти напругу, змінюючи температуру. Таке явище застосовують під час роботи інфрачервоних сканерів. Спеціально для цього призначений датчик, що має контакт з поверхнею пальця, функціонує відповідно до даного способу приладу, через це є можливість отримувати дані температури при контакті елементів приладу з опуклостями і западинами на відбитку пальця.

Застосування цієї технології має ряд переваг, одні з яких це відсутність впливу на стабільну роботу приладу електростатичного розряду та комфортне використання, так як подушечка пальця не чутлива до випромінювання. Окрім цього, за допомогою приладів, робота яких базується на даному методі, є можливість отримувати достовірну інформацію з подушечки пальця, не залежачи від температури навколишнього середовища та отримати дані про помилковий палець, більшість з методів не мають такої можливості.

Єдиним недоліком даного способу є те, що вихідний цифровий відбиток пальця користувача не є постійним, має бути чітка його фіксація на поверхні. Це відбувається унаслідок того, що під час перебування поверхні відбитка пальця на пристрої перепад температур утворює значну кількість напруги, яка поступово зменшується за дуже малий проміжок часу (менше десятої секунди), тому що температура пальця та сканера поступово врівноважились.

1.3 Інформаційні ознаки відбитків пальців

Кожен відбиток пальця окремої людини є унікальним і має дві характерні групи: глобальні характеристики і локальні. Глобальні сигнали – ті, які можна побачити неозброєним оком і без спеціального обладнання:

- 1) Візерунок відбитка пальця;
- 2) Область зображення – найбільша частина, що містить усю інформацію;
- 3) Ядро – точка і в центрі відбитка або певний його фрагмент;
- 4) Точка дельти, що є початковою точкою і може бути місцем злиття або розділу папілярних ліній, а також може бути набагато меншою за розміром;
- 5) Тип лінії – визначається двома великими лініями що йдуть спочатку паралельно, а потім – по краях усієї області зображення;
- 6) Лічильник ліній – визначає кількість ліній, що існують в усій області зображення та між ядром і точкою дельти.

До другої групи функцій відносяться локальні функції, що називаються мінуціями (minutiae) – це унікальні параметри відбитка, які характеризують точки, де змінюється форма лінії (наприклад, закінчення, роздвоєння, злам тощо). Вони включають розташування точок, які описані даними лініями та об'єктами. Один відбиток пальця людини складається приблизно з 70 мінуцій (мікровиступів).

Через те, щоб полегшити опис і сам процес автентифікації при дослідженні характеристик папілярні узорів відбитків пальців поділяються на загальні та окремі (деталі), що у більш масштабному вигляді розміщуються на нігтьових фалангах пальців. Візерунки, що розміщуються на середніх та основних фалангах пальців, а також на долонях, містять меншу кількість інформації. За загальними спільними характеристиками узорів можна розділити на такі види: дугові, петлясті й завиткові.

Петлясті узорі, в свою чергу, можуть бути як ульнарними (os ulnaris), так і й радіальними (os radialis), назви яких мають походження від латинських назв кісток передпліччя.

У свою чергу дуговий тип візерунка складається з папілярних ліній, які починаються з одної сторони подушечки пальця, та закінчується на іншій, із різною силою згинаються посередині лінії у виді шатра або у вигляді дуже пологої хвилі. Узорі даного типу можна зустріти із вірогідністю, що складає близько 5% випадків від загальної їх кількості.

Якщо розглядати петлястий тип узорів папілярні лінії, то вони, створюючи центральну область, починаються з одного краю відбитку до його центру, після чого йде різкий поворот, і лінії знов приймають напрямок назад, повертаючись до тої ж самої початкової границі пальця. Такі лінії при цьому утворюють так звану петлю, через що отримали свою назву. Місце, де закінчується петля узору, що становить його відкриту ділянку та обернена до границі пальця, має назву «ніжок» (або гілок) петлі, а її область, що має закруглену форму на її верхівці, мають назву - голівки. Навколо петлі розміщуються три направлені лінії, що під нею формують фігуру, яка має схожу форму на грецьку літеру "дельта" (δ). Об'єкти такого вигляду у дактилоскопії мають таку саму назву - дельта. У випадку, якщо «низівки» петлі направлені у сторону великого пальця, то дана петля має назву «радіальна», якщо напрямок - у сторону мізинця, таку називають ульнарною. Якщо розглядати статистику існування того чи іншого виду петель узорів відбитків пальців, то радіальні зустрічаються приблизно у 5 відсотках випадках по відношенню до усіх візерунків, що існують на пальцях, а ульнарні – близько 60 відсотків.

Завитковий узор в свою чергу є у вигляді кількості концентричних овалів, кіл, спіралей, клубків або петель, скраю них, близько до границь відбитка пальця,

розміщуються два узору типу дельта. З дуже малою ймовірністю можна зустріти завиткові типи узорів, що мають три дельти, ще рідше, що мають чотири.

Загальні характеристики візерунків дають змогу розділяти відбитки пальців за типами, і у випадках їх відмінностей зробити висновок про відсутність схожості чи збігів. Для того, щоб отримати позитивний висновок щодо індивідуальну схожість, не рахуючи факт збігу, загальних характеристик, необхідним фактом, що повинен бути, є збіг визначеної якісного та кількісного комплексу окремих характеристик, одними з яких є початок та кінець ліній, їх поєднання та розмежування, містки, острівці, гачки, вічка, пунктири, повороти ліній тощо.

Сліди відбитків рук створюються унаслідок факту утворення поту з потових залоз, що розміщуються на поверхні долонь людини, крім цього важливу роль грає існування на долоні жирів та її перенесення на інші поверхні, частини тіла, гаджети, що завжди мають тонкий шар залишків таких потових виділень або жиру.

При пошуку слідів рук і відбитків пальців не слід забувати про правило огляду поверхонь предметів, з якими є ймовірність, що з могла мати контакт особа. Видимі сліди рук дуже легко розпізнаються при огляді. Якщо ж розглядати сліди, що важко помітити, та невидимі сліди, то для того, щоб їх виявити, потрібно використовувати певні спеціальні техніки і способи. Сліди, що важко помітити, доволі легко можна розпізнати при огляді місця їх ймовірного знаходження під кутом, що є косо спрямованим по відношенню проти ока спостерігача, а також доброму освітленні. Дані сліди потрібні бути видимими й контрастними, для чого вони повинні бути оброблені спеціально для цього призначеними порошками, які прилипають до потожирового шару відбитка, за допомогою магнітної або із коротким ворсом щітки.

Слід зазначити, що у той самий час на темних поверхнях застосовуються світлі порошки (наприклад, окис цинку, свинцю, або ж аргенторат, він же порошок

алюмінію), а на світлих - темні (окис міді, графіт, магнітні порошки або сажу). Далі потрібно зробити копії слідів, що обуло виявлено при застосуванні порошків, після чого помістити відбитки на липку світлу чи темну дактилоскопічну плівку. Якщо розглядати низку пластичних матеріалів, на них можуть залишатись об'ємні відбитки (волога штукатурка чи пластилін). У такому випадку роблять фотознімок за правилами масштабної фотографії, далі виготовляються зліпки за допомогою медичного гіпсу, або ж металу, що легко плавиться, спеціальних полімерних речовин.

1.4 Огляд біометричної ідентифікація за відбитком пальця

Загалом, біометричні технології розпізнаванні відбитків пальців людини можна розділити на дві групи: ідентифікації та зіставлення. Перша група використовує у своїй роботі всі десять відбитків пальців (широко використовується у судовій системі). У методах, що відносяться до другої групи, найчастіше зіставляються відбитки одного пальця, іноді з кількома параметрами пальців. Як правило, існує три типи технологій сканування відбитків, а саме: що базується на основі мікрочіпів, оптична та ультразвукова. Також існують методи електронних засобів ідентифікації відбитків пальців. До найпоширеніших з них відносяться оптичний, температурний, радіо-тисковий та мікроелектромеханічний.

Станом на сьогодні, способи біометричної ідентифікації у різних системах контролю та управління доступом у світовому масштабі виглядає таким чином:

- 1) Відбиток пальця руки — 34 %;
- 2) Райдужна оболонка ока — 34 %;
- 3) Геометрія руки — 25 %;
- 4) Розпізнання обличчя — 15 %;
- 5) Верифікація голосу — 11 %;
- 6) Верифікація підпису — 3 %.

Існує основний міжнародний стандарт, який регулює криптографічні протоколи автентифікації та ідентифікації, а саме Міжнародна організація зі стандартизації та Міжнародна електротехнічна комісія ISO / IEC 9798, які складаються з наступних частин:

- 1) ISO / IEC 9798-1 - "Загальна модель";
- 2) ISO / IEC 9798-2 - "Механізми, що використовують симетричні алгоритми шифрування";
- 3) ISO / IEC 9798-3 - "Автентифікація суб'єкта з використанням алгоритму відкритих ключів";
- 4) ISO / IEC 9798-4 - "Механізми, що використовують функцію криптографічного контролю";
- 5) ISO / IEC 9798-5 - Механізми, що використовують технологію нульових знань.

У даних документах заявник і верифікатор мають секретний симетричний ключ або парний вибіркового ключ зв'язку, для отримання якого використовується надійний сервер.

Характеристика користувача даним способом є ефективним, оскільки загальні риси обличчя можуть виявитися нечіткими. Однак, через те, що дані від різних людей завжди унікальні, для поширення бази даних на першому рівні зазвичай використовується глобальний сигнал. Мікроточки використовуються на останньому рівні розпізнавання.

Як правило, в даний час використовуються стандарти ANSI (Американський національний інститут стандартів) та ФБР США. Прийнято зберігати декілька зображень одночасно у базі шаблонів для того, щоб підвищити ефективність ідентифікації. Крім цього, допускаються дрібні деталі та зміни різного характеру. У

такому разі співвідношення сторін зображень залишається без змін, так як вони друкуються на одному й тому самому пристрої.

Для якісного розпізнавання відбитка пальця людини при біометричній ідентифікації особи дуже важливим є якість зображення та відсутність шуму. Це можуть бути змащення відбитку при скануванні, область пальця, де не може не бути яскраво виражено папілярних ліній, з яких немає змоги отримати інформацію, яка характеризує відбиток. Причинами цього можуть бути занадто жирна або суха шкіра рук, великі пори, рух пальцем при знятті відбитка.



Рисунок 1.6 – Приклади варіантів сканування відбитків пальців [5]

Головні ключові характеристики ідентифікації відбитків пальців, завдяки яким цей метод став дуже популярним на ринку підприємств, це практичність, простота використання і високий рівень безпеки. Відбитки пальців людини є деталізованими, мають унікальність, важкість у обігу та практичність і надійність у житті

користувачів, що робить їх придатними для того, щоб слугувати маркерами розрізняння обличчя протягом усього життя. Усього є два головних способи, для того, щоб перевірити відбиток пальців людини: у відповідності до характерних точок та рельєфу усієї площі пальців. Сенса першого з них полягає в тому, що спеціальним зчитувачем стираються лише певні деталі, що відносяться саме до даного відбитка пальця, і далі іде підрахунок їх відношення щодо розташування на пальцях. Під час другого способу видаляється уся поверхня пальця та робиться аналіз усієї площі відбитка пальця. На сьогоднішній день біометричними технологіями дуже часто комбінуються обидва методи одночасно. Такий спосіб дає змогу обійти виникнення недоліків, які можуть з'явитися унаслідок раніше перерахованих алгоритмів, та підвищити точність кінцевого розпізнавання. Зняття відбитка пальця за допомогою оптичного сканера не витрачає багато часу. Зображення відбитка пальців створюється за допомогою невеликих розмірів CCD-камери, що існує як окремий технічний пристрій, а також її легко вбудувати в клавіатуру. Далі використовуючи спеціально підібрані алгоритми, відбувається кодування відбитка пальця і перетворення на цифрове зображення, шляхом схематичного переносу характерних ділянок відбитка, що є унікальними перетинами ліній і викривлень відбитка. Після відбувається кодування схематичного зображення точок та відправлення у базу даних біометричної системи верифікації. Такого роду цифрові зображення можуть мати у собі до сотні мікроточок. З цього можна зробити висновок, що пристрій, за допомогою алгоритма, зберігає не зображення, а саме унікальні мікротипи з місць розташування, через що конфіденційні дані ідентифікаційних параметрів користувачів даної технології будуть у безпеці, так як зображення відбитків пальців неможливо відтворити, маючи тільки такі шаблони. Великою перевагою ультразвукового сканування є те, що за допомогою даного методу можна видалити необхідні дані, не спотворюючи забрудненнями на поверхні пальця. Окрім цього, є можливість навіть дати характеристику ультразвуку відбитків пальців, використовуючи гумові рукавички. Окрім цього, варто зазначити,

що в даний час технології біометричної ідентифікації мають захист від підробки відбитків пальців так само, як і поверхня пальців, що має подряпини або пошкодження, так як мікросхеми пристроїв мають змогу робити аналіз фізичних характеристик шкіри пальця. На сьогоднішній день більше ніж п'ятдесят виробників по всьому світу виготовляють такого роду пристрої.

Порівнюючи з іншими вже існуючими методами верифікації, використання методу розпізнавання за допомогою відбитків пальців є одним з найбільш зручних біометричних методів. У процесі перевірки справжності елементів можливість виникнення помилки набагато менша, ніж під час інших методів біометричної верифікації. Але варто зазначити, що на точність відображення відбитків пальців і правильного аналізу системою мають вплив саме ділянки пальця, а також положення пальця відносно до скануючого пристрою. Те, як у кінцевому результаті впливають дані характеристики відбитків пальців, має залежність від вартості системи та різновиду перевірки відтисків пальців. Наприклад, бруд на поверхні ускладнює ідентифікацію кожного з мікроблоків. Також важливим є положення пальців при скануванні. Засоби сканування відбитків пальців зазвичай не займають багато місця і можуть бути вбудовані в комп'ютерну мишу або комп'ютерну клавіатуру.

Процес автентифікації за відбитками пальців є можливим у тому випадку, коли є відсутнім повний відбиток пальця на шкірі та навіть невелика кількість незначних обривків папілярних ліній – при користуванні піроскопом - визначення унікальних характеристик побудови вихідних протоків потових залоз у папілярних лініях і побудови границь цих папілярних візерунків, місць їх початку і закінчення. Для процесу визначення також можна застосовувати і відбитки окремих зон долоні людини, що називається пальмоскопією.

2 АЛГОРИТМ ВЕРИФІКАЦІЇ ВІДБИТКІВ ПАЛЬЦІВ ЦИЛІНДР-КОДІВ

2.1 Дослідження принципів побудови системи циліндр-кодів

Даний алгоритм, що розглядається у цій магістерській роботі, було представлено Раффаелем Каппеллі, Маттео Феррара та Девідом Мальтоні, членами IEEE, у грудні 2010 року. Ці науковці дослідили алгоритм МСС, що є представленням верифікації відбитків пальців на основі 3D структур даних, а саме – циліндрів, що у свою чергу побудовані з дрібних об'єктів: відстаней і кутів мінуцій. Дані циліндри можуть бути створені за допомогою підмножини обов'язкових функцій, що визначені такими міжнародними стандартами, як ISO/IEC 19794-2 (2005). В основі алгоритму існує той факт, що завдяки саме незмінності побудованого циліндра, його фіксованої довжини та бітово-орієнтованого кодування, деякі прості, але дуже ефективні метрики можуть бути гарним способом для обчислення локальних подібностей та їх консолідацій у глобальному розгляді.

Завдяки значній кількості експериментів над базами даних FVC2 можна зробити висновок про перевагу МСС по відношенню до інших трьох достатньо відомих алгоритмів, а також описати можливість результатів дуже ефективної (і сумісної) реалізації верифікації відбитків пальців для неважких побудов.

Розпізнавання особистостей за даними відбитків пальців – це проблема, яка вивчається більше 50 років різними науковцями. На даний момент є доступними велика кількість ефективних способів, але, все ж таки, проблема вирішення розробки точних алгоритмів верифікація відбитків пальців не є вирішеною у повній мірі та залишається актуальною.

Слід взяти до уваги, що більшість з алгоритмів порівняння відбитків пальців, що існують, побудовані на таких даних, як розгалуження (або біфуркація), або

закінчення лінії. В алгоритмах схожого типу схожі між собою частини відбитків пальців перетворювались у 2D точковий шаблон для подальших обчислень, для того щоб шляхом глобального вирівнювання, задля збігу деталей у просторі, вирішити поставлену у задачі проблему. На жаль, більшість глобальних алгоритмів, що базуються на порівнянні деталей відбитків пальців, не є повністю надійними по відношенню до нелінійного спотворення відбитків пальців, а також вимагають громіздких обчислень.

За останній час дані недоліки були усунені шляхом представлення алгоритмів зіставлення локальних структур відбитка пальця. Локальні структури характеризуються атрибутами, що є інваріантні по відношенню до глобальних перетворень (поворот тощо), через що за їх допомогою можливе порівняння, не роблячи глобального вирівнювання структур. Через виникнення збігу локальних структур відбитків пальців характерне виникнення зменшення обсягу інформації, яка доступна для розрізнення відбитків пальців. Слід зазначити, що, все ж таки, переваги обох відповідностей структур, локальних та глобальних, є можливість зберегти шляхом впровадження гібридні стратегії, основною ідеєю якої є процес локального зіставлення структур відбитка пальця, а після цього - етапу консолідації. Варіант зіставлення за даними локальних структур дає змогу швидко та більш точно визначати деталі візерунків відбитків пальців, що збігаються саме локально. Процес консолідації спрямований на перевірку того, чи успішно зберігаються локальні збіги структур у глобальних, а також міру їх збігу. У процесі розрахунків, етап консолідації не є обов'язковим, при цьому результат може бути отриманий безпосередньо з локальної відповідності структур. Локальна відповідність також може призвести до результату із ранньою відмовою у випадку із шаблоном, що містить точки відбитків пальців, які значно відрізняються. Розвиток алгоритмів, що базуються на зіставленні локальних характеристик, призвів до трьох напрямків підходів методів:

1) Існуючі підходи, локальні структури яких, у більшості випадків, формувалися шляхом підрахунку кількості деталей відбитків, що потрапляють у зазначену область, і не мають глобальної консолідації;

2) Підходи до створення алгоритмів вчених, які першим змогли зробити ефективне кодування збігів сусідніх деталей в області незмінних розмірів і кутів, і запропонували глобальну консолідацію;

3) Багато варіантів методів, які розширюють набір функцій і враховують такі параметри, як: локальну орієнтацію деталей, локальну частоту, форму хребта тощо.

Локальні структури невеликого розміру можна класифікувати як найближчі на основі сусідів і на основі фіксованого радіуса. У цьому випадку сусідніми по відношенню до центральних контрольних мінуцій визначаються їх найближча кількість K до них мінуцій. Це призводить до появи дескрипторів, що мають фіксовану довжину, які зазвичай узгоджуються дуже ефективно. Існують раніше представлені алгоритми, у яких сусідніми мінуціями визначаються усі мінуції, що знаходяться ближче до центральної контрольної точки, ніж даний радіус R . Довжина дескриптора залежить від змінної, а також і залежить від щільності локальних структур. Це може призводити до більш складного процесу локального узгодження структур, але, можна вважати, що цей спосіб є більш чутливим до мінуцій, що відсутні або є фальшивим. Недоліками цього способу є:

1) Абсолютне кодування радіальних кутів (відповідне відносне кодування яких позначається як dR , що у свою чергу вимагає складного локального узгодження;

2) Відсутність різниці у напрямках між центральними точками та сусідніми. Окрім цього, підхід, як у способу з фіксованим радіусом, може призвести у подальшому до помилок на границі: зокрема, структури поблизу границі локального регіону в одному з двох відбитків пальців може бути невідповідними через локальне спотворення або неточність розташування, це може спричинити переміщення тих

самих структур за межі локального регіону іншого відбитка пальця. Раніше розглянута методика, запропонована Феном [6], не має такого роду недоліків і може вважатися ефективним алгоритмом локального узгодження із фіксованим радіусом. Зокрема, проблема границь розглядається шляхом дослідження мінуцій, розташованих неподалік від кордону, а не таких, що відповідають зазначеним, а як мінуції, що знаходяться поблизу кордону, як такі, що мають бути зіставленими.

У даній роботі розглядається нова локальна репрезентацію лише для мінуцій, що спрямовані на поєднання переваг обох структур: що базуються на основі сусідства, так і структур із фіксованим радіусом, при цьому їх існуючі недоліки не погіршують працездатність.

Розглядається основна мета цієї роботи, підсумовуються переваги даної техніки. У алгоритмі визначаються локальні структури мінуцій і досліджується, яким чиним потрібно виміряти подібність між ними. Пропонує чотири прості підходи до консолідації локальних подібностей у глобальному плані. Описується велика кількість експериментів для порівняння даного підходу з трьома реалізаціями добре відомих підходів, що описані далі, і містять лише мінуції. Подано деякі заключні зауваження щодо розглянутого алгоритму.

2.2 Опис етапів алгоритму циліндр-кодів

Слід розглянути основні мотиви, що спонукали науковців розробити нову методику зіставлення локальних мінуцій [7]:

- 1) Є потреба у розробці алгоритмів, що є точними і сумісних, і при цьому вони розглядають лише мінуції. Більшість нещодавно запропонованих алгоритмів порівняння відбитків пальців використовують кілька додаткових параметрів, але не мінуцій. Багаточисленні дослідження показали, що поєднання функцій (особливо, що є частково незалежними одна від одної) є дуже ефективним методом, щоб підвищити точність кінцевих результатів. Якщо подивитись на

ситуацію з іншої сторони, окрім мінуцій, досі немає конвергенції щодо стандартів, що точно визначають і кодують дані додаткові функції. Одним із перших алгоритмів, що намагався вирішити дану проблему є CDEFFS (2008) [8], який все ще знаходиться на ранній стадії розробки. Широкомасштабна розробка алгоритмів відбитків пальців по всьому світу вимагає нового покоління точних методів із високою можливістю взаємодії. Через це вважається, що алгоритми зіставлення лише мінуцій відповідають стандарту ISO/IEC 19794-2 (2005) (або дуже схожій метриці ANSI/INCITS 378 (2004) [9]) та буде відігравати головну роль у наступні роки. Окрім цього, шаблони, що містять лише мінуції, також дозволяють стискати в кілька сотень байтів важливу інформацію про відбитки пальців, що дозволяє зберігати їх на недорогих смарт-картках;

- 2) Переносимість на легких архітектурах. Одним із ефективних способів захистити біометричні програми від зовнішніх атак є обмеження обчислень усередині закритої системи, тобто безпечної апаратної платформи, такої як смарт-карта або система на чіпі. На жаль, обчислювальна потужність цих недорогих захищених платформ у сотні чи тисячі разів нижча, ніж у сучасного ПК, і алгоритми, які потребують ресурсів, не можуть бути виконані через це. Після цього розробники алгоритмів сконцентрували свою увагу на розробці спрощених оптимізованих версій, що часто засновані на методах зіставлення локальних мінуцій та інформації, що була попередньо обчислена. Однак останні результати розробок показали, що найбільш успішні існуючі алгоритми зіставлення карток не можуть конкурувати з відповідними реалізаціями ПК, і необхідні подальші дослідницькі зусилля.
- 3) Придатність до методів захисту шаблонів. Захист шаблонів в даний час отримує багато уваги через великі переваги, які він може забезпечити, серед них: незворотність, різноманітність і поворот. На жаль, проектування ефективних методів захисту шаблонів без узгодження відповідного падіння точності є дуже

складним і вимагає існування вирівнювання, фіксованої довжини і кодування характеристик, що є непохитні до шуму. На сьогоднішній день ще не було запропоновано повністю задовільного рішення цієї проблеми.

Локальне представлення мінущій, що було введено і розглянуто в даній роботі, засноване на тривимірних структурах даних - циліндрах, що побудовані з інваріантних відстаней і кутів в сусідстві кожної мінущії. Циліндри можуть бути створені, починаючи з підмножини обов'язкових ознак в стандартах, таких як ISO/IEC 19794-2. Зокрема, у даній метриці береться до уваги тільки положення і напрямок мінущій, а не тип мінущій і їх якість. Слід зазначити, що тип мінущій не є робастною рисою, і визначення якості мінущій семантично не є чітким у стандартах, і при цьому може призвести до проблем з інтерперабельністю (створення систем з незалежних розподілених структур). Завдяки тому, що присутній факт інваріантності циліндрів, фіксована довжині та побітно орієнтованоме кодування, можна визначити деякі прості, але ефективні метрики для обчислення подібності циліндрів. Окрім цього, пропонується чотири методи глобального оцінювання, задля того, щоб об'єднати локальні подібності в унікальну глобальну оцінку, яка визначає загальну схожість між двома відбитками пальців. Основними перевагами нового методу, що має назву Minutia Cylinder-Code, є:

- 1) Алгоритм, заснований на циліндр-кодах — це метрика із фіксованим радіусом, тому вона краще впорається із відсутніми або помилковими мінущіями, у порівнянні із підходами, що засновані на основі найближчого сусідства;
- 2) На відміну від традиційних методів із фіксованим радіусом, метрика на основі циліндр-кодів базується на інваріантному кодуванні фіксованої довжини для кожної мінущії, що значно спрощує обчислення схожості локальних структур;
- 3) Проблеми при обчисленні, що пов'язані із границями, вирішуються без додаткового навантаження на етапах кодування та зіставлення;

- 4) Локальні спотворення та невеликі помилки розпізнавання точок допускаються завдяки застосуванню згладжених функцій, які є стійкими до помилок, саме на етапі кодування;
- 5) Алгоритм циліндр-кодів ефективно справляється з нечіткими (шумними) областями відбитків пальців, із якими зазвичай використовуються алгоритми вилучення мінуцій, і є розміщення близьких один до одного мінуцій; це уможливлюється ефектом насичення, що виробляється обмежуючою функцією;
- 6) Побітно орієнтоване кодування, що є однією з можливих реалізацій алгоритму циліндр-кодів, робить циліндр, який відповідає надзвичайно простим і швидким, скорочуючи його до послідовності бітових операцій (наприклад, XOR), що можуть бути ефективно реалізовані майже на будь-якого рівня потужності процесорах.

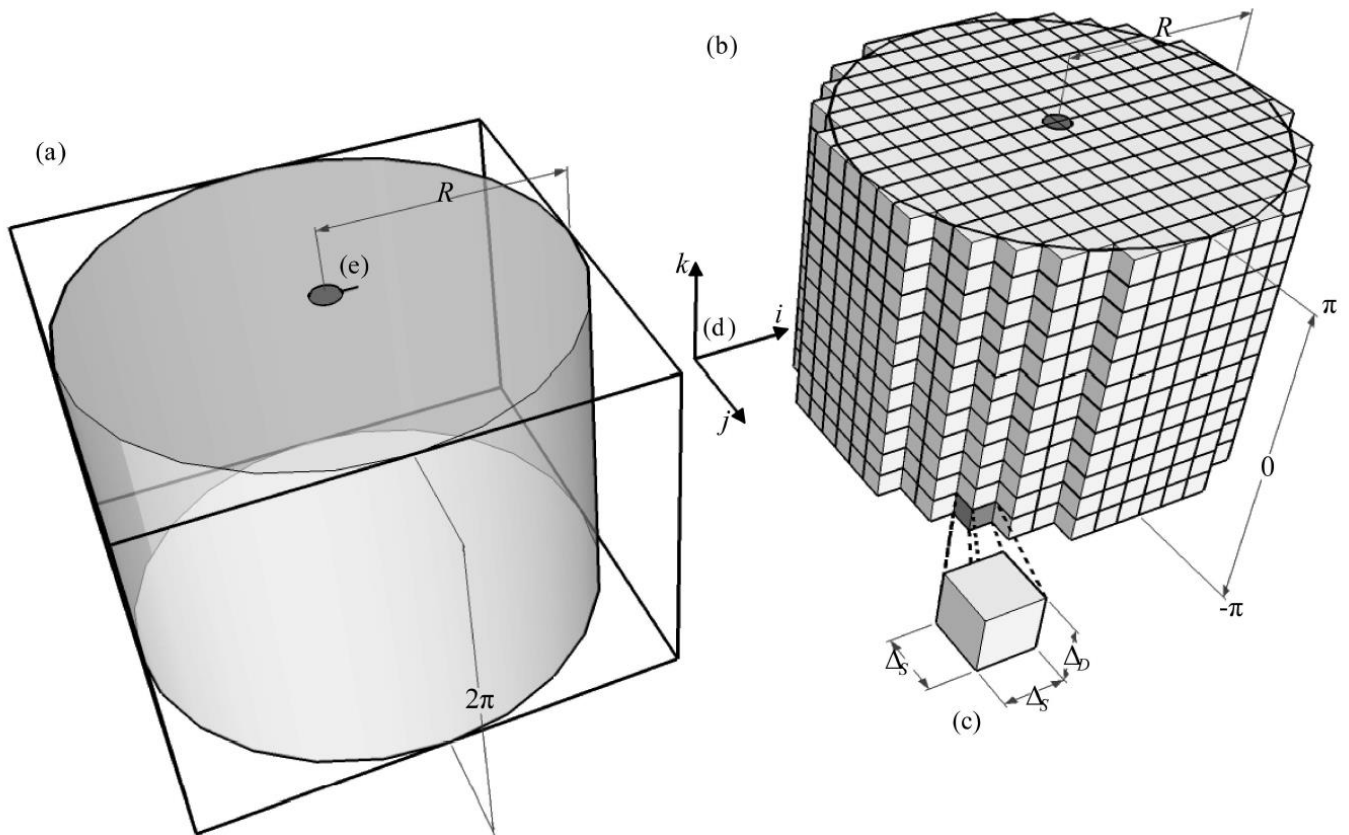


Рисунок 2.1 – Локальна структура – циліндр [7]

На графіку зображено локальні структури, що пов'язані з певною мінуцією, де позначає: (а) циліндр з заданими кубоїдами, (b) дискретизація із кубоїдів в клітини (с), що мають розміри $\Delta_S \times \Delta_S \times \Delta_D$. Слід зазначити, що зображено тільки осередки тих клітини, центр яких знаходиться в межах циліндра. Також є важливим, що кубоїд обертається таким чином, щоб (d) осі були напрувлені до (e) напрямку відповідної до неї мінуції.

2.3 Розгляд локальних структур алгоритму

Метрика верифікації відбитків пальців на основі циліндр-кодів представляє область місцевих структур відповідно до з кожної мінуції. Дана структура кодує просторові та спрямовані відношення між мінуцією, разом з її фіксованим радіусом, і границями, і при цьому може бути доступно представлена у вигляді циліндра, основа та висота якого пов'язані з просторовою та напрувленою інформацією, відповідно до малюнка.

Нехай значення $T = \{m_1, m_2, \dots, m_n\}$ — шаблон ISO/IEC 19794-2. Кожна мінуція m — це триплет $m = \{x_m, y_m, \theta_m\}$, x_m, y_m — координати розташування мінуцій, θ_m — напрямок мінуції в діапазоні $[0; 2\pi]$. Далі описується, як побудована локальна структура заданої мінуції m , створення цілого набору циліндрів з T , також вводиться міра подібності між циліндрами. Крім цього, робиться фокус на біто-орієнтованій ефективній реалізації даної метрики.

2.3.1 Побудова циліндра конкретної мінуції

Локальна структура, пов'язана з даною мінуцією $m = \{x_m, y_m, \theta_m\}$, представлена у вигляді циліндра з радіусом R і висотою 2π , основа якого зосереджена на розташуванні мінуції із координатами (x_m, y_m) .

Циліндр знаходиться всередині кубоїда, основою якого є вирівняна за напрямками мінуція θ_m ; кубоїд поміщено в ділянки (клітини) $N_c = N_s \times N_s \times N_D$.

Кожна клітина представляє собою маленький кубоїд, що має основу $\Delta_S \times \Delta_S$ і висоту Δ_D , де $\Delta_S = \frac{2R}{N_S}$ та $\Delta_D = \frac{2R}{N_D}$.

Кожна клітина може бути однозначно ідентифікована за трьома індексами (i, j, k) , що позначають її позицію в кубоїді, оточеному циліндром, у якому $i, j, k \in I_S = \{n \in \mathbb{N}, 1 \leq n \leq N_S\}$ та $k \in I_D = \{n \in \mathbb{N}, 1 \leq n \leq N_D\}$.

Припустимо, що:

$$d\varphi_k = -\pi + (k - \frac{1}{2}) \cdot \Delta_D \quad (2.1)$$

це кут, який пов'язаний з усіма клітинами на висоті k у циліндрі, і нехай:

$$p_{i,j}^m = \begin{bmatrix} x_m \\ y_m \end{bmatrix} + \Delta_S \cdot \begin{bmatrix} \cos(\theta_m) & \sin(\theta_m) \\ -\sin(\theta_m) & \cos(\theta_m) \end{bmatrix} \cdot \begin{bmatrix} i - \frac{N_S+1}{2} \\ j - \frac{N_S+1}{2} \end{bmatrix} \quad (2.2)$$

це двовимірна точка, що відповідає центру комірок з індексами i, j (яка є проекцією на основу циліндра), виражена в просторових координатах шаблону контрольної точки; оскільки ці точки проектується на основу, індекс k не потрібен.

Для кожної комірки (i, j, k) числове значення $C_m(i, j, k)$ обчислюється шляхом накопичення внесків від кожної точки мінуції m_t , що належить сусідству $N_{p_{i,j}^m}$ з $p_{i,j}^m$.

$$N_{p_{i,j}^m} = \{m_t \in T; m_t \neq m, d_S(m_t, p_{i,j}^m) \leq 3\sigma_S\}, \quad (2.3)$$

де $3\sigma_S$ – це радіус сусідства, та $d_S(m_t, p_{i,j}^m)$ – це евклідова відстань між мінуцією m та точкою p .

Функція $C_m: I_S \times I_S \times I_D \rightarrow V$ є визначеною наступним чином:

$$C_m(i, j, k) = \begin{cases} \Psi \left(\sum m_t \in N_{p_{i,j}^m} (C_m^S(m_t, p_{i,j}^m) \cdot C_m^D(m_t, d\varphi_k)) \right) & \text{if } \xi_m(p_{i,j}^m) = \text{valid} \\ \text{invalid otherwise,} & \end{cases} \quad (2.4)$$

де:

- 1) $V = [0,1] \cup \{invalid\}$ є кодоменом функції – значення, які вона може приймати.
- 2) Два терміни $C_m^S(m_t, p_{i,j}^m)$ і $C_m^D(m_t, d\phi_k)$ є просторовим і спрямованим внеском контрольних точок m_t відповідно.

$$3) \quad \xi_m(p_{i,j}^m) = \begin{cases} valid & \text{if } d_s(m, p_{i,j}^m) \leq R \text{ and} \\ & p_{i,j}^m \in Conv_{Hull}(T, \Omega) \\ invalid & \text{otherwise,} \end{cases} \quad (2.5)$$

де $Conv_{Hull}(T, \Omega)$ це опукла оболонка контрольних точок у T , що збільшена шляхом додавання зміщення Ω пікселів. Інтуїтивно зрозуміло, що дана комірка вважається валідною (дійсною) тоді і тільки тоді, коли її центр $p_{i,j}^m$ розташовується в точці перетину основи циліндра з опуклою оболонкою, визначеною всіма дрібницями в T . Ця умова є важливою для уникання розгляду ділянок циліндра, які, ймовірно, знаходяться поза зоною відбитків пальців і, отже, не можуть містити відповідну інформацію.

- 4) $\Psi(v) = Z(v, \phi_\psi, \tau_\psi)$ — це сигмоподібна функція, що контролюється двома параметрами (ϕ_ψ і τ_ψ), яка обмежує внесок щільних кластерів дрібниць (що є типовим для так званих шумних областей), і гарантує, що кінцеве значення буде знаходитися в діапазоні $[0, 1]$; функція із сигмою визначається як:

$$Z_{(v,\mu,\tau)} = \frac{1}{1 + e^{-\tau(v-\mu)}} \quad (2.6)$$

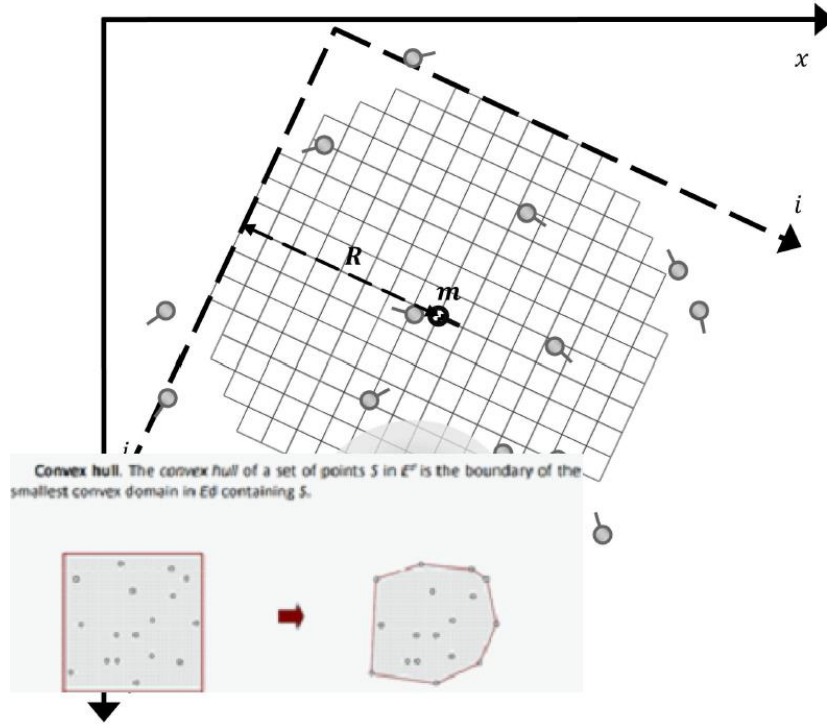


Рисунок 2.2 – Зображення циліндра у розрізі [7]

У розрізі циліндра, що пов'язаний з мінуцією m , зображені усі деталі, які є складовою конструкції циліндра. Слід зауважити, що вони не обов'язково повинні лежати всередині основи циліндра, оскільки допускається зміщення $Z_{\sigma S}$. Значення $G_S(t)$ в околицях даної комірки (із центром $p_{i,j}^m$) є виділеними (темніші області представляють вищі значення). Чорні мінуції – це ті, які розташовані в межах $G_{p_{i,j}^m}$.

Зазвичай значення $C_m(i, j, k)$ комірки, що є валідною, представляє ймовірність знайти найближчу мінуцію $p_{i,j}^m$ з різницею напрямків відносно m , що розташована близько до $d\varphi_k$. Ця ймовірність отримується унаслідок підсумовування внесків усіх мінуцій, що відносяться до сусідства $N_{p_{i,j}^m}$. Внесок кожної мінуції m_t визначається як добуток C_m^S та C_m^D .

$C_m^S(m_t, p_{i,j}^m)$ – це просторовий внесок, який точки мінуцій m_t надають комірці (i, j, k) . Дана комірка визначається функцією евклідової відстані між m_t і $p_{i,j}^m$.

$$C_m^S(m_t, p_{i,j}^m) = G_S(d_S(m_t, p_{i,j}^m)) \quad (2.7)$$

де

$$G_S(t) = \frac{1}{\sigma_S \sqrt{2\pi}} e^{\left(-\frac{t^2}{2\sigma_S^2}\right)} \quad (2.8)$$

є функцією Гауса з нульовим середнім і S стандартним відхиленням.

На Рисунку 2.2, що графічно зображує значення $G_S(t)$ в околицях даної комірки, контрольні точки, що лежать у колі із радіусом $R, R + 3\sigma_S$, все ще вносять свій внесок у $C_m(i, j, k)$, що дозволяє уникнути неприємного ефекту кордону.

$C_m^D(m_t, d\varphi_k)$ – це спрямований внесок мінуції m_t ; він визначається як функція таких параметрів:

1) $d\varphi_k$ та

2) різниці напрямків між θ_m і θ_{m_k} . Інтуїтивно зрозуміло, що значення внеску є високим, коли 1) і 2) знаходяться близько по відношенню один до одного.

$$C_m^D(m_t, d\varphi_k) = G_D\left(d\phi(d\varphi_k, d_\theta(m, m_t))\right) \quad (2.9)$$

де $d\phi(\theta_1, \theta_2)$ є різницею між двома кутами θ_1, θ_2 :

$$d\phi(\theta_1, \theta_2) = \begin{cases} \theta_1 - \theta_2 & \text{if } -\pi \leq \theta_1 - \theta_2 < \pi; \\ 2\pi + \theta_1 - \theta_2 & \text{if } \theta_1 - \theta_2 < -\pi; \\ -2\pi + \theta_1 - \theta_2 & \text{if } \theta_1 - \theta_2 \geq \pi. \end{cases} \quad (2.10)$$

Дирекційна відмінність, де $d_\theta(m, m_t) = d\phi(\theta_m, \theta_{m_t})$ - це дирекційна відмінність між двома мінуціями.

$G_D(\alpha)$ — площа функції Гауса, що має нульове середнє і стандартне відхилення σ_D на інтервалі $[\alpha - \frac{\Delta_D}{2}, \alpha + \frac{\Delta_D}{2}]$:

$$G_D(\alpha) = \frac{1}{\sigma_D \sqrt{2\pi}} \exp \left[-\frac{\alpha^2}{2 \cdot \sigma_D^2} \right] \quad (2.11)$$

де G_D - відхилення, що буває нульовим, середнім і стандартним.

Ділянка $C_m(i, j, k)$ може виявитися валідною або не валідною. Це залежить від значення просторової і дирекційної контрибуцій. Тому воно належить одному з варіантів:

- 1) Ділянка є валідною - $C_m(i, j, k) \in [0, 1]$;
- 2) Ділянка не є валідною - $C_m(i, j, k)$.

2.3.2 Створення набору циліндрів

Набір циліндрів, що отримується із шаблону T деталей ISO/IEC 19794-2, визначається, як показано на малюнку:

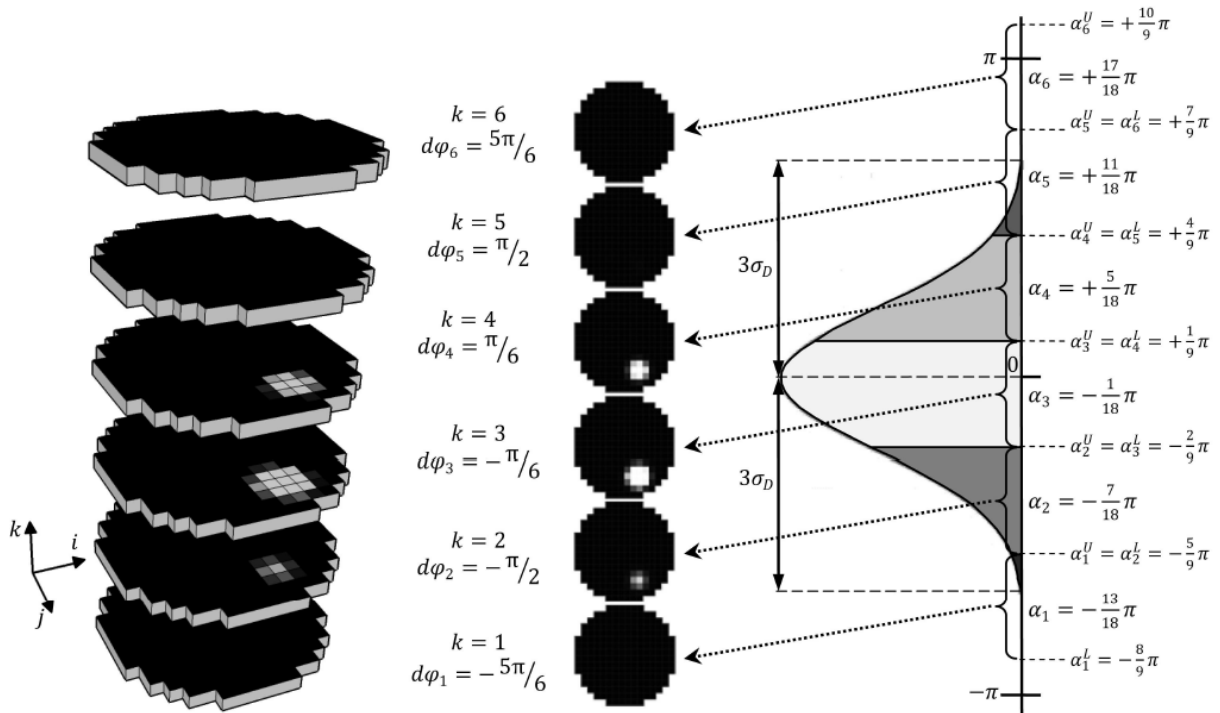


Рисунок 2.3 – Складові частин розрізу циліндра [7]

При цьому значення параметрів:

$$\begin{aligned}
\sigma_D &= \frac{2\pi}{9} & \alpha_k &= (d\varphi_k, -\pi/9) \\
\Delta_D &= \frac{\pi}{3} & \alpha_K^L &= \alpha_k - \pi/6 \\
d_\theta(m, m_1) &= -\pi/9 & \alpha_K^U &= \alpha_k + \pi/6
\end{aligned} \tag{2.12}$$

На зображенні продемонстрована локальна структура, що пов'язана з заданою контрольною точкою m у спрощеному випадку, де є лише один контрольний елемент, який вносить внесок у значення комірки $C_m(i, j, k)$.

Може існувати більш простий випадок, коли лише одна контрольна мінуція m_1 вносить вклад у циліндр, що пов'язаний із контрольною мінуцією m . Різні $C_m(i, j, k)$ значення представлені на рисунку 2.4 різними рівнями сірого (чим світліше - тим більше). Области N_D (у цьому прикладі - шість) під кривою Гауса графічно виділені, а відповідні значення в (2.9) і (2.12) представлені чисельно для кожного значення k : зокрема, $\alpha_k = d\phi(d\varphi_k, d_\theta(m_1, m_2))$ – вхідне значення функції G_D у (2.9) виразі, α_K^L та α_K^U – нижня та верхня межі інтеграла в (2.12) відповідно. На практиці контрольна точка m_1 сприяє створенню більшої кількості секцій циліндра з різною вагою, відповідно до різниці в її напрямках з m_1 . При цьому, ненульові значення комірки не є ідеально симетричними відносно неї самої, яка містить m_1 . Це відбувається по тій причині, що m_1 не розташовується точно в центрі комірки.

$$CS = \{C_m | C_m \text{ is not invalid, } m \in T\}, \tag{2.13}$$

де C_m – циліндр, який пов'язаний з контрольною точкою m , що містить значення $C_m(i, j, k)$. Циліндр C_m вважається недійсним (invalid) у таких випадках:

- 1) У циліндрі міститься менше, ніж $\min_{VC}$ валідних комірок;
- 2) Існує менше, ніж $\min_M$ мінуцій, які вносять внесок у циліндр, іншими словами - є меншими, ніж $\min_M$ мінуцій m_t таких, що $d_S(m_t, m) \leq R + 3\sigma_S$ з $m_t \neq m$.

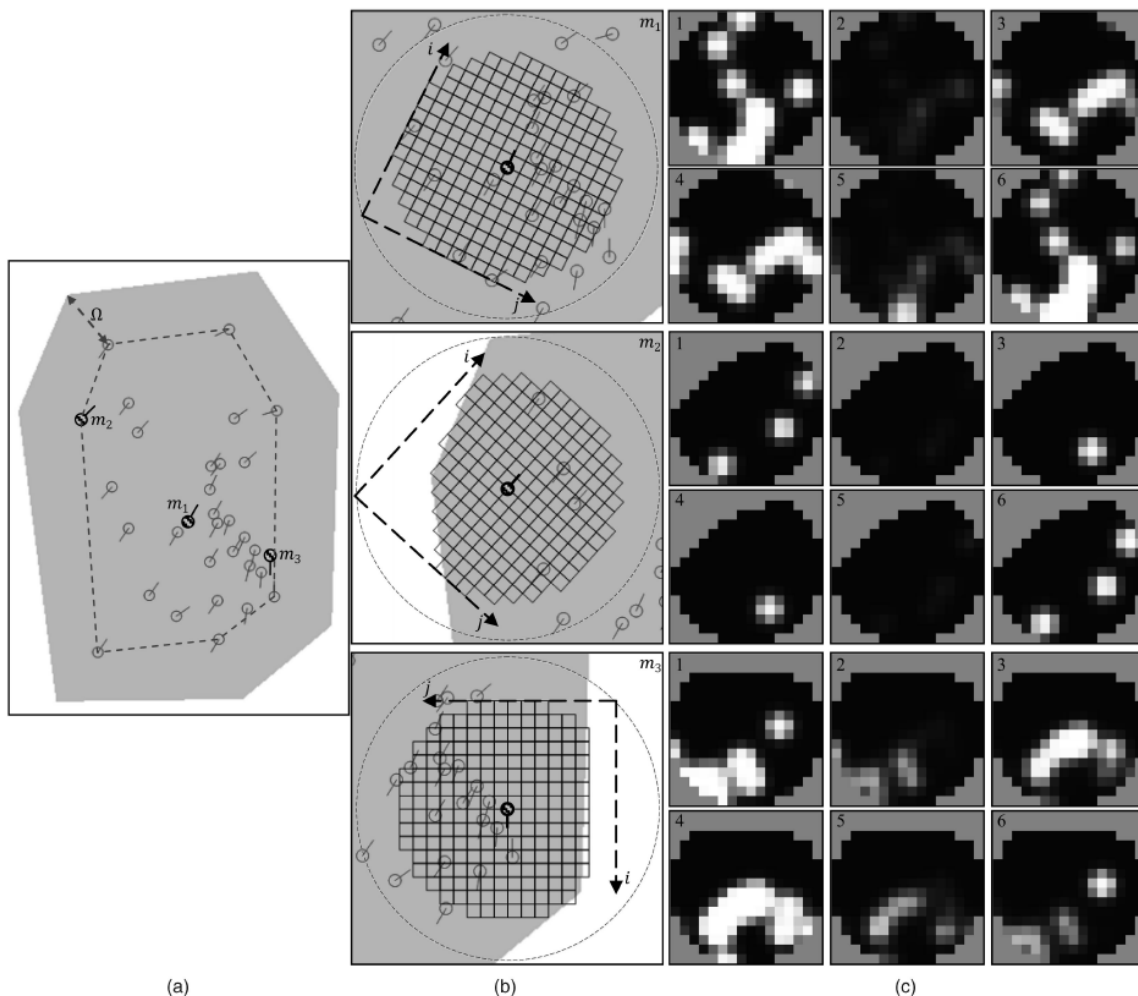


Рисунок 2.4 – Шаблони точок і циліндри [7]

На малюнку зображені шаблони точок мінуцій та три циліндри з відповідного набору циліндрів, де (a) - шаблон мінуцій із відповідною опуклою оболонкою. Для кожної з трьох позначок, виділених у (a), стовпець (b) показує основу відповідного циліндра (зображені лише дійсні клітини); мінуції в межах пунктирних кіл – ті мінуції, які вносять внесок у значення комірки циліндра. Стовпець (c) показує значення клітинок трьох циліндрів для кожного значення $k \in \{1, \dots, 6\}$ – елементи більш світлого кольору означають вищі значення); при цьому секції циліндра в (c) обертаються відповідно до напрямку відповідних контрольних точок (мінуцій).

2.3.3 Визначення схожості між двома циліндрами

Кожен циліндр являє собою локальну структурою даних, яка має наступні властивості:

- 1) Є інваріантною при переміщенні й обертання, якщо: вона кодує відстані і відмінності напрямку між ними мінущіями його основою; обертається відповідно до напрямку даної мінущії;
- 2) Незмінна по відношенню до недоліків шкіри (невеликих за важкістю), проти невеликих помилок визначення ознак. Завдяки наявності згладженого характеру функцій визначення внеску кожної мінущії (формули (2.9) та (2.12)), та до функції обмеження Ψ в (2.4);
- 3) З фіксованою довжиною, що задається кількістю комірок N_c .

З наведених вище причин, подібність між двома циліндрами можна з легкістю визначити за допомогою векторної кореляційної міри, що описана в наступних параграфах даної роботи.

Припустимо, що дано циліндр C_m , нехай $lin: I_S \times I_S \times I_D \rightarrow \mathbb{N}$ — функція, що лінеаризує індекси комірок циліндра:

$$lin(i, j, k) = (k - 1) \cdot (N_S)^2 + (j - 1) \cdot N_S + i \quad (2.14)$$

і нехай при цьому $c_m \in V^{N_c}$ буде вектором, який отримано від C_m (V є кодоменом - набором, який включає у себе усі можливі значення заданої функції - формули (2.5)). Відповідно до формули (2.14):

$$c_m[lin(i, j, k)] = C_m(i, j, k). \quad (2.15)$$

Розглянемо наступну ситуацію: дано дві мінущії a і b , нехай c_a і c_b - вектори, що отримані від циліндрів C_a і C_b . Вони являють собою два відповідні елементи $c_a[t]$ і $c_b[t]$, що вважаються відповідними виключно при умові, якщо $c_a[t] \neq invalid$ та $c_b[t] \neq invalid$ виконуються одночасно. Нехай $c_{a|b}, c_{b|a} \in [0, 1]^{N_c}$ — два вектори, що походять від c_a та c_b , враховуючи лише сумісні елементи:

$$c_{a|b}[t] = \begin{cases} c_a[t] & \text{if } c_a[t] \text{ and } c_b[t] \text{ are matchable} \\ 0 & \text{otherwise,} \end{cases} \quad (2.16)$$

$$c_{b|a}[t] = \begin{cases} c_b[t] & \text{if } c_b[t] \text{ and } c_a[t] \text{ are matchable} \\ 0 & \text{otherwise.} \end{cases} \quad (2.17)$$

На практиці елементи, що співпадають, є відповідними перетину дійсних комірок двох циліндрів.

Подібність між двома циліндрами визначається наступним чином:

$$\gamma(a, b) = \begin{cases} 1 - \frac{\|c_{a|b} - c_{b|a}\|}{\|c_{a|b}\| + \|c_{b|a}\|} & \text{if } C_a \text{ and } C_b \text{ are matchable} \\ 0 & \text{otherwise,} \end{cases} \quad (2.18)$$

де два циліндри є тотожними, якщо виконуються наступні умови:

- 1) Різниця в напрямках двох мінуцій не перевищує δ_θ ($\delta_\theta(a, b) \leq \delta_\theta$);
- 2) Існує як мінімум $\min_{ME}$ відповідних елементів у двох векторах c_a і c_b є сумісними;
- 3) $\|c_{a|b}\| + \|c_{b|a}\| \neq 0$.

Перша умова виконує роль зменшення кількості відповідних циліндрів, припускаючи максимально можливе обертання двох відбитків пальців; друга умова дозволяє уникнути порівняння циліндрів із занадто малим допустимим перетином; третя умова виключає випадок, при якому досить великий перетин двох валідних циліндрів не містить жодної інформації.

Варто звернути увагу на те, що $\gamma(a, b)$ буде завжди знаходитися в діапазоні $[0,1]$. Нуль - це відсутність подібності, а одиниця - максимальна подібність. Далі, залежно від контексту, $\gamma(a, b)$ буде розглядатися як подібність циліндра, подібність локальної структури циліндра або подібність мінуцій. Унаслідок того, що циліндри й мінуції співвідносяться як 1:1, між ними гнучкість їх значень не призводить до неоднозначності.

2.3.4 Двійкова (bit-based) реалізація

Характеристики локальних структур та ступеня подібності, що було впроваджено в попередніх розділах, стверджують про те, що метрика циліндр-кодів добре підходить для того, щоб реалізувати її у двійковому вигляді. Для цих цілей $\Psi(v)$ у формулі (2.5) може бути змінено наступним чином:

$$\Psi_{Bit}(v) = \begin{cases} 1 & \text{if } v \leq \mu_\Psi \\ 0 & \text{otherwise,} \end{cases} \quad (2.19)$$

таким чином обмежуючи кодомен $C_m(i, j, k)$ до бінарних значень 0, 1 та недійсних значень. У такому випадку реалізації даний циліндр C_m може бути збережено як двобітовий вектор $c_m, \hat{c}_m \in \{0, 1\}^{N_c}$ першим зберігає значення комірки, а другий - дійсність комірки (формула (2.14)):

$$c_m[\text{lin}(i, j, k)] = \begin{cases} 1 & \text{if } C_m(i, j, k) = 1 \\ 0 & \text{otherwise,} \end{cases} \quad (2.20)$$

$$\hat{c}_m[\text{lin}(i, j, k)] = \begin{cases} 1 & \text{if } C_m(i, j, k) \neq \text{invalid} \\ 0 & \text{otherwise.} \end{cases} \quad (2.21)$$

На практиці ж вектор $\hat{c}_m$ може бути використано як двоїчну маску для вибору допустимих бітів у c_m таким чином, два вектори, що визначено в формулах (15) і (16), можуть бути обчислені наступним чином:

$$c_{a|b} = c_a \text{ AND } \hat{c}_{a|b}, \quad c_{b|a} = c_b \text{ AND } \hat{c}_{ab} \quad (2.22)$$

де AND - порозрядна операція and (кон'юнкція) між двома біт-векторами, а $\hat{c}_{ab} = \hat{c}_{a|b} \text{ AND } \hat{c}_b$ є перетином двох масок відбитків. Отже, подібність між двома циліндрами можна обчислити наступним чином:

$$\gamma_{Bit}(a, b) = \begin{cases} 1 - \frac{\|c_{a|b} \text{ XOR } c_{b|a}\|}{\|c_{a|b}\| + \|c_{b|a}\|} & \text{if } C_a \text{ and } C_b \text{ are matchable} \\ 0 & \text{otherwise,} \end{cases} \quad (2.23)$$

де XOR позначає бітову виключну диз'юнкцію між двома бітовими векторами. Слід звернути увагу, що норму бітового вектора можна просто знайти шляхом обчислення квадратного кореня з кількості бітів, що мають значення один.

Отже, маємо кількість операцій з плаваючою комою та цілих чисел, які беруть участь у обчисленні подібності між двома циліндрами для звичайної та бітової реалізації відповідно. При цьому бітова реалізація вимагає лише п'яти операцій із плаваючою комою та дуже невеликої кількості цілочисельних і побітових операцій. Отже, формули (2.20) і (2.21) можна реалізувати дуже ефективно, навіть на пристроях із слабкою потужністю.

2.4 Глобальна оцінка результату

Для того, щоб порівняти два шаблони мінуцій – два відбитки пальців людини – єдина загальна оцінка, яка може вказувати на їх загальну подібність, має бути отримана з локальних подібностей. Далі розглянуто чотири способи для об'єднання місцевих подібностей у глобальну оцінку. Для глобального зіставлення можуть бути розроблені більш точні методи, але основна ідея даного підходу - можливість ефективної реалізації на пристроях легкої архітектури.

Перші два методи можна називати «локальними техніками», так як вони об'єднують лише локальні схожості; два наступні – так званий крок консолідації, який потрібен для того, щоб отримати оцінку, яка відображає те, наскільки локальні відносини зберігаються на глобальному рівні. В експериментальній оцінці, де алгоритм циліндр-кодів порівнюється з трьома добре відомими локальними алгоритмами, ці чотири методи застосовуються не тільки до даної метрики, а і до інших.

Розглянемо два дані шаблони деталей ISO/IEC 19794-2: $A = \{a_1, a_2, \dots, a_{n_A}\}$ та $B = \{b_1, b_2, \dots, b_{n_B}\}$, нехай:

1) $\gamma(a, b)$ — локальна подібність між точками $a \in A$ і $b \in B$, при цьому $\gamma: A \times B \rightarrow [0, 1]$;

2) $\Gamma \in [0, 1]^{n_A \times n_B}$ — матриця, що містить усі локальні подібності, з $\Gamma[r, c] = \gamma(a_r, b_c)$.

2.4.1 Сортвання за локальною подібністю

При використанні даного методу відбувається сортвання усіх локальних подібностей та обирається верхній n_P ; припустимо, що P буде множиною вибраних пар мінуцій - індекс n_P :

$$P = \{(r_t, c_t)\}, t = 1, \dots, n_P, 1 \leq r_t \leq n_A, 1 \leq c_t \leq n_B \quad (2.24)$$

при цьому для знаходження глобальної оцінки потрібно розрахувати середнє арифметичне значення відповідних локальних подібностей:

$$S(A, B) = \frac{\sum_{(r,c) \in P} \Gamma[r, c]}{n_P}. \quad (2.25)$$

Значення n_P не є постійним, так як воно частково залежить від кількості мінуцій у двох шаблонах:

$$n_P = \min_{n_P} + \lfloor (Z(\min\{n_A, n_B\}, \mu_P, \tau_P)) \cdot (\max_{n_P} - \min_{n_P}) \rfloor \quad (2.26)$$

де μ_P , τ_P , $\min_{n_P}$ і $\max_{n_P}$ — параметри, Z — сигмоїдна функція, яка визначена у формулі (2.5), та $\lfloor \cdot \rfloor$ - оператори округлення.

2.4.2 Дослідження локальної подібності

Даний алгоритм вирішує задачі лінійного призначення на матриці Γ , тобто для знаходження множини n_P пар $P = \{(r_i, c_i)\}$, що максимізує $S(A, B)$ у (2.26) без урахування одних і тих же мінуцій більше одного разу. Значення n_P і загальна оцінка розраховуються у формулах (2.24) і (2.25), відповідно.

Основна ідея методу полягає в тому, щоб з кожною ітерацією змінювати локальні подібності на основі сумісності між зв'язками мінущій. Враховуючи пару мінущій (a, b) , якщо глобальні зв'язки між a та деякими іншими дрібницями в A сумісні з глобальними зв'язками між b та відповідними дрібницями в B , тоді локальна подібність між a та b посилюється, інакше вона послаблюється.

Як попередній крок, n_P пари (r_i, c_i) вибираються за допомогою алгоритму локальної подібності (Local Similarity Assignment), з $n_P = \min\{n_A, n_B\}$, при цьому дуже часто $n_R \gg n_P$.

Припустимо, що $\lambda_t^0 = \Gamma[r_t, c_t]$ - початкова подібність пари t ; подібність на ітерації i та наступної процедури:

$$\lambda_t^0 = w_R \cdot \lambda_t^{i-1} + (1 - w_R) \cdot \frac{\left(\sum_{\substack{k=1 \\ k \neq t}}^{n_R} \rho(t, k) \cdot \lambda_k^{i-1} \right)}{n_R - 1} \quad (2.27)$$

де $w_R \in [0, 1]$ - ваговий коефіцієнт, та:

$$\rho(t, k) = \prod_{i=1}^3 Z(d_i, \mu_i^\rho, \tau_i^\rho) \quad (2.28)$$

$$d_1 = |d_S(a_{r_t}, a_{r_k}) - d_S(b_{c_t}, b_{c_k})| \quad (2.29)$$

$$d_2 = |d_\phi(d_\theta(a_{r_t}, a_{r_k}), d_\theta(b_{c_t}, b_{c_k}))| \quad (2.30)$$

$$d_3 = \left| d_\phi \left(d_R(a_{r_t}, a_{r_k}), d_R(b_{c_t}, b_{c_k}) \right) \right| \quad (2.31)$$

$\rho(t, k)$ - є мірою сумісності між двома парами мінущій: мінущія (a_{r_t}, a_{r_k}) з шаблону A та мінущії (b_{c_t}, b_{c_k}) з шаблону B . Значення сумісності базується на подібності між трьома функціями, які є інваріантними для повороту та зсуву; воно розраховується як добуток трьох змінних: d_1 , d_2 та d_3 , які нормалізуються за допомогою сигмоїдних функцій з певними параметрами. d_1 позначає подібність між просторовими відстанями контрольних точок, d_2 порівнює різниці в напрямках, у той

час як d_3 порівнює радіальні кути. Радіальний кут визначається як кут між ребром, що з'єднує дві мінуції, та напрямком першої з них:

$$d_R(m_1, m_2) = d\phi\left(\theta_{m_1}, \text{atan2}(-y_{m_2} + y_{m_1}, x_{m_2} - x_{m_1})\right). \quad (2.32)$$

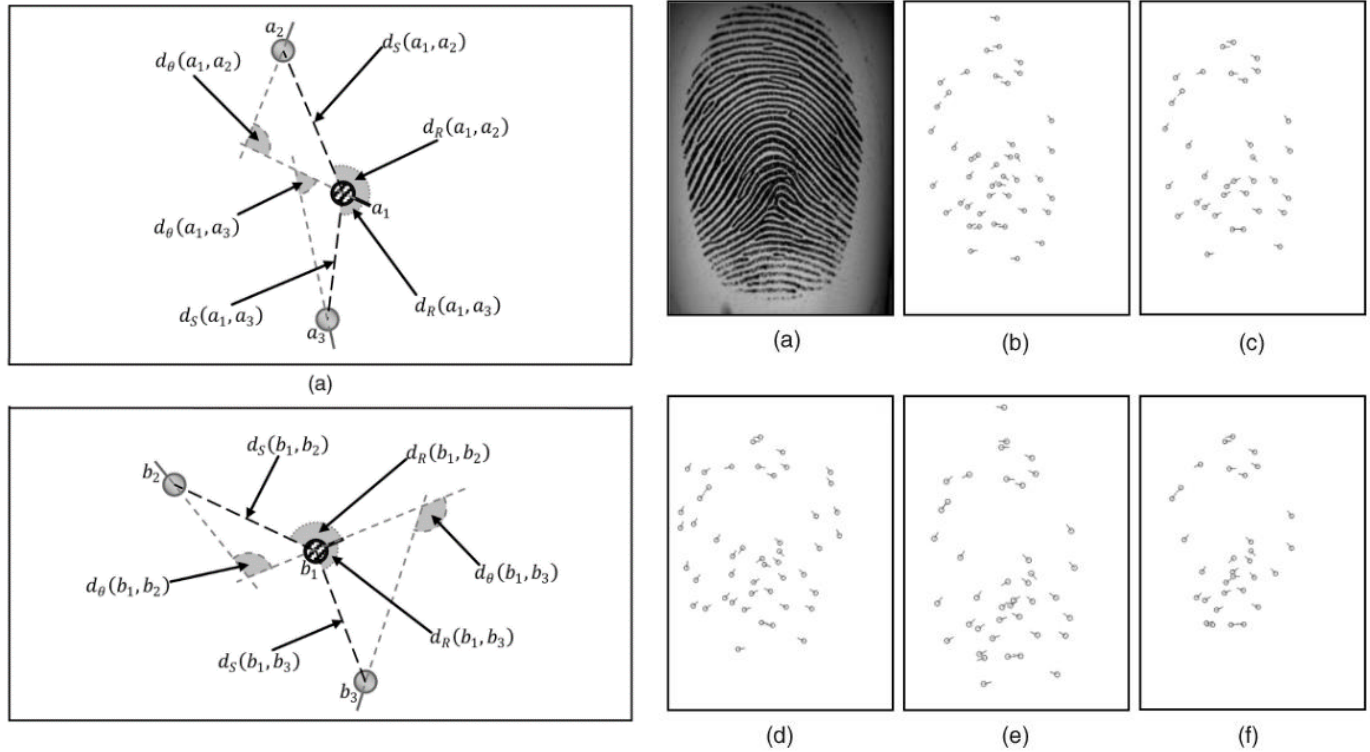


Рисунок 2.5 – Радіальні кути [7]

n_{rel} ітерацій процедури релаксації виконується на всіх n_R парах; тоді, ефективність пари t розраховується як:

$$\varepsilon_t = \frac{\lambda_t^{n_{rel}}}{\lambda_t^0}. \quad (2.33)$$

Судячи з попередньо описаної інформації, можна зробити висновок, що високої ефективності можливо досягти для тих пар мінуцій, подібність яких значно посилюється через високу сумісність з іншими парами, тоді як пари локальних структур, які спочатку випадково отримали високу подібність, будуть знижені, через це їх остаточний показник ефективності буде досить низьким.

Щоб визначити загальну оцінку, пари n_p , що мають найбільшу ефективність, вибирають з пар n_p . Глобальна оцінка обчислюється із використанням значень подібності $\lambda_t^{n_{rel}}$ замість значень у матриці Γ .

2.5 Експериментальна оцінка алгоритму

Для того, щоб оцінити точність і ефективність алгоритму циліндр-кодів, його розробниками було проведено експерименти, які виконують роль порівняння його конкретно з реалізаціями трьох добре відомих методів зіставлення локальних деталей [10], [11], [12].

Існувало декілька серій експериментів цього алгоритму. Перший з них був оснований п'яти наборах шаблонів даних відбитків пальців ISO/IEC 19794-2, і після цього ретельно оцінено. Як шаблон використовувався FVC2006 DB2 по тій причині, що його було створено із використанням оптичного датчика, що мав велику площу і достатньо високу якість, через що при результатах експерименту можна біло отримати велику кількість інформації. Кожен із використаних наборів даних містить 1680 шаблонів ISO/IEC 19794-2, що в свою чергу містить у собі 1680 відбитків пальців. Роздільна здатність при цьому - 250 точок на дюйм, при якій немає можливості вилучити усю інформацію про мінуції, що спонукає виникнення помилок у подальших діях і результатах, враховуючи не тільки алгоритм циліндр-кодів, але й інші методи, з якими він порівнюється. У всіх випадках кодування точок мінуцій відбувається при 500 dpi. Вчені (Jiang та Ratha) при проведенні експерименту не враховували таку інформацію про відбитки пальців, як кількість хребтів, тому що враховувались тільки важливі дані, що зазначені у документації ISO/IEC 19794-2. Мова, що використовувалась – C++. Кожну із шести метрик було об'єднано з кожним із алгоритмів глобальної оцінки, загалом - було отримано 24 наборів даних для перевірки.

У процесі тестування кожен із існуючих шаблонів порівнювався з рештою шаблонів відбитків пальців, у результаті було отримано коефіцієнт - FNMR. Для того, щоб отримати коефіцієнт помилкових збігів – FMR, було порівняно перші з кожних двох шаблонів відбитків пальців у наборі, що називається симетричним порівнянням. При цьому порівняння одних і тих самі шаблонів у зворотньому напрямку не виконується, щоб уникнути помилок. У результаті невдачі порівняння оцінка відповідності дорівнює 0.

Слід зазначити параметри, що враховувались для кожного шаблону при порівнянні для отримання оцінок ефективності:

- 1) Рівний рівень помилок (EER);
- 2) FMR (найнижчий FNMR для FMR 0:1%);
- 3) Середній час відповідності: Tcs - середній час створення локальних структур даних ISO/IEC 19794-2; Tls - середній час обчислення всіх локальних подібностей між локальними структурами з двох шаблонів; Tgs - середній час прорахування глобальної оцінки локальних подібностей;
- 4) Середній розмір пам'яті локальних структур (у байтах).

Загальний найкращий результат досягається за допомогою набору MCC16 із використанням техніки LSA-R, у наслідок чого MCC16 мав вірогідність зайняти 9 місце у рейтингу відкритої категорії FVC2006. Через те, що алгоритми FVC2006 враховує більшу кількість даних - поле орієнтації, щільність виступів тощо, його точність є значно високою.

На рисунку продемонстровано середнє значення EER за п'ятьма наборами даних DS2[a-e], кожен з яких має чотири методи глобальної оцінки.

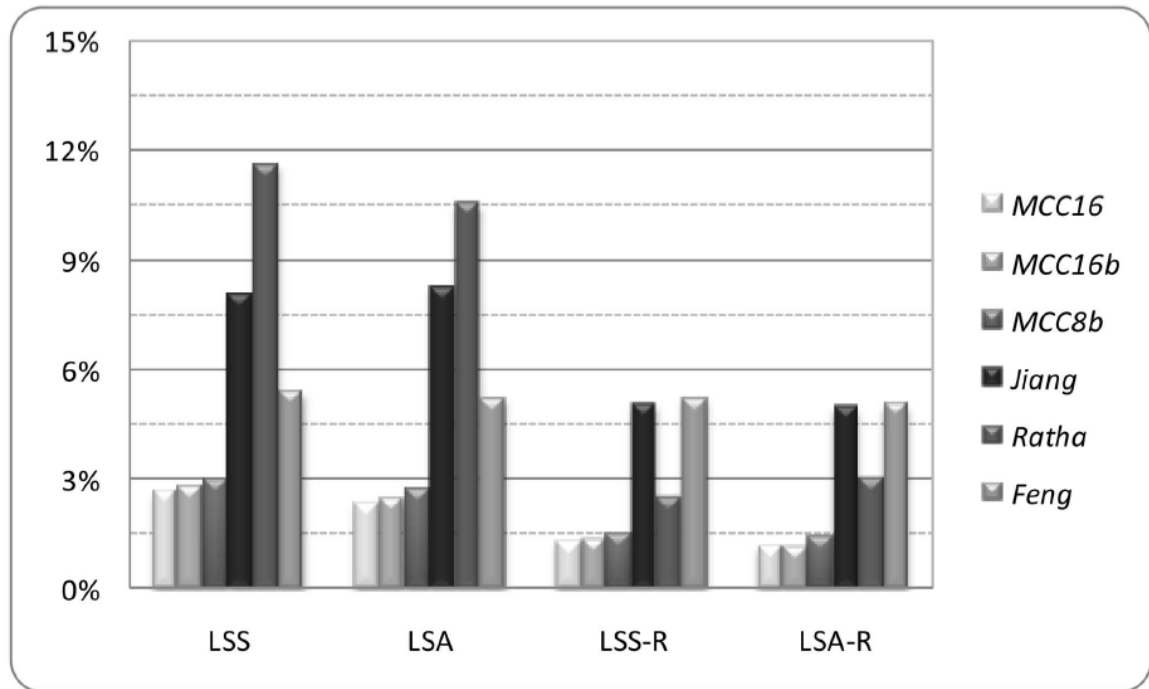


Рисунок 2.6 – Результати ефективності тестування кожного із наборів даних [7]

Перевага результатів за допомогою метрики циліндр-кодів дуже гарно видно на графіку, порівняно із іншими метриками, так як середній рівень помилок є нижчим за показники аналогічних алгоритмів.

Стосовно ефективності алгоритмів, при вимірюванні середнього часу, який необхідний метриці циліндр-кодів для того, щоб створити локальні структури з відповідного шаблону стандарту ISO/IEC 19794-2, він становить (T_{cs}) від 4,2 мс до 21 мс. Отриманий час виконання програми є більшим, порівняно з іншими алгоритмами, але це не є перешкодою до застосування метрики, так як вирішення відповідності циліндрів не потребують громіздких обчислень, і при цьому під час програмної реалізації «один до багатьох» набір циліндрів попередньо обчислюється лише один раз по відношенню до кожного шаблону, а не під час кожного порівняння.

Середній час, що необхідний для обчислення глобальної оцінки (T_{gs}) не має залежності від типу локального алгоритму зіставлення, скоріш за все це може

відбуватися через специфічний розподіл локальних подібностей, що було створено алгоритмами, що у середньому потребує меншої кількості ітерацій.

3 ОПИС ПРАКТИЧНОЇ РЕАЛІЗАЦІЇ АЛГОРИТМУ

Дана матриця q_1 , що створена у середовищі Mathcad, відображає кількість нерелевантних ділянок. Цей вид матриці відповідає параметру $Ns = 16$.

Надалі q_1 є основою доповнення до створення повної маски нерелевантних осередків. Розміри ділянок за основою $\Delta s := \frac{2 \cdot R}{Ns} = 8.75$.

$$q_1 := \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Рисунок 3.1 – Створена матриця

І за висотою, що дорівнює $\Delta d := \frac{2 \cdot \pi}{Nd} = 1.047$. Допоміжний кут опуклої оболонки буде дорівнювати $\gamma := \frac{\pi}{1000000}$ (Радіан).

Для того, щоб прочитати шаблон із даними відбитка пальця, він поміщується у змінну подвійного вкладеного вектора, що виглядає наступним чином: $Name1 := "Templ_TXT/"$.

Відбувається читання та перетворення файлу до потрібного вигляду.

```

Tem := || F ← floor (runif (150 , 0 , .01))
        || for i ∈ 0 .. 149
        || || Name ← concat (Name1 , num2str (i) , “_”)
        || || for j ∈ 0 .. 11
        || || || Name2 ← concat (Name , num2str (j) , “.txt”)
        || || || (Fi)j ← READFILE (Name2 , “delimited”)
        || F

```

Рисунок 3.2 – Функція перетворення файлу

Матриця із даними шаблону набуває наступного вигляду:

$$\left(Tem_0 \right)_0 = \begin{bmatrix} 0.576 & 73 & 354 \\ 0.576 & 85 & 213 \\ 0.384 & 85 & 378 \\ 0.192 & 87 & 432 \\ 0.384 & 94 & 289 \\ 5.288 & 98 & 95 \\ 3.142 & 106 & 110 \\ 4.904 & 112 & 35 \\ 1.763 & 113 & 26 \\ \vdots & & \end{bmatrix}$$

Рисунок 3.3 – Матриця із даними шаблону

```

DD := || for k ∈ 0 .. Nd − 1
        || || ck ← || for i ∈ 0 .. Ns − 1
        || || || for j ∈ 0 .. Ns − 1
        || || || || cci,j ← 0
        || || || cc
        || c

```

Рисунок 3.4 – Перетворення шаблону

Наступним кроком реалізації алгоритму є формування циліндрів кодів по черзі для всіх шаблонів. Для цього створюється змінна *NameCC* := “CC_DB2/”. Після цього

реалізується функція пошуку чергової вершини оболонки, та її побудова. Далі виконується функція визначення допустимих розташувань релевантних осередків, що має наступний вигляд:

$$\begin{array}{l}
 ab(xx) \leftarrow \left\| \begin{array}{l}
 w \leftarrow xx \\
 \text{for } ia \in 0 \dots \text{last}(xx^{(0)}) - 1 \\
 \left\| \begin{array}{l}
 ab_{ia,0} \leftarrow \frac{w_{ia,1} \cdot w_{ia+1,0} - w_{ia+1,1} \cdot w_{ia,0}}{w_{ia+1,0} - w_{ia,0}} \\
 ab_{ia,1} \leftarrow \frac{w_{ia+1,1} - w_{ia,1}}{w_{ia+1,0} - w_{ia,0}}
 \end{array} \right\| \\
 ab
 \end{array} \right.
 \end{array}$$

Рисунок 3.5 - Визначення допустимих розташувань

Обчислюється та формується матриці ab коефіцієнтів рівнянь прямих ліній, що є кордонами опуклої оболонки.

Далі необхідним є побудова функції, що необхідна для сигмоподібних оцінок числових значень осередків. При цьому, ми можемо бачити центрований гауссіан $Gs(t)$, звичайний сигмоїд $Z(v)$, бінаризуючий сигмоїд $Zb(v)$, одновимірний масив кутів $d\varphi$, асоційованих з кожним із шарів осередків, що є вектором, та інтеграл від гауссіана - $Gs(\alpha)$.

$$\begin{aligned}
Gs(t) &\leftarrow \text{dnorm}(t, 0, \sigma s) \\
Z(v) &\leftarrow \frac{1}{1 + \exp(-\tau \Psi \cdot (v - \mu \Psi))} \\
Zb(v) &\leftarrow \text{if } v \geq \mu \Psi \begin{cases} 1 \\ \text{else} \\ 0 \end{cases} \\
d\varphi &\leftarrow \begin{cases} \text{for } k \in 0 \dots Nd - 1 \\ \quad \begin{cases} d\varphi_k \leftarrow -\pi + (k + 0.5) \cdot \Delta d \end{cases} \\ d\varphi \end{cases} \\
Gd(\alpha) &\leftarrow \int_{\alpha - \frac{\Delta d}{2}}^{\alpha + \frac{\Delta d}{2}} \text{dnorm}(t, 0, \sigma d) dt
\end{aligned}$$

Рисунок 3.6 – Функція оцінки осередків

Після цього виконується саме формування циліндр-кодів. Першим кроком для цього є формування функції обчислення ділянок мінуції циліндра, що має номер *mit*.

Розглянемо наступні дві функції. Функція валідації довільної точки *M*, що повертає "1", якщо точка *M* знаходиться всередині розширеної ConvexHull опуклої оболонки, і "0" у протилежному випадку.

$$Valid(M, yy) \leftarrow \begin{cases} F \leftarrow 1 \\ \text{for } k \in 0 \dots \text{last}(yy^{(0)}) \\ \quad \begin{cases} \text{if } z_k \cdot M_{0,1} < z_k \cdot (yy_{k,0} + yy_{k,1} \cdot M_{0,0}) \\ \quad F \leftarrow 0 \end{cases} \\ F \end{cases}$$

Рисунок 3.7 – Функція валідації точки

Друга функція – обчислення координат центрів осередків з урахуванням розвороту кубоїду.

$$P(M0, \theta0) \leftarrow \begin{array}{|l} \text{for } k \in 0 \dots Ns - 1 \\ \quad \text{for } m \in 0 \dots Ns - 1 \\ \qquad q_{k,m} \leftarrow M0 + \Delta s \cdot \begin{bmatrix} \cos(\theta0) & -\sin(\theta0) \\ \sin(\theta0) & \cos(\theta0) \end{bmatrix} \cdot \begin{bmatrix} m - \frac{Ns-1}{2} \\ \frac{Ns-1}{2} - k \end{bmatrix} \\ \qquad q \end{array}$$

Рисунок 3.8 – Обчислення координат

Наступний крок - підготовка структури кубоїду. Можна побачити, що відбувається завантаження координат мінуції *num* та перевірка валідності циліндра в умові.

$$Cc(num) \leftarrow \begin{array}{|l} Cc \leftarrow DD \\ xy0 \leftarrow \begin{bmatrix} T_{num,1} \\ T_{num,2} \end{bmatrix} \\ count0 \leftarrow 0 \\ \text{for } k \in 0 \dots \text{last}(T^{(0)}) \\ \quad \text{if } k = num \\ \quad \quad \text{continue} \\ \quad \text{else if } \left| xy0 - \begin{bmatrix} T_{k,1} \\ T_{k,2} \end{bmatrix} \right| \leq R + 3 \cdot \sigma s \\ \quad \quad \quad count0 \leftarrow count0 + 1 \\ \text{if } count0 < minM \\ \quad \text{return "invalid"} \end{array}$$

Рисунок 3.9 – Перевірка валідності циліндра

У наступній функції виконується обчислення координат центрів осередків при повороті, формування повної маски валідних (релевантних) осередків, та виконується перевірка валідності за кількістю релевантних осередків.

```

p ← P  $\left( \begin{bmatrix} T_{num,1} \\ T_{num,2} \end{bmatrix}, T_{num,0} \right)$ 
q_2 ← for k ∈ 0 .. Ns - 1
      for m ∈ 0 .. Ns - 1
        q_{k,m} ← q_{-1_{k,m}} • Valid(p_{k,m}^T, ab(xyCH_{over}))
      q
if  $\sum_{jj=0}^{Ns-1} |q_{-2}^{(jj)}|^2 < 152$ 
  return "invalid"

```

Рисунок 3.10 – Обчислення координат

Для того, щоб реалізувати метрику далі, необхідно виконати кроки обчислення просторового, дирекційного та повного числових вкладів у осередок, і в решті-решт сформувати циліндр для даної мінуції, записати отримані файли та провести контрольне читання.

Також, після цього, корисним буде провести експериментальне дослідження показників ефективності FAR та FRR, а саме порівняти циліндри з перевіркою всіх умов взаємної сумісності та вичислити показники кореляційної схожості двох циліндрів.

Отже, можна зазначити, що до переваг метрики циліндр-кодів можна віднести те, що:

- 1) Вона є стійкою до повороту або зсуву зображення через кодування лише взаємно залежних дистанцій та дирекційних відмінностей кутів мінуцій, що розташовані поряд.
- 2) Є незмінною щодо незначних спотворень малюнка на локальному рівні, що відбувається по тій причині, що існують властивості злагодження гауссових вагових функцій.

- 3) Якщо розглядати паралелепіпед, у який було вписано локальну структуру – циліндр, то в його обсязі в результаті отримуються вектори числових кодів, що мають незмінну довжину, рівну кількості релевантних та нерелевантних ділянок.

Недоліки, що можна віднести до алгоритму циліндр-кодів:

- 1) Обчислення можуть виявитись дуже громіздкими та мати багато опису, що відбувається у перу чергу по причині циліндра, що було обрано у якості геометричного примітиву.
- 2) Поки немає удосконалення методу глобальної оцінки алгоритму, а також існує його неоднозначність.
- 3) Алгоритм містить у собі велику кількість елементів, які не містять у собі інформації в складі нерелевантних ділянок, та ділянок, що не було розглянуто у процесі реалізації умови порівняння. Даний фактор зменшує чутливість до знаходження схожостей та відмінностей тих шаблонів, що порівнюються між собою.

ВИСНОВКИ

На сьогоднішній день технологічний прогрес в інформаційних технологіях набув своїх обертів, тому існує безліч систем біометричної ідентифікації людини, що мають різні принципи роботи та відрізняються ціновим діапазоном та показниками параметрів, що вимірюють стійкість до злому. Дуже важливим є тип використання біометричних даних людини. Біометричні системи відрізняються за даними, що використовують під час автентифікації, це можуть бути як відбитки пальців, так і геометрія судин долоні, сітківка ока, голос або підпис. При цьому використання цих типів може поєднуватися одночасно. В даній роботі увагу було приділено саме автентифікації за відбитком пальця людини, так як він є найпопулярнішим в інформаційному просторі у різних сферах діяльності, у тому числі й повсякденному житті людини, комфортним при використанні, і тому потребує подальших досліджень, удосконалення і створення нових алгоритмів його роботи.

Розглянутий алгоритм верифікації відбитків на основі циліндр є технікою, що представляє лише мінуції – точок відбитків пальців - та їх зіставлення для розпізнавання відбитків пальців. Вона оснований на надійності дискретизації границь кожної мінуції в тривимірну структуру, що являє собою циліндр, і складається з комірок. Для того, щоб відрізнити два відбитка пальця, використовувались прості в обчисленні, але при цьому ефективні методи консолідації схожості між собою циліндрів. Було розглянуто порівняння алгоритму циліндр-кодів із трьома схожими підходами, проаналізовано отримані результати експериментів (понад дев'ять мільйонів спроб зіставлення).

Як висновок, можна стверджувати, що експериментальні результати дослідженого алгоритму циліндр-кодів демонструють більшу точність розпізнавання,

ніж добре відомі методи локального зіставлення лише мінуцій, також демонструє достатньо високу швидкість роботи і підходить для використання при кодуванні апаратного забезпечення побітно. Можна сказати, що особливості метрики циліндр-кодів також надають можливість розробки у подальшому нових ефективних методів розпізнавання відбитків пальців та захисту шаблонів, що є головними задачами при її удосконаленні у майбутньому.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

- 1 Генетичне підґрунтя відбитка пальців. URL: <https://zbruc.eu> (дата звернення: 02.11.2022).
- 2 Відбиток пальця. URL: <https://uk.wikipedia.org> (дата звернення: 08.11.2022).
- 3 Thales Cogent Fingerprint Scanners: what they are and how they work. URL: <https://www.thalesgroup.com> (дата звернення: 02.11.2022).
- 4 Phone's Fingerprint Sensor. URL: <https://www.reliancedigital.in> (дата звернення: 28.10.2022).
- 5 Як змінити відбитки пальців і чи це можливо. URL: <https://bigbro.com.ua> (дата звернення: 03.11.2022).
- 6 Feng J. Combining Minutiae Descriptors for Fingerprint Matching: Pattern Recognition. 2008. Vol. 41. P. 342-352.
- 7 Cappelli R., Ferrara M., Maltoni D. Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition. December 2010. Vol. 32. P. 2128-2141.
- 8 Data Format for the Interchange of Extended Fingerprint and Palmprint Features: Addendum to ANSI/NIST-ITL 1-2007. ANSI/NIST, Working Draft 0.2. 2008.
- 9 INCITS 378-2004: Finger Minutiae Format for Data Interchange. ANSI/INCITS Standard. 2004.
- 10 Jiang X., Yau W. Y. Fingerprint Minutiae Matching Based on the Local and Global Structures. 2000. Vol. 2. P. 6038-6041.
- 11 Ratha N. K., Pandit V.D., Bolle R.W. Robust Fingerprint Authentication Using Local Structural Similarity. 2000. P. 29-34.

- 12 Feng J. Combining Minutiae Descriptors for Fingerprint Matching. 2008. Vol. 41. P. 342-352.
- 13 Фен Д., Цай А. Індексуювання відбитків пальців з впровадженням інваріантів хребта. 2006.
- 14 International biometrics and identity association. URL: www.ibia.org (дата звернення: 13.11.2022).
- 15 ISO/IEC 19794-2:2005. Information Technology: Biometric Data Interchange Formats. 2005. Part 2: Finger Minutiae Data.
- 16 James W. Yang A. Dab Fingerprint Verification System Based on Classical Methods.
- 17 Sha L., Zhao F., Tang X. Minutiae-Based Fingerprint Matching Using Subset Combination. 2006. P. 566-569.
- 18 Handbook of Fingerprint Recognition / Maltoni D. and others. 2009.
- 19 Hrechak A. K., McHugh J. A. Automated Fingerprint Recognition Using Structural Matching: Pattern Recognition. 1990. Vol. 23. P. 893-904.
- 20 Biometric terminals add security to a variety of processes. URL: www.bioscrypt.com (дата звернення: 05.10.2022).
- 21 Шрамко В. Н. Захист комп'ютерів: електронні системи ідентифікації та аутентифікації. 2004.
- 22 Системи ідентифікації. URL: www.acoder.org (дата звернення: 07.11.2022).