Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

Многомодальна біометрична верифікація за структурою райдужної оболонки ока і відбитку пальця
(тема)

Виконав: Чурсінов Д. Г.
(прізвище, ініціали)
студент 2 курсу, групи БДІРм 19-1
Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва освітньої програми)

Керівник доцент Гріненко Т. О.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Халімов Г.З.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Комп'ютерної інженерії та управління
(повна назва)

Кафедра Безпеки інформаційних технологій
(повна назва)

Рівень вищої освіти другий (магістерський)

Спеціальність 125 Кібербезпека
(код і повна назва)

Тип програми освітньо-професійна
(освітньо-професійна, або освітньо-наукова)

Освітня програма «Безпека державних інформаційних ресурсів»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2020 р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентові *Чурсінову Данилу Геннадійовичу*
(прізвище, ім'я, по батькові)

1. Тема роботи *Многомодальна біометрична верифікація за структурою райдужної оболонки ока і відбитку пальця*
затверджена наказом по університету від "22" жовтня 2020 р. № 1413Ст
2. Термін подання студентом роботи (проекту) 11.12.2020
3. Вихідні дані до роботи (проекту) стандарти, щодо безпеки алгоритмів біометричних систем верифікації, дослідження сучасних засобів захисту біометричних систем, мова програмування – Python, програмні бібліотеки: opencv, pillow.
4. Зміст пояснювальної записки (перелік питань, що потрібно розробити)
1. Порівняльний аналіз біометричних систем верифікації.
2. Біометрична система верифікації людини на основі структури райдужної оболонки ока.
3. Біометрична система верифікації людини на основі відбитків пальців.
4. Розробка моделі мультимодальної біометричної системи верифікації людини.
5. Розробка та опис програмного забезпечення, що реалізує розроблену модель.
5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій *Презентаційний матеріал у вигляді слайдів*
6. Основна література та джерела: ДСТУ ISO/IEC 9798-3:2002 Інформаційні технології. Методи захисту. Автентифікація суб'єктів. Частина 3. Механізми з використанням методу цифрового підпису, ДСТУ ISO 7498-2:2004 Системи оброблення інформації. Взаємозв'язок відкритих систем базова еталонна модель. Частина 2. Архітектура захисту інформації, Anil K. Jain, Karthik Nandakumar and Arun Ross, "50 years of biometric research, Accomplishments, Challenges and Opportunities", 2016, vol.79, pp.80-105.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів магістерської атестаційної роботи	Термін виконання етапів роботи	Примітка
1	*Отримання завдання*	*25.09.20*	
2	*Аналіз літературних джерел за темою атестаційної роботи*	*25.09.20-28.09.20*	
3	*Порівняльний аналіз біометричних систем та їх вразливостей*	*28.09.20-15.10.20*	
4	*Аналіз методів обробки зображень та алгоритмів роботи біометрії за райдужкою та відбитком пальця*	*15.10.20-11.11.20*	
5	*Розробка моделі мультимодальної системи верифікації та її програмної реалізації*	*11.11. 20-25.11. 20*	
6	*Оформлення пояснювальної записки*	*25.11. 20-04.12. 20*	
7	*Представлення роботи на перевірку*	*11.12.2020*	

Дата видачі завдання _25_ ___вересня___2020 р.

Студент _____
(підпис)

Керівник роботи (проекту) _____ __доцент Гріненко Т. О._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка про бакалаврську атестаційну роботу: 98 с., 35 рис., 5 табл., 2 дод., 7 джерел.

АВТЕНТИФІКАЦІЯ, БІОМЕТРИЧНА ВЕРИФІКАЦІЯ ОСОБИ, ВІДБИТОК ПАЛЬЦЯ, РАЙДУЖНА ОБОЛОНКА ОКА, ОБРОБКА ЗОБРАЖЕННЯ, ІДЕНТИФІКАЦІЯ, СКЕЛЕТИЗАЦІЯ, СЕГМЕНТАЦІЯ, ОСОБЛИВА ТОЧКИ, НОРМАЛІЗАЦІЯ.

Об’єкт дослідження – верифікація особи за структурою райдужної оболонки ока та відбитком пальця.

Предмет дослідження – мультимодальна біометрична система верифікації зображень райдужної оболонки ока та відбитка пальця.

Мета роботи – ознайомлення з основними принципами щодо верифікації зображень райдужної оболонки та відбитків пальця, аналіз основних методів верифікації та обробки зображень райдужної оболонки та відбитків пальця для подальшого їх порівняння з еталоном, надання пропозицій щодо застосування цих методів у процесі автентифікації, розробка рекомендацій для підвищення безпеки біометричних технологій, розробка моделі мультимодальної біометричної системи верифікації та реалізація програмного забезпечення відносно розробленої моделі.

Методи дослідження – аналіз існуючих алгоритмів роботи біометричних систем автентифікації, порівняння алгоритмів обробки зображень біометричних характеристик людини, розробка алгоритму мультимодальної біометричної системи верифікації за зображеннями райдужної оболонки ока та відбитка пальця.

Наведено результати порівняльного аналізу найпоширеніших біометричних систем автентифікації, алгоритмів та методів роботи систем на основі відбитків пальців та зображень структури райдужної оболонки ока, що є найбільш надійними з поширених біометричних систем. Виділені переваги та недоліки існуючих біометричних технологій, проблеми, які виникають на етапах роботи цих систем та розроблені рекомендації для підвищення безпеки вказаних біометричних технологій. Розроблена модель мультимодальної біометричної системи верифікації людини, надана функціональна характеристика та проведений аналіз прогнозованих переваг та недоліків розробленої моделі, а також реалізоване програмне забезпечення для здійснення верифікації за структурою райдужної оболонки ока та відбитком пальця.

ABSTRACT

Attestation work contains: 98 p., 35 fig., 5 tab., 2 applications, 7 sources.

AUTHENTICATION, BIOMETRIC PERSONAL VERIFICATION, FINGERPRINT, IRIS, IMAGE PROCESSING, IDENTIFICATION, SKELETIZATION, SEGMENTATION, SPECIAL POINTS, NORMALIZATION.

Object of research – verification of the face by the structure of the iris and fingerprint.

Subject of research – multimodal biometric system for verification of iris and fingerprint images.

Purpose of the work – acquaintance with the basic principles of verification of iris images and fingerprints, analysis of basic methods of verification and processing of images of the iris and fingerprints for further comparison with the standard, providing proposals for the use of these methods in the authentication process, development of recommendations for biometric security, development of a model of a multimodal biometric verification system and implementation of software relative to the developed model.

Research methods – analysis of existing algorithms of biometric authentication systems, comparison of algorithms for image processing of human biometric characteristics, development of an algorithm for a multimodal biometric verification system based on images of the iris and fingerprint.

The results of comparative analysis of the most common biometric authentication systems, algorithms and methods of operation of systems based on fingerprints and images of the structure of the iris, which are the most reliable of the common biometric systems. The advantages and disadvantages of existing biometric technologies, the problems that arise during the operation of these systems and developed recommendations to improve the security of these biometric technologies. A model of a multimodal biometric human verification system has been developed, a functional characteristic and an analysis of the predicted advantages and disadvantages of the developed model have been provided, as well as software for verification of iris structure and fingerprint has been implemented.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАК, ОДИНИЦЮ І ТЕРМІНІВ

BMP – Bitmap Picture;

CASIA – Chinese Academy of Sciences;

CER – Crossover error rate;

DPI – Dots Per Inch;

FAR – False Acceptance Rate;

FRR – False Rejection Rate;

FTE – Failure enroll rate;

IAFIS – Integrated Automated Fingerprint Identification System;

PIL – Python Imaging Library;

PIN – Personal Identification Number;

QR – Quick Response code;

SIFT – Scale-invariant feature transform;

БД – база даних;

ЕОМ – електронна обчислювальна машина;

ІГ – ієрархія гаусинів;

КМОП – комплементарний метал-оксид-напівпровідник;

ПЗ – програмне забезпечення;

РГ – різниця гаусинів;

ВСТУП

У наш час паролі, коди, ідентифікаційні номери стали життєвою необхідністю. Наприклад, щоб отримати готівку з банкомату, вам потрібно вводити PIN-код, щоб отримати доступ до вашого поштового сервісу або до мобільного телефону, необхідний пароль. У світлі останніх подій, що відбуваються у світі, особливо в зв'язку з ростом розвитку комп'ютерних технологій, питанням безпеки приділяється все більше уваги.

Таким чином, людина повинна зберігати у своїй пам'яті безліч різних комбінацій цифр та літер. Щоб полегшити цей процес, компанії, що спеціалізуються на виробництві сучасних технологій та комп'ютерних сервісів, почали займатися розробкою біометричних технологій. Біометрія – це наука, що вивчає можливості використання різних характеристик людського тіла для ідентифікації кожної конкретної людини. Протягом останніх років використання біометричних технологій привернуло до себе дуже велику увагу. Переваги – простота у використанні, зручність та надійність.[5]

Біометричні технології можуть бути використані для ідентифікації людей шляхом поєднання фізіологічних або поведінкових особливостей людини з інформацією, яка описує суб'єкта. Втратити або забути біометричні дані практично неможливо, оскільки вони є невід'ємною частиною кожної людини, і це перевага, яку вони отримують над ключами, паролями або кодами. Біометричні технології, які включають, серед іншого, обличчя, голос, розпізнавання відбитків пальців, рук та райдужки є основним компонентом біометричних систем.

Однак біометричні технології все ще значною мірою розробляються, незважаючи на той факт, що вони використовувались у різних додатках протягом останніх 40 років. Крім того, біометричні системи складають лише частину системи верифікації. Проблема полягає в тому, що системи, мають необхідність адекватного захисту. В даний час не вистачає даних та досліджень, які головним чином відносяться до широкомасштабного впровадження біометричних ідентифікаторів, включаючи їх використання у різних сферах життя людини. Також варто зазначити, що біометричні системи не дають 100%-вий результат роботи, а це призводить до постійного питання поліпшення алгоритмів, які використовуються для верифікації.

Мета атестаційної роботи полягає у вирішенні проблем помилкових результатів роботи біометричних систем та поліпшенні безпеки інформації, яка захищена вище вказаними системами. Для вирішення поставлених проблем пропонується використовувати мультимодальні системи біометричної верифікації.

Мультимодальна або багатофакторна біометрія – це процес верифікації або ідентифікації людини для якого використовуються декілька біометричних характеристик, наприклад, відбиток пальця та структура райдужної оболонки ока. Мультимодальні системи мінімізують вірогідність несанкціонованого доступу до даних та значно полегшують процес верифікації для користувачів.

При використанні біометрії, як засобу верифікації, необхідно постійно використовувати додаткові паролі, які можуть бути використані у випадку, якщо людина не має можливості пред'явити ту, чи іншу біометричну характеристику. Якщо мультимодальна система біометричної верифікації буде реалізована послідовно, замість додаткових паролів можливо використовувати інший варіант біометрії, це значно пришвидшить процес верифікації користувача. У системах, де велику роль відіграє точність верифікації, можливо використовувати багатомодульні біометричні системи з паралельною реалізацією. У таких випадках прийняття рішення системою, будується одноразово на основі двох ключових шаблонів отриманих від користувача. Також, даний вид систем, унеможливлює несанкціонований доступ злодія, який заволодів або підробив ту, чи іншу біометричну характеристику власника.[3]

З темпами розвитку біометрії, можна зробити висновок, що мультимодальні системи біометричної верифікації є дуже перспективним напрямком роботи. У найближчому майбутньому дані системи змінять існуючу біометрію на основі однієї з характеристик людини.

1 АНАЛІЗ БІОМЕТРИЧНИХ СИСТЕМ ВЕРИФІКАЦІЇ

Біометричні дані – це фізичні або біологічні характеристики або атрибути, які можна виміряти. Їх можна використовувати як засіб доказу того, що ви є тим, за кого себе видаєте, або як засіб доказу, без розкриття вашої особистості, що у вас є певне право (наприклад, доступ до системи), так само, як PIN-код (особистий ідентифікаційний номер) або пароль. Вирішальна різниця в тому, що біометричні дані є частиною вас, а не те, що ви знаєте або можете забрати з собою.[4]

Фізіологічні біометричні характеристики включають зріст, вагу, запах тіла, форму руки, візерунок вен, сітківку або райдужну оболонку ока, обличчя, візерунки на шкірі, пальці або відбитки пальців. Приклади поведінкової біометрії - голос, хода, інтенсивність набору даних на клавіатурі та інше (див. рисунок 1.1).

Рисунок 1.1 – Фізіологічні та поведінкові характеристики біометрії

Хоча іноді стверджують, що ДНК не слід класифікувати, як біометричну характеристику, оскільки воно не спостерігається зовні, для цілей наукових

досліджень ДНК вважається біометричної характеристикою, оскільки це властивість тіла, яке можна використовувати для ідентифікації та перевірки.

Біометричні характеристики вважаються «відмінними». Біометричні дані залежать від методу, який використовується для його вимірювання і процесу, за допомогою якого дві однакові біометрії збігаються. Таким чином, немає біометричної характеристики, в якій процес відбору відмінних даних відтворюється ідентично. Біометричні характеристики можна враховувати, як міст, який з'єднує ідентифікаційний запис і особу, якій цей запис належить. Таким чином він встановлює «надійний» метод для зв'язку збереженої ідентичності з фізичною особою, яку вона представляє. Цей тип біометричної перевірки особистості розповсюджений і необхідний в багатьох випадках.

1.1 Загальні відомості про біометричні технології

Ключова відмінність біометрії від інших цифрових ідентифікаторів, таких як паролі, PIN-коди або ключові карти – це те, що біометричні дані не можна втратити або забути; в біометрії характеристики вимірювання є частиною тіла або поведінки людини, вони завжди будуть присутні при необхідності. Причому процес ідентифікації автоматизований або є напівавтоматичним. У деяких випадках ця автоматизація імітує те, що люди роблять в повсякденному житті (поведінку або голос), але для більшості технологій автоматизація необхідна, тому що люди самі по собі не змогли б розрізняти більшість з вище представлених характеристик (розпізнавання райдужної оболонки ока, відбитків, геометрії руки та інше).[3]

Біометрична ідентифікація – це статистичний процес. Варіації умов між реєстрацією і автентифікацією, а також тілесні зміни (тимчасові або постійні) означають, що ніколи не буває 100% -го збігу. Для пароля або ПІН-коду варіанта відповіді завжди два, якщо він точно такий же, як був збережений – це позитивна відповідь, якщо відрізняється – запит буде відхиллено, для біометричних даних немає чіткої межі між збігом і розбіжністю. Отже, чи існує збіг, залежить не тільки від двох наборів даних для порівняння, а також те, яка похибка вважається допустимою. Ймовірність збігу 90% може або не може вважатися прийнятною, це залежить від реалізації і вимог безпеки.

Внаслідок такого, статистичні біометричні системи ніколи не є точними на 100%. Можливі два види помилок біометричних систем: помилкові збіги (FAR) і помилкові відмови (FRR). Хибний збіг відбувається, коли отриманий шаблон ключів помилково відповідає шаблону, збереженому при реєстрації, хоча ці два шаблони взяті у двох різних людей. Хибні відмови відбуваються, коли отриманий шаблон не оцінюється, як відповідність шаблону, збереженому при реєстрації, хоча обидва з них мають приналежність до однієї людини. Ці

коефіцієнти помилок варіюються від однієї біометричної технології до іншої, і залежать від налаштування порога рішень. Якщо виставлений поріг в 99% система буде мати більшу кількість помилкових відмов і мінімальну помилкових збігів і так далі. Тому будь-який біометричний додаток повинен передбачати резервну процедуру для вирішення цих помилок.

Резервні процедури в рівній мірі необхідні для людей, які зазнають труднощів з наданням будь-яких біометричних даних. Це може бути що завгодно, наприклад людина з забинтованим пальцем або обличчям. Отже, резервні процедури будуть необхідні, щоб впоратися з різноманітними видами таких проблем.

Другий момент, про який варто згадати, полягає в тому, що самі біологічні дані, так звані зразки, як правило вони не зберігаються в системі біометричної верифікації у вигляді зображень. Зображення райдужної оболонки ока, відбитків пальців або обличчя перетворюються математичним шляхом за допомогою різних алгоритмів. Результат роботи алгоритму зберігається в файлах фіксованого формату, так званих шаблонах.

Використання біометричних алгоритмів полегшують постійне порівняння характеристик витягнутих під час реєстрації. Алгоритми різні для кожної технології та до недавнього часу ця процедура вважалася незворотною, тобто неможливо з шаблону відтворити зразок, який був його джерелом.

Ще одна перевага використання алгоритмів створення шаблонів полягає в тому, що новий або вихідний шаблон може бути легко відтвореним його власником, якщо раніше створений шаблон був вкрадений і використовувався третьою особою, ваш відбиток залишається при вас і процес створення нового шаблону не є проблемою. Але ця перевага одночасно є і недоліком, це описується в другому розділі атестаційної роботи.

Типи біометричних додатків. З функціональної точки зору поточне використання біометрії можна віднести до двох категорій: верифікація та ідентифікація.

Верифікація (відповідність один до одного) – це перевірка, щоб переконатися, що людина, яка відправила запит дійсно та, правами якого вона дійсно хоче скористатися. Можливо передбачити два типи перевірки: з централізованим сховищем або розподіленим:

– перевірка з централізованим сховищем являє собою централізовану базу даних. База (створюється один раз при реєстрації і оновлюється з кожним додатковим користувачем), де зберігаються всі біометричні дані і пов'язані з ними ідентифікаційні дані, біометричний зразок заявленої особистості витягується з бази даних;

– верифікація з розподіленим сховищем визначає те, що біометричні дані зберігаються в пристрої, що запам'ятовує, яке належить людині, наприклад, смарт-карта або чіп, інтегрований в документ, що засвідчує особу.

Ідентифікація (відповідність "один до багатьох") використовується, щоб розкрити особистість людини, коли вона невідома (користувач не претендує на особистість). На відміну від верифікації, для процесу ідентифікації необхідна тільки центральна база даних, в якій зберігаються записи для всіх людей, відомих системі; без центральної бази даних, процес ідентифікації неможливий. Коли особистість розпізнається, вона надає живий біометричний зразок, наприклад знімається відбиток пальця або сканується райдужна оболонка ока. Дані обробляються, і в результаті отримання біометричного шаблону порівнюється з усіма записами в базі даних, щоб знайти збіг (або список можливих збігів). Потім система повертає в якості відповіді або збіг (або список можливих збігів), який вона знайшла, чи не відповідність до жодного. Ідентифікація, як і верифікація також може привести до одного з двох типів помилок описаних вище.

1.2 Порівняльний аналіз біометричних систем

Всі біометричні технології, мають ряд переваг і недоліків, які роблять їх більш-менш придатними для конкретних додатків. На сьогоднішній день ринок біометричних технологій досить різноманітний (див. рисунок 1.2).

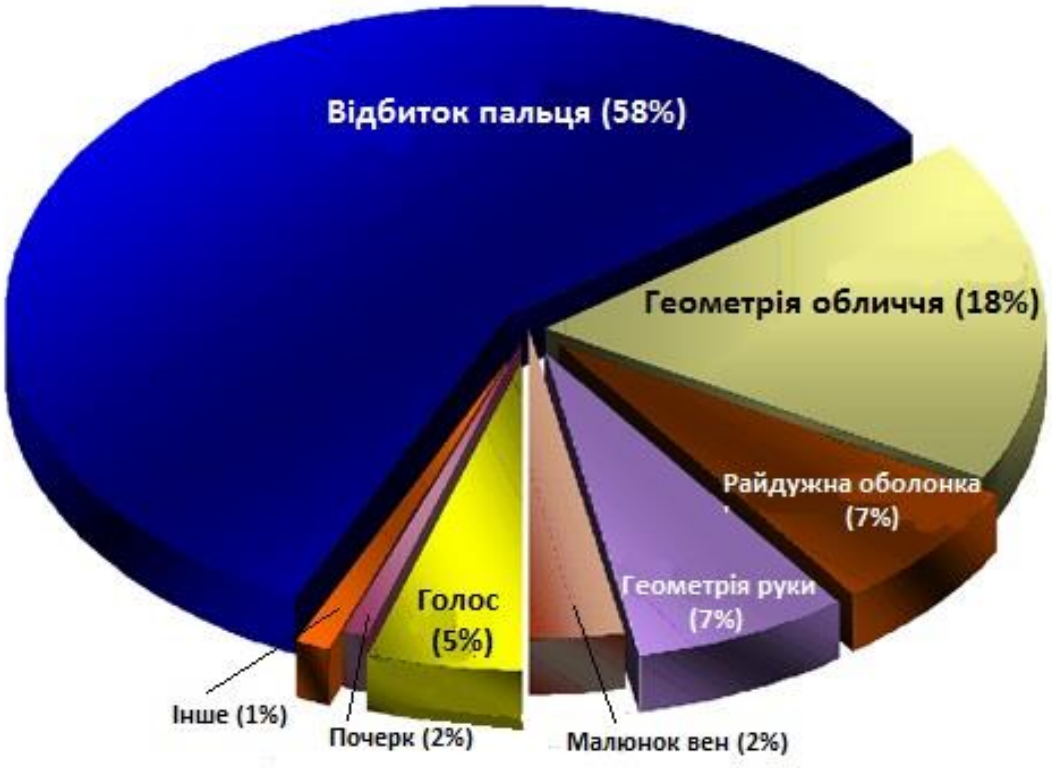

Рисунок 1.2 – Ринок біометричних технологій

Порівняння технологій, поза контекстом, будь то продуктивність, зручність використання або будь-які інші.[7]
критерії вводить в оману, оскільки воно неправильно відображає результат для конкретних цілей. Однак, маючи огляд ймовірних переваг або обмежень по кожній технології можна зробити висновки про те, які програми можуть використовувати ті чи інші варіанти біометрії або які мультимодальні комбінації краще працюють в системах доступу (див. рисунок 1.2). Також можна визначити конкретні налаштування, наприклад, поріг порівняння, для кожної з систем. Кращий спосіб домогтися цього - порівняти варіанти біометрії по всім самим розповсюдженим критеріям порівняння.

Різні методи біометрії мають свої особливості. В ході аналізу літератури можна підсумувати переваги і недоліки пов'язані з кожним методом (див. таблицю 1.1). Залежно від цих особливостей можна прийняти рішення про використання конкретного виду системи в конкретному додатку.

Таблиця 1.1 – Порівняння біометричних характеристик для автентифікації за їх перевагами та недоліками.

Назва х-ки	Переваги	Недоліки
Райдужна оболонка ока	–Висока точність (візерунок райдужки відповідає 1-му з 10-ти мільярдів людей). –На точність не впливає носіння окулярів або контактних лінз. –Відсутність фізичного контакту з системою. –Невеликий розмір шаблону. –Перспективна швидкість обробки (від 2-х до 5-ти секунд). –Мінімальний коефіцієнт помилкового прийняття. –Залишається стабільною впродовж життя. –Високо захищена і має високий ступінь випадковості.	–Сканер повинен видавати якісні зображення. –Потрібна співпраця користувача для точного сканування. –Менша зручність у використанні, користувач повинен тримати камеру нерухомо під час сканування. –Повинно бути гарне освітлення. –Можуть заважати повіки або зіниці. –Неточності на великій відстані сканування. –Захворювання очей, можуть також давати помилкові результати. –Висока якість зображення.

Продовження таблиці 1.1

Відбиток пальця	–Зручний у зчитуванні. –Простий у використанні та має невеликий розмір шаблону. –Висока унікальність. –Досить дешева технологія. –Швидкість сканування та обробки. –Досить проста обчислювальна складність.	–На результат впливає вологість шкіри або її текстура. –Фізичний контакт з системою –Незручність взимку під час носіння рукавиць, або для жінок з довгими нігтями. –Травми рук можуть запобігти роботі системи.
Сітківка ока	–Не можливо підробити. –Дуже надійна, оскільки немає двох людей з однаковим візерунком сітківки. –Частота помилок – 1 на 10 000 000 (практично 0%). –Високоточна технологія. –Забезпечує найбільшу безпеку в автентифікації.	-Не дуже зручна перевірка для користувача. -Такі захворювання, як катаракта, глаукома, діабет тощо, впливають на точність результатів. -Реєстрація та сканування повільні. -Обмежене використання. -Висока ціна технології. -Людина повинна знаходитись дуже близько до сканера.
Будова вушної раковини	–Фіксована форма та зовнішній вигляд. –Найбільш стабільна і обчислювальна складність. –Швидка ідентифікація. –Короткий час обробки.	–Висока ймовірність помилок розпізнання. –Неякісне розпізнавання через волосся, шапки та сережки. –Не вважається дуже унікальним.
Геометрія руки	–Зручність сканування. –На результат не впливає вологість шкіри або її текстура. –Проста у використанні та невеликий розмір шаблону. –Може працювати в складних умовах. –Має низький рівень відмови в реєстрації (FTE).	–Не унікальна та не точна. –Ефективна лише для дорослих. –FAR (коефіцієнт помилкового прийняття) та FRR (коефіцієнт помилкового відхилення) відносно високі. –Носіння дорогоцінностей може стати перешкодою під час сканування. –Досить дорого.

Продовження таблиці 1.1

Голос	–Легко реалізувати. –Не потрібно зайвих нових пристроїв. –Невисока вартість. –Зручне використання. –Відсутність варіації при зчитуванні.	–Сприйнятливий до якості мікрофона та шумів. –Хвороби горла або грип впливають на точність. –Можна легко підробити. –Високий рівень помилкової невідповідності. –Значне зниження продуктивності через фактори, що впливають на вхідні дані системи.
Частота набору тексту	–Не потребує особливого апаратного забезпечення або датчиків та низька вартість. –Швидка ідентифікація.	–Хвороби, зміна клавіатури, тощо, може змінити ритм набору тексту. –Не зріла технологія. –Мала зручність у використанні.
Відбиток долоні	–Більше відмінних рис можуть бути захопленими порівняно з відбитками пальців. –Більш придатний для системи верифікації, ніж відбитки пальців. –Більш надійний і постійний протягом життя.	–Сканери великого розміру та мають високу ціну. –Проблеми з розпізнаванням зображень низької якості. –Варіації освітленості та спотворення при неконтрольованому навколишньому середовищі.
Підпис	–Підпис не може бути вкрадений. –Низький FAR. –Має широке визнання у громадськості. –Має неваріативний характер. –Швидкість, особливо для великої кількості необхідних операцій. –Немає необхідності у конфіденційності. –Легко відновити шаблон, якщо його вкрали.	–Існуватиме можливість змін у шаблонах реальних зразків, наприклад, зміна поведінки під час підписання. –Професіонали можуть підробити підписи, щоб обдурити систему. –Проблеми перевірки достовірності.

Продовження таблиці 1.1

Рух губами	–Відмінний і незмінний атрибут для кожної людини. –Використовується фахівцями криміналістики для навчання кримінальної поліції. –Розмір шаблону невеликий і залежить від статичного зображення рота. –Біометрична характеристика вимагає присутності користувача для зчитування. –Може бути гібридною з системою розпізнання по голосу або обличчю.	–Варіації посмішки можуть викликати помилки при розпізнанні. –Захворювання губ також впливають на якість роботи системи. –Змінність характеристики впродовж життя –Не достатньо унікальна –Сканування займає деякий час

Отже, як ми з’ясували біометричні ознаки включають різні підмножини характеристик тіла, але не всі такі підмножини придатні для ідентифікації. Наприклад, фотографія одної певної частини тіла (обличчя) достатньо для багатьох цілей, тоді як фотографії інших частин тіла (скажімо, ліктів або стоп) марно. Рішення за яким певна характеристика тіла, придатна для біометричного використання, може бути зроблено за наступними критеріями (див. таблицю 1.2):

Таблиця 1.2 Критерії оцінки біометричних систем

Універсальність	Має надавати можливість уявлення людини тільки за цією характеристикою.
Відмінність	Мають бути унікальними для кожної людини.
Постійність	Характеристики повинні залишатись незмінними впродовж життя.
Збірність	Унікальні фізичні характеристики людини мають легко зчитуватись та збиратись, для прискорення автентифікації.
Продуктивність	Ступінь точності зчитаних даних має бути досить високим.
Прийнятність	Характеристика повинна бути загально прийнятою та не викликати у користувачів бажання відмовитись від використання системи.
Стійкість	Біометрична характеристика має бути стійкою до відтворення, щоб запобігти викраденню даних для подальшого несанкціонованого доступу.

Було проведено оцінку найбільш популярних біометричних технологій, з тих, що висвітлені у даній атестаційній роботі відповідно до цих семи критеріїв (див. таблицю 1.3). Однак, слід пам’ятати, що ступінь, в якій кожен критерій повинен виконуватися, чітко залежить від призначення системи в якій він використовується. Перевірка прикордонного контролю повинна бути проведена за кілька секунд; пошук злочинця може зайняти місяці. Зручний додаток, скажімо, плата за дороги, може прийняти значний коефіцієнт помилок; банківська система вимагатиме набагато нижчої. Для цього необхідно розглянути цілі, для яких може бути використана біометрія.

Таблиця 1.3 – Експертна оцінка біометричних технологій

Назва системи / Критерій	Універсальність	Відмінність	Збірність	Постійність	Продуктивність	Прийнятність	Стійкість
Відбиток пальця	A	A	B	B	A	A	B
Обличчя	A	B	A	B	B	A	B
Райдужна оболонка ока	A	A	B	A	A	B	B
Геометрія руки	A	B	A	B	A	A	A
Сітківка ока	A	A	B	A	A	C	A
Хода	A	B	A	B	C	B	B
Відбиток руки	B	A	B	A	A	B	B
Структура вуха	B	B	B	B	A	B	B
Підпис	C	C	A	B	B	A	B
Голос	B	C	B	C	B	A	C
Частота набору тексту	C	C	B	C	C	B	B

A – висока оцінка, B – середня оцінка, C – низька оцінка.

Важливим аспектом біометричної технології є оцінка їх відсотка правильних рішень. Ефективність будь-якої біометричної системи автентифікації може бути оцінена за різними параметрами, як було описано вище це можуть бути помилкові пропуски (FAR) та помилкові відмови (FRR).

Окрім цих двох параметрів ще існують наступні види помилок: помилка відмови у реєстрації (FTE), коли особа по тим чи іншим причинам не може бути зареєстрована у системі, наприклад відсутність деякої біометричної характеристики, CER – коефіцієнт перехідних помилок, значення при якому помилкові відхилення та помилкові пропуски еквівалентні.

Порівняння біометричних систем за вище описаними параметрами можна побачити у таблиці 1.4:

Таблиця 1.4 – Порівняння біометричних технологій за ефективністю

Критерій	Відбиток пальця	Обличчя	Райдужна оболонка ока	Геометрія руки	Сітківка	Голос	Частота набору тексту
FAR	0,001 %	0,103 %	0,009 %	2 %	0,0001%	2 %	7 %
FRR	0,001 %	0,047 %	$1*10^{-6}$ %	2 %	$1*10^{-5}$ %	10 %	0,10 %
CER	0,01 %	0,75 %	0,021 %	1 %	0,80 %	5-6 %	1,8 %
FTE	1 %	0,2 %	0,5 %	0,9 %	0,80 %	0,01%	-

Якщо розглядати варіанти біометрії не з точки зору ефективності, можна виділити декілька загальних аспектів для порівняння, а саме зручність у використанні, ціна, популярність, швидкість зчитування даних, буденні фактори, що можуть завадити зчитуванню даних та точність. Аналіз за даними аспектами проведено у таблиці 1.5.

Таблиця 1.5 – Порівняння біометричних технологій за загальними аспектами.

Аспект	Відбиток пальця	Обличчя	Райдужна оболонка	Геометрія руки	Сітківка	Підпис	Голос	Частота набору тексту
Представлений	1981	2000	1995	1986	1999	1970	1998	2005
Ціна	C	B	A	A	A	-	C	C
Популярність	A	A	A	C	C	A	B	C
Зручність	A	A	A	B	C	A	A	B
Швидкість	A	B	B	A	B	A	B	C
Безпека	B	B	A	B	A	B	B	C
Фактори помилок	Вік, вологість, забрудненння, травма	Вік, освітлення, окуляри, волосся	Окуляри, погане освітлення	Вік, травма	Окуляри, контактні лінзи	Зміна підпису	Простуда, грип	Зміна клавіатури, травма пальця

A – висока оцінка, B – середня оцінка, C – низька оцінка.

1.3 Аналіз проблемних питань при впровадженні біометричних систем

Широке впровадження біометричних додатків викликає ряд проблем. У цьому пункті атестаційної роботи проводиться аналіз існуючих проблем біометричних систем верифікації. На сьогодні є чотири проблеми, які посідають перше місце в обговоренні біометричних технологій, а саме проблеми безпеки, конфіденційності, сумісності і витрат (див. рисунок 1.3).

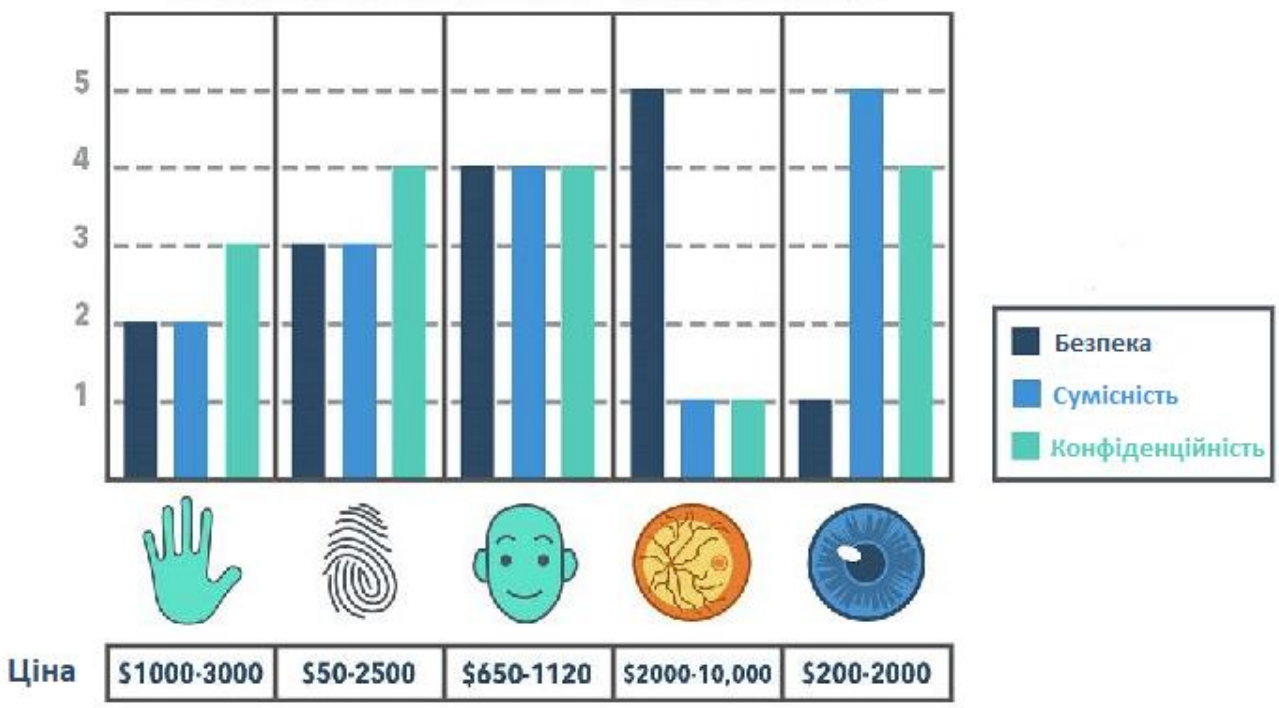

Рисунок 1.3 – Проблеми при впровадженні біометричних систем

Перша проблема це безпека, тобто ймовірність втручання в роботу системи третьої сторони, ступінь цієї проблеми, залежить від усієї архітектури системи, а не тільки від використовуваних технологій. Біометрична безпека не може покладатися на секретність, як у випадку з паролями і особистими ідентифікаційними ключами, тому що більшість біометричних даних людини може легко отримати: обличчя може бути сфотографоване, голоси можуть бути записані, відбитки пальців можуть бути зняті з дверей, і навіть ДНК можна отримати лише з одного волоса. Тому заходи безпеки повинні покладатися на робочі характеристики системи. Як зазначалося вище, біометричні системи верифікації працюють з тими ж чотирма етапами, що і традиційні системи верифікації: реєстрація, зберігання, отримання та зіставлення. На кожному з цих кроків є потенційні варіанти дій для обходу.

На етапі реєстрації особа записується в базу даних системи на підставі біометричних даних. Якщо злочинець успішно зареєструвався під чужим ім'ям на підставі підроблених документів, неможливо буде визначити його справжню особистість за допомогою системи верифікації. Фактично, він привласнив собі чужу особистість.

На рівні зберігання можна отримати доступ до збережених даних і управляти ними. Залежно від того, дані знаходяться в центральній базі даних або на накопичувачі, такому як смарт-карта або смартфон, потрібно розробляти свої варіанти підвищення безпеки.

У момент отримання ступінь складності підробки біометричних даних залежить від використовуваних біометричних даних. Наприклад, підробку відбитків пальців в минулому було порівняно легко обійти, так як системи були досить простими, але ускладнення методів пошуку особливостей відбитків пальців ускладнює надання підроблених даних. Незалежно від того, що може бути зроблено для системи на етапі отримання, система також може бути вразлива на етапі зіставлення. Наприклад, під час зіставлення, при достатній вразливості на рівні рішення, в реалізації системи, можливо понизити поріг рішення, тоді виявлення вторгнення також стає малоймовірним.

Інші фактори, які необхідно враховувати, включають в себе інформацію про спосіб зберігання цих даних, чи є збережені дані зашифрованими чи ні, вибір методу передачі даних з центральної бази даних або локальних носіїв.

Необхідно застосовувати ряд технічних заходів безпеки, добре відомих в області захисту інформації та захисту даних, що передаються. Це підвищує безпеку, але в той же час збільшує витрати. В цілому важливо відмовитися від припущення, що використання біометричного ідентифікатора є абсолютним доказом особистості. Біометрія також підлягає помилкам і варіантами обходу. Правда, вони повинні бути більш безпечними ніж традиційні системи верифікації, так як використання біометрії зростає, але вона не досконала. Якщо можливість помилки або шахрайства ігнорується, тоді загальний рівень безпеки фактично буде знижений до нуля.

Проблема конфіденційності. Біометрична ідентифікація і верифікація генерують цифрові дані. В першу чергу звичайно в якості ідентифікатора використовуються дані – наприклад, шаблон відбитка пальця. Система створює слід для зчитування системою кожен раз, коли виконується верифікація. Таким чином, з точки зору захисту даних підвищується кількість питань безпеки: які дані зберігаються, як вони зберігаються (централізовано в базі даних або децентралізовано на смарт-картах), у кого є доступ до даних, для яких цілей доступ до даних можуть отримати та інші.

Крім того, конфіденційність тісно пов'язана з питанням прийнятності для користувачів. Окремо від переваг конфіденційності системи ідентифікації, якій

довірився користувач, у нього можуть виникнути питання з приводу того, що дані недостатньо захищені, а їх конфіденційність недостатньо ціниться власниками системи. Такі організації не зможуть домогтися від населення довіри для співпраці.

Питання сумісності. Як і для будь-якої нової технології, функціональна сумісність відіграє важливу роль для розвитку біометрії. Наприклад, чим ширше можна використовувати біометричну систему, тим вона корисніша. Це стосується як побутового рівня, де явно корисно, якщо паспорт можна надати всього лиш приклавши палець і закінчується на бізнес рівні, коли всю необхідну інформацію можна отримати аналогічним способом. Однак це не обов'язково означає, що необхідно використовувати одні і ті ж біометричні дані - одна характеристика може відповідати за одну дію, друга надавати будь-яку іншу інформацію.

На національному та міжнародному рівнях проводиться значна робота з розвитку стандартів, які будуть корисні для просування розробки відкритих систем біометрії і підвищення сумісності з ними.[7] Однак, на відміну від можливості взаємодії «звичайних» технологій, біометрія не завжди може бути бажаною, в тому сенсі, що повна відсутність сумісності може створювати бар'єри, які можуть обмежувати передачу особистих даних.

Більш того, як вказано вище, оскільки люди мають в своєму розпорядженні безліч різних біометричних даних, існує можливість для різних додатків використовувати різні біометрії. Також системи, несумісні на різних біометричних рівнях, наприклад, центральна база даних вимагає райдужну оболонку ока, а система проходу кордону використовує розпізнавання відбитків пальців, всі вони можуть бути сумісні на рівні передачі даних, тобто вони все ще можуть обмінюватися даними про місце і час проведених ідентифікацій.

Проблема витрат. Як і будь-яка інша система ідентифікації, біометрична ідентифікація має свою вартість. Ця вартість сильно різниться між технологіями: наприклад, ідентифікація ДНК, яка вимагає значного втручання людини, коштує на порядок дорожче, ніж базове розпізнавання відбитків пальців. Але в рамках однієї технології ціни будуть відрізнятися надзвичайно сильно між недорогим простим і якісним обладнанням.

Оскільки вибір технологій і необхідний рівень оснащення залежать від конкретного призначення використовуваної системи біометричної верифікації, аналіз потреб – це та мета, яка допомагає визначити ступінь витрат. Масштаб додатків також має вирішальне значення, оскільки він теж включається у витрати. Витрати можуть бути розподілені між великою кількістю учасників великомасштабної реалізації. У розрахунок вартості повинні в рівній мірі входити заходи щодо забезпечення безпеки даних (шифрування, між мережеві екрани ті інше) та захист даних (відстеження використання даних). Нарешті,

важливо враховувати загальні реальні витрати: вони включають, зокрема, резервну систему, що є необхідною в будь-якому біометричному додатку.

Більшість систем біометричної ідентифікації все ще знаходяться в стадії розробки, і немає реального масового ринку, тому поки немає значного ефекту масштабу. Це повинно змінитися, як тільки буде запущено достатню кількість великомасштабних додатків і біометрія буде впроваджена у всіх сферах життя людини. Крім того, технічний прогрес, який спирається на досягнення в області інформаційних технологій повинен з часом знизити витрати. Поки що перші програми несуть високий рівень витрат, але незабаром можна очікувати різке зниження цін.

Ключове питання, пов'язане з витратами – це, звичайно, той хто за них платить. Це дуже вагомий фактор, який в цілому впливає на розвиток біометричних систем автентифікації. Це питання буде залежати в основному від відносної переговорної здатності розробників додатків з урядом, компаніями та іншими організаціями. Оскільки біометрія потребує зменшення кількості випадків шахрайства і помилок, тим самим знижуючи поточні витрати розробників на безпеку.

У цьому пункті була викладена основа для обговорення біометричної ідентифікації. Було визначено, що таке біометрія, якими критеріями вона повинна відповідати, для яких функціональних і практичних цілей вони використовуються, а також були розглянуті деякі з ключових питань, пов'язаних з впровадженням біометричної ідентифікації.

1.4 Многомодальні біометричні системи верифікації

В даний час широко розгорнуті біометричні системи, засновані на одній технології, з різними рівнями успіху, в різних контекстах додатків (аеропорти, паспорта, фізичний і логічний контроль доступу та інші). Однак, комбінуючи більше одного варіанту біометрії, реалізуючи тим самим многомодальну систему, підвищується надійність роботи і тим самим може бути збільшена вірогідність визнання користувачів. Послідовне комбінування менш надійних технологій може підвищити загальну продуктивність системи, і їх паралельне об'єднання може підвищити гнучкість системи (див. рисунок 1.4), надавши альтернативні режими для процесу верифікації або ідентифікації.

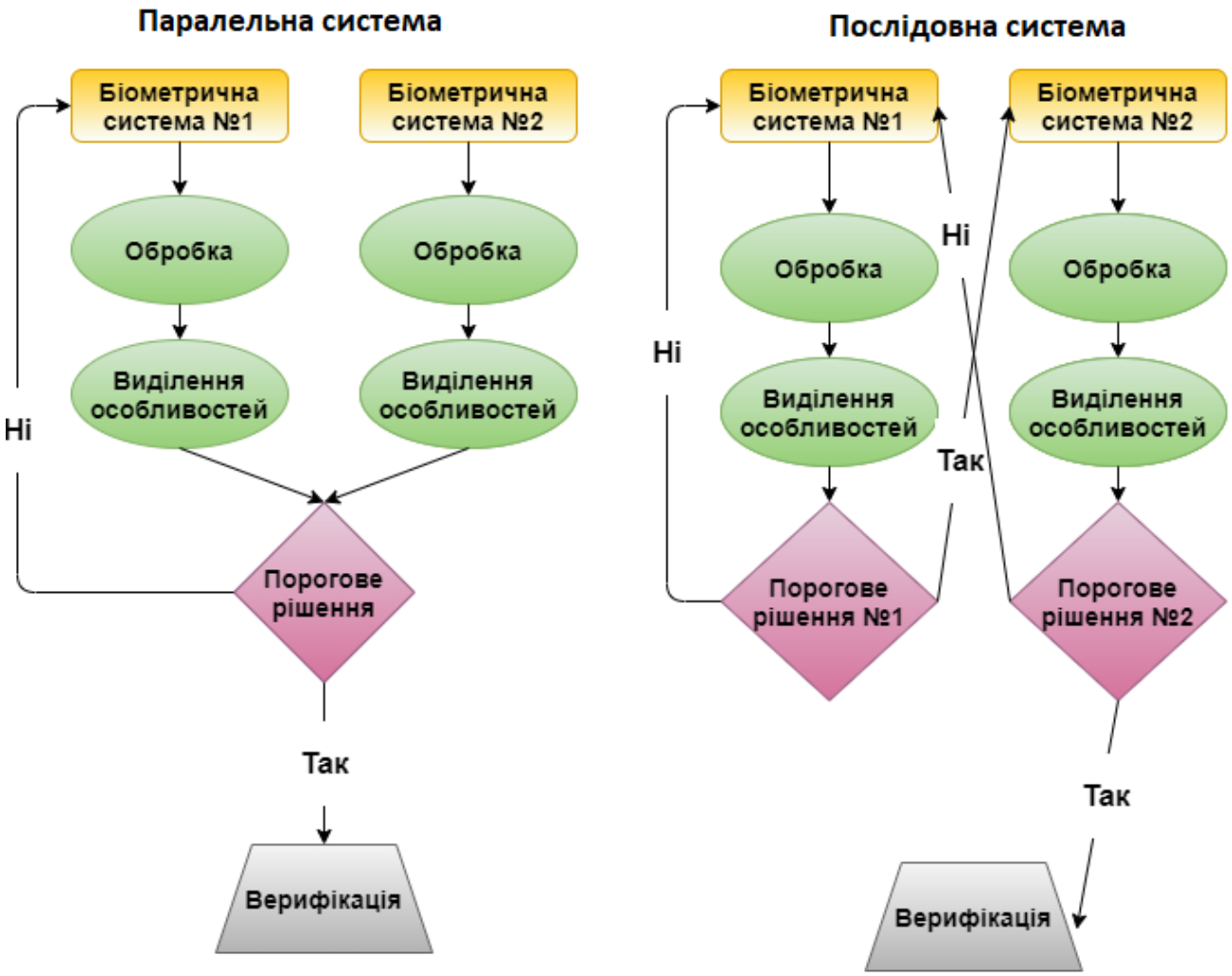

Рисунок 1.4 – Паралельна та послідовна схеми мультимодальної біометричної верифікації

Одномодальні біометричні системи можуть бути схильні до багатьох типів помилок. Вивчення таких помилок допоможе при проектуванні мультимодальних систем, які можуть дати поліпшені робочі характеристики. Деякі помилки можуть бути викликані шумом, пов'язаним з отриманими даними.

Шум може бути створений різними способами: через характеристику датчика (наприклад, зображення не в фокусі); поганими умовами навколишнього середовища (відбите світло під час отримання зображення особи); з поведінки користувача (неправильно поставлений палець). Як наслідок, біометричні вхідні дані можуть бути неправильно зіставлені, а користувач помилково відхилений. Але комбінуючи відповідні технології разом, такий шум може бути мінімізований, а кінцевим результатом могло б бути менше помилкових відмов.

Інший тип помилок пов'язаний з внутрішньокласовою змінністю. Біометричні дані будуть природно варіюватися від одного збору даних до

іншого. Ця внутрішньокласова змінність може бути сильніше для деяких людей, особливо під час моніторингу поведінкових біометричних особливостей - таких як підпис, голос або хода. Зазвичай це призводить до варіацій між отриманими і зареєстрованими даними, які впливають на процес зіставлення і можуть привести до відмови системи. Знову ж, поєднання технологій зі змішаною внутрішньокласовою змінністю може привести до систем, які в цілому демонструють кращу продуктивність.

Інші типи помилок пов'язані з розходженням індивідуальних біометричних характеристик. Комбінуючи дві різні функції, можна підвищити загальну продуктивність.

Ще один аспект ефективності, пов'язаний з проектуванням мультимодальних систем може звести до мінімуму можливість підробки і атак на системи які не перевіряють користувача на те, що він живий. У цьому випадку об'єднання біометричних технологій в послідовність, ймовірно, буде протидіяти таким атакам, оскільки буде потрібно набагато більше зусиль, щоб обдурити комбіновану систему. В застосування мультимодальних систем може значно підвищити продуктивність системи автентифікації в порівнянні з одномодальними системами.

Дві (або більше) модальності можуть бути об'єднані паралельно для створення системи, яка дозволить більш гнучке використання. Наприклад, біометричні системи, створені для розпізнавання відбитків пальців та обличчя, може дозволити використовувати тільки зображення обличчя для перевірки, коли у користувачів виникають проблеми зі зняттям відбитків пальців, і навпаки. Більш того, ця процедура може виявитися надзвичайно корисною для тих користувачів, які тимчасово втратили здатність надавати одну зі своїх біометричних характеристик (наприклад, тимчасова проблема із зором, що виключає сканування райдужної оболонки). Те ж саме може застосовуватися у випадках коли люди відмовляються використовувати певну модальність (наприклад, в релігійних або медичних цілях).

Таким чином, мультимодальна система забезпечує підвищену гнучкість за рахунок надання альтернативи процесу верифікації. Виходячи з цього можна зробити висновок, що така система буде більш соціально адаптована.

Якщо коротко, при розробці мультимодальної системи необхідно відповісти на деякі питання.

Які біометричні технології будуть поєднуватися? Вибір знову в основному обумовлено вимогами програми. Крім необхідності підвищити продуктивність або зручність використання системи, інші чинники, такі як доступні ресурси (включаючи необхідну обчислювальну потужність) і витрати (на комбіновані технології) також слід враховувати. Наприклад, для мобільної платформи, яка

використовує смартфон з камерою, можна використовувати верифікацію по обличчю, оболонці ока або голосу.

На якому етапі слід поєднувати технології? Так як модулі можуть об’єднуватись на різних рівнях, необхідно врахувати призначення системи, для цього розглянемо всі можливі рівні, на яких можна об'єднати різні модулі біометричної системи:

– об’єднання на рівні виділення ознак, скомпонованих в одну єдину вхідну інформацію;

– на рівні прийняття рішень шляхом об'єднання рішень окремих біометричних систем. Останній варіант може бути проблематичним, якщо системи не погодяться. У цьому випадку це може привести до подальших помилок («погана» продуктивність, система погіршить швидкість своєї роботи);

– на рівні балів, шляхом об'єднання балів, отриманих різними системами. В цьому випадку комбінація враховує оцінки, отримані різними системами для прийняття остаточного рішення.

Отже, загальна продуктивність збільшується за умови, що обрана правильна схема злиття. У деяких випадках два комбінованих методи можуть бути синхронні (наприклад, рух і голос записуються разом, коли людина говорить, для мінімізації можливості шахрайства). У таких випадках цікаво об'єднати інформацію на більш ранній стадії, а саме: відразу після функції вилучення і побудувати унікальну систему, приймаючи в якості вхідних даних комбінацію цих особливостей.

2 СИСТЕМА БІОМЕТРИЧНОЇ ВЕРИФІКАЦІЇ ЗА СТРУКТУРОЮ РАЙДУЖНОЇ ОБОЛОНКИ ОКА

Після проведеного аналізу у першому розділі атестаційної роботи можна зробити висновок, що найбільш з надійніших варіантів біометричної верифікації людини є система, яка працює на основі структури райдужної оболонки ока. У цьому розділі буде розглянуто основну методику роботи системи та алгоритм для виділення та порівняння особливих точок на зображеннях райдужної оболонки ока. Також буде представлено аналіз безпеки вище зазначеної системи та надання рекомендацій, які позволять підвищити безпеку роботи системи біометричної верифікації за райдужною оболонкою ока.

2.1 Алгоритм біометричної верифікації за райдужною оболонкою ока

Виходячи з інформації описаної у першому розділі можна зробити висновок, що останні досягнення інформаційних технологій і зростаючі вимоги до безпеки привели до швидкого розвитку розумних систем верифікації особистостей на основі біометрії. Біометрія використовує фізіологічні або поведінкові характеристики для точної верифікації людини. Райдужна оболонка найкраща характеристика, яку можна використовувати для верифікації в порівнянні з обличчям, підписом, голосом або сітківкою ока.

Алгоритм поєднує в собі всі характеристики, які повинна мати біометрична особливість людини. Рисунок райдужки унікальний для кожної людини. Також, структура райдужної оболонки правого і лівого ока відрізняється, що дозволяє проводити верифікацію за двома факторами тільки за допомогою райдужної оболонки. До того ж райдужка є незмінною людською характеристикою, яка є дуже стабільною протягом часу.

Пристрій, який використовується для сканування райдужної оболонки ока – камера. Це буде зручно для популяризації серед користувачів так як на сьогодні фотоапарат, камера в планшеті або смартфоні це буденність. Також рисунок райдужки є найбезпечнішим з усіх варіантів біометрії так як його не можна підробити, але можливо відновити за допомогою шаблону ключових точок (див. пункт 2.4). У наш час не мало важливий фактор гігієни, біометрія на основі райдужки не вимагає фізичного контакту з камерою, таким чином зводячи це питання до мінімуму.

Отже, розпізнавання райдужної оболонки ока – це процес верифікації людини за аналізом візерунка райдужної оболонки. Автоматизований метод розпізнавання райдужної оболонки відносно молодий, патентується тільки з 1994 року. Райдужна оболонка – це м'яз всередині очей, який регулює розмір

зіниці, контролюючи кількість світла, що потрапляє в око. Це кольорова частина очей з забарвленням залежно від кількості меланіну (пігмент всередині м'язу). Райдужка - це відкрита біометрична характеристика, доступна для віддаленої оцінки за допомогою систем машинного зору. Хоча забарвлення і структура райдужки генетично пов'язані, деталі візерунка не мають між собою нічого спільного.

Біометрична система розпізнання райдужної оболонки ока повинна складатися з ряду підсистем, які відповідають кожному етапу розпізнавання райдужної оболонки. Основні етапи:

– отримання зображення (захоплення зображення ока);
– сегментація (визначення області райдужної оболонки ока і зіниці)
– нормалізація (створення узгодженого за розмірами уявлення області райдужної оболонки в полярній системі координат)
– виділення та кодування ознак (створення шаблону, який містить тільки самі відмінні риси райдужки).

Входом в систему буде зображення ока, а на виході буде шаблон ключових точок радужки , який формує математичне уявлення області райдужної оболонки.

2.2 Методика обробки зображень райдужної оболонки ока

Етап отримання зображення. Оскільки на етапах отримання зображення райдужної оболонки визначається якість отриманого зображення, від цього етапу залежать всі інші етапи верифікації. Таким чином були розроблені ідеальні умови для отримання якісного зображення: зображення має зніматися камерою високої якості, по можливості з 3CCD (технологія виділення кольору). Камера повинна бути розташована на відстані приблизно в 9 см від ока користувача. Зразкова відстань між користувачем і джерелом світла близько 12 см.

Етап сегментації зображення є першим етапом розпізнавання райдужної оболонки. На даному етапі виділяється фактична область райдужної оболонки на цифровому зображенні ока. Область райдужки можна уявити двома колами, перше розділяє кордон райдужки і склери, другий - всередині першого, для розділу кордонів райдужної оболонки і зіниці. Успіх сегментації залежить від якості зображення очей. Центр зіниці можна використовувати що б визначити зовнішній радіус райдужної оболонки. Внутрішні і зовнішні кордони райдужки можна визначити шляхом знаходження крайового зображення за допомогою оператора Кенні. Алгоритм складається з 5 окремих кроків:

1. Згладжування: фільтрація і розмиття зображення для видалення шумів, так що б пікселі, що створюють плями, були зменшенні (див. рисунок 2.1).

Рисунок 2.1 – Фільтроване та розмите зображення.

2. Пошук градієнтів: в точках / пікселях, де колір потрапляє в аналогічну порогову область. Групування знайдених елементів (див. рисунок 2.2). Краї повинні бути відзначені там, де градієнти зображення мають великі розміри.

3. Не максимальне придушення: частина зображення, яка повинна бути опрацьована є лінійної, а не круглою або опуклою, отже, гранична область, відповідна прямокутній формі, виноситься на локальні максимуми які потім повинні бути відзначені як край елемента. (див. рисунок 2.2).

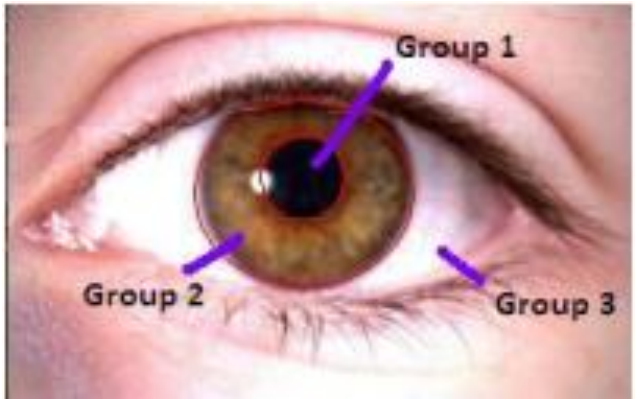

Рисунок 2.2 – Групування градієнтів та пошук кордонів зіниці та райдужки

4. Подвійний поріг: потенційні межі визначаються граничним значенням.

5. Відстеження крайок (див. рисунок 2.3): визначаються кінцеві кромки, пригнічуючи всі ребра, які не пов'язані з основним ребром (Наприклад: видалення накладених вій на зображення райдужної оболонки).

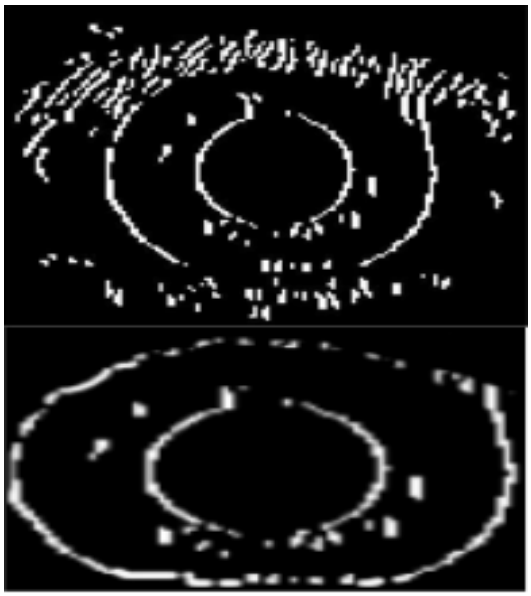

Рисунок 2.3 – Процес відстеження крайок

Після того, як область райдужної оболонки сегментована, наступним етапом є нормалізація цієї частини, щоб зробити можливою генерацію коду райдужної оболонки і подальшого його порівняння. Потрібно нормалізувати зображення райдужної оболонки, щоб представлення райдужки було загальним для всіх та з аналогічними розмірами. Процес нормалізації передбачає розгортання райдужки і перетворення її в полярну систему координат. Тобто райдужка перетворюється в стандартний (фіксований) формат одного розміру (див. рисунок 2.4).

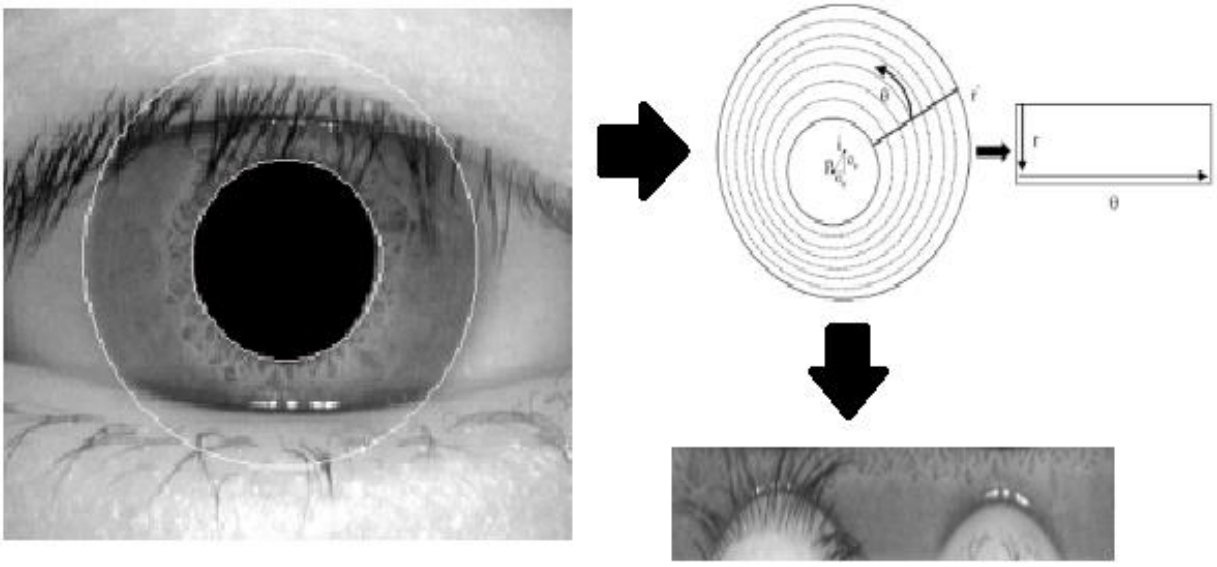

Рисунок 2.4 – Схема нормалізації райдужної оболонки ока

Після нормалізації зображення області райдужки в тому чи іншому вигляді необхідно знайти та виділити її інформаційні ознаки або ключові точки. Ці ознаки повинні в максимальному обсязі володіти такими властивостями:

- незалежність від умов реєстрації зображення, включаючи всі варіації умов зйомки та зміни самого ока (розміру зіниці або положення повік);
- незмінність при повторних реєстраціях однієї персони, повторні реєстрації повинні проводитись протягом багатьох років;
- унікальність, для відміни позитивного результату для сторонніх користувачів.

Зміни форми та забарвлення елементів райдужки виникають, зазвичай, внаслідок зміни стану організму. Проте кількість елементів структури райдужки настільки велика, що при порівнянні двох еталонів досить збігу лише частини параметрів, щоб вважати, що еталон належить одній людині.

Ознаками райдужки можуть вважатися загальні характеристики: колір, яскравість, контрастність, форма зіниці, тощо. Колір райдужної оболонки - добре відома її властивість. Проте колір райдужки в цілому дає мало інформації, так як за цією ознакою, з урахуванням точності його виміру, люди розбиваються на мале число класів. Тому колір райдужки в цілому пропонується як додаткова ознака, в основному в системах розпізнавання по обличчю, поряд з іншими ознакам. На сьогодні у якості ключових точок частіше за все обираються відмінні особливі точки на зображенні райдужної оболонки ока, які виділяються при різних масштабах зображення. Для захоплення усього діапазону масштабів треба використовувати розкладання на декілька масштабів. Існує досить багато алгоритмів для вирішення цієї задачі: фільтр Гауса, фільтр Габора, оператор Лапласа, тощо.

Отже, розпізнавання райдужної оболонки ока виявилося одним з найбільш надійних біометричних ознак для особистої верифікації. Насправді рисунки райдужної оболонки мають стабільні, незмінні і відмінні риси для особистого користування. Надійна авторизація та автентифікація стають необхідними для багатьох повсякденних потреб людини. Розпізнаванню райдужної оболонки приділялося більше уваги через її високу надійність. Але для того, щоб витягнути функції райдужної оболонки ока, потрібно враховувати фактори, які впливають на неї, а саме деякі практичні чинники, такі як неточна локалізація, сегментація, зміни радіуса зіниці і різний масштаб вхідних зображень.

Мета дослідження в даному пункті атестаційної роботи полягає в адаптації все більш широкого використання біометричної системи райдужки, а також зменшення ймовірності помилок, що виникають при чинниках впливу описаних в минулому реченні. Після аналізу існуючих алгоритмів виділення особливостей на зображеннях у якості алгоритму виділення особливих точок на зображенні райдужної оболонки ока для подальшої програмної реалізації було обрано

алгоритм SIFT (див. пункт 2.3). Це ефективний алгоритм виділення ознак райдужної оболонки на основі модифікованого масштабно-інваріантного алгоритму перетворення ознак. Алгоритм реалізований та представлений програмною бібліотекою для розробки «Opencv»..

2.3 Алгоритм виділення особливостей зображення SIFT

Алгоритм SIFT ідеально підходить і застосовується для розпізнавання райдужної оболонки. Він витягує особливі точки, які є надійними, стабільними та різноманітними. Вектор ознак інваріантний до переміщення зображення, масштабування, повороту і частково інваріантний до змін освітленості. Алгоритм може ефективно знаходити інформаційні ознаки з природних особливостей вен на райдужній оболонці, тому він може вирішити традиційну проблему низької швидкості ідентифікації по райдужці. Крім того, попередня обробка зображення райдужної оболонки підвищує швидкість роботи алгоритму.

Математичну модель алгоритму SIFT можна розбити на чотири основних етапи: знаходження ключових точок, відсіювання ключових точок, визначення напрямку точки та побудова дискриптору.

У пошуку ключових точок основним є побудова ієрархії гаусіанів, які розраховуються за (2.1) і їх різниць (далі РГ) розрахованих по (2.2). Гаусіаном є зображення з розмитим гаусовим фільтром, РГ в свою чергу є різниця гаусіанів, яка вичисляється шляхом попіксельного віднімання гаусіанів з різним радіусом розмиття.

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y) \quad (2.1)$$

L – значення гаусіану в точці (x, y), G – гаусове ядро, σ – радіус розмиття, I – початкове зображення.

$$D(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) = L(x, y, k\sigma) - L(x, y, \sigma) \quad (2.2)$$

D – різниця гаусіанів, $k\sigma$ – наступний радіус розмиття.

У пункті 2.1 був зроблений висновок, що ключові точки виділені на зображенні райдужки повинні бути стабільні до змін масштабу. Масштабуючі зображення – це вхідні зображення згладжені фільтром з різним радіусом розмиття. Доведено, що різні масштаби розмиті гаусовим фільтром можуть відповідати початковому зображенню. Загалом проблема масштабованості зображень райдужної оболонки вирішується за допомогою знаходження ключових точок початкового зображення в різних ступенях розмиття. Для цього створюється ієрархія гаусіанів (далі ІГ), весь простір ІГ розбивається на ділянки,

які називаються октавами. При переході від однієї октави до наступної зображення райдужної оболонки стає в два рази менше. Паралельно цьому шляхом віднімання будується ієрархія РГ (див. рисунок 2.5). Виділення ключових точок відбувається шляхом порівняння точки з точками її околиці, точка буде вважатися ключовою якщо її значення більше або менше, ніж значення точок в її околицях.

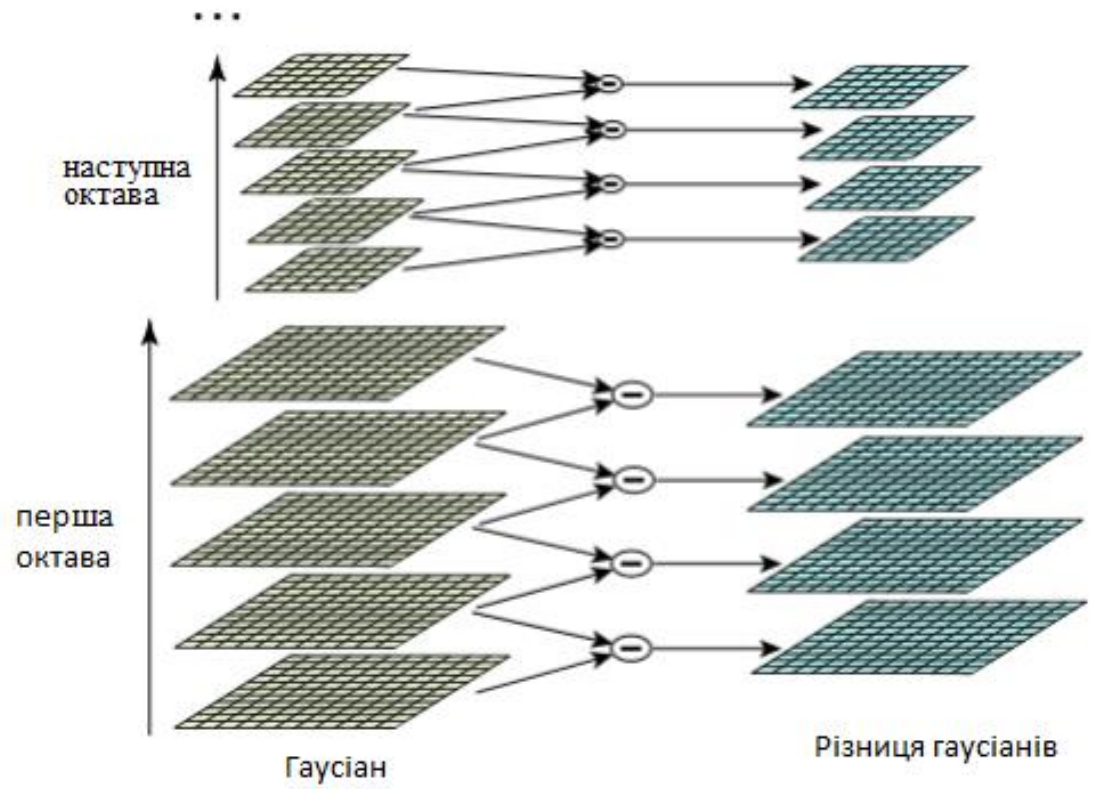

Рисунок 2.5 – Ілюстрація процесу побудови піраміди гусіанів.

На другому етапі роботи алгоритму відбувається відсіювання знайдених ключових точок. Ключова точка перевіряється на освітленість та на її положення на зображенні райдужки. Тобто якщо точка погано освітлена або знаходиться на кордоні об'єкта (межа зіниці і райдужної оболонки) дана точка буде виключена зі списку особливих. Такі типи точок мають великий вигин, який можна визначити матрицею Гессе (2.1). Алгоритм перевірки:

$$H = \begin{bmatrix} D_{xx} & D_{xy} \\ D_{yx} & D_{yy} \end{bmatrix} \tag{2.3}$$

Нехай T (H) – слід матриці (2.4), а Det (H) – визначник (2.5):

$$T\,(H) = D_{xx} + D_{yy} = \alpha + \beta \tag{2.4}$$

$$Det\ (H) = D_{xx} * D_{yy} - (D_{xy})^2 = \alpha + \beta \quad (2.5)$$

Нехай r - відношення великої вигину до меншого (2.6):

$$\alpha = r\beta \quad (2.6)$$

тоді:

$$\frac{T\ (H)^2}{Det\ (H)} = \frac{(\alpha + \beta)^2}{\alpha\beta} = \frac{(r\beta + \beta)^2}{r\beta^2} = \frac{(r+1)^2}{r} \quad (2.7)$$

Виходячи з цього отримуємо умову, при якій ключова точка буде розглядатися далі (2.8):

$$\frac{T\ (H)^2}{Det\ (H)} < \frac{(r+1)^2}{r} \quad (2.8)$$

Після визначення ключових точок алгоритм приступає до третього етапу роботи, де необхідно визначити напрямок ключової точки. Обчислення орієнтації відбувається шляхом обчислення напрямків градієнтів сусідніх точок. Даний етап вирішує проблему повороту зображення описану в пункті 2.1. Для розрахунку береться кілька сусідніх точок, зазвичай це квадрат 4x4. Для кожної точки розраховується значення градієнта (2.9) і його напрямок (2.10)

$$m\ (x,y) = \sqrt{(L(x+1,y) - L(x-1,y))^2 + (L(x,y+1) - L(x,y-1))^2} \quad (2.9)$$

$$\theta(x,y) = \arctan\left(\frac{L(y,x+1) - L(x,y-1)}{L(x+1,y) - L(x-1,y)}\right) \quad (2.10)$$

Після того, як були знайдені напрямки для всіх особливих точок, алгоритм переходить до п’ятого етапу роботи побудови дескрипторів (див. рисунок 2.6). На цій стадії алгоритму обчислюються значення дескрипторів. Перед обчисленням дескриптора вибирається, скільки точок навколо ключової буде враховуватися (зазвичай беруть 16 особливих точок). Далі для кожної точки будується гістограма, аналогічна гістограмі орієнтації ключових точок. Після цього формується вектор чисел. Цей вектор і є дескриптор SIFT.

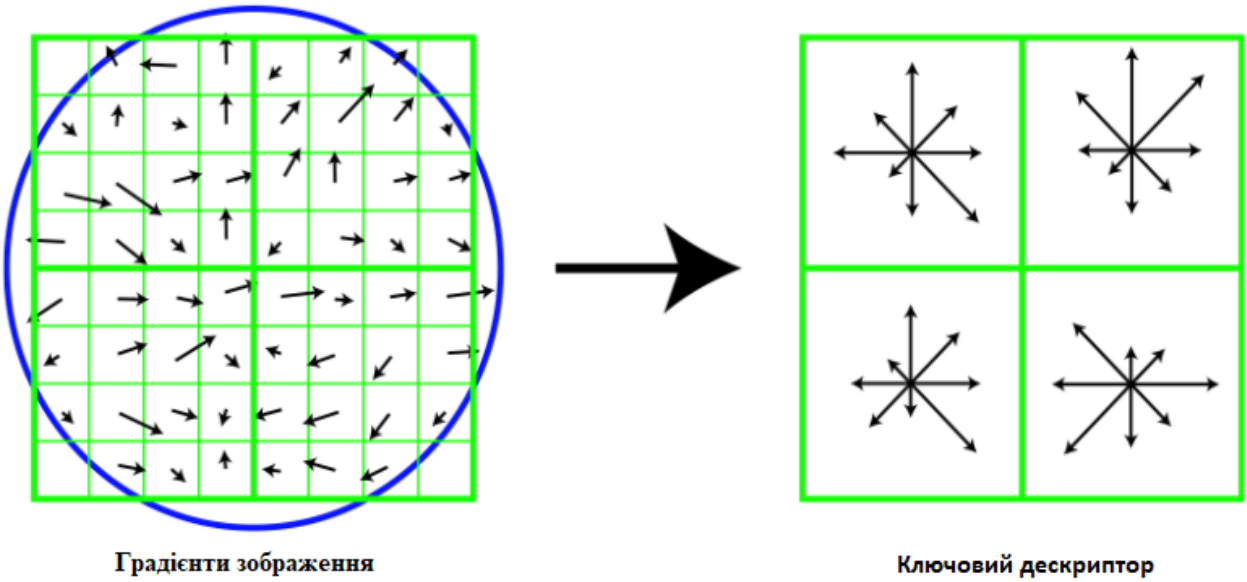

Рисунок 2.6 – Побудова дескрипторів.

Проведений вище аналіз показує, що алгоритм SIFT, який спочатку був придуманий для знаходження і розпізнавання зображень різних масштабів і під різними кутами, ідеально підходить для розпізнавання райдужної оболонки ока. Більш того, первісна обробка зображення райдужної оболонки значно прискорює роботу представленого алгоритму.

2.4 Вразливості та варіанти їх вирішення для систем верифікації за структурою райдужної оболонки ока

Біометрична верифікація за структурою райдужної оболонки ока до недавнього часу вважалася однією з найнадійніших. Зокрема, тільки недавно дослідники зосередилися на можливості відновлення синтетичних біометричних зображень райдужної оболонки, які потенційно можуть бути введені в біометричну систему, тим самим підірвавши її корисність. У більшості систем на основі райдужної оболонки використовуються так звані коди райдужних оболонок, які представляють собою двійкове подання малюнка райдужної оболонки.

Коди райдужки - це надзвичайно компактне уявлення райдужної оболонки ока. У біометричному співтоваристві вважалося, що бінарні шаблони не розкривають достатньо інформації, щоб відновити з них вихідне зображення райдужної оболонки ока (схема вилучення традиційно вважалася односторонньої функцією). Однак це переконання було поставлене під сумнів дослідниками в літературі, які досліджували оборотність кодів райдужки. Зокрема в джерелі [2] представлений імовірнісний метод реконструкції на основі

генетичних алгоритмів. Атаки проводилися шляхом зіставлення синтетично реконструйованих зображень райдужної оболонки з оригінальними. В даному розділі ми звертаємося до проблем безпеки, розкритим у даному джерелі, пропонуючи ефективні заходи протидії для виявлення синтетичного візерунка райдужної оболонки, реконструйованого з реального коду райдужки. Таким чином, основна мета даного розділу - розробити надійні рішення фактичної вразливості, з метою підвищення рівня безпеки.

Пропоноване глобальне рішення даної вразливості класифікує вхідну вибірку на реальне або синтетичне зображення після двоетапного підходу до перевірки. Кожен з двох етапів можна розглядати, як конкретний контрзахід проти конкретної вразливості системи.

Етап 1: додаткові апаратні засоби. Являє собою автентифікацію в реальному часі. Даний запропонований варіант вирішує проблему до того, як зображення надходить в систему. Це здійснюється на рівні камери для зчитування райдужки. Наприклад: включення додаткового світла (діода) для перевірки реакції зіниці людини на світло або взаємодія з користувачем на рівні системи, яка зчитує зображення райдужної оболонки, наприклад, додаткових підказок з проханням кліпнути очима, поміняти кут камери, тощо.

Етап 2: виявлення краю. Це дозволяє захистити системи від спроб шахрайства з використанням дуже простого зображення, схожого на райдужну оболонку ока, такі як показані у верхньому ряді на рисунку 2.7. Данні зображення ніколи не повинні прийматися. Цей захисний механізм спрацьовує відразу після виявлення райдужки і перед виконанням будь-якої попередньої обробки. Він працює з усім захопленим окулярним зображенням, щоб переконатися, що представлений в систему зразок максимально наближений до реального зображення очей.

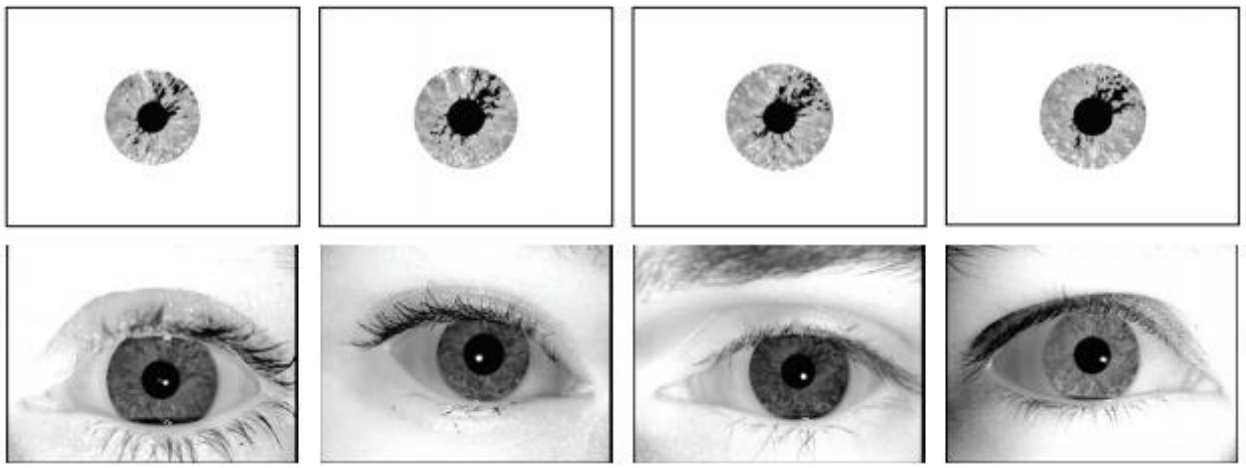

Рисунок 2.7 – Відтворення райдужки з коду

Для досягнення цієї мети на зображенні визначається край очей, вії, тощо. Виявлений об'єкт за межами кордонів райдужної оболонки використовується в якості відмінної ознаки між реальними і простими синтетичними зображеннями. Це гарантує, що зображення з однорідним фоном (див. рисунок 2.7) не буде допущено в систему.

Також для запобігання крадіжки шаблону ключів, необхідно передбачати шифрування даних або використання додаткових односпрямованих функцій, після обробки якими шаблон ключів райдужки буде не можливо відновити.

Отже, в даному пункті представлений двоетапний метод захисту від атак з використанням реконструйованих зображень райдужної оболонки ока. Були зроблені висновки, що його здатність виявляти спроби шахрайського доступу з використанням синтезованих зображень райдужної оболонки ока велика, тим самим метод вирішує важливі недоліки безпеки, виявлені при оцінці вразливості сучасної системи біометричної автентифікації на основі райдужної оболонки ока.

3 СИСТЕМА БІОМЕТРИЧНОЇ ВЕРИФІКАЦІЇ ЗА ВІДБИТКАМИ ПАЛЬЦІВ

Найпоширенішою біометричною технологією автентифікації користувачів є верифікація за відбитками пальців. Основою на якій базується система є використання унікального малюнка папілярних ліній на пальцях людей та візерунків, які вони утворюють. Сканер зчитує папілярний візерунок, перетворює його в цифрову модель і потім проводить порівняння з раніше зареєстрованим малюнком відбитка, який прийнято вважати еталонним. Основною перевагою даного варіанту біометрії є легкість в застосуванні та впровадженні. Так само варто відзначити універсальність даного методу, яка полягає в можливості застосування методу в рішенні задач ідентифікації будь-якого рівня і будь-якого роду діяльності.

Відбиток пальця можна отримати, застосовуючи сканер відбитків пальців. У зв’язку з тим, що відбиток пальця досить малий, необхідне застосування вузько направлених методів. У відбитку виділяються 2 типу ознак: глобальні та локальні. Локальні ознаки описують точки зміни структури ліній папілярного візерунка (закінчення, роздвоєння, розрив та ін.) (див. рисунок 2.8). Папілярний малюнок складається з:

– області візерунка – область відбитка, що містить глобальні ознаки;

– ядра (центру) – ділянка середини відбитка або області малюнка;

– дельти – початкова точка з’єднання або розгалуження ліній папілярного візерунка, або коротка лінія, вироджена в точку;

– типу лінії, які починаються як паралельні дві лінії та оминають всю область відбитка;

– лічильника ліній – число ліній між ядром, дельтою і областю образу.

Окрім вище перерахованих локальних особливих ознак, виділяють також основні класи малюнків відбитка пальця (глобальні ознаки). Їх класифікують наступним чином (див. рисунок 3.1):

– петля;

– дуга (або дельта);

– спіраль.

Вони допомагають полегшити алгоритм ідентифікації, який займає значно більше часу тому, що особа яка представляє свій відбиток є невідомою. За глобальними ознаками можна класифікувати дані та групувати їх на етапі реєстрації у базі даних.

Практика показує, що відбитки пальців різних людей можуть мати однакові основні ознаки (тип малюнка або ядра), але аж ніяк неможлива наявність однакових мікро-ознак візерунка відбитка. Тому глобальні ознаки

використовують для поділу бази даних на класи на етапі реєстрації. На другому етапі розпізнавання використовують вже локальні ознаки.

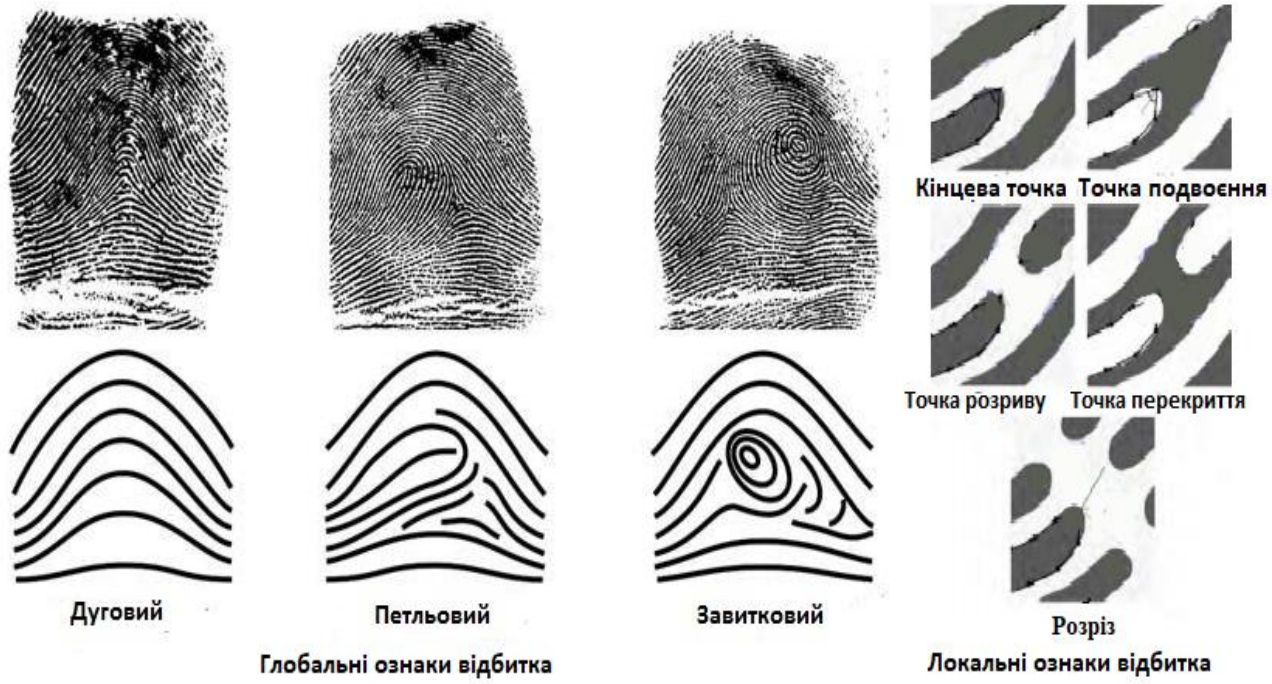

Рисунок 3.1 – Глобальні та локальні особливості відбитків пальців

Схема алгоритму верифікації відбитків пальців так само, як і розпізнання радужної оболонки (див. розділ 2) ока можна розділити на два основні етапи. Перший – обробка вхідного зображення, другий – пошук особливих точок та їх порівняння. Алгоритм обов'язково повинен включати в себе: бінаризацію зображення, скелетизацію, метод виділення та порівняння особливостей.

3.1 Обробка зображень відбитків пальців

Бінаризація зображень – це метод обробки зображення, який здійснює конвертацію кольорового зображення або зображення у відтінках сірого в монохромне зображення, тобто зображення де використовуються тільки два типи пікселів (чорні та білі) (див. рисунок 2.9). Оскільки для багатьох задач програмної обробки зображень колір не грає важливої ролі, бінаризація грає велику роль при розпізнаванні зображень, особливо образів, наприклад: штрих-кодів, QR-кодів, текстів, креслень та інших.

Самий простий спосіб кодування точки зображення це бінарний, коли пікселі розділяються та приймають два значення 0 або 1. Більш складний спосіб кодування – це градації сірого, стан точки визначається параметром яскравості, який приймає значення від 0 до 255, таким чином одна точка може кодуватися одним байтом.

Бінаризаційна обробка зображень включає у себе деякі нюанси, тому умовно її можна розділити на два способи: пороговий і адаптивний. Перетворити картинку з градації сірого в бінарну можна простим середнім пороговим перетворенням, але даний спосіб використовується тільки для рівномірно освітлених зображень та відноситься до порогового способу. В іншому випадку обрати вдалий поріг яскравості для всієї картинки може виявитися важким завданням (див. рисунок 3.2).

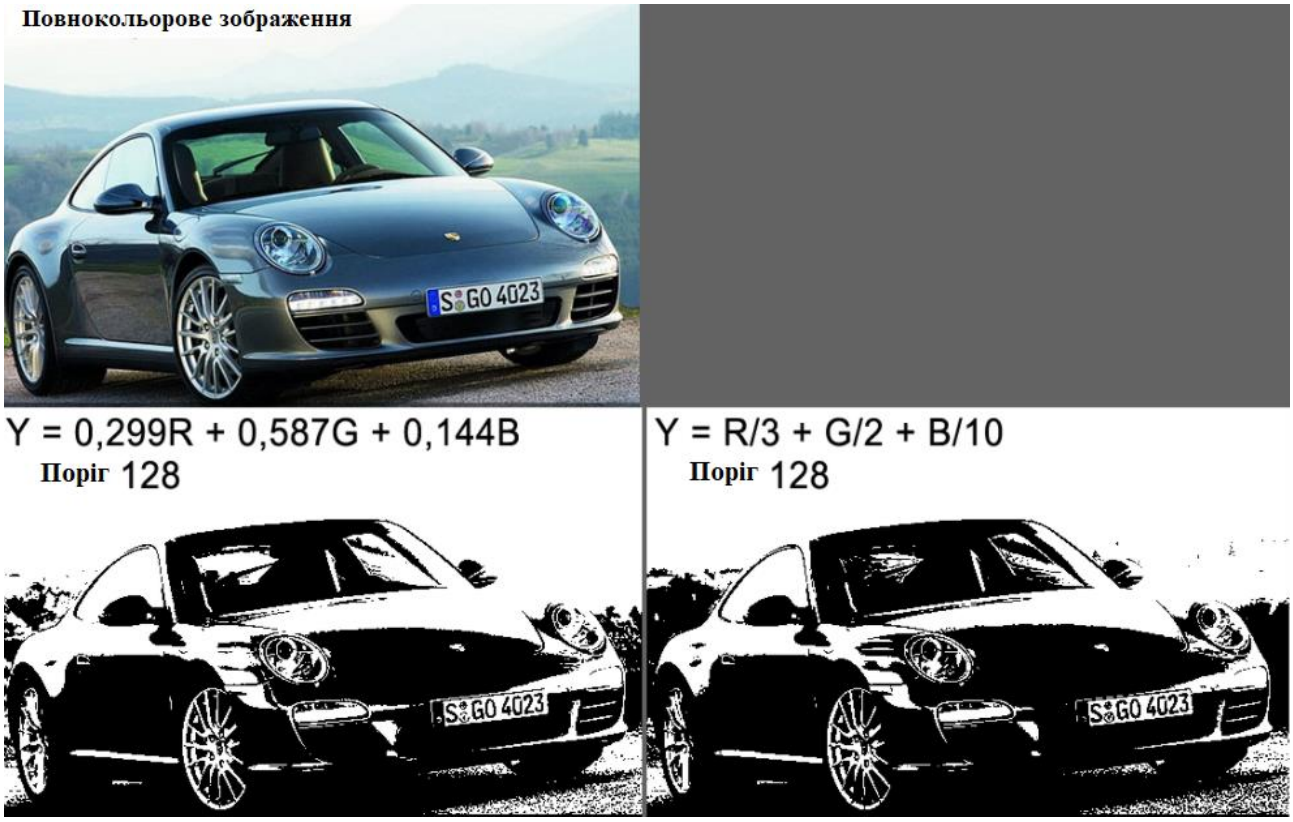

Рисунок 3.2 – Бінаризація зображення за різними параметрами

Для кожної точки розглядається її околиця і поріг вибирається тільки для цієї околиці. Зрозуміло, що кожен раз самостійно обирати поріг яскравості для кожної околиці, незручно, тому для вибору порога зазвичай використовуються різні методи та критерії, наприклад поріг можна вибрати як середню яскравість околиці або кожен раз розраховувати його за допомогою різних критеріїв.

Наступним етапом алгоритму верифікації за відбитками пальців є скелетизація зображення. Скелетом в комп'ютерній графіці називається безліч точок, рівновіддалених від кордонів фігури. Скелет підкреслює геометричні і топологічні властивості фігури, такі як її з'єднання, зв'язність, довжина, напрямок, ширина. Фактично скелет є поданням форми фігури, спрощує її подальший аналіз. У разі аналізу зображень з відбитками пальців, як фігури виступають папілярні лінії пальця. Перші методи скелетизації були розроблені

під час розв'язання задачі розпізнавання букв і тексту на зображенні, наприклад, на від сканованому аркуші паперу. Багато напрацювань, створені в рамках даної предметної області, так само можна застосувати й для задачі розпізнавання відбитків пальців.

До процедури скелетизації прописані наступні загальні вимоги: виділенні лінії повинні мати товщину в один елемент (піксель), лініям та вузлам вхідного зображення повинні відповідати лінії та вузли обробленого зображення, а також форма об’єкта, складеного з ліній, не повинна сильно спотворюватися.

В якості найбільш популярних алгоритмів скелетизації бінарного зображення можна назвати хвильовий алгоритм, алгоритм потоншення областей та шаблонний метод.

Хвильовий метод. Його завданням є векторне представлення зображення у вигляді графа - тобто визначення кінцевих точок, точок перетину (вершини графа), а також ліній і дуг, що складають фігури (ребра графа). Метод полягає в аналізі шляху проходження сферичної хвилі по зображенню. На кожному етапі аналізується зсув центру мас точок, що утворюють новий крок хвилі, щодо його попередніх положень. Після завершення побудови скелета за допомогою сферичної хвилі, отриманий результат оптимізується і аналізується, відшукуються особливі точки фігури. Приклад поширення хвилі по фігурі в даному методі скелетизації наведено на рисунку 3.3.

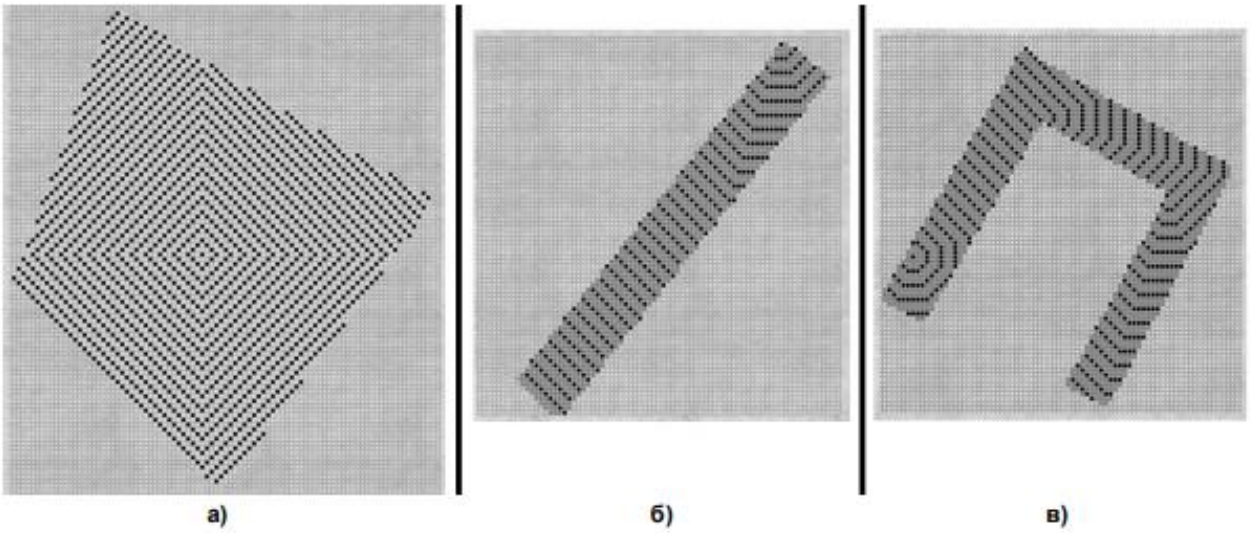

Рисунок 3.3 – Хвильовий фронт: а – без перешкод, б – на прямій, в – по фігурі

Даний алгоритм добре підходить для розпізнавання букв, оскільки буква, як правило, є цілісною одиночною фігурою невеликого розміру, з невеликою кількістю розгалужень і перетинів. Для створення ж скелета відбитку пальців даний алгоритм підходить гірше: структура фігури (папілярних ліній пальця)

набагато складніше, поширення хвилі і її подальший аналіз проходить з великими похибками.

Алгоритм стоншення областей. Даний алгоритм заснований на простому аналізі околиці кожної з його інформативних точок. Сусіди в околиці інформативного пікселя нумеруються по ланцюжку від 1-го до 9-го.

Залежно від кольорів зафарбовування навколишніх пікселів, обчислюються два параметри:

– A (P) – число переходів від білого пікселя до чорного в ланцюжку;

– B (P) – загальна кількість всіх чорних пікселів в околиці. Залежно від значень цих параметрів.

Також має значення зафарбовування конкретних пікселів у зв'язній області з чотирьох (пікселі 2, 4, 6, 8), приймається одне з двох рішень - або зафарбувати центральний піксель в білий колір, або залишити його в тому ж вигляді.

Після того, як всі інформативні пікселі зображення пройшли дану процедуру обробки, алгоритм обходу запускається знову, але вже на обробленому зображенні. Алгоритм вважається завершеним тоді, коли після чергової ітерації не було зафарбовано жодного пікселя зображення. Після цього отриманий результат вважається справедливим (див. рисунок 3.4).

Рисунок 3.4 – Застосування алгоритму стоншення областей

За рахунок своєї простоти, алгоритм має високу швидкість роботи і збіжності. Однак простота аналізу одночасно є і його недоліком: зокрема, можуть зберігатися шуми, що знаходилися на оригінальному зображенні. Ці шуми можуть надати свій вплив при визначенні особливих точок, а, внаслідок чого, і на результат верифікації відбитка.

Шаблонний метод скелетизації. Скелетизація за допомогою шаблонного методу є найбільш швидкою та простою у своїй реалізації. Загалом для

шаблонної скелетизації існує декілька наборів своїх закодованих правил, тобто шаблонів. Суть методу полягає в аналізі області зображення з 9-ти пікселів за допомогою даних шаблонів.

Зазвичай шаблонний метод використовує перший набір шаблонів, оскільки на відміну від використання другої сукупності шаблонів, в ньому потрібна реалізація лише одного обходу зображення. Але, для того, щоб знизити рівень неточності, застосовується частина шаблонів з другої сукупності. Є відповідність шаблонів матриці 3×3, в якій центральний елемент - це поточний піксель в обході зображення. Основна частина будується на базі восьми основних шаблонів (див. рисунок 3.5).

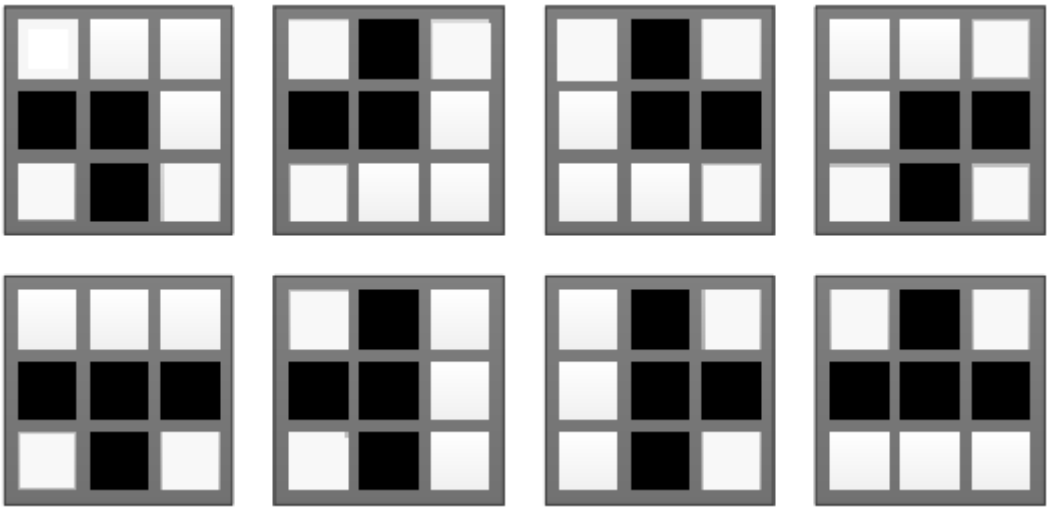

Рисунок 3.5 – Основний набор шаблонів

Оскільки алгоритм потребує одного обходу зображення є велика вірогідність утворення шумових пікселів, які у подальшому будуть помилково розпізнаватись, як особливі точки. Тому, чотири шаблони з другого набору необхідні для того, щоб усувати це самий шум(див. рисунок 3.6).

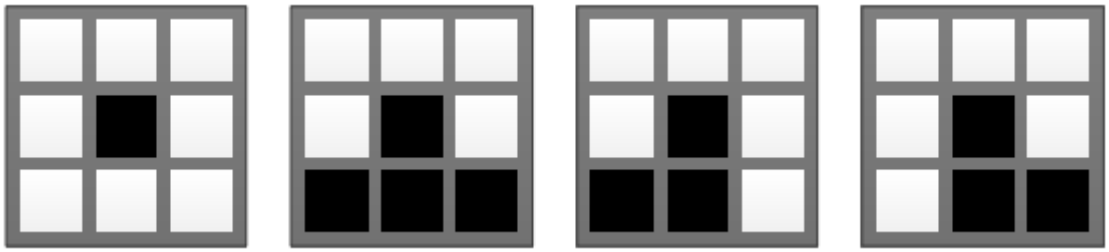

Рисунок 3.6 – Шумовий набор шаблонів

При цьому чотири шаблони з другого набору необхідно повернути на 90, 180 і 270 градусів, їх пошук здійснюється за допомогою другого обходу зображення.

Якщо 8-зв'язкова область відповідає одному з шаблонів, то йде фарбування центрального пікселя в білий колір. Обхід триває до тих пір, поки перефарбовуються пікселі.

Приведені вище приклади, доводять, що з використанням процесу скелетизації вдається створювати прості за реалізацією та ефективні алгоритми виділення та потоншення ліній на зображенні. Отже, скелетизація зображення є дуже важливим компонентом біометричних систем заснованих як на порівнянні відбитків пальців, так і на інших біометричних характеристиках.

3.2 Алгоритм порівняння відбитків на основі пошуку особливих точок

Що стосується алгоритмів виділення особливостей відбитка для подальшого порівняння, розглянемо і зробимо аналіз найпопулярніших на сьогоднішній день.

Перший алгоритм це порівняння по візерунку малюнка папілярних ліній. В якості основного об'єкта алгоритму виступає особливість побудови схеми папілярних ліній на зображенні пальця. Зображення ділиться на маленькі квадрати, розмір яких впливає на швидкість і складність реалізації алгоритму. Положення ліній в кожному квадраті описується параметрами синусоїдальної хвилі (зсув фази, напрямок і довжина хвилі). Саме ці параметри використовуються, як особливості відбитка і надалі порівнюються. Перевагою даного алгоритму є швидкість роботи і низькі показники вимог для якості зображень. Головним недоліком можна назвати складну реалізацію і математичну базу.

Наступний популярний алгоритм порівняння зображень називається кореляційний. Суть алгоритму дуже проста, зображення порівнюються за пікселями зі зміщенням кутів нахилу. Перевага алгоритму в тому, що він прекрасно працює з зображеннями поганої якості. Найбільший недолік це швидкість роботи. Якщо розглядати алгоритм з точки зору ідентифікації, час роботи порівняно великий. В останні роки цей алгоритм мало використовується.

Алгоритм порівняння шаблонів. Механізм роботи даного алгоритму схожий з роботою алгоритму знаходження і порівняння ключових точок, тільки в якості особливостей крім ключових точок використовуються додаткові характеристики. Це може бути будь-яка з глобальних особливостей пальця або додаткових параметрів для локальних. Наприклад: кут вигину папілярної лінії або її товщину, клас папілярного візерунка, відстань між лініями і ін. Алгоритм

не вимагає дорогих та складних обчислювальних засобів, але так само вимагає високої якості зображення.

Для програмної реалізації мультимодальної системи верифікації(див. розділ 4) мною був обраний найпопулярніший на сьогодні алгоритм порівняння відбитку на основі порівняння ключових точок.

Як було з'ясовано вище алгоритм розпізнавання відбитків пальців по ключових точках базується на трьох основних етапах: обробка зображення, виділення ключових точок та порівняння з еталоном.

На першому етапі зображення бінаризується та переводиться у чорно-білий формат, далі проводиться скелетизація, лінії папілярного візерунка зображення відбитка тоншають до одного пікселя, усуваються шуми і помилкові об'єкти, які можуть бути прийняті за ключові точки. Визначається контур відбитка, граничні точки та виділяються контрольні точки. Виділення контрольних точок і визначення координат цих точок виконується в первинній системі координат. Зіставлення двох відбитків пальців базується на порівнянні координат контрольних точок та їх типів(див. рисунок 3.7).

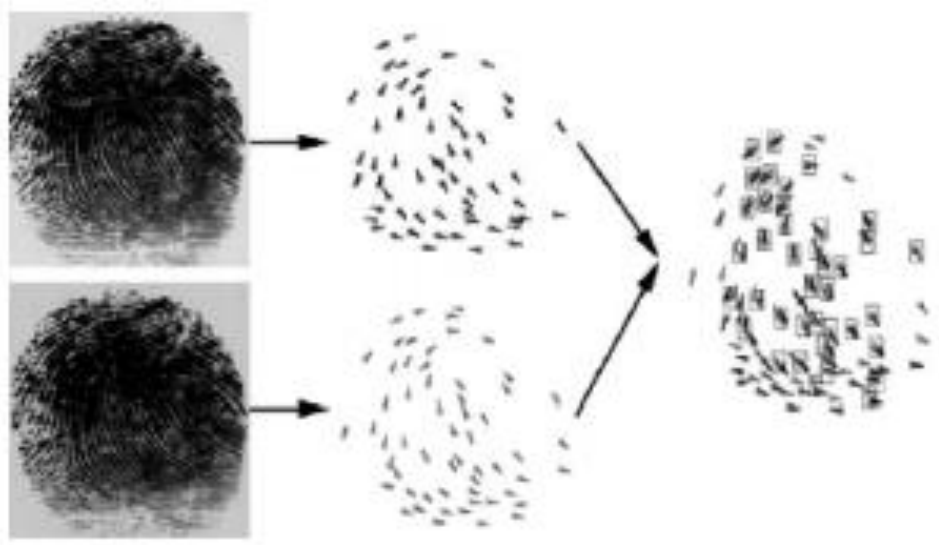

Рисунок 3.7 – Порівняння відбитків за ключовими точками

Порівняння контрольних точок проводиться кожна з кожною. В околиці кожної контрольної точки проводиться порівняння найближчих точок, якщо точка розташовується на допустимому віддаленні, то ці точки зараховуються, як збіг. Зсув контрольних точок може досягати до 10% від довжини рамки зображення відбитка пальця. Перед кожним зіставленням відбитків пальців обчислюється міра близькості двох відбитків пальців. Для визначення міри близькості вноситься невеликий кут повороту відбитка і зміщення його центру. Зіставлення виконуються до тих пір, поки не будуть перебрані всі можливі кути повороту одного відбитка і можливі поєднання пікселів центральної області.

Рішення про верифікацію приймається за найбільшим значенням міри близькості з усіх варіантів зіставлень, якщо воно не менше заданого порога. Число порівнянь контрольних точок двох відбитків необхідне для прийняття рішення про ідентифікацію дорівнює (3.1):

$$N_i = N_d * N_p * N_{sp} \quad (3.1)$$

де N_d – число кроків повороту одного відбитку; N_p– число пікселів у центральній області; N_{sp} – число контрольних точок в одному з відбитків.

Даний алгоритм дозволяє розділити зіставлення відбитків, а також знизити залежність ймовірності розпізнавання відбитку пальців від поворотів, зсувів. Швидкість розпізнавання відбитку збільшується завдяки додатковому етапу пошуку найбільш достовірних пар базових відрізків.

З графічного зображення виділяються ключові характерні точки з яких формується цифрова модель відбитка. У сучасних системах береться від 12- 24 ключових точок. Так як була проведена попередня бінаризація та скелетизація зображення забезпечує просту основу для виділення особливих точок. Першим кроком, щоб виділити ключові точки, необхідно здійснити покращення скелета зображення, тобто видалити помилкові точки, які з’явилися внаслідок скелетизації.

Для виділення особливих точок зображення розбивається на блоки 3х3 пікселів і до 8-ми сусідніх пікселів здійснюється підрахунок. Піксель у центрі виділеної області вважається особливою точкою, навколо нього здійснюється підрахунок. Підрахунок починається якщо центральний піксель є нульовим (чорним), після цього алгоритм дій простий – якщо навколо центрального пікселя існує ще один нульовий (чорний) піксель, то точка є кінцевою. Якщо навколо центрального пікселя існує два нульові (чорні) пікселя, то це точки папілярної лінії, які не мають відношення до ключових точок. Якщо навколо центрального пікселя існує три нульові (чорні) пікселя, то це точка подвоєння (див. рисунок 3.8).

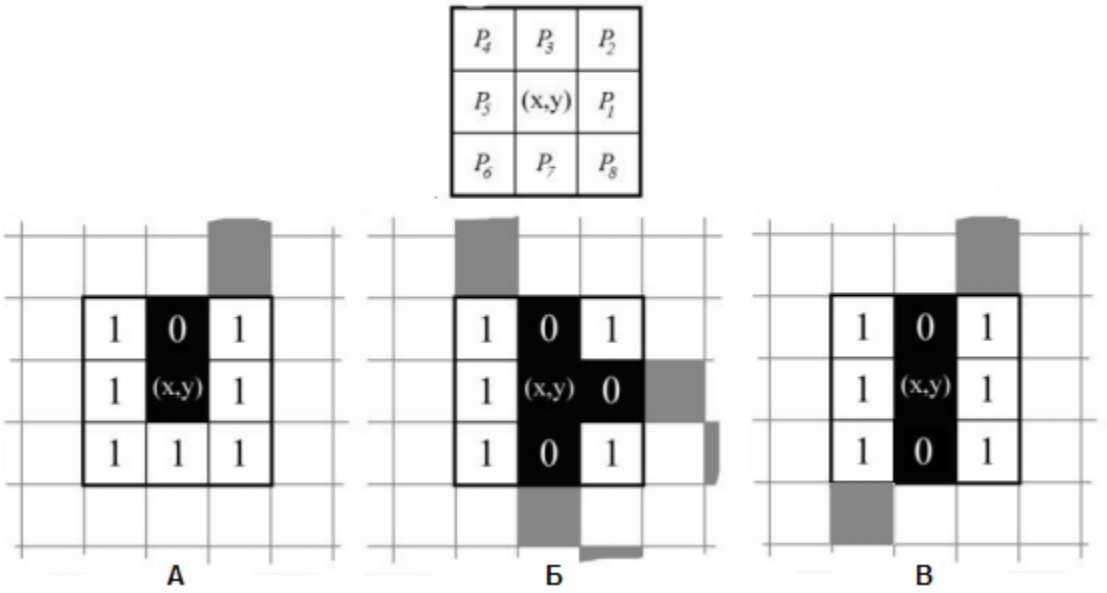

Рисунок 3.8 – Виділення особливих точок: А – кінцева точка, Б – точка подвоєння, В – точка лінії

Також, можна підрахувати точки перетину папілярних ліній, якщо в області зображення 2х2 пікселя, всі 4-ри пікселя є нульовими, то це точка перетину (див. рисунок 3.9).

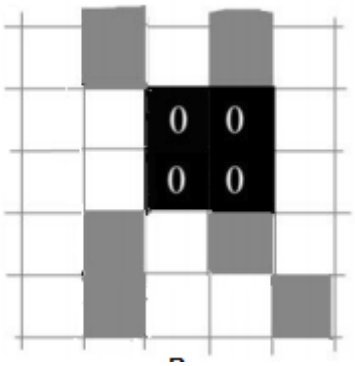

Рисунок 3.9 – Виділення особливих точок перетину

Порівняння особливих точок, здійснюється згідно обраного алгоритму. Найпростіший варіант виділити на зображеннях область певного розміру (від розміру залежить точність, з якою буде здійснюватися перевірка, оптимально 30х30 пікселів). Послідовність виділених особливих точок порівнюється за збіжністю точок одного типу у відповідній області. Підраховується кількість точок, які збіглися та сумарна кількість усіх точок та розраховується вірогідність приналежності.

При виборі більшої кількості ключових точок, сучасних обчислювальних ресурсів не достатньо для швидкої роботи системи в зв’язку з високою

обчислювальною складністю. При виборі меншої кількості точок, існує велика ймовірність допуску чужого відбитка пальця. Тому необхідно розраховувати оптимальне значення, для вирішення обох проблем. У зв'язку з цим алгоритм розпізнавання відбитків має середні показники FAR и FRR (див. пункт 1.2) На сьогоднішній день значення даних параметрів FRR-0.01%, FAR-0.000001%. Таким чином можливо для кожного конкретного випадку обирати або високу швидкість розпізнавання, або високу безпеку системи.

Головною перевагою представленого алгоритму є велика швидкість його роботи та відносна простота реалізації. Саме ці фактори сприяли тому, що на сьогоднішній день алгоритм розпізнання образу відбитка пальця за ключовими точками є найпоширенішим у даному класі біометричних систем автентифікації.

Недоліками даного методу порівняння зображень відбитків є досить критичні вимоги до якості зображення, тобто зображення повинно мати достатньо високий дозвіл, а умови його отримання майже ідеальні (датчик та палець повинні бути сухими та чистими). Якщо розглядати алгоритм з точки зору ідентифікації людини, його швидкодія також значно знижується.

3.3 Вразливості та варіанти їх вирішення для систем верифікації за відбитками пальців

Відомий факт, що існує ряд переваг біометричних технологій в порівнянні з традиційними методами ідентифікації. Ухвалення адекватних заходів проти збільшення ризиків безпеки в сучасному світі, супроводжується переходом на системи ідентифікації нового покоління на основі біометричних технологій. Тому самі біометричні системи повинні задовольняти високим вимогам безпеки.

Найпопулярніша біометрична система верифікації на сьогодні заснована на порівнянні відбитків пальців. На жаль, виробники даних біометричних технологій не завжди враховують заходи безпеки. У публікаціях, присвячених біометричним технологіям на основі відбитків, вказуються недоліки та слабкі місця цих технологій (див. рисунок 3.9).[3] Оскільки біометрія за відбитками становить технологічну основу для великомасштабної і дуже чутливою системи ідентифікації, яка вже використовується в Україні (наприклад, біометричні або закордонні паспорти), проблема адекватної оцінки безпеки даних біометричних технологій є актуальною.

Рисунок 3.10 – Атаки на біометричні системи верифікації

Систематичні дослідження з аналізу безпеки технології верифікації основаних на біометрії з'явилися тільки в останні роки. У цьому пункті атестаційної роботи пропонується підхід до аналізу проблем безпеки біометричних систем і варіантів їх вирішення.

Уразливості біометричних систем в основному пов'язані зі структурою системи, біометричної системою. В першу чергу була проаналізована структура алгоритму (див. пункт 2.1 та 2.2) і проведений пошук слабких місць системи біометричної верифікації на основі відбитків пальців. Логічна структура аналізованої системи складається з чотирьох основних модулів (див. рисунок 3.10):

– сенсор (датчик зчитування відбитку);
– модуль вилучення ознак;
– модуль порівняння;
– база даних еталонів.

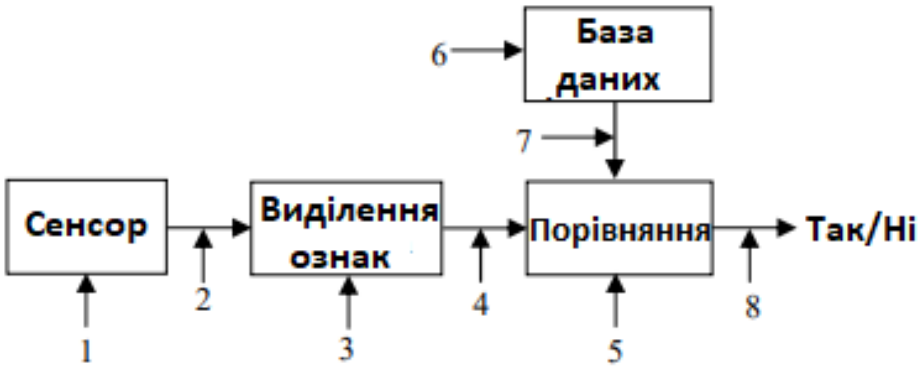

Рисунок 3.10 – Вразливі місця системи

1. Надання датчику підробленого біометричного зразка. Підроблений біометричний зразок, наприклад підроблений палець або його зображення для датчика, щоб потрапити в систему.

2. Відтворення збережених цифрових сигналів для підміни біометрії: збережений сигнал відтворюється в системі ігноруючи датчик. Наприклад, відтворення старої копії зображення відбитка пальця.

3. Відмова в отриманні ознак: набір ознак формується самозванцем за допомогою вкрадених даних з системи.

4. Підміна біометричної характеристики. Ознаки, витягнуті з вхідного сигналу, замінюються підробленими.

5. Атака на порівняння: атаки на відповідний модуль призводять до заміни оцінок збігів підробленими.

6. Підміна шаблонів в базі даних: база даних збережених шаблонів може бути локальною або віддаленою. Зловмисник робить спробу підробити один або кілька біометричних шаблонів в базі даних. В результаті чого підроблена особистість авторизована або законний користувач стикається з відмовою в обслуговуванні.

7. Атака на канал між базою даних шаблонів і відповідним модулем: в той час, як шаблони передаються по каналу зв'язку в базу даних, дані в каналі можуть бути змінені зловмисником.

8. Протидія процесу остаточного рішення: якщо остаточне рішення може бути припинене або заблоковане, тоді функція системи автентифікації буде скасована.

Структура, архітектура, виробництво або впровадження чужої системи в біометричну також можуть підвищувати в ній уразливості. Є чотири основних точки уразливості:

– операційні системи;
– біометричне прикладне програмне забезпечення;
– програмне забезпечення для датчика;

– обладнання та драйвери.

Виходячи з цього можемо сформувати загальний список актуальних проблем для всіх типів систем біометричної верифікації:

– Адміністрування: умисні або ненавмисні адміністративні помилки.

– Користувач: законний користувач хоче підвищити свої привілеї до адміністративного рівня.

– Підміна: підроблені біометричні дані використовуються для автентифікації в якості законного користувача.

– Імітація: зловмисник імітує біометричні характеристики законного користувача.

– Не виявлення: атаки, які не виявлені системою, можуть стимулювати нові атаки.

– Стійкість до відмов: результат ненормальних умов використання біометричної системи.

– Електроенергія: відключення електроенергії.

– Сила: обхід біометричної системи для доступу. Цього можна досягти, доклавши фізичні зусилля проти законного користувача, щоб надати датчику біометричні дані.

– Фальсифікація: підробка обладнання системи.

– Муляж: слід відбитка може бути використаний для створення штучних відбитків пальців.

– Атака методом грубої сили: зловмисник повторно представляє біометричні характеристики системі для того, щоб пройти автентифікацію. Цей тип атаки залежить від параметра FAR.

– Атаки близнюків: біометричні характеристики самозванця дуже схожі на характеристики зареєстрованого користувача.

– Підроблений шаблон: введення підробленого біометричного шаблону в базу даних або на смарт-карти.

– Шум: доступ може бути отриманий зловмисником при впливі шуму на систему отримання біометричних даних.

– Відмова в обслуговуванні: атака відмови в обслуговуванні спрямована на те, щоб перешкодити користувачеві отримати законний сервіс.

Отже, в біометричних системах існує безліч точок атаки і проблем. Використовуючи наведений список з них, можна ідентифікувати уразливості для конкретних систем. Біометрична система може не мати всіх проблем або точок атаки. Список досить загальний і легко застосовний до будь-якої системи. Для конкретної системи важливо враховувати її властивості для виявлення можливих проблем. Мета аналізу проблем – визначити можливість використання слабких місць в біометричних системах, для подальшого вирішення цих проблем.

Існує три категорії порушників загроз для біометричних систем.

Самозванець: людина, яка навмисно чи ненавмисно прикидається уповноваженим. Самозванець може бути авторизований чи ні.

Зловмисник: будь-яка особа або будь-яка система, яка намагається порушити роботу біометричної системи. Мотивом може бути несанкціонований доступ або відмову\а в обслуговуванні.

Авторизовані користувачі: авторизовані користувачі біометричної системи, ненавмисно компрометуючі біометричний пристрій або систему. Ця категорія відповідає ненавмисним людським помилкам, наприклад помилки адміністратора при налаштуванні системи.

Важливо розробити і провести тести на проникнення для кожної атаки з використанням певних проблем. Тому існує проблема правильної методології тестування для визначення стійкості біометричних систем за рахунок вжитих заходів протидії певним атакам.

Як заходи, які можуть значно убезпечити біометричні системи верифікації можна назвати наступні: для атак на сенсор, можна використовувати додаткові перевірки, що б скомпрометувати муляж, наприклад зчитувати температуру пальця або попросити користувача його змістити, для атак на внутрішні модулі систем, необхідна використовувати незворотні функції, шифрувати ключові шаблони, а так само використовувати додатковий фактор автентифікації, це може бути PIN-код, пароль, токен або інший варіант системи заснованої на біометричних характеристиках людини (див. розділ 4).

4 РОЗРОБКА МОДЕЛІ МНОГОМОДАЛЬНОЇ БІОМЕТРИЧНОЇ СИСТЕМИ ВЕРИФІКАЦІЇ ЗА СТРУКТУРОЮ РАЙДУЖНОЇ ОБОЛОНКИ ОКА ТА ВІДБИТКУ ПАЛЬЦЯ

Сумуючи проведений аналіз у розділах 1, 2 та 3 атестаційної роботи було зроблено висновок, що з усіх варіантів систем біометричної верифікації людини найбільш надійними є системи на основі порівняння структури райдужної оболонки ока та відбитків пальця. Наведенні системи мають найбільш високі показники, за якими оцінюються біометричні системи верифікації. Також наведені системи широко використовуються у світі та добре проаналізовані світовими експертами.

Вище зазначені системи мають найнижчі показники помилок першого роду (відмова у доступі користувачеві, що має на це право) та помилок другого роду (пропуск користувача, що не має права доступу). Виходячи з усього вище описаного для розробки мультимодальної системи верифікації було обрано саме ці варіанти біометрії.

Обрані методи біометричної верифікації мають свої особливості та алгоритми, які можна розділити на два основних напрями: обробка вхідного зображення та виділення ключових точок для порівняння. Для кожного варіанту біометрії алгоритми обробки та виділення різні (див. розділ 1 та 2), але загальна схема для різних варіантів систем залежить від цілей її призначення.

4.1 Мета створення моделі мультимодальної системи верифікації

Захист на основі біометричних параметрів людського тіла, зокрема за відбитком та райдужкою, має низку незаперечних плюсів: комфортність, простота та безпека. Весь процес автентифікації проходить швидко та є автоматизованим і не вимагає від користувача додаткових дій для отримання доступу в систему.

Проведений аналіз також показав, що використання відбитка та райдужки для верифікації користувача є одними з найбільш зручних біометричних систем. Імовірність помилок першого та другого роду при автентифікації людини за допомогою мультимодальної системи набагато менше в порівнянні з біометричними системами верифікації, які використовують одну характеристику. Крім того, пристрої зчитування приведених характеристик досить поширені та компактні.

У більшості випадків робота з важливою інформацією має на увазі також своєчасне прийняття рішень і безперервне управління ходом виконання. У зв'язку з цим існує необхідність безперервного підтвердження особи (в разі якщо

людина з якоїсь причини покине своє робоче місце, то будь-хто в цей час зможе задавати команди управління або здійснити перегляд конфіденційної інформації). Таке підтвердження особи значно полегшується так, як система може працювати автоматично, а вводити пароль після кожної команди – це досить обтяжливий процес.

Хоча на ринку існують готові системи біометричної верифікації, але на ряду зі своїми перевагами вони мають ряд недоліків, таких як закритість вихідного коду і алгоритму, а також висока ціна та недбале збереження ключових шаблонів біометричних характеристик. Внаслідок чого є сенс в розробці системи, яка б надавала можливість всім розробникам мати готову базу для розробки власних проектів на основі мультимодальних біометричних технологій.

Створювана система носить пошуково-дослідницький характер і спрямована на полегшення розробки алгоритмів обробки зображень та виділення ключових особливостей, спрощення аналізу експериментальних даних і виявлення загальних закономірностей.

4.2 Розробка моделі мультимодальної системи верифікації

При автентифікації використовується один або кілька механізмів, щоб показати, що ви є тим, за кого себе видаєте. Сучасні дослідження показують, що відбитки пальців не так захищені, як захищений пароль, що складається з букв і цифр, цифр і спеціальних символів. Дана модель пропонує замість пароля райдужну оболонку користувача, яка також є однією з найнадійніших систем розпізнавання фізіологічної біометрії.

Однак використання райдужки може мати і деякі недоліки, пов'язані з серйозними порушеннями безпеки, які були представлені в пункті 2.4. На тій підставі, що риси райдужної оболонки обмежені і незмінні, якщо зловмисник отримує доступ до бази даних, в якій вони збережені, безпека системи може бути непоправно скомпрометована. Щоб впоратися з цією проблемою, питання захисту структури шаблону райдужної оболонки стає дуже важливим. Теж саме можна сказати і про систему біометричної верифікації на основі розпізнавання відбитків пальців (див. пункт 3.4).

В даному пункті обговорюється модель багатофакторної біометричної автентифікації, яка допоможе вирішити всі вище перераховані вразливості.

Огляд літератури показує, що вже є багато досліджень пов'язаних з багатомодульною системою біометричної верифікації [1-5]. Але в цьому дослідженні основна увага приділяється моделі багатофакторної автентифікації з використанням відбитка пальця і розпізнавання райдужної оболонки.

Один тільки відбиток пальця не забезпечує повної безпеки; в цілях підвищення безпеки системи відбитків пальців вона була поєднана з розпізнаванням райдужної оболонки користувача. Основні цілі дослідження в даному пункті:

– Обґрунтувати мету створення моделі (див. пункт 4.1).

– Побудувати модель багатомодульної системи біометричної верифікації за структурою райдужки і розпізнання відбитків пальців з урахуванням всіх методів обробки вхідних зображень і алгоритмів виділення і порівняння ключових точок.

– Дати характеристику функціональної структури розробленої моделі для мультимодальної системи верифікації.

– Проаналізувати побудовану модель з точки зору її прогнозуючих переваг та недоліків.

В ході проведеного аналізу в розділах 2 і 3, було зроблено висновок, що для систем біометричної верифікації заснованої на розпізнаванні райдужки і відбитків пальців можна виділити два етапи роботи. Перший етап роботи має на увазі обробку вхідних зображень, другий - виділення і порівняння наборів ключових точок на зображенні, для пальця це візерунок папілярних ліній, для райдужної оболонки - особливі точки, які інваріантні для масштабу або повороту зображення.

При обробці зображень біометрії для райдужки існує загальний алгоритм дій які необхідно впровадити в систему, а саме: сегментація та нормалізація зображення. Для відбитка пальця основними етапами обробки є бінаризація та скелетизація зображення. В якості методу скелетизації було вибрано шаблонний алгоритм (див. пункт 3.1).

Для виділення ключових точок на зображенні райдужної оболонки ока був обраний алгоритм SIFT (див. пункт 2.2). У свою чергу для відбитків пальців найперспективнішим є алгоритм порівняння з особливих точок (див. пункт 3.2). Виходячи з усього перерахованого вище була побудована наступна модель багатофакторної біометричної верифікації (див. рисунок 4.1).

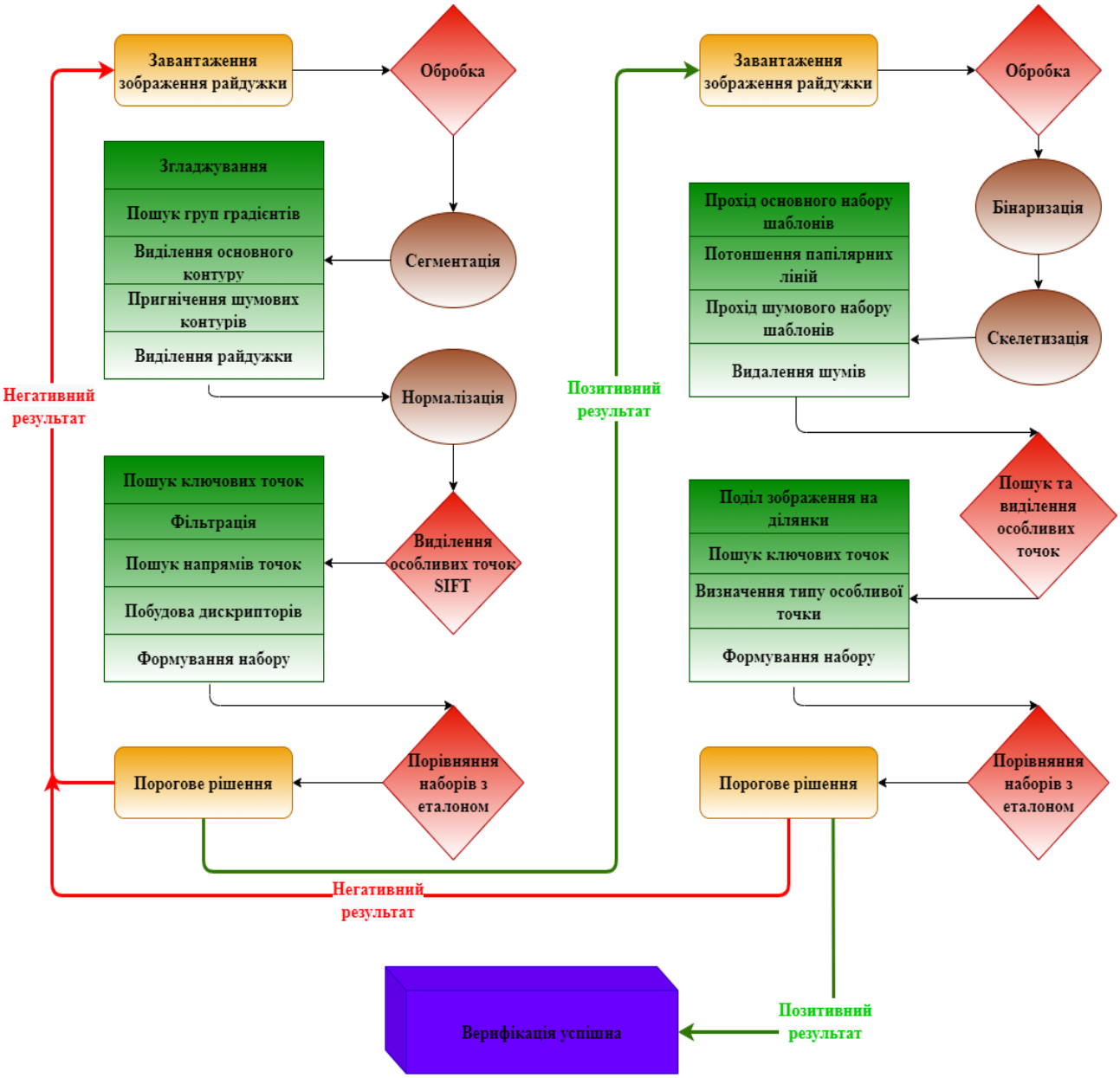

Рисунок 4.1 – Модель мультимодальної біометричної системи верифікації

4.3 Функціональна характеристика розробленої моделі

Функціональна характеристика розробленої моделі (див. рисунок 4.1) мультимодальної біометричної верифікації людини за структурою райдужної оболонки ока і розпізнавання відбитку пальця.

1. Завантаження першого зображення в модуль верифікації особистості по структурі райдужної оболонки ока.

2. У підсистемі аналізу і обробки зображення райдужної оболонки відбувається сегментація за допомогою оператора Кенні (див. пункт 2.1). Зображення фільтрується і розмивається, пікселі з великою різницею значень градієнтів розбиваються на групи, на кордоні груп виділяються кордони

райдужки і утворюється основна лінія краю, придушуються всі елементи які перетинають і не є основною крайової лінією. Далі зображення нормалізується, зображення райдужної оболонки розгортається в полярну систему координат і приводиться до одного єдиного розміру і формату.

3. У підсистемі виділення ключових точок відбувається пошук особливостей зображення, за допомогою розмиття і отримання різниць зображень розмитих з різним значенням фільтра. Далі відбувається фільтрація знайдених точок і перевірка на їх становище, а також достатню освітленість. Для відфільтрованого списку точок, за допомогою точок їх околиці, визначається їх напрямок. Після знаходження напрямків, також визначаються напрямки для точок сусідніх з ключовою і на основі цього будується дескриптор (див. пункт 2.2).

4. Розпізнавання райдужки відбувається шляхом порівняння координат ключових точок і їх дескрипторів з аналогічними даними отриманих з зображення еталона.

5. Підсистема визначення, на основі порога, вирішує результат верифікації. Якщо результат позитивний програма продовжує роботу і переходить до другого модулю виконання, а саме до порівняння відбитків, в іншому випадку програма повертає користувача на перший етап і виводить повідомлення про невдалу спробу верифікації.

6. Завантаження другого зображення в модуль порівняння відбитків пальців.

7. У підсистемі аналізу і обробки другого модуля, зображення проходить порогову бінаризацію і скелетизацію за допомогою шаблонів. Далі визначаються і видаляються шуми, які утворилися в результаті шаблонної скелетизації зображення (див. пункт 3.1).

8. Система пошуку ключових точок ділити отриманий образ на ділянки, після чого відбувається прохід з метою пошуку особливих точок. У набір ключових точок, потрапляють координати і тип знайденої точки (див. пункт 3.2).

9. Розпізнавання відбитка щодо еталона відбувається на основі параметрів кожної точки з двох наборів.

10. Система визначення порогу, яка визначає результат верифікації на основі зіставлення відбитків пальців. При позитивному рішенні програма повідомляє користувачеві, що верифікація пройшла успішно, інакше програмна реалізація повертається до пункту 1 в даному списку.

4.4 Аналіз розробленої моделі

Розроблену в даному розділі модель для програмної реалізації мультимодальної системи біометричної автентифікації можна проаналізувати використовуючи її прогнозуючі переваги і недоліки.

Переваги побудованої моделі:

– Ключовий шаблон райдужної оболонки або відбитка пальця в даній моделі можна розглядати як заміну пароля, який зазвичай використовується для додаткового фактору біометричної верифікації, що мінімізує можливість втрати даних, для верифікації так, як відбиток або райдужка прив'язані до користувача на все життя;

– Відбиток пальця в поєднанні з райдужною оболонкою ока значно підвищує безпеку системи верифікації

– Сучасне дослідження показує, що відбиток пальця, як і райдужна оболонка не є секретними даними так, як вони відкриті і прив'язані до користувача і при великому бажанні приховати їх не можливо. На відміну від ключового шаблону цих характеристик використовуваних в системах автентифікації. Реалізована модель повністю мінімізує наслідки крадіжки або підробки однієї з цих характеристик.

– Якщо розглядати хеш ключового шаблону відбитка або райдужної оболонки, як додатковий індекс ключ, значення захисту одного з цих факторів значно зменшується. У гіршому випадку, якщо зловмисник отримає зображення відбитка пальця, воно просто діє як додатковий ідентифікатор, а не в якості основного ключа для верифікації, відповідно зловмисник не зможе зламати систему використовуючи тільки відбиток пальця або райдужну оболонку.

– Користувачеві не потрібно нічого запам'ятовувати; Розпізнання відбитків пальців і райдужної оболонки ока система проводить автоматично, що значно прискорює і спрощує процес верифікації.

Обмеження і недоліки системи розробленої системи мультимодальної біометричної верифікації:

– У користувача повинна бути хороша конфігурація мобільного пристрою з високоякісною камерою і чутливим сенсором для зчитування відбитку.

– Під час захоплення зображення райдужної оболонки і сканування відбитку користувач повинен зосередитися. Розташувати мобільний камеру прямо і в фіксований кут для захоплення зображення, знаходиться в добре освітленому приміщенні. Сканер відбитка і сканований палець повинен бути сухим.

– Погане покриття мобільної мережі в Україні створює ймовірність відмови в системі через те, що система вчасно не отримала вхідні зображення.

– Комплексний механізм розпізнавання райдужної оболонки ока і відбитка пальця робить систему дорожче.

– Користувач не може бути перевірений або авторизований без коректних вхідних зображень.

– Модель багатофакторної автентифікації, розроблена в атестаційної роботі не підходить для систем, які не використовують мобільний телефон, ноутбук або додаткові технічні засоби для своєї роботи.

– Модель багатофакторної автентифікації, яка використовується в якості дослідження вимагає архітектури клієнт-сервер і є даремною для автономних систем, які не використовують додаткові технічні засоби для зчитування біометричних характеристик.

5 ОПИС ПРОГРАМНОЇ РЕАЛІЗАЦІЇ МУЛЬТИМОДАЛЬНОЇ СИСТЕМИ ВЕРИФІКАЦІЇ

5.1 Постановка задачі програмної реалізації

Реалізувати програму для здійснення многомодальної верифікації людини за структурою райдужної оболонки ока і відбитку пальця. Вхідні зображення необхідно обробити, виділити набір ключових точок та порівняти зображення з існуючим еталоном у базі. У програмі необхідно реалізувати два основних модулі. Перший модуль для роботи з зображенням райдужної оболонки ока. Модуль повинен приймати, обробляти, порівнювати два зображення з райдужними оболонками ока та виводити результати перевірки користувачу.
Таким чином, було розроблено наступний алгоритм для реалізації першого модуля програми верифікації:

– реалізувати простий інтерфейс для роботи з користувачем;

– реалізувати функцію для вибору вхідних зображень та подальшого порівняння райдужних оболонок ока;

– реалізувати функцію, яка здійснює бінаризацію вхідних зображень;

– реалізувати функцію, яка здійснює сегментацію райдужної оболонки ока;

– реалізувати функцію для пошуку особливих та формування набору ключових точок;

– реалізувати функцію для здійснення порівняння ключових точок з еталоном;

– забезпечити можливість перегляду результатів роботи програми, після кожного етапу обробки зображень;

– розробити функцію для представлення результату порівняння користувачеві. Якщо результат верифікації негативний, виводити користувачу відповідне повідомлення з проханням пройти верифікації знову, якщо результат верифікації позитивний – переходити до другого модуля програми.

Другий модуль програмного забезпечення повинен приймати зображення відбитків пальця для подальшої верифікації. Модуль повинен включати в себе наступний функціонал:

– інтерфейс для вибору порівнюваних зображень відбитків пальця;
– функцію для бінаризації зображень;
– функцію для скелетизації зображень;
– функцію для пошуку, виділення та формування набору ключових точок;
– функцію для порівняння двох сформованих наборів особливих точок;
– функцію для виводу результату роботи користувачу.

Якщо верифікація пройшла успішно користувач повинен бачити оброблені зображення відбитків пальців з виділеними ключовими точками та процент точок, що збіглися, якщо результат верифікації негативний, то користувачу виводиться відповідне повідомлення з проханням повернутися до першого етапу та пройти верифікацію спочатку.

5.2 Загальні відомості

У даній атестаційній роботі реалізований алгоритм, який забезпечує многомодальну біометричну верифікацію людини за структурою райдужної оболонки ока та відбитку пальця. Алгоритм реалізований на мові Python, операційною системою Windows 10 (x64).

На першому етапі роботи програмна реалізація приймає два інфрачервоних зображення очей, як вхідні дані та дає відповідні оцінки після порівняння двох райдужних оболонок. Програмна реалізація вирішує, чи відповідають вхідні зображення одній людині. Спочатку алгоритм локалізує область райдужної оболонки ока на двох зображеннях очей, ідентифікує та кодує ключові точки, що характеризують кожну з райдужних оболонок, а потім використовує алгоритм SIFT, наданий OpenCV, для порівняння двох наборів ключових точок. SIFT (Scale-invariant feature transform) – це алгоритм, який використовується в комп'ютерному зорі для виявлення та опису локальних особливостей на зображеннях. Для тестування була використана база даних зображень райдужної оболонки, надана Інститутом автоматики Китайської академії наук (CASIA), що містить понад 15 тисяч зображень очей. Мною було проведено 30 тестових експериментів. Якщо обрано правильний поріг порівняння та коректні параметри для сегментації райдужної оболонки коефіцієнт помилкового прийняття дорівнює 0 (відсутність збігів у порівнянні між оболонками ока двох різних осіб). У свою чергу коефіцієнт помилкового відхилення становить близько 25%, тобто алгоритм дає правильну відповідь у 75% випадків при порівнянні зображень райдужної оболонки ока, що належать одній людині.

Після порівняння зображень райдужних оболонок ока формується результат перевірки на основі встановленого порогу порівняння, якщо результат негативний, користувач отримує відповідне повідомлення з проханням пройти верифікацію знову, якщо результат роботи першого модуля позитивний програма переходить до другого модулю перевірки.

На другому етапі роботи програма приймає два чорно-білих зображення відбитків пальців. Вхідні зображення скелетизуються за допомогою шаблонного методу скелетизації (див. пункт 3.1). На отриманих скелетах зображень виконується пошук ключових точок та формується їх список. Список зберігає у собі координати ключових точок, а також їх тип (кінцева, точка подвоєння або

точка перетину папілярних ліній). Набори ключових точок порівнюються на відповідних ділянках зображення та формується результат порівняння у відсотковому співвідношенні (результат позитивний, якщо відсоток збігів більше ніж 75), після чого користувачеві виводиться кінцевий результат верифікації (див. рисунок 5.1)

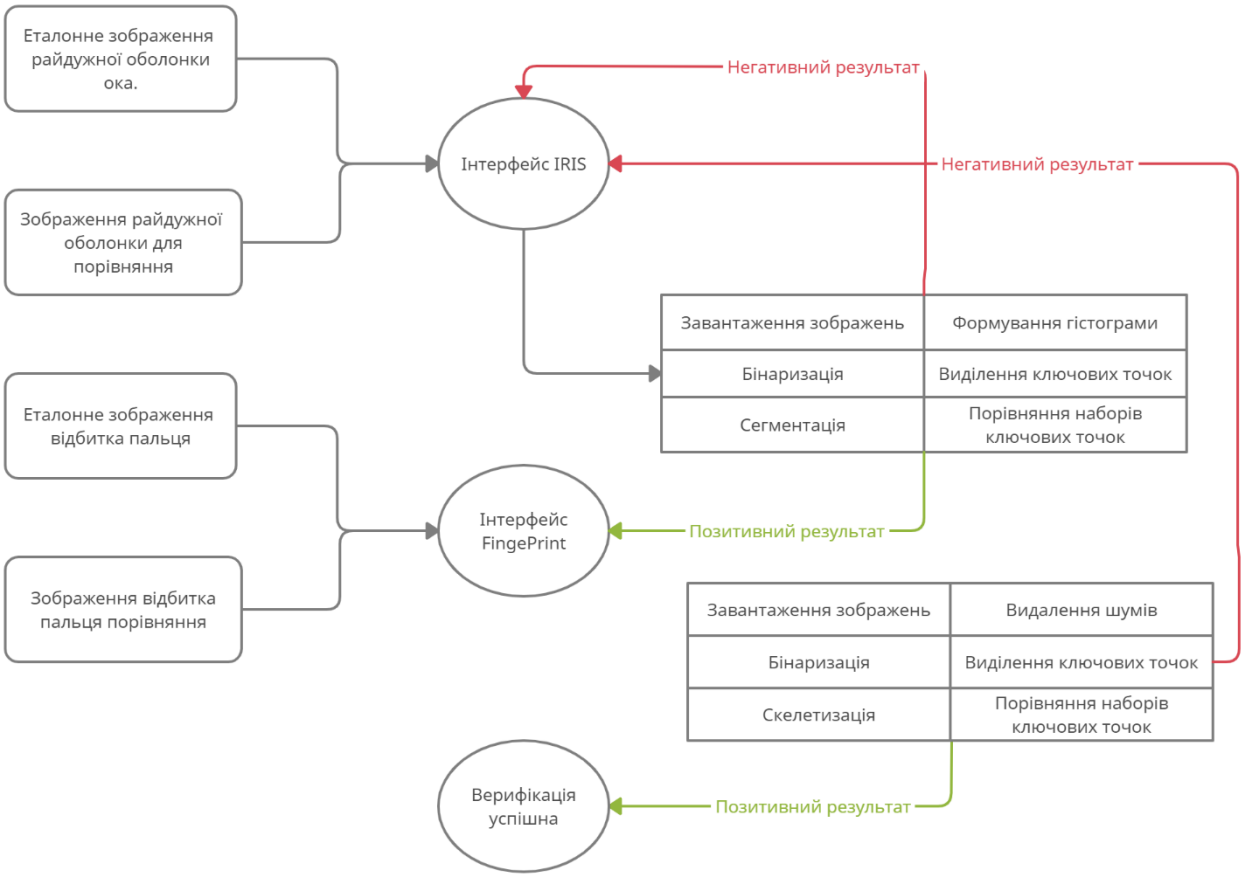

Рисунок 5.1 – Загальна схема програмної реалізації

Код реалізованої програми MultiFactorBiometric.exe знаходиться у двох файлах. Перший файл має назву irisRecognition.py, файл відповідає першому модулю програми та призначений для роботи з райдужними оболонками ока. Другий файл має назву fingerPrint.py, файл реалізує вище описаний другий модуль програми, який відповідає за роботу з зображеннями відбитків пальців.

Програмна реалізація призначена для здійснення многомодальної верифікації людини на основі райдужної оболонки ока та відбитка пальця. Програма обробляє вхідні зображення біометричних характеристик людини, а саме зображення райдужних оболонок та відбитків пальця, виділяє особливі точки на зображеннях, здійснює порівняння та виводить відповідний результат.

Програма запускається за допомогою файлу MultiFactorBiometric.exe, у папці MultiFactorBiometric. Також програму можна запустити, за допомогою

файлів у яких міститься код, якщо на комп'ютері встановлені відповідні програмні засоби (див. пункт 5.4).

Вхідні дані обираються користувачем самостійно та можуть знаходитися як на персональному комп'ютері користувача, так і на переносному диску. Зображення можуть мати будь-який сучасний та поширений формат, рекомендовано: jpg або png.

Вихідні дані першого модулю відображаються після завершення кожного етапу обробки, після перегляду результату для продовження потрібно натиснути будь-яку клавішу. Відображення роботи згідно етапу:

1. Відображення вхідного інфрачервоного зображення.
2. Виділення контуру зіниці та райдужної оболонки.
3. Сегментація зображення.
4. Сегментоване зображення з виділеними ключовими точками.
5. Порівняння сегментів вхідних зображень, виділення точок, що збіглись на кожному сегменті.
6. Також у консолі відображається загальна кількість ключових точок на кожному сегменті райдужної оболонки ока.

Вихідні дані другого модулю відображаються у вікні результату, який містить оброблені зображення відбитків пальців з виділеними ключовими точками. Сині точки є кінцевими точками папілярних ліній, червоні – точки подвоєння, зелені – точки перетину. Також у вікні результату відображене відсоткове співвідношення між особливими точками вхідних зображень та кінцевий результат верифікації.

5.3 Використовувані технічні та програмні засоби

Для запуску програми немає необхідності у використанні потужного персонального комп'ютера. Програма може запускатися на персональному комп'ютері будь-якої конфігурації. Особисто мною для реалізації поставленої задачі та тестування було використано комп'ютер наступної конфігурації:

– процесор: Intel Core i3-10100M 3.6GHz/6MB;
– оперативна пам'ять: 8.00 ГБ;
– вінчестер: 750 ГБ;
– відеокарта: AMD Radeon HD 6370 2ГБ;

Встановлена операційна система Windows 10. Тип системи: 64-розрядна операційна система, процесор x64.

Програмна реалізація була розроблена у середовищі JetBrains PyCharm версії 2020.1.1 x64. PyCharm –середовище для програмної розробки на мові програмування Python. Програма була протестована за допомогою інтерпретатора мови Python версії 2.7.6

Для програмної реалізації також було використано декілька сторонніх бібліотек: PIL (бібліотека Python призначена для роботи з растровою графікою), numpy (модуль, який включає в себе загальні математичні та числові операції, у вигляді реалізованих функцій), cv2 (бібліотека комп'ютерного зору, призначена для обробки, аналізу та класифікації зображень), cPickle (модуль призначений для перетворення довільного об'єкта у серію байтів), matplotlib (бібліотека двовимірної графіки, для створення зображень), cx_Freeze (бібліотека для компіляції коду Python у програму формату .exe)

5.4 Опис логічної структури програми

Алгоритм роботи першого модулю програми:

– завантаження вхідних зображень райдужної оболонки ока;
– зчитування вхідних зображень;
– бінаризація зображень;
– сегментація райдужної оболонки ока
– виділення особливих точок;
– порівняння особливих точок;
– вивід результату порівняння;
– вибір подальших дій, згідно результату.

Основні функції першого модулю програмної реалізації:

Функція "vidjet" відповідає за простий інтерфейс першого модулю включає в собі три функції "openRef" для вибору перевіреного зображення райдужної оболонки ока, "openVer" для вибору перевірочного зображення та "start" виконує запуск програми(див. рисунок 5.2).

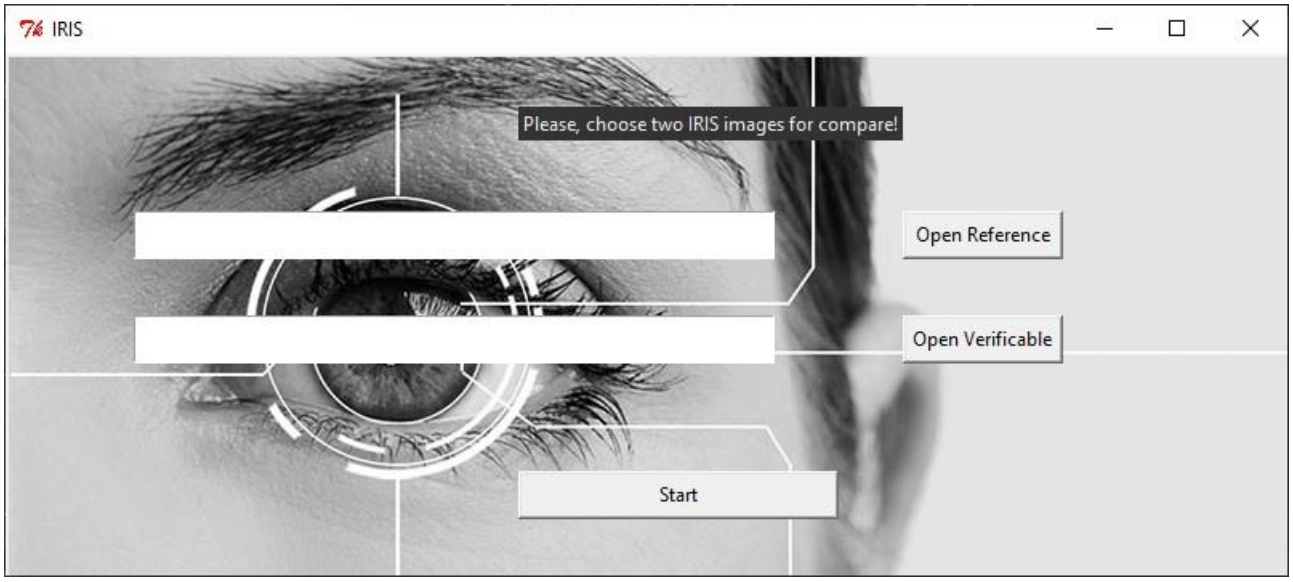

Рисунок 5.2 – Результат роботи функції "vidjet"

Функція “loadImage” виконує завантаження зображення до системи, якщо функція відпрацьовує успішно, користувачу виводиться завантажене зображення. Якщо зображення не було завантажено програма повернеться до головного вікна (див. рисунок 5.3).

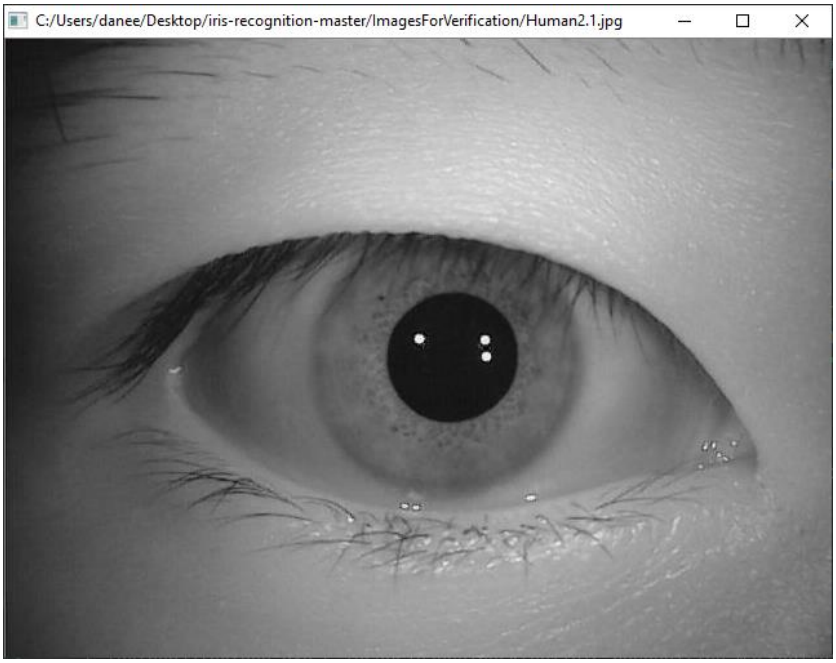

Рисунок 5.3 – Результат роботи функції “loadImage”

Функція getEdges забезпечує бінаризацію зображення, виділення меж зіниці та райдужної оболонки ока, виводить результат роботи (див. рисунок 5.4).

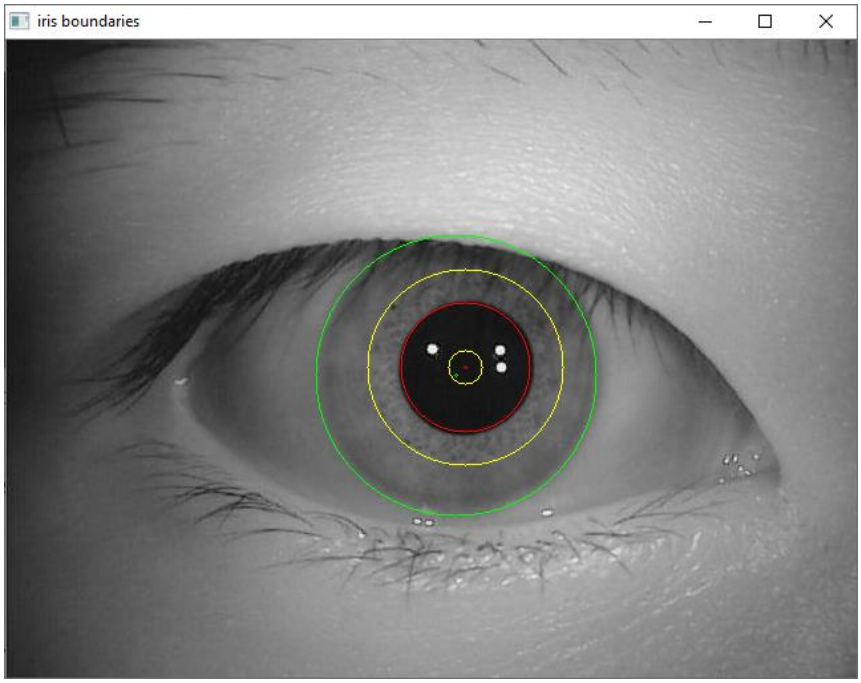

Рисунок 5.4 – Результат роботи функції “getEdges”

Функція “getEqualizedHistogram” маскує верхню частину райдужної оболонки ока на яку зазвичай накладаються вії та яка частково прихована повіками. Генерує вирівняну гістограму ока (див. рисунок 5.5).

Рисунок 5.5 – Результат роботи функції “getEqualizedHistogram”

Функції “getRois” “loadKeypoints” та “loadDescriptors” розбивають оброблені зображення на сегменти, виділяють та позначають ключові точки на зображенні (див. рисунок 5.6).

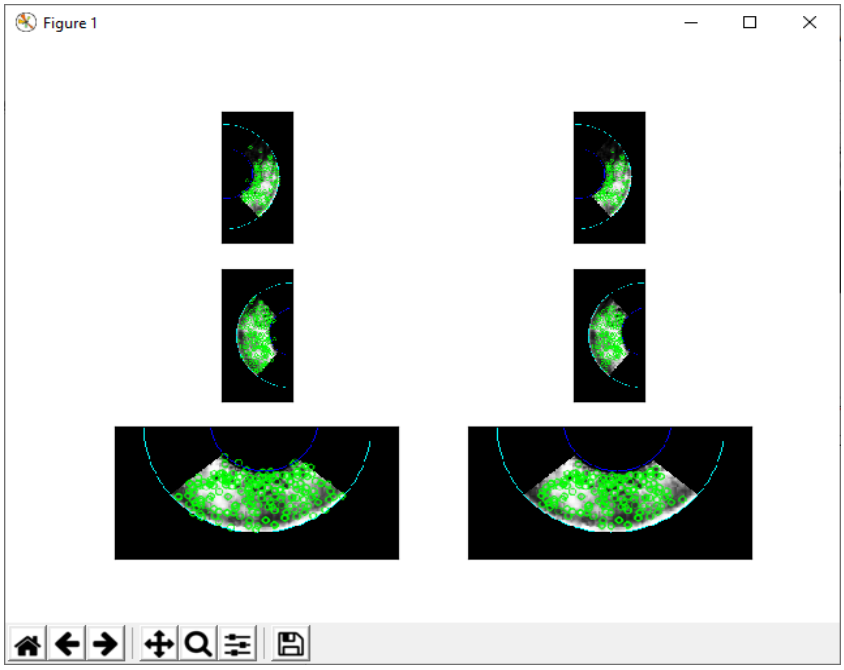

Рисунок 5.6 – Результат роботи функцій “getRois” “loadKeypoints” та “loadDescriptors”

Після усіх вище зазначених кроків аналогічні дії виконуються с другим вхідним зображенням. Коли сформовані обидва набори особливих точок, викликається функція “getAllMatches” яка відповідає за порівняння та виділення повного набору особливих точок, які збіглися на обох вхідних зображеннях, результат порівняння виводиться на екран (див. рисунок 5.7)

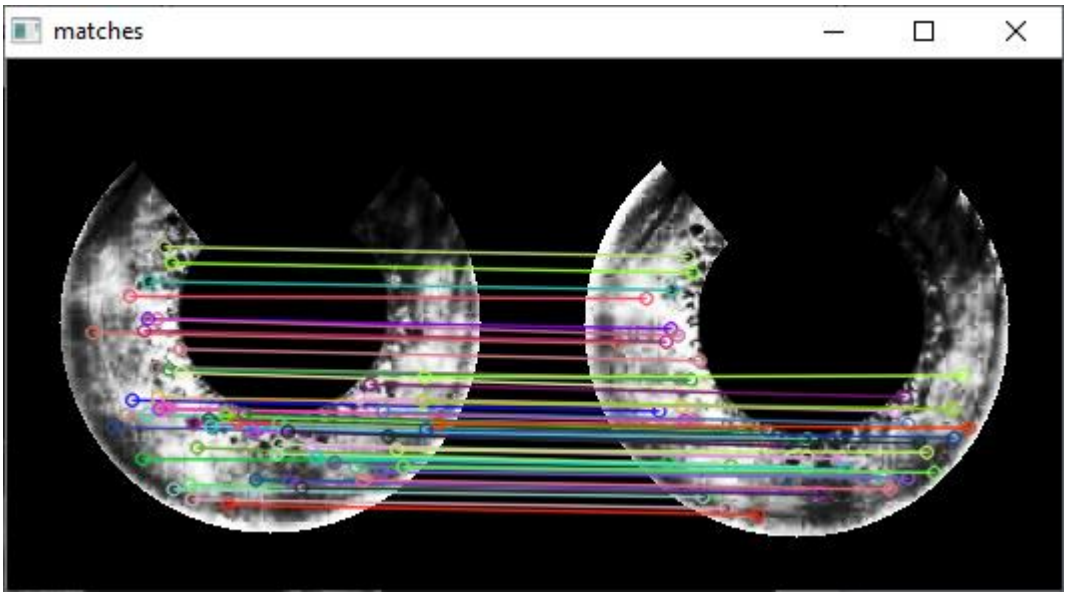

Рисунок 5.7 – Результат роботи функції “getAllMatches”

Далі програма вирішує результат верифікації райдужних оболонок ока, якщо поріг не пройдений, вертаємося до головного вікна (див. рисунок 5.8), якщо поріг відповідає заданому, або вище програма приступає до виконання другого модулю роботи (див. рисунок 5.9)

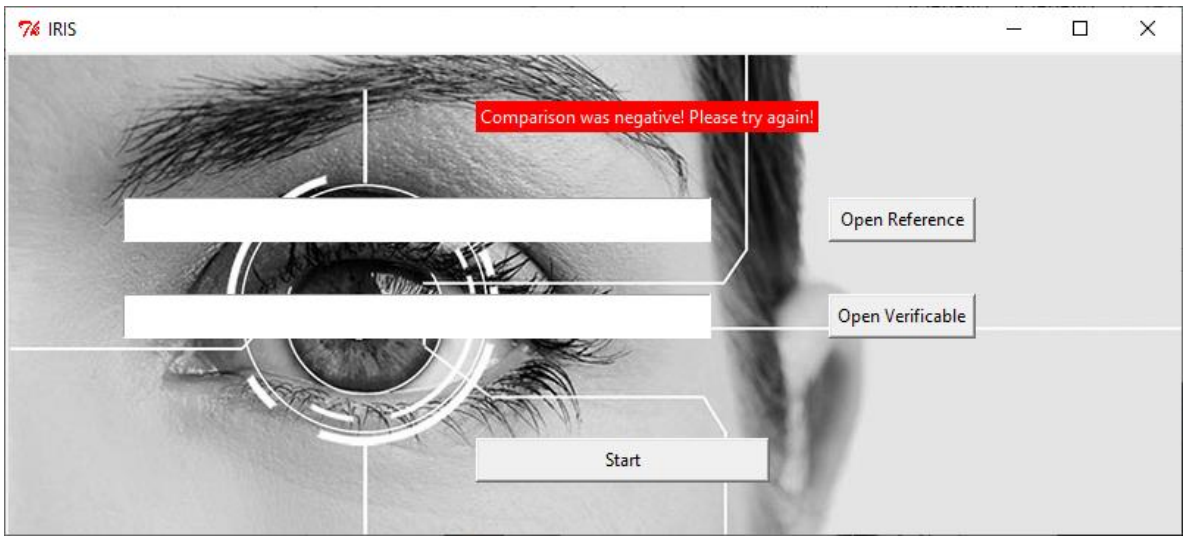

Рисунок 5.8 – Негативний результат верифікації

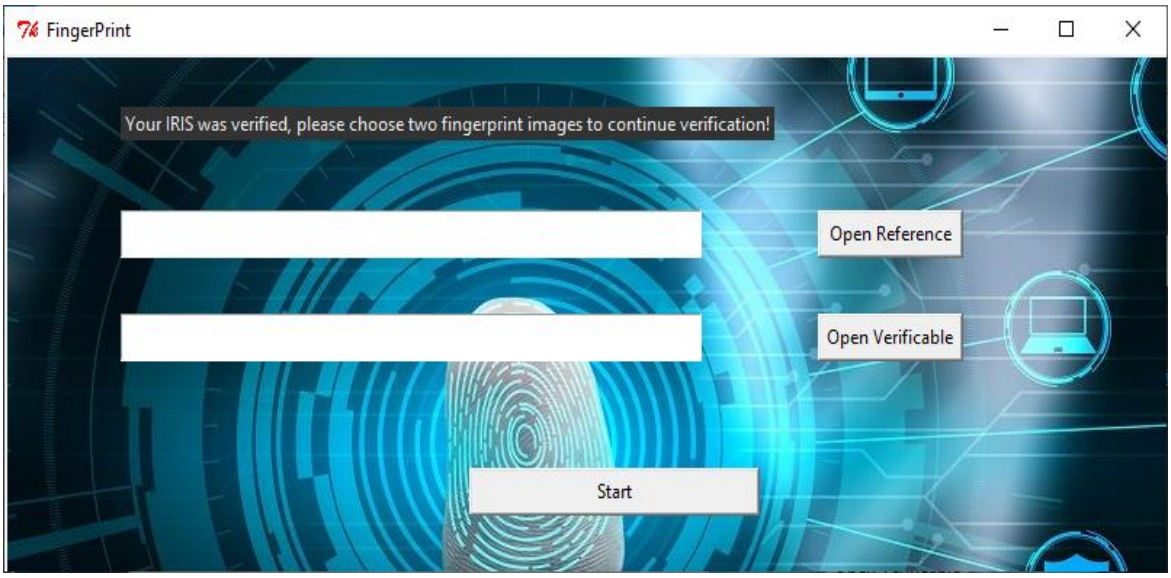

Рисунок 5.9 – Позитивний результат верифікації

Алгоритм роботи другого модулю програмної реалізації:

– вибір та завантаження зображень для верифікації відбитків;
– бінаризація та скелетизація вхідних зображень;
– пошук ключових точок;
– видалення шумових точок;
– порівняння сформованих наборів ключових точок;
– вивід результату роботи.

У другому модулі програми реалізовані наступні функції. Фукція “fingerVidjet” аналогічно функції “vidjet” у першому модулі реалізує простий інтерфейс для користувача з вибором потрібних зображень відбитків пальців та кнопкою запуску. Функція “skeletezation” запускає скелетизацію зображення. На вході бінарне зображення. Функція виконується поки видаляється хоча б один піксель. В першу чергу зображення проходить по основним шаблонам для скелетизації, після того, як був здійснений прохід без видалення пікселя зображення проходить по шумовому набору шаблонів. Схема роботи функції представлена на рисунку 5.10.

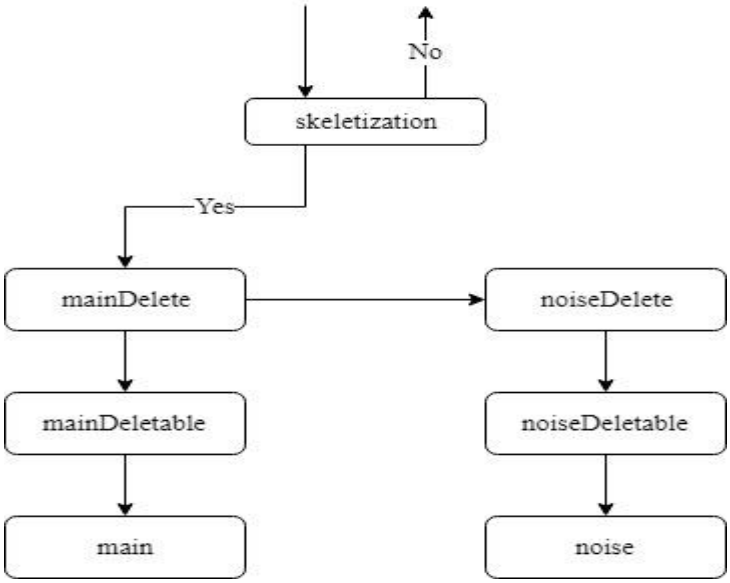

Рисунок 5.10 – Схема роботи функції “skeletization”

Файл point.py містить головну функцію “check_finger”, яка здійснює виклик наступних етапів роботи програми: “binary_image” та “skeletization” – реалізують бінаризацію та скелетизацію вхідного зображення, “create_listPoints” – підрахунок та формування наборів ключових точок,
“matching_similarPoints” – порівняння та виділення особливих точок на зображенні, вивід результату роботи. Схема роботи point.py представлена на рисунку 5.11, результат роботи другого модулю програми – дивитися рисунок 5.12.

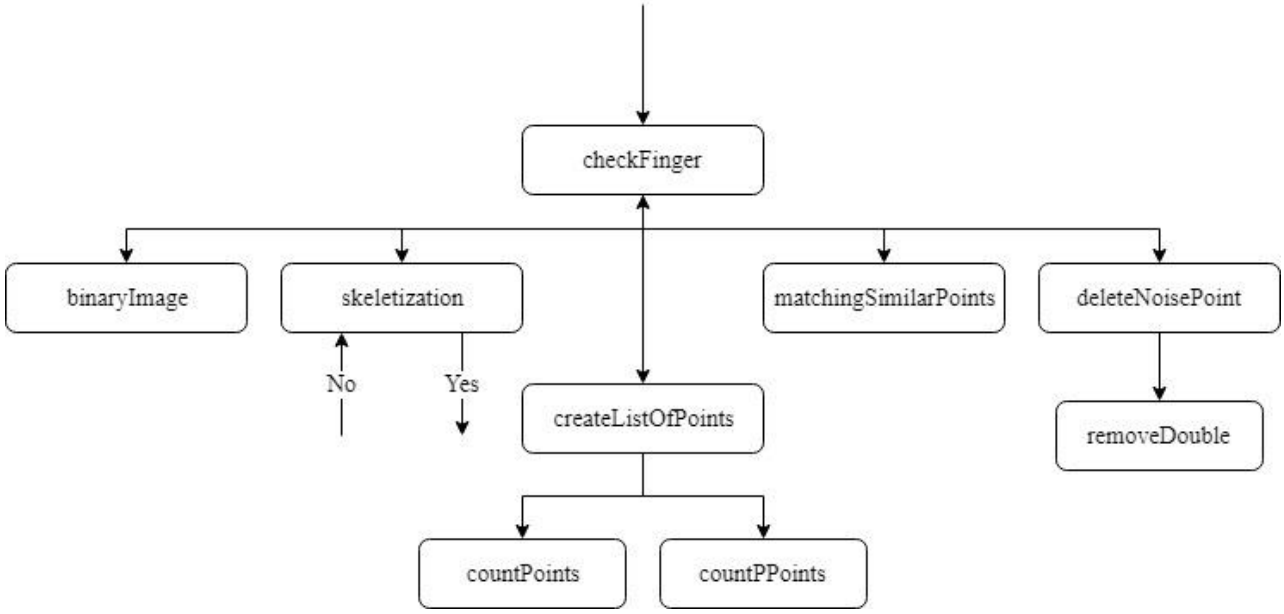

Рисунок 5.11 – Схема роботи points.py

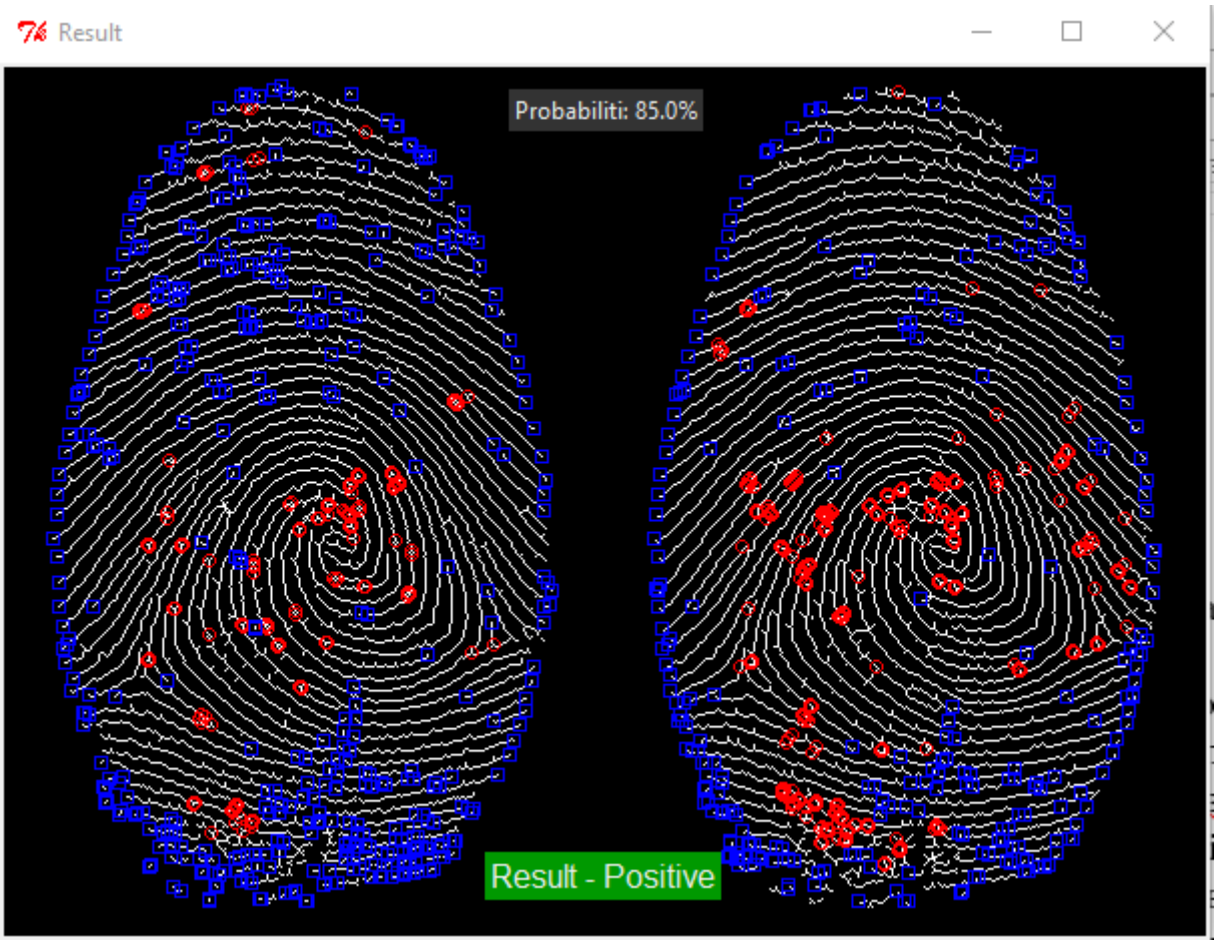

Рисунок 5.12 – Результат роботи другого модулю програми

ВИСНОВКИ

Важливість та актуальність питань захисту інформації давно займають важливе місце в сучасному житті людини. Причини такої уваги до цієї проблеми є досить очевидними – від якості забезпечення захисту інформації залежить життя кожної людини. Біометричні технології є одним з основних компонентів, для забезпечення захисту інформації сьогодні та має великий потенціал для розвитку у майбутньому. Біометрія сьогодні має дуже високі темпи розвитку та застосування у різних сферах життя. Переваги очевидні – процес захисту інформації стає більш зручним, легким та надійним.

У ході аналізу проведеного у першому розділі атестаційної роботи було з’ясовано, що біометричні системи верифікації людини ніколи не дають 100%-вий результат роботи. Також, для усіх типів біометричних систем існують загальні проблеми, а саме: безпека, конфіденційність, ціна та сумісність. Якщо розглядати варіанти біометрії окремо, то можна виділити особливі проблеми під кожний тип біометричної системи. Усі варіанти біометричних систем, які використовуються у наш час були порівняні за низкою показників, а саме: відсоток помилкових відхилень та пропусків, можливість відмови у реєстрації, за критеріями універсальності, відмінності, сталості та продуктивності, а також за їхніми перевагами та недоліками. Після аналізу вище вказаних проблем, зроблено висновок, що мультимодальні системи верифікації вирішують низку поставлених питань до біометричних систем.

У якості модулів для розробки було обрано алгоритми верифікації за структурою райдужної оболонки ока та відбитків пальців. Було сформовано загальну схему для реалізації мультимодальної системи верифікації. Проаналізовано проблеми для кожної з підсистем та розроблено рекомендації для підвищення ефективності роботи.

Розроблено модель мультимодальної біометричної системи верифікації, проаналізовано її функціональну характеристику та наведено прогнозуючі переваги та недоліки системи.

Для модулю верифікації за структурою райдужної оболонки ока у якості методу пошуку особливих точок зображення було обрано алгоритм SIFT, алгоритм у повній мірі відповідає вимогам поставленим до біометрії на основі райдужної оболонки ока та вважається перспективним для застосування у цьому напрямі. Алгоритм виділяє ключові особливості на зображенні, які відповідають варіативності, тобто є незмінними при масштабуванні та повороті зображень. Для обробки зображення райдужки було розроблено та реалізовано етапи сегментації та нормалізації вхідних даних.

Для підсистеми на основі порівняння відбитків пальців у якості методу верифікації було обрано алгоритм порівняння відбитків на основі пошуку особливих точок. У ході порівняння алгоритмів верифікації зображень відбитків пальця було з’ясовано, що головною перевагою даного алгоритму є відносна швидкість його роботи. Представлений алгоритм не потребує складних математичних розрахунків. В силу простоти реалізації і швидкості роботи алгоритми даного класу є найбільш поширеними на сьогоднішній день. При аналізі методів скелетизації, було зроблено висновок, що найбільш простим за своєю реалізацією є шаблонний метод скелетизації. У той же час, даний метод є найбільш швидким за часом роботи, оскільки він потребує лише одного обходу зображення.

Розроблено та протестовано програмне забезпечення, яке реалізує мультимодальну верифікацію людини за зображеннями райдужної оболонки ока та відбитку пальця.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Pfalz J.L., Rosenfeld A. Computer Representation of Planar Regions by their Skeletons. Communications of the Association for Computing Machinery, 1967, vol. 10, no. 2, p.125.

2. Galbally, J., Ross, A., Gomez-Barrero, M., Fierrez, J., and Ortega-Garcia, J., “Iris image reconstruction from binary templates: An efficient probabilistic approach,” Journal of Computer Vision and Image Understanding (2013). (Minor comments, under 3rd review). p.120

3. Anil K. Jain, Karthik Nandakumar and Arun Ross, “50 years of biometric research, Accomplishments, Challenges and Opportunities”, Pattern Recognition Letters, 2016, vol.79, pp.80-105.

4. A. K. Jain, A. Ross and S. Pankanti, “Biometrics, A Tool for Information Security”, IEEE Transactions on Information Forensics And Security, 2006, vol.1, no.2, pp. 125 – 144.

5. A. Auclair, L. Cohen и N. Vincent, «How to Use SIFT Vectors to Analyze an Image». p.72

6. J. Daugman, High Confidence Visual Recognition of Persons by a Test of Statistical Independence, Pattern Analysis and Machine Intelligence, IEEE Transaction on, Vol. 15, No. 11, pp. 1148-1161, 1993.

7. Jain, A. K., Ross, A., and Pankanti, S., “Biometrics: a tool for information security,” IEEE Trans. on Information Fonrensics and Security 1(2), 125–143 (2006).

8. N. Y. Khan, B. McCane и G. Wyvill, «SIFT and SURF Performance Evaluation Against Various Image Deformations on Benchmark Dataset» International Conference on Digital Image Computing: Techniques and Applications, 2011.

9. ДСТУ ISO/IEC 9798-3:2002 Інформаційні технології. Методи захисту. Автентифікація суб’єктів. Частина 3. Механізми з використанням методу цифрового підпису.

10. ДСТУ 7564:2014 Інформаційні технології. Криптографічний захист інформації. Функція хешування.

11. ДСТУ ISO 7498-2:2004 Системи оброблення інформації. Взаємозв’язок відкритих систем базова еталонна модель. Частина 2. Архітектура захисту інформації.