Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

Рівень вищої освіти другий (магістерський)

Порівняльний аналіз ефективності методів біометричного шаблону на основі обробки райдужної оболонки ока
(тема)

Виконала:
студентка 2 курсу, групи АМСЗІм-18-1
Чернікова В.Г.
(прізвище, ініціали)

Спеціальність: 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми: освітньо-наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма: Адміністративний менеджмент у сфері захисту інформації
(повна назва освітньої програми)

Керівник: професор кафедри ІКІ ім. В.В. Поповського Філіппенко О.І.
(посада, прізвище, ініціали)

Допускається до захисту
Зав. кафедри _____ Лемешко О.В.
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет Інфокомунікацій
(повна назва)
Кафедра Інфокомунікаційної інженерії імені В.В. Поповського
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 125 Кібербезпека
(код і повна назва)
Тип програми освітньо- наукова
(освітньо-професійна або освітньо-наукова)
Освітня програма Адміністративний менеджмент у сфері захисту інформації
(повна назва)

ЗАТВЕРДЖУЮ
Зав. кафедри_____
(підпис)
«____» _____2020 р.

ЗАВДАННЯ
НА АТЕСТАЦІЙНУ РОБОТУ

студентці Черніковій Валерії Георгіївні .
(прізвище, ім'я, по батькові)

1. Тема роботи: Порівняльний аналіз ефективності методів біометричного шаблону на основі обробки райдужної оболонки ока
затверджена наказом по університету від « 17 » березня 2020р. № 465 Ст.
2. Термін подання студентом роботи до екзаменаційної комісії 10.05.2020 р.
3. Вихідні дані до роботи: ISO/IEC TR 24741:2007 Information technology – Biometrics tutorial (ГОСТ Р 54412-2011), ISO/IEC/TR 24722:2007 Information technologies. Biometrics. Multimodal and other multibiometric fusion. (ГОСТ Р 54411-2011)
4. Перелік питань, що потрібно опрацювати в роботі:
1) Класифікація біометричних методів автентифікації
2) Аналіз методів захисту біометричного шаблону
3) Огляд процесу розпізнавання користувача по райдужній оболонці
4) Дослідження алгоритму розпізнавання по райдужній оболонці
5) Дослідження алгоритмів біохешу
6) Дослідження ефективності методів захисту біометричного шаблону

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, плакатів):
Демонстраційний матеріал у вигляді ppt-презентації

6. Консультанти розділів роботи

Найменування розділу	Консультант (посада, прізвище, ім'я, по-батькові)	Позначка консультанта про виконання розділу	
		(підпис)	(дата)
Основна частина	доцент Філіппенко Олег Ігорович		

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	17.02.2020	Виконано
2	Збір матеріалів для дослідження	01.03.2020	Виконано
3	Розробка 1 розділу	25.03.2020	Виконано
4	Розробка 2 розділу	08.04.2020	Виконано
5	Розробка 3 розділу	15.04.2020	Виконано
6	Розробка 4 розділу	25.04.2020	Виконано
7	Розробка 5 розділу	01.05.2020	Виконано
8	Розробка 6 розділу	08.05.2020	Виконано
9	Оформлення атестаційної роботи	10.05.2020	Виконано

Дата видачі завдання 17 лютого 2020 року

Студентка _____ Чернікова В. Г.
(підпис) (прізвище, ініціали)

Керівник роботи _____ доцент Філіппенко О.І.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 82 с., 33 рис., 15 таблиць, 28 джерел.

АВТЕНТИФІКАЦІЯ, БІОМЕТРИЧНА СИСТЕМА, СТІЙКІСТЬ, ФІЛЬТР, БІОМЕТРИЧНИЙ ШАБЛОН, РАЙДУЖНА ОБОЛОНКА, АЛГОРИТМ.

Об'єкт дослідження – процес біометричної автентифікації.

Предмет дослідження – алгоритми захисту біометричного шаблону райдужної оболонки ока.

Мета роботи – математичне та програмне моделювання алгоритмів захисту біометричного шаблону райдужної оболонки ока, дослідження їх ефективності та порівняння.

Методи досліджень – математичне та програмне моделювання, аналіз та порівняння.

За останній час системи біометричної автентифікації набули значної популярності, оскільки користувачам в цьому випадку не потрібно пам'ятати пароль. Системи біометричної автентифікації по райдужній оболонці тільки отримують розвиток, тому алгоритм отримання біометричного шаблону райдужної оболонки та механізм його захисту можуть мати різний вигляд і не є стандартизованими.

У роботі досліджена одна з таких систем та оцінені її властивості. Також вирішена актуальна задача вибору методу захисту біометричного шаблону райдужної оболонки ока. Для вирішення задачі було запропоновано алгоритм обробки зображення у поєднанні із різними методами захисту біометричного шаблону, проведено програмне і математичне моделювання створення біохешу та його порівняння з еталоном. В результаті тестування було визначено стійкість кожного з методів до накладання шуму та визначена ймовірність виникнення помилок.

ABSTRACT

The report contains: 82 p., 33 fig., 15 tables, 28 sources.

AUTHENTICATION, BIOMETRIC SYSTEM, STABILITY, FILTER BIOMETRIC TEMPLATE, IRIS, ALGORITHM.

A research object is the biometric authentication process.

The subject of research is algorithms of iris biometric template protection.

An aim of work is mathematical and program modeling of algorithms of the iris biometric template protection, researching of their efficiency and comparison.

Methods of researches are mathematical and program modeling, analysis and comparison.

Recently, biometric authentication systems have gained considerable popularity, since users in this case do not need to remember the password. Iris biometric authentication systems are only being developed, so the algorithms of image processing algorithm and iris biometric template protection can have a different form and they are not standardized.

In this paper, one of this system is examined and tested. Also, the actual problem of choosing a method for iris biometric template protection is solved. To solve the problem, an algorithm for image processing was proposed, software and mathematical modeling of the creation of the iris biohash and comparison with the standard were carried out. As a result of testing, the stability of each algorithm was determined to noise and the probability of errors was determined.

ЗМІСТ

Перелік скорочень, умовних позначень, символів, одиниць і термінів……..... 7
Вступ……..... 8
1 Класифікація біометричних методів автентифікації…… 10
1.1 Статичні методи біометричної автентифікації……... 12
1.2 Динамічні методи біометричної автентифікації……. 25
2 Аналіз методів захисту біометричного шаблону…….. 30
2.1 Атаки на біометричні шаблони ……... 32
3 Огляд процесу розпізнавання людини по райдужній оболонці ока……... 35
3.1 Технологія розпізнавання по райдужній оболонці……. 39
3.2 Райдужна оболонка ока як біометричний параметр…….……. 41
3.3 Загальний алгоритм розпізнавання по райдужній оболонці…..... 44
4 Дослідження алгоритму розпізнавання по райдужній оболонці……... 47
5 Дослідження алгоритмів біохешу…… 56
6 Дослідження ефективності методів захисту біометричного шаблону 60
Висновки……. 79
Перелік джерел посилання…… 80

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ І ТЕРМІНІВ

ДНК – дезоксирибонуклеїнова кислота
США – Сполучені Штати Америки
ERR – Equal Error Rate
FAR – False Acceptance Rate
FRR – False Rejection Rate
MSE – Mean Square Error
SNR – Signal to Noise Ratio

ВСТУП

Швидкими кроками інформаційні технології проникають в усі сфери життєдіяльності суспільства. Незважаючи на те, що призначення кожного інформаційного виробу різне, проблема збереження конфіденційності, цілісності та забезпечення даних є спільною. Згідно з результатів досліджень більшість звичайних працівників, які мають доступ до конфіденційної інформації, не надає особливої уваги надійному захисту даних. Між можливістю викрадення конфіденційних інформації та можливістю назавжди втратити доступ до важливих даних серйознішою проблемою вони вважають другу. Про це свідчить велика кількість легких паролів, їхнє збереження на аркуші паперу під клавіатурою, розголошення паролів та інші випадки. Таким чином для боротьби із першою проблемою слід подолати другу. Забування паролю та втрата фізичного ключа мають стати неможливими. На цьому етапі у захист конфіденційної інформації вступають засоби біометричної автентифікації. Замість пам’яті тіло людини турбується про зберігання «ключа», а втрата такого «ключа» є неймовірно низькою.

Протягом багатьох років спостерігалося постійне зростання біометричних технологій по всьому світу з безлічі причин, але в основному через те, що особиста ідентифікація та автентифікація стають все більш важливими. Від прикордонного та імміграційного контролю для виявлення злочинців до розблокування мобільних пристроїв практичне використання біометричних систем швидко зростає. На даний час вартість таких систем стає дешевшою, а технології, за допомогою яких можна здобути біометричні параметри, є вбудованими в більшість гаджетів. Крім того, такі системи стають більш простими у використанні і обслуговуванні, а розвиток нових ефективних алгоритмів для обробки біометричних характеристик людини сприяє зменшенню ймовірності помилок відмови у доступі зареєстрованому користувачу та допуску зловмисника у систему. Нажаль, поряд із новими механізмами розвиваються і нові атаки, але прогрес не стоїть на місці і пропонуються нові методики захисту.

Людське тіло має велику кількість унікальних індивідуальних характеристик. На даний час багато з них використовується у системах біометричної автентифікації. Але найбільшу популярність отримують ті з них, в

яких індивідуальні характеристики людини легко вилучити. Зручність використання та вартість таких систем набагато ліпші на відміну від інших.

Зазвичай робота біометричних систем полягає у перетворення біометричних характеристик людини у біометричний шаблон, який представляє собою набір даних у двійковому форматі. Нажаль, вилучення та перетворення у байт код унікальних характеристик людини не є фінішним етапом. Аналогічно збереженню паролю у відкритому вигляді, не хешуючи його, зберігання біометричного коду є небезпечним. Використання звичайних хеш-функцій для біометричного коду є неможливими, адже необхідно забезпечити можливість розпізнавати різні зразки однієї й тієї ж унікальної характеристики. При зміні одного елементу звичайна хеш-функція буде повністю змінена, що перешкодить розпізнаванню власника біометричного зразка. Таким чином, для вирішення цього використовуються алгоритми біохешу, проблема вибору якого є актуальною в сучасному світі.

Дана робота присвячена дослідженню системи біометричної автентифікації по райдужній оболонці ока. У роботі описуються найбільш широко використовувані системи біометричної автентифікації, визначаються їх недоліки та переваги, розглядається алгоритм біометричного розпізнавання по райдужній оболонці ока людини у комбінації із різними методами захисту біометричного шаблону, описується програмна реалізація зазначеного алгоритму на мові Java та досліджується ефективність та швидкість роботи кожного із методів захисту біометричного коду у комбінації з іншими етапами розпізнавання. Метою даної роботи є порівняння розглянутих методів захисту біометричного шаблону, виявлення їх переваг та недоліків і визначення найкращого з них.

1 КЛАСИФІКАЦІЯ БІОМЕТРИЧНИХ МЕТОДІВ АВТЕНТИФІКАЦІЇ

Ідея ідентифікації людини за допомогою частин її тіла з’явилася наприкінці дев’ятнадцятого століття. Процес перенесення багатьох сфер життєдіяльності у цифровий світ не оминув і біометрію. Завдяки швидкому розвитку технологій було виявлено значно більше унікальних індивідуальних особливостей людини.

Ще кілька десятків років потому було виявлено, що деякі фізіологічні характеристики людини є унікальними. Сучасні методи біометричної автентифікації, що використовують такі характеристики, отримали назву статичні. Значно пізніше було виявлено, що ідентифікувати людину можна і за допомогою її підсвідомих рухів в процесі виконання будь-якої звичайної дії. Поведінкові характеристики людини стали основою для динамічних методів біометричної автентифікації. Класифікація методів біометричної автентифікації наведена на рис. 1.1 [1].

Рисунок 1.1 – Методи біометричної автентифікації

Статичні та динамічні методи автентифікації об’єднують наступні критерії до біометричних параметрів [1].

1) Біометрична ознака має бути присутньою у кожної людини без винятку.

2) Існування двох людей з однаковими біометричними параметрами має бути неможливим.

3) Біометричні характеристики мають бути незмінні з часом.

4) Необхідно, щоб ознаки мали можливість бути вилученими.

5) Суспільство не має бути проти вилучення та збору цих ознак.

На даний час спостерігається активний розвиток обох типів методів. На сьогодні виділяють вісім найпопулярніших біометричних параметрів, за допомогою яких можна ідентифікувати людину:

- райдужна оболонка;
- сітківка ока;
- термограма обличчя;
- обличчя;
- відбитки пальців;
- підпис;
- геометрія руки;
- голос.

Менш поширеними є наступні параметри:

- запах;
- форма вух;
- дезоксирибонуклеїнова кислота (ДНК);
- шкірне відображення;
- клавіатурний почерк;
- хода.

Таким чином, виходячи з наведеної інформації можна зробити висновок, що статичні методи біометричної автентифікації є часто використовуваними на світовому ринку. У наступних підрозділах розглянуті найбільш поширені статичні та динамічні методи автентифікації, їхні переваги і вади та описаний механізм вилучення біометричних зразків для кожного з методів.

1.1 Статичні методи біометричної автентифікації

Статична біометрія є більш поширеним та відомим типом біометричної автентифікації, який, як правило, вважається дуже сприятливим для споживачів і пропонує позитивний досвід користувача. Він використовує фізичні функції, такі як відбитки пальців, райдужну оболонку ока, сітківку ока, геометрію руки, геометрію або термограму обличчя, і все частіше використовується у будь-яких ситуаціях, будь то розблокування смарт-пристроїв, вхід в мобільні банківські рахунки або фактичне завершення транзакцій.

Автентифікація за відбитками пальців є одна з найпопулярніших біометричних систем. Завдяки своїй унікальності та незмінності з часом відбитки пальців використовуються для ідентифікації вже більше століття. Останнім часом такі системи стають автоматизованими, тобто біометричними завдяки розвитку обчислювальних можливостей. Ідентифікація відбитків пальців популярна через притаманну їй простоту придбання, численні джерела та доступність для збору. Практика використання відбитків пальців як методу ідентифікації осіб застосовується з кінця дев’ятнадцятого століття, коли англійський вчений Френсіс Галтон визначив деякі характеристики, за якими можна визначити відбитки пальців. «Точки Галтона» стали фундаментом для розвитку ідентифікації за відбитками пальців. Ідентифікація відбитків пальців розпочала свій перехід до автоматизації на початку другої половини двадцятого століття разом з появою обчислювальних технологій. З появою комп'ютерів підмножина точок Галтона була використана для розробки автоматизованої технології відбитків пальців.

Для збору цифрового зображення поверхні відбитків пальців використовуються різні типи датчиків - оптичний, ємнісний, ультразвуковий та тепловий. Оптичні датчики знімають відбиток пальця і є найпоширенішим датчиком сьогодні.

Відбиток пальців, як правило, представляє собою серію темних ліній, що представляють високу частину шкіри хребта тертя. Ідентифікація відбитків пальців ґрунтується, головним чином, на деталях, або на розташуванні та напрямку кінців хребта та роздвоєння вздовж шляху. На рис. 1.2 зображений приклад відбитку пальцю з виділеними деталями для автентифікації [2].

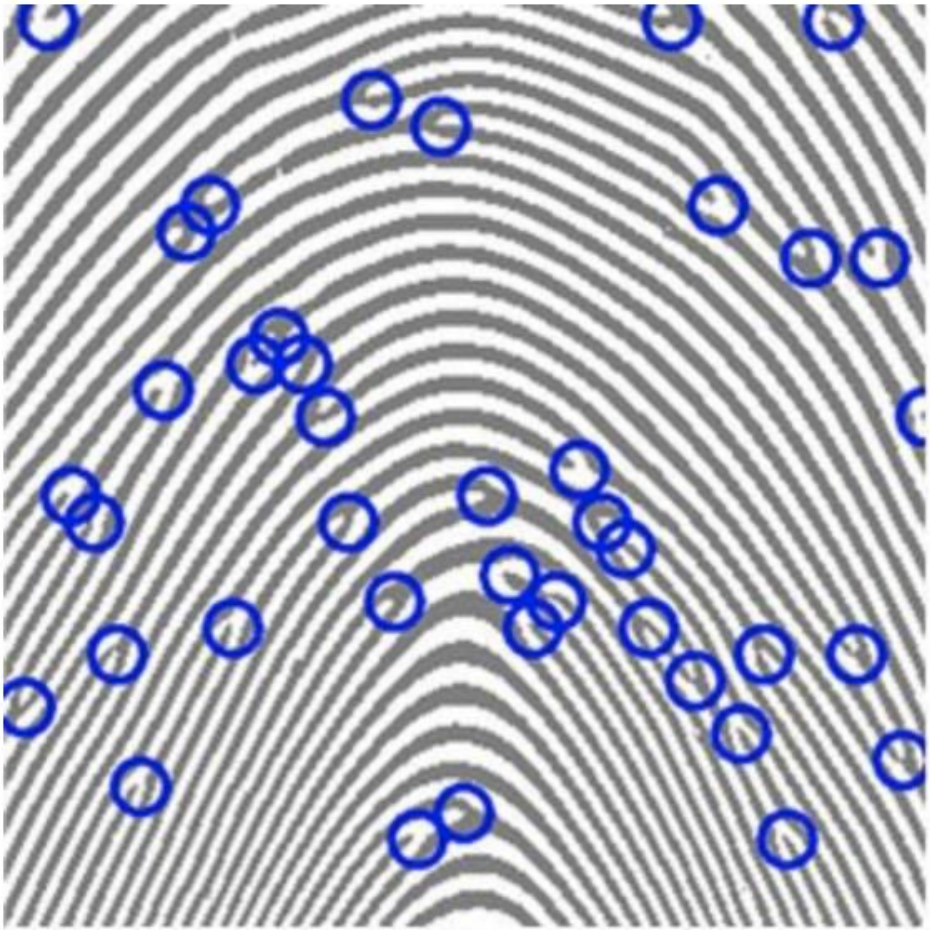

Рисунок 1.2 – Приклад відбитку пальцю із виділеними характерними для ідентифікації деталями

Даний метод автентифікації має наступні переваги:

- легкість у використанні;
- зручність;
- надійність;
- не потребує зображення високої якості.

До недоліків можна віднести такі факторі:

- складність розпізнавання маленьких дітей у зв’язку з невеликим розміром пальців;
- відмова доступу зареєстрованого користувача через пошкодження поверхні пальця.

Розпізнавання за сітківкою ока є однією з найвідоміших біометричних технологій, але також є однією з найменш безпечних. Сканування сітківки відображає унікальні візерунки сітківки людини. Кровоносні судини в сітківці поглинають світло легше, ніж навколишні тканини, і їх легко ідентифікувати при

відповідному освітленні. Приклад рисунку кровоносних судин сітківки ока наведений на рис. 1.3 [3].

Рисунок 1.3 – Приклад кровоносних судин сітківки ока людини, які використовуються для її автентифікації

Сканування сітківки проводиться шляхом випромінення в очі людині непомітного пучка низько енергетичного інфрачервоного світла під час огляду окуляра сканера. Цей промінь світла простежує стандартизований шлях на сітківці. Після того як пристрій сканування фіксує зображення сітківки, спеціалізоване програмне забезпечення збирає в шаблон унікальні характеристики мережі кровоносних судин сітківки. Алгоритми сканування сітківки вимагають високої якості зображення і не дозволять користувачеві зареєструватися або перевірити, поки система не зможе зробити зображення достатньої якості [3]. Сканування сітківки - це дуже надійна технологія, оскільки вона є дуже точною та складною підробкою, з точки зору ідентифікації. Однак ця технологія має помітні недоліки, включаючи складне придбання зображення та обмежені програми для

користувачів. Створений шаблон сітківки зазвичай є одним з найменших з будь-якої біометричної технології. Часто сканування сітківки може зайняти відносно велику кількість часу через необхідність багаторазового збору зображень, що може викликати дискомфорт у користувача. Складна мережа судин сітківки є фізіологічною характеристикою, яка залишається стабільною протягом життя людини. Як і у випадку з відбитками пальців та зразків райдужної оболонки, генетичні фактори не визначають точну картину судин сітківки. Це дозволяє технології сканування сітківки розмежовувати однакових близнюків та забезпечувати надійну ідентифікацію. Сітківка містить щонайменше стільки ж індивідуальних даних, скільки відбиток пальця, але, на відміну від відбитка пальця, є внутрішнім органом і менш чутлива до навмисних чи ненавмисних модифікацій. Окремі захворювання, пов’язані з очима, та захворювання, такі як катаракта та глаукома, можуть зробити людину нездатною використовувати технологію сканування сітківки, оскільки судини можуть бути затемненими.

Біометрична система автентифікації по райдужній оболонці ока на даний час вважається найточнішою біометричною системою серед тих, які зараз доступні на ринку. Як і відбиток пальців, райдужка є унікальною фізіологічною характеристикою людини, що означає, що на планеті не існує двох однакових візерунків. Також покрита рогівкою райдужна оболонка ока добре захищена від пошкоджень, що робить її придатною частиною тіла для біометричної автентифікації.

Райдужна оболонка представляє собою кольорову частину ока, що оточує зіницю. Візерунок райдужної оболонки людини унікальний і залишається незмінним протягом усього життя. За своєю структурою райдужна оболонка складається з еластичної матерії, яка називається трабекулярною мережею. Вона представляє собою сітчасте утворення, яке складається з поглиблень, гребінчастих стяжок, борозен, кілець, зморшок, веснянок, судин і інших характеристик. Малюнок райдужної оболонки ока складається близько зі 260 ключових точок, які можуть бути використані для розпізнавання особистості, на відміну від відбитку пальця, який має близько 16 ключових точок для ідентифікації. Приклад рисунку райдужної оболонки ока зображений на рис. 1.4.

Рисунок 1.4 – Візерунок райдужної оболонки ока

Розпізнавання райдужної оболонки вимагає вдосконаленої цифрової камери для зйомки зображень деталізованих унікальних структур райдужної оболонки. Камери райдужної оболонки можуть точно сканувати райдужну оболонку від десяти сантиметрів до приблизно двох метрів і навіть можуть працювати крізь окуляри або контактні лінзи на місці [4]. Якщо райдужна оболонка не травмується або не пошкоджується будь-якими проблемами зі здоров'ям, вона з часом залишатиметься незмінною і лише одне початкове зарахування може тривати назавжди. Таким чином, біометричної автентифікації по райдужній оболонці має наступні переваги.

1) Розпізнавання по райдужній оболонці ока має високу точність серед різних типів біометричних технологій.

2) Процедура розпізнавання по райдужній оболонці ока має велику швидкість.

3) Оскільки райдужна оболонка відрізняється між лівим і правим оком, розпізнавання може здійснюватися кожним оком окремо.

4) Можливо розрізнити близнюків.

5) Розпізнавання по райдужній оболонці можна використовувати навіть у тому випадку, коли людина одягає шапку, маску, окуляри або рукавички.

6) Завдяки використанню інфрачервоної камери розпізнавання можливе навіть вночі або в темний час доби.

7) Без необхідності торкатися пристрою можлива безконтактна автентифікація, що робить його гігієнічним у використанні.

Ідентифікація долоні, як і ідентифікація відбитків пальців, ґрунтується на сукупності інформації, поданої у відбитку гребня тертя. Ця інформація включає в себе потік фрикційних гряд, наявність або відсутність ознак уздовж окремих контурів гребня тертя та їх послідовностей та складні деталі одного гребня. Для збору цифрового зображення поверхні долоні можна використовувати різноманітні типи датчиків: ємнісний, оптичний, ультразвуковий та тепловий. Деякі системи розпізнавання долонь сканують всю долоню, а інші вимагають сегментування долонь на менші ділянки для оптимізації роботи. Приклад пристрою для сканування долоні наведений на рис. 1.5 [4].

Рисунок 1.5 – Пристрій для сканування візерунка долоні

Автентифікація за допомогою судинного візерунка руки відбувається із використанням ближнього інфрачервоного світла або методами відбиття або передачі. У способі відбиття ближче до інфрачервоних променів випромінюються до долоні, яку слід ідентифікувати, і відбите світло фіксується для автентифікації. Оскільки вени знаходяться під шкірою людини, комусь іншому складно їх скопіювати або вкрасти, тому така система автентифікації є більш захищеною порівняно з деякими іншими біометричними ознаками. Оскільки судинні візерунки долоні різноманітні та складні, вони дають достатню інформацію для виявлення однієї особи серед великої популяції. Приклад такого візерунка зображений на рис. 1.6 [4].

Рисунок 1.6 –Судинний візерунок долоні

Як результат, така автентифікація є надійною та високоточною. Оскільки автентифікація за судинним візерунком долоні є безконтактним типом біометричної ідентифікації, вона підходить для використання в додатках, які потребують високого рівня гігієни, або для використання в громадських додатках.

Система біометричної автентифікації по обличчю здатна ідентифікувати або перевіряти людину з цифрового зображення або відеокадру з джерела відео. Існує кілька методів, які використовують системи розпізнавання по обличчю, але в

цілому вони працюють, порівнюючи вибрані риси обличчя із заданого зображення в межах бази даних. Технологія розпізнавання обличчя використовує компонування рис обличчя та їх відстань одна від одної для ідентифікації людини.

Розрізняють 2-D розпізнавання обличчя і 3-D розпізнавання. 3D розпізнавання обличчя має можливість досягати кращої точності, ніж його 2D аналог. Це дозволяє уникнути таких підводних каменів 2D алгоритмів розпізнавання обличчя, як зміна освітлення, різний вираз обличчя, макіяж та орієнтація голови. У зв'язку з тим, що переважна більшість камер отримують картинку без будь-якої глибини, більшість програм та технологій ідентифікації по обличчю людини використовують розпізнавання по 2D зображенню. Унікальність даного методу полягає у тому, що він не вимагає створення спеціалізованих сенсорів для отримання зображення, адже зображення обличчя можна отримати зі звичайною камери системи відеоспостереження. На рис. 1.7 наведений приклад зображення для 2D ідентифікації по обличчю із виділеними характеристиками, які використовуються в процесі розпізнавання [5].

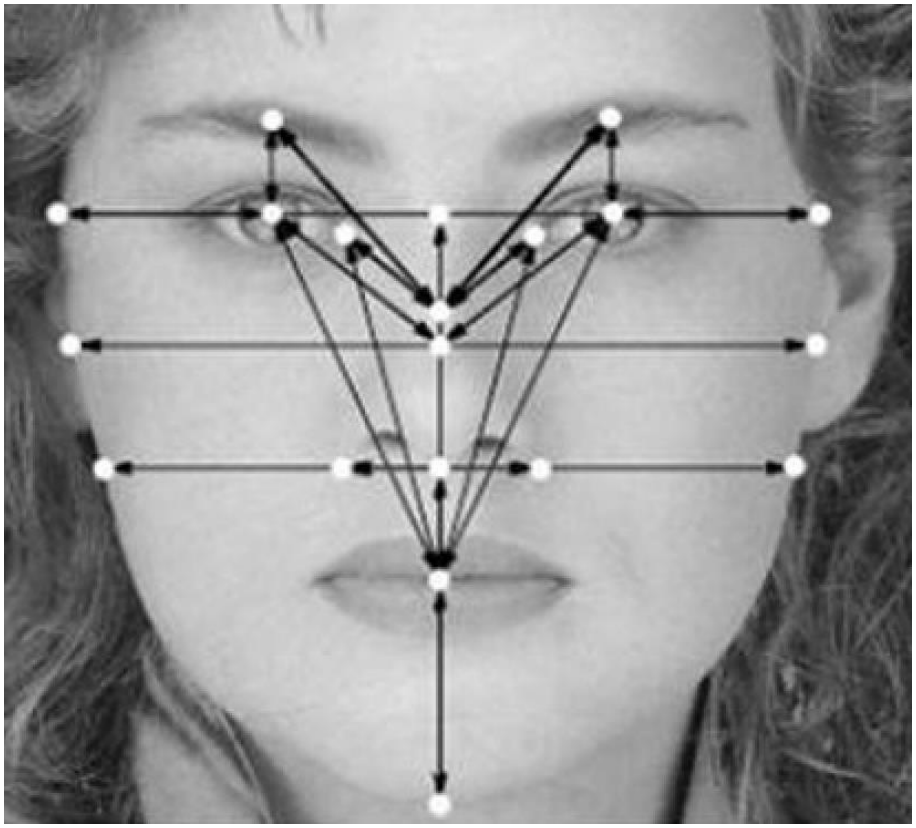

Рисунок 1.7 – Приклад зображення для 2D автентифікації по обличчю

Варто зазначити, що фотографія обличчя присутня практично на будь-якому документі, що посвідчує особу, а значить впровадження цієї технології на практиці не пов'язане з різноманітними нормативними проблемами і труднощами соціального сприйняття технології. Також отримати зображення обличчя можна неявно для самої людини. Таким чином ,біометрія обличчя оптимально підходить для побудови систем моніторингу та прихованої ідентифікації.

Інший підхід полягає у використанні 3D-моделі для підвищення точності розпізнавання на основі традиційних зображень шляхом перетворення голови у відомий вигляд. Крім того, більшість 3D-сканерів набувають як 3D-сітку, так і відповідну текстуру. Реєстрація в системі також не є складною та не забирає багато часу. Зазвичай обличчя освітлюється світлом ближньої частини інфрачервоного діапазону. Структура світла перетворюється на поверхні обличчя. Завдяки цьому відеокамера точно фіксує відбите світло. Це світлове зображення реконструюється за допомогою тривимірного алгоритму. Таким чином створюється трьох вимірне сітчасте зображення обличчя за допомогою тріангуляціонного методу. Приклад такого сітчастого зображення наведений на рис. 1.8 [5].

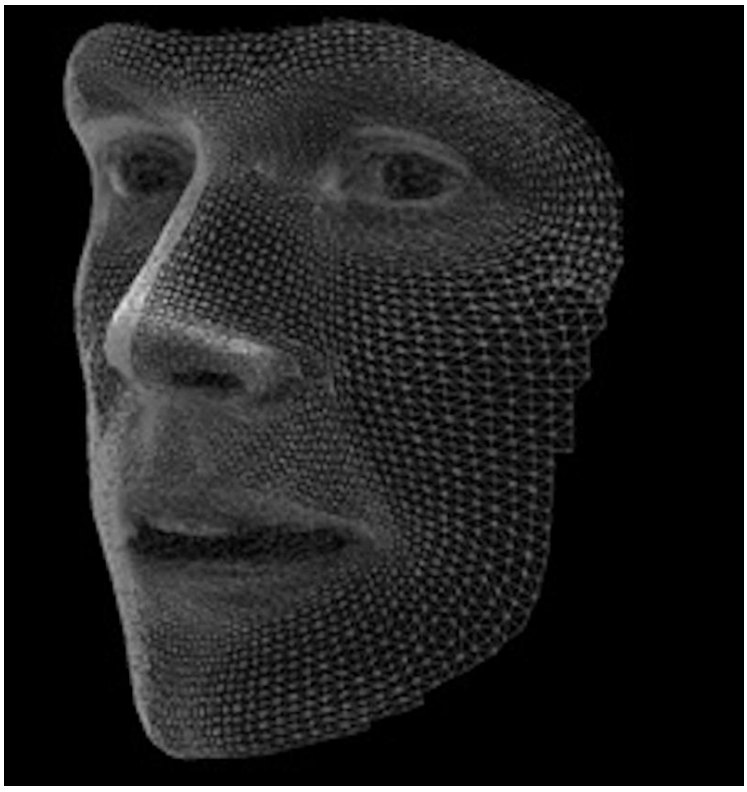

Рисунок 1.8 – Приклад сітчастого зображення для 3D автентифікації по обличчю

Геометрія особи може вимірюватися в міліметрах. Відновлене зображення не зберігається в базі даних; а навпаки, біометричний образ витягується з геометрії особи і у вигляді числової послідовності зберігається в базі даних.

Основним технологічним обмеженням методів 3D розпізнавання обличчя є придбання 3D-зображення, яке зазвичай вимагає спеціальної камери. Альтернативно, для створення тривимірної моделі зі значною подальшою обробкою можуть використовуватися кілька зображень з різних кутів зі звичайної камери [5].

Зазвичай розпізнавання особи в будь-якій біометричній системі виконується в кілька етапів:

- виявлення особи;
- оцінка якості;
- побудова шаблону;
- зіставлення і прийняття рішення.

Розпізнавання обличчя має ряд переваг у порівнянні з іншими біометричними засобами.

1) Мільярди існуючих цифрових зображень обличчя з незліченних джерел надзвичайно корисні для цілей машинного навчання.

2) Майже у всіх смартфонах, планшетах та ноутбуках є вбудовані фронтальні камери, які дозволяють зробити високоякісні знімки «селфі». Це дозволяє зручно збирати живий зразок розпізнавання обличчя для порівняння з шаблоном.

3) Зйомка зображення обличчя за допомогою передньої камери на телефоні може виконуватися пасивно та одночасно під час натискання клавіш, щоб покращити відповідність продуктивності та виявлення життєдіяльності.

До недоліків можна віднести наступне.

1) Варіації поз, старіння, окуляри, вираз обличчя та волосся на обличчі можуть ускладнити розпізнавання.

2) Відмінності між датчиками камери та налаштуваннями також можуть негативно вплинути.

3) Висока доступність зображень обличчя в соціальних мережах та інших засобах масової інформації означає, що шахраї можуть легше отримати зображення потенційних жертв шахрайства, які можуть бути використані для підробки.

Людське обличчя випромінює тепло, яке можна відчути за допомогою спеціальних датчиків, тобто теплових камер, чутливих у тепловій інфрачервоній смузі електромагнітного спектру. Перепади температури на поверхні обличчя виробляють тепловий малюнок, який називається термограмою, яку можна візуалізувати як двовимірне зображення, тобто тепловий образ. Завдяки наявності в шкірі обличчя дуже відмінних та постійних фізіологічних характеристик, термограми містять важливу інформацію, яку можна використовувати для розпізнавання обличчя. Різні об'єкти випромінюють різний діапазон інфрачервоної енергії відповідно до їх температури та характеристик. Діапазон температури обличчя та тіла людини майже однаковий і досить рівномірний, коливаючись від 35,5 °C до 37,5 °C, забезпечуючи стійку теплову ознаку. Теплові структури обличчя випливають насамперед із структури поверхневих судин під шкірою. Структура вен і тканин обличчя є унікальною для кожної людини, а отже, інфрачервоні зображення також унікальні. Приклад термограми обличчя людини зображений на рис. 1.9 [5].

Рисунок 1.9 – Термограма обличчя людини

Термограми є візуальними проявами кількості інфрачервоної енергії, випромінюваної, переданої та відбитої об'єктом, які потім перетворюються в зрозумілу температуру і відображаються як зображення розподілу теплоти. Інфрачервона енергія і сам інфрачервоне світло представляють собою електромагнітне випромінювання з більш довгими хвилями, ніж випромінювання видимого світла, що тягнеться від номінального червоного краю видимого спектру довжини від 700 нм до 1 мм.

Використання спеціальних масок, проведення пластичних операцій, старіння організму людини, охолодження шкіри обличчя в морозну погоду не впливають на точність термограми. Даний метод не має широкого поширення через невисоку якість автентифікації.

Серед різних можливих типів систем біометричної ідентифікації людини ДНК забезпечує найбільш надійну ідентифікацію людини. ДНК є цифровим і не змінюється протягом життя людини. Тіло людини складається приблизно з 60 трильйонів клітин. ДНК, яку можна вважати основою для дизайну людського тіла, знаходиться в середині ядра кожної клітини. ДНК є полімером і складається з нуклеотидних одиниць, кожна з яких має три частини: основу, цукор та фосфат. Тому дані ідентифікації ДНК використовуються в криміналістичних науках. З негативної сторони, найбільшою проблемою у використанні ДНК є час, необхідний для вилучення нуклеїнової кислоти та оцінки даних [6]. Крім того, є ще кілька інших проблем, такі як висока вартість аналізу, питання, порушені монозиготними близнюками, та етичні проблеми.

Запах тіла може використовуватися як біометричний ідентифікатор. Завдяки хімічній структурі запаху, на яку не впливають тілесні зміни, точність таких систем є достатньо висока. Первинний запах людини містить складові, стійкі з часом незалежно від дієти або факторів навколишнього середовища. Вторинний запах містить складові, які є присутніми внаслідок дієти та факторів навколишнього середовища. Третій запах містить компоненти, які є присутніми через вплив сторонніх джерел, а саме лосьйони, мило, парфуми. Таким чином, біометричні системи автентифікації за запахом мають використовувати первинний запах.

Перша система біометричної ідентифікації за запахом тіла були розроблені у 2014 році у Мадридському політехнічному університеті. Дослідники стверджують, що тіло кожної людини має постійні помітні «малюнки запахів», на

які не впливають ні хвороби, ні дієта, ні вік. Дослідники створили сенсор, здатний розпізнавати «унікальні малюнки» запахів людського тіла і впізнавати їх носія з точністю 85 %. Недоліками таких систем є велика вартість і складність пристроїв реєстрації запаху.

Як і інші біометричні параметри такі, як обличчя, райдужна оболонка та палець, вухо, як біометричний параметр, має велику кількість специфічних та унікальних особливостей, що дозволяють ідентифікувати людину. Морфологія вуха змінюється після віку десяти років. Медичні дослідження показали, що значні зміни форми вуха трапляються лише до восьми років та після сімдесяти років. Вуха ростуть симетрично в розмірах і починають випинатися вниз по мірі старіння людини, але це є вимірюваним ефектом. Дослідження свідчать, що вухо змінюється лише 1,22 мм на рік. Також кольоровий розподіл вуха, на відміну від обличчя, майже рівномірний. Вушні дані можна фіксувати навіть без усвідомлення предмета здалеку. Цифрова камера знімає профільні зображення обличчя людей у навколишньому середовищі з різних ракурсів, з яких ділянка вуха сегментується та обробляється. Приклад зображення вуха, який використовується для автентифікації людини із виділеними характерними рисами наведений на рис. 1.10 [5].

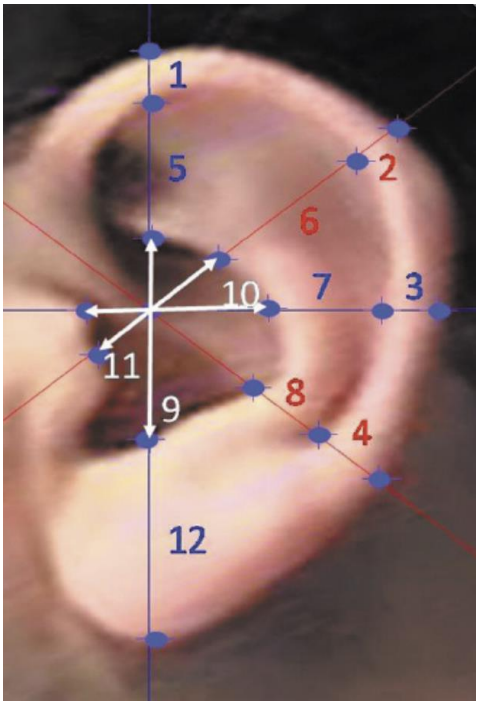

Рисунок 1.10 – Приклад зображення для автентифікації по вуху людини

Потім вектори функцій аналізуються в різних тестових випадках, які складаються з обертання обличчя під різними кутами, різними умовами освітлення, тощо. Недоліком таких систем є те, що паси волосся, або аксесуари можуть знизити результативність таких систем. Вони можуть використовуватися у комбінації з іншими біометричними системами автентифікації.

Незважаючи на простоту використання, статична біометрія має вади безпеки. Найголовнішою проблемою є те, що дані не можуть бути скинуті. Це дає можливість шахраям вкрасти їх, якщо вони здатні обдурити технологію. Наприклад, у 2013 році група німецьких хакерів успішно підробила дані німецького міністра оборони за допомогою фотографій високої чіткості, тоді як дослідникам Національного інституту інформатики в Токіо нещодавно вдалося відновити відбиток пальця з фотографії.

1.2 Динамічні методи біометричної автентифікації

Зазначені вищу вразливості статичних методів біометричної автентифікації призвели до того, що багато людей ставлять під сумнів ефективність та безпеку статичних методів, що допомагає прокласти шлях для більш широкого використання біометричних методів, основою яких є поведінка людини. Ця технологія запроваджує новий, динамічний підхід до автентифікації, аналізуючи складні зразки поведінки. Поведінкова біометрія аналізує внутрішні характеристики, а не зовнішні особливості. Вона вплітається у схеми використання та вивчає, як користувач нормально поводиться під час використання свого пристрою, будуючи унікальний поведінковий профіль, що складається з величезної кількості змінних - від руху всередині сайту чи програми до взаємодії користувача з пристроєм, включаючи тиск пальцем. Складність та рівень деталізації, що стосується, означає, що створений профіль практично неможливо імітувати навіть для найскладніших шахраїв. Він також пропонує зручність для користувачів тим, що він функціонує непомітно у фоновому режимі, і вони постійно ідентифікуються просто завдяки використанню свого пристрою. Оскільки виникає занепокоєння щодо того, чи статична біометрія настільки ж непереможна для нападу, як колись передбачалося, автентифікація поведінки швидко з'являється як більш безпечна альтернатива [7]. Прикладами

динамічної автентифікації є автентифікація за рукописним або клавіатурним почерком, за голосом, мовою тощо.

Розпізнавання за голосом та мовою представляють собою дві окремі біометричні системи автентифікації. Обидві є безконтактними, заснованими на програмному забезпеченні технології, і як такі зараховуються до числа найбільш зручних біометричних даних при регулярному використанні. Розпізнавання голосу, також, часто називають голосовим відбитком. Вимірюючи звуки, які користувач видає під час розмови, для розпізнавання голосу програмне забезпечення вимірює унікальні біологічні фактори, які в поєднанні виробляють голос людини. Головні риси голосу формуються трьома головними властивостями:

- механіка коливань голосових складок;
- анатомія мовного тракту;
- система управління артикуляцією.

Головними ознаками, за якими відбувається ідентифікація особистості, є голосове джерело, резонансні частоти мовного тракту, їх затухання та динаміка управління артикуляцією. До голосового джерела входять: середня частота основного тону, контур і флуктуації частоти основного тону і форма імпульсу збудження. Спектральні характеристики мовного тракту описуються обвідною спектру та його середнім нахилом, формантними частотами або довготривалим спектром. Також, розглядається також тривалість слів, ритм, рівень сигналу, частота й тривалість пауз.

Голосові відбитки можна вимірювати пасивно, оскільки користувач говорить природним чином у розмові або активно, якщо вона змушена говорити парольну фразу. Ключовим моментом є те, що справжнє розпізнавання голосу вимірює деталізацію голосу і не залежить повністю від розмовного коду чи фрази. Розпізнавання мовлення, з іншого боку, є технологією інтерфейсу користувача. У сьогоднішньому все більш мобільному та підключеному світі надзвичайно важливим є наявність вільних можливостей інтерфейсу. Технологія розпізнавання мови, яка також називається голосовою командою, дозволяє користувачам взаємодіяти з технологіями та керувати ними, розмовляючи з ними. Комбіноване розпізнавання мови та голосу може бути потужним дуетом, здатним одночасно виконувати автентифікацію та запропонувати вільний інтерфейс.

Обидва методи розпізнавання мають наступні недоліки:

- шумова компонента;
- низька стійкість до відтворення звукозапису з магнітофону;
- зміна голосу або його відсутність в залежності від стану здоров’я;
- не завжди зручні у використанні.

Метою процесу розпізнавання підписів є ідентифікація записувача певного зразка, тоді як мета процесу перевірки підпису - підтвердити або відхилити зразок. Зразок написання можна перевірити двома окремими методиками. Перший прийом - статичний. Він вимагає, щоб особа подала свій підпис на папері, де вона буде оцифрована через оптичний сканер або камеру. Дані, у свою чергу, запускаються за допомогою програмного алгоритму, який розпізнає текст за допомогою аналізу його форми. Ця методика називається «офлайн» режимом розпізнавання. Офлайн розпізнавання рукописних текстів є важливою формою біометричної ідентифікації, оскільки підписи - це соціально прийнятий метод ідентифікації, який зазвичай використовується для банківських, кредитних карток та різних бізнес-операцій. Офлайн-обробка підписів зазвичай використовується в системах автоматизації офісу, які підтверджують чеки, кредитні картки, контракти та історичні документи. Статичне, офлайн розпізнавання рукописного тексту виконується після того, як текстовий зразок заповнений оцифрований. Оптично захоплені дані зображення потім перетворюються в бітовий візерунок. Офлайн-обробка підписів налічує майже сорок функцій, включаючи аналіз центру ваги, ребер та кривих для автентифікації. Таким чином, розпізнавання підпису в режимі офлайн може бути складним завданням через нормальну мінливість підписів і те, що динамічна інформація щодо шляху ручки недоступна. Більше того, вибіркові дані зазвичай обмежені лише невеликою кількістю підписів на особу. Відповідність форми зазвичай розглядають шляхом визначення та співставлення ключових точок, щоб уникнути проблем, пов’язаних із виявленням та параметризацією кривих.

Динамічне розпізнавання підписів використовує для розпізнавання анатомічні та поведінкові характеристики, які індивід проявляє, підписуючи своє ім’я або іншу фразу. Пристрої динамічного підпису не слід плутати з автономними системами збору електронних підписів, які використовуються для зйомки графічного зображення підпису і є загальними в місцях, де торговці фіксують підписи для авторизації транзакцій. Такі дані, як захоплений напрямок,

штрих, тиск та форма підпису особи можуть давати можливість почерку бути надійним індикатором особи. Динамічне розпізнавання підписів використовує різноманітні характеристики при аналізі почерку людини. Ці характеристики різняться у використанні та важливості від постачальника до постачальника і збираються за допомогою чутливих до контактів технологій, таких як спеціальні планшети, що реєструють підпис у режимі реального часу. Характеристики, які використовуються для динамічного розпізнавання підпису, майже неможливо повторити. На відміну від графічного зображення підпису, який може бути відтворений підготовленим шахраєм, комп'ютерною маніпуляцією чи ксерокопією, динамічні характеристики є складними та унікальними для стилю почерку особистості. Головним недоліком даного методу є те, що він не завжди зручний для користувачів.

У динаміці натискання клавіш використовується унікальний біометричний шаблон для виявлення осіб на основі введення тексту, ритму та швидкості. Сирі вимірювання, які використовуються для динаміки натискання клавіш, відомі як "час перебування" та "час польоту". Час затримки - це тривалість натискання клавіші, а час польоту - тривалість між натисканнями клавіш. Отже, динаміку натискання клавіш можна описати як алгоритм, заснований на програмному забезпеченні, який вимірює час перебування та час польоту для автентифікації особи.

У 2004 році дослідники запропонували ідею автентифікації за допомогою біометрії натискання клавіш та виявили кілька основних переваг та недоліків у використанні цього біометричного для автентифікації. По-перше, дослідники дійшли висновку, що вимірювання динаміки натискання клавіш є доступним і ненав'язливим, оскільки для цього потрібне дуже мало апаратного забезпечення, крім клавіатури, що робить його легким для використання на підприємствах, по відношенню до входів на робочих станціях та інших точках безпеки доступу відносно низька вартість. По-друге, оскільки кожне натискання клавіші повністю фіксується натисканням клавіші та часом натискання, дані можуть передаватися через з'єднання з низькою пропускною здатністю.

Даний метод має наступні недоліки. По-перше, введення шаблонів може бути нестабільним та непослідовним, оскільки щось на зразок тісних м'язів та потових рук може суттєво змінити шаблон введення людини. Також було

встановлено, що шаблони введення тексту залежать від типу клавіатури, що використовується. Це може значно ускладнити перевірку.

Людська хода є унікальною особливістю, яку можна використовувати для розпізнавання людини. Метод розпізнавання на основі ходи поєднує в собі ряд переваг, таких як висока стійкість до шахрайства, безпечний збір даних, відсутність необхідності в явній взаємодії з користувачем та безперервна і міжміська автентифікація. Ця комбінація робить ходу придатним біометричним параметром для перевірки користувачів. Однак коливання ходи у людей похилого віку більш значні, ніж у молодих людей через зміни фізичної сили, пов'язані зі старінням. Як результат, розпізнавання ідентичності старших дорослих на основі ходи є складнішим завданням. Головним недоліком даного методу біометричної автентифікації є необхідність наявності спеціального обладнання. Для аналізу ходи використовується кілька камер, а саме відеокамер або інфрачервоних, розміщених навколо доріжки або бігової доріжки, які пов'язані з комп'ютером. У пацієнта є маркери, розташовані в різних точках тіла. Пацієнт спускається по біговій доріжці, а комп'ютер обчислює траєкторію кожного маркера в трьох вимірах. Для обчислення руху підлеглих кісток застосовується модель. Це дає повне розбиття руху кожного суглоба.

Динамічні методи біометричної автентифікації також не є ідеальними. Поведінка користувачів часто змінюється залежно від їх місця - наприклад, за офісним столом чи лежачи в ліжку - і люди також схильні діяти по-різному, коли вони втомилися або поспішають.

Найкраща безпека є поєднанням безлічі технологій автентифікації. Наприклад, розпізнавання обличчя може поєднуватися з іншими біометричними характеристиками такими, як поведінкова біометрія, сканування відбитків пальців або іншими методами захисту, такими як паролі, використання надійних пристроїв або шляхом аналізу контексту на основі місцезнаходження, даних транзакцій та характеристик пристрою.

Отже, виходячи з переваг та недоліків усіх зазначених вище методів біометричної автентифікації, можна зробити висновок, що одним з найбільш точніших, стійких до підробки, безпечних для здоров’я, зручних для користувачів та поширених у використанні є метод розпізнавання людини по райдужній оболонці ока.

2 АНАЛІЗ МЕТОДІВ ЗАХИСТУ БІОМЕТРИЧНОГО ШАБЛОНУ

Процес ідентифікації зазвичай включає велику базу даних біометричних шаблонів, і фаза верифікації полягає у відновленні відповідного шаблону в базі даних. Централізоване зберігання незахищених біометричних даних є головною загрозою для конфіденційності користувачів. Біометрична автентифікація не обов'язково використовує централізовану базу даних, і для багатьох додатків необхідний додатковий захищений елемент як смарт-карта для зберігання біометричних даних. Однак централізоване зберігання захищених біометричних даних є можливою альтернативою, якщо цей централізований підхід не є загрозою конфіденційності та безпеці системи.

Схеми біометричної автентифікації мають великий потенціал у побудові захищених систем. Як правило, схема біометричної автентифікації складається з двох фаз. Під час фази зарахування користувач, реєструє свої біометричні дані, які відправляються на надійний сервер. Біометричний шаблон створений для користувача зберігається на якомусь центральному сервері або на пристрої, який може переноситися, наприклад, смарт-картці. Збереження біометричного шаблону на смарт-картці має такі недоліки:

- не підходить для достатньо масштабних додатків;
- шаблон може бути викрадений;
- велика вартість;
- не є зручним для користувача, оскільки користувач має завжди носити його з собою.

Під час фази автентифікації користувач надає інший біометричний зразок, який порівнюється з шаблоном на сервері чи пристрої. Автентифікація завершується успіхом, якщо новий зразок відповідає шаблону згідно з деякою функцією відповідності. У цьому випадку біометричний шаблон користувача надає важливу інформацію для успішної автентифікації. Після цього користувач отримує відповідь від системи стосовно того схвалено подальший доступ чи відхилено його [8]. Описаний вище процес роботи системи біометричної автентифікації наведений на схемі, яка зображена на рис. 2.1.

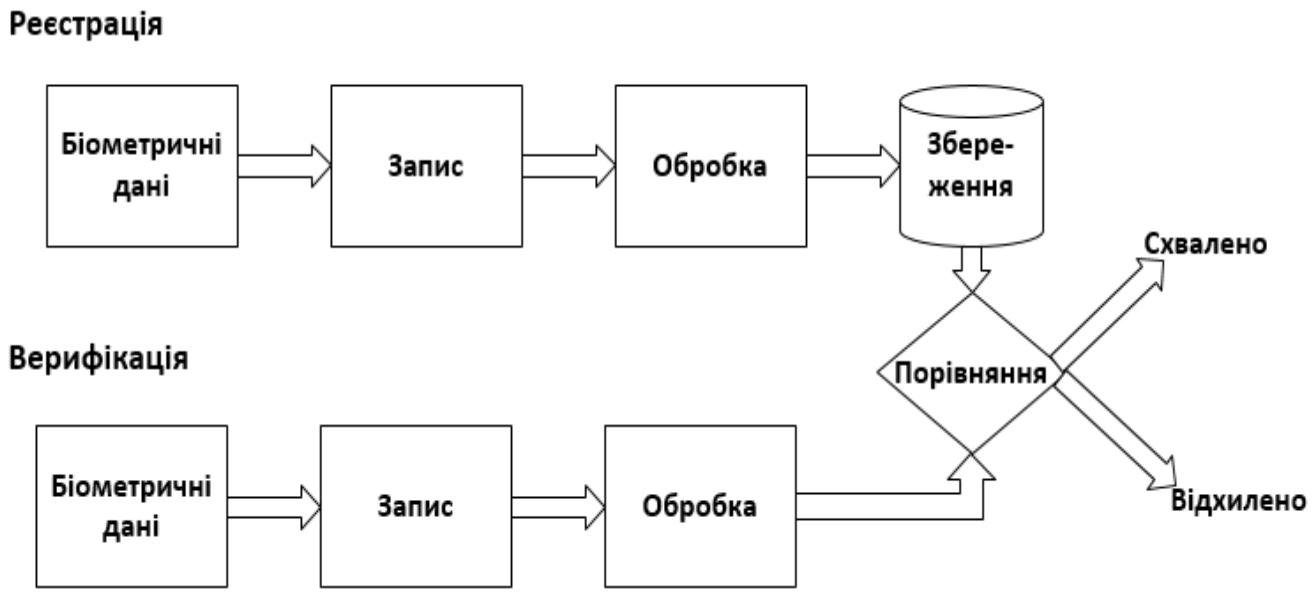

Рисунок 2.1 – Схема біометричної автентифікації

Після автентифікації шаблон потенційно дозволяє зловмиснику отримати достатню кількість даних, які представляють користувача. Тому важливо не допускати зловмисників до вилучення біометричних шаблонів користувачів. Викрадення таких даних є серйозною проблемою, оскільки пошкоджені та заблоковані біометричні шаблони не можуть бути відкликані як паролі. Ця проблема є значно серйознішою порівняно з традиційними системами автентифікації на основі пароля чи сертифікатів, де компрометовані облікові дані користувачів можуть бути легко відкликані. У випадку зі звичайним паролем для його захисту використовуються криптографічні хеш-функції. Але такий спосіб не підходить для захисту біометричних даних. Зазвичай, біометричні шаблони, що мають ідентифікувати одну людину, не є повністю ідентичними, оскільки можуть бути зроблені під різним кутом нахилу, освітленням або іншими оточуючими факторами [9]. Таким чином, у разі використання звичайної хеш-функції зміна однієї одиниці байт-коду зробленого з шаблону призведе до повної зміни хеш-функції. Це може призвести до помилок у розпізнаванні, незважаючи на те, що зміни були незначні. Для вирішення цієї проблеми слід використовувати спеціальні методи.

Методи захисту біометричних шаблонів зберігають модифіковану версію біометричного шаблону і розкривають якомога менше інформації про оригінальну біометричну ознаку, не втрачаючи можливості ідентифікувати людину. Такі методи мають задовольняти наступним критеріям:

- крос-збіг захищених шаблонів має бути неможливим;
- скасування скомпрометованого шаблону і створення нового з тих самих біометричних даних має бути можливим;
- ефективність роботи біометричної системи не повинна погіршуватися системою захисту шаблону.

Такі методи також метод можуть розглядатися як двох факторний метод автентифікації, який поєднує особистий пароль або секретний ключ з біометричним захистом для отримання захищеного бінарного шаблону, який використовується для автентифікації.

Методи захисту шаблонів можна класифікувати на дві групи: біометричні криптосистеми та методи, засновані на трансформації або засолювання. Біометричні криптосистеми або з’єднують секрети з біометричними даним для формування безпечного біометричного шаблону, або генерують секрети з біометричних даних за допомогою деяких інших допоміжних даних. Секрети можна успішно отримати під час спроби перевірки. Підходи, засновані на перетворенні, спотворюють або рандомізують біометричні дані з використанням функцій, які забезпечують, щоб вихідні дані не могли бути реконструйовані з трансформованих шаблонів. Біометричні шаблони трансформуються на основі параметрів, отриманих із зовнішньої інформації, наприклад, ключів користувача або паролів.

Біометричне хешування є одним із методів на основі трансформації, в якому біометричний шаблон користувача перетворюється на захищений двійковий рядок. Одна переваг біометричного хешування полягає у простоті відкликання трансформованого шаблону шляхом зміни відповідного секретного ключа. Крім того, використовуючи однакові біометричні дані, користувач може бути розпізнаний для різних служб за допомогою різних біометричних хешей, що генеруються з різних секретних ключів [10]. Таким чином, два записи, представлені двом різним системам, не можуть бути пов'язані, а діяльність користувача залишається приватною.

2.1 Атаки на біометричні шаблони

Узагальнена біометрична система складається з датчика, модуля вилучення функцій, бази даних біометричних шаблонів, модуля відповідності та

прикладного пристрою, який керується відповіддю відповідника. Дослідники визначили різні варіанти атак на такі системи .До них відносяться такі атаки, як «троянський кінь», фішинг атаки, атаки на «front-end», атаки на канал зв’язку. Можливі атаки на біометричні системи наведені на рис. 2.2.

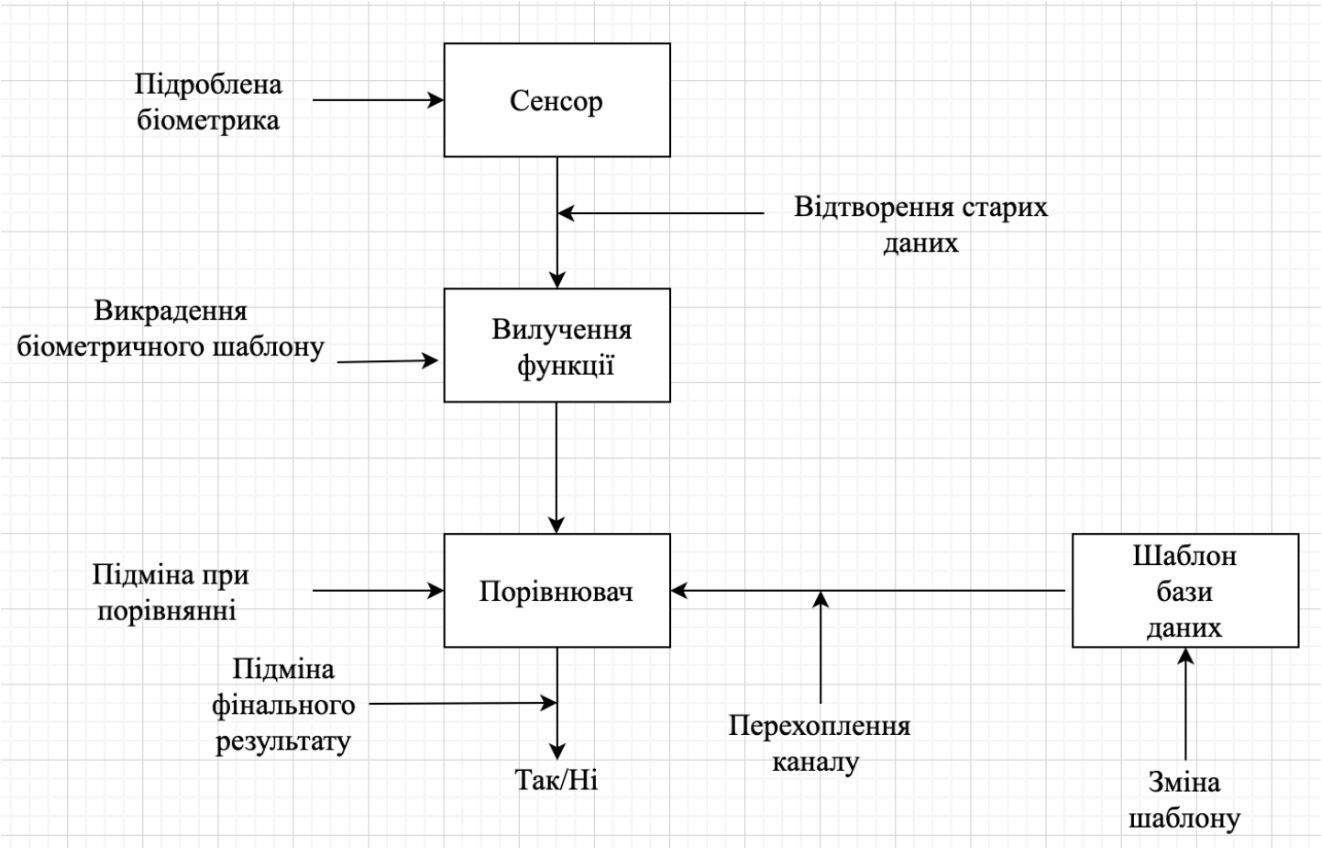

Рисунок 2.2 – Можливі атаки на системи біометричної автентифікації

Несанкціонований доступ до біометричних шаблонів у первозданному вигляді є однією з найсерйозніших загроз конфіденційності та безпеці користувачів.

Біометричні системи можуть бути атаковані шляхом викриття параметра, а саме ключа, що застосовується для трансформації біометричних шаблонів. У випадку, коли перетворення обернено, оригінальну біометрію можна реконструювати. У цьому випадку безпека знаходиться в секреті ключа. Якщо трансформація не є зворотною, то зловмисник може спробувати приблизно відновити початкові біометричні шаблони. Також було досліджено, о що коли декілька трансформованих шаблонів генеруються з одного і того ж оригінального шаблону, їх можна зламати методом, який має назву «Attack via Record Multiplicity». Зокрема, даючи перетворений шаблон, зловмисник може знайти

зворотні рішення, обернувши перетворення [11]. Через властивість функцій перетворення «багато-в-одну» може бути декілька рішень, одне з яких є оригінальним. Зловмисник може придумати спосіб вибрати правильне рішення.

Одним з головних обмежень методів біометричного хешування є їх низька продуктивність, коли зловмисники володіють секретним ключем. Було досліджено, що просте зменшення розмірності даних та дискретизація, як це робиться в більшості методів біометричного хешування, можуть бути вразливими до атак знаходження першотвору. Дана атака полягає у спробі відшукати біометричний код із заданим значенням хеш-кодування.

За останні роки було запропоновано декілька схем захисту біометричних даних, які намагаються захистити конфіденційність біометричних шаблонів без використання ключа. Наприклад, однією з таких схем є метод візуальної криптографії, який розкладає біометричне зображення на два шумоподібні зображення, звані аркушами, які зберігаються у двох різних базах даних. Під час автентифікації два аркуші перекриваються, щоб створити тимчасове зображення для відповідності. Одне з обмежень цього методу полягає в тому, що він вимагає двох спільних баз даних для спільної роботи, що може бути не практичним для деяких застосувань. Інший метод захисту біометричного відбитка пальця поєднує два відбитки пальців з двох різних пальців для створення нового шаблону. Для автентифікації потрібні два відбитка пальців запиту. Даний метод пропонує двоступеневий процес узгодження для відповідності двох відбитків пальців запиту комбінованому шаблону. Однією з переваг цього методу є те, що при використанні комбінованого шаблону повна характеристика єдиного відбитка пальця не буде порушена при викраденні бази даних [12]. Обидві ці схеми вразливі до атак вторгнень, оскільки порівняно легко отримати або наближення вихідного біометричного шаблону, або попереднє зображення трансформованого шаблону у випадку скасування відбитків пальців. Таким чином, хоча біометричні криптосистеми можна проаналізувати за допомогою інформаційних теоретичних метрик, наприклад, таких як ентропія, безпека методів, заснованих на трансформації, ґрунтується на складності зворотності перетворення.

3 ОГЛЯД ПРОЦЕСУ РОЗПІЗНАВАННЯ ЛЮДИНИ ПО РАЙДУЖНІЙ ОБОЛОНЦІ ОКА

Розпізнавання райдужної оболонки залишається однією з найбільш точних та доступних форм ідентифікації. Кожна райдужна оболонка є унікальною, тому якщо у людини використовуються обидві райдужки для ідентифікації, шанс помилки при розпізнаванні надзвичайно малий. На відміну від кількох інших характеристик людини, які зараз використовуються для ідентифікації, структури райдужної оболонки стабілізуються у віці десяти місяців і залишаються незмінними до кінця життя. Колись дороге та складне програмне та апаратне забезпечення для систем розпізнавання по райдужній оболонці ока зараз стає більш економічним і вигідним варіантом для багатьох організацій та підприємств.

Системи розпізнавання людини по райдужній оболонці ока набули широкого поширення в багатьох сферах життєдіяльності людини. Широке поширення такі системи здобули у прикордонній безпеці. Завдяки своїм перевагам біометричні системи автентифікації на основі райдужної оболонки ока використовуються працівниками служби безпеки в аеропортах, кордонах та служб корпоративного захисту протягом останніх двадцяти років. Кілька країн, включаючи Об’єднані Арабські Емірати та Саудівську Аравію, почали використовувати цю технологію для заявників на отримання віз ще в 2002 році. Однак цю технологію зараз можна вважати глобальною, і кількість країн, які використовують її для визначення заявників на візи значно збільшилася і зараз включає Канаду, Нідерланди, Сполучені Штати Америки (США) та інші. В США також використовують технологію розпізнавання по райдужці для ідентифікації усіх військовослужбовців Сполучених Штатів для підвищення безпеки та дозволу на доступ до військових об'єктів [13].

За останні десять ідентифікація по райдужній оболонці ока здобула популярності у фінансовій сфері, а саме у фінансових технологіях. У цій галузі розпізнавання по райдужної оболонки все частіше використовується як інструмент автентифікації для онлайн-додатків через банківські послуги завдяки збільшенню доступності рентабельних інформаційних технологій. Незважаючи на те, що використання сканування райдужної оболонки є значною мірою опцією "відключення" для цієї сфери, воно також успішно використовується у набагато ширших програмах. Наприклад, для запобігання шахрайству та махінаціям у

соціальних виплатах у 2009 році уряд Індії створив унікальний ідентифікаційний орган, який за три роки зарахував 1,25 мільярда індійських громадян у свою програму посвідчення особи, записуючи дані про райдужку та відбитки пальців кожного громадянина. Це мало величезний вплив на зменшення шахрайства із соціальними виплатами і зараз також продовжує використовуватися для того, щоб допомога надходила тим, хто найбільше потребує. Раніше більше ніж половина допомоги уряду Індії регулярно привласнювалася шляхом шахрайства. Слідом за цим успіхом такі країни, як Індонезія, Сінгапур та Мексика, наслідували цю заяву за власними версіями, в тому числі й зразками райдужної оболонки на паспортних даних. У 2013 році розпізнавання по райдужній оболонці почало використовуватися для визначення та управління розподілом фінансової допомоги біженцям конфліктів у Сирії, Судані, М'янмі, Афганістані та Малаві [14].

Незважаючи на те, що розглянуті вище сфери життєдіяльності людини користуються розпізнаванням райдужної оболонки вже кілька років, сфера охорони здоров’я відносно недавно почала впровадження біометричних систем. Використання біометричних даних, таких як розпізнавання райдужної оболонки, дозволяє медичним працівникам легко ідентифікувати осіб та зіставляти їх із медичними записами. Нещодавно Всесвітня організація охорони здоров'я перерахувала точну ідентифікацію пацієнта до одного із дев'яти пріоритетів щодо покращення безпеки пацієнтів у всьому світі. Внесення цього пріоритету означає зменшення кількості помилок через неправильну ідентифікацію та дублювання записів у системах охорони здоров’я. Отже, догляд за пацієнтами прискорюється при забезпеченні правильного призначення ліків правильній особі. Використання біометричних інструментів, таких як сканування райдужної оболонки для ідентифікації, також є особливо корисним, коли пацієнт не може надати інформацію для підтвердження своєї ідентичності через хворобу або неможливість ефективно спілкуватися. Розширений доступ до медичної допомоги має вирішальне значення для просування та захисту будь-якого суспільства. Завдяки медичному прогресу та розширеному доступу також виникає посилений тиск на медичні послуги для своєчасного надання якісної допомоги. Оцифрування записів є важливим інструментом зменшення тиску, заміною трудомістких паперових систем, що вразливі до людських помилок і нагляду. Автоматизовані системи можуть використовувати розпізнавання по райдужній оболонці ока для

підтвердження претензій на медичне страхування, прискорення виплат, стабілізації фінансування та захисту майбутніх ініціатив у галузі охорони здоров'я [15].

Неможливо не відзначити швидке впровадження технології розпізнавання по райдужній оболонці ока у смартфони та інші гаджети. Компанія Samsung першою вивчила наявні можливості для включення технології розпізнавання по райдужці у свої телефони як метод автентифікації та розблокування пристрою. Прагнучи зберегти інформацію своїх клієнтів якомога безпечніше, Samsung додала розпізнавання по райдужці поряд із іншими формами біометричної безпеки. Розпізнавання райдужної оболонки розташоване поряд із розпізнаванням відбитків пальців та обличчям. Ці додаткові функції безпеки гарантують користувачам захист доступу до їх найбільш особистої інформації. Також використання ідентифікації по райдужній оболонці ока може стати частиною двох факторного процесу автентифікації для пільгового доступу до таких додатків, як Інтернет-банкінг і навіть безпечний доступ електронною поштою. Це дасть можливість використовувати розпізнавання по райдужці рідше, ніж для кожного розблокування пристрою, додаючи до безпеки на найважливіші додатки, створюючи додатковий рівень довіри до безпеки.

Слід відзначити, що зараз поширюються системи віддаленої біометричної автентифікації по райдужній оболонці ока у «хмарі». Система розпізнавання по райдужній оболонці дозволяє авторизованому користувачеві отримувати доступ до програмного забезпечення як послуги хмарного сервера. Прикладом такого сервісу є система IriSecureID. Вона забезпечує різноманітні функції розпізнавання райдужної оболонки, включаючи реєстрацію, перевірку, ідентифікацію та дуплікацію програм та розробників корпоративних служб. IriSecureID дозволяє легко інтегруватися в будь-які існуючі програми. Як хмарний сервіс, який є масштабованим та доступним, вона може бути застосована у широкому колі корпоративних програм. Така система складається з IriSecureIDService, розгорнутого на хмарному сервері, програмного компонента під назвою IriSecureIDAdapter на стороні клієнта та клієнтського додатка під назвою IriSecureID Client. Клієнтська програма підключається до камери IriShield для зйомки зображень райдужної оболонки та використовує IriSecureIDAdapter для надсилання запитів на реєстрацію чи відповідність до IriSecureIDService через

захищений канал зв'язку. Загальна схема віддаленої біометричної автентифікації наведена на рис. 3.1 [16].

Рисунок 3.1 – Модель системи віддаленої біометричної автентифікації

Таким чином, враховуючи зазначену вище інформацію, можна зробити висновок, що використання систем віддаленої біометричної автентифікації по райдужній оболонці допоможе знизити рівень злочинності, покращити діяльність сфери охорони здоров’я та полегшити життя багатьох користувачів, звільнивши їх від необхідності запам’ятовувати пароль. Також варто відзначити, що завдяки

тому, що дані системи є автоматизованими, поширення корупції у них не може бути можливим.

3.1 Технологія розпізнавання по райдужній оболонці ока

Концептуально систему автоматизованого розпізнавання райдужної оболонки можна розділити на три частини. Перший набір питань оточує придбання зображення. Другий набір стосується вилучення необхідних характеристик з райдужки та створення захищеного біометричного коду. Третя частина стосується узгодження витягнутого шаблону райдужної оболонки із записами бази даних кандидатів.

Однією з головних проблем автоматизованого розпізнавання по райдужній оболонці є зйомка якісного зображення райдужної оболонки, яка має залишатись не помітною для людини, не спричиняючи їй дискомфорт. Враховуючи, що райдужна оболонка є порівняно невеликою, зазвичай становить близько одного сантиметру в діаметрі, часто має темний колір і людина дуже чутлива до своїх очей, ця справа потребує ретельної інженерії. У зв’язку з цим необхідно надати увагу наступним факторам. По-перше, бажано придбати зображення райдужної оболонки з достатньою роздільною здатністю та різкістю для підтримки розпізнавання. По-друге, важливо мати достатній контраст у шаблоні райдужної оболонки, не змінюючи рівень освітленості, який може дратувати користувача. По-третє, ці зображення повинні бути добре обрамлені, тобто бути по центру, не надто обмежуючи дії користувача, не вимагаючи від оператора використання окуляра, підборіддя або іншого контактного розташування. Також дефекти на придбаних зображення, наприклад, такі, як дзеркальні відображення предметів, оптичні відхилення повинні бути максимально усунені.

Існуючі системи розпізнавання райдужної оболонки змогли відповісти на виклики роздільної здатності та фокусування зображення за допомогою стандартної оптики. Зазвичай такі системи фіксують зображення діаметром райдужної оболонки, як правило, від 100 до 200 пікселів на відстані 15–46 см за допомогою 330-мм об'єктива. Через необхідність утримувати рівень освітленості відносно низьким для комфорту оператора, оптична діафрагма не може бути занадто малою. Захоплення швидкості відео використовується обома системами. Як правило, цього достатньо для захисту від розмиття через рухи очей за умови,

що оператор намагається підтримувати стійкий погляд [17]. Додаткові дослідження показали, що зображення потенційної якості для підтримки розпізнавання райдужної оболонки можуть бути отримані в досить різних умовах. Наприклад, зображення райдужки можна придбати на відстані до метра, використовуючи стандартну відеокамеру з телеоб'єктивом. Крім того, зображення райдужної оболонки можна придбати в дуже близькому діапазоні, коли користувач носить на голові дисплей, обладнаний світлодіодними освітлювачами, мікромініатюрною оптикою та камерою. Ще одним фактором, на який слід звернути увагу, є темний колір очей. До цієї проблеми використовують різні підходи. Перший використовує точковий джерело світла на основі світлодіодів разом із стандартною відеокамерою. Другий використовує дифузне джерело та поляризацію спільно з камерою із низьким рівнем освітлення. Також було досліджено, що для реєстрації темних очей краще проводити в ближньому інфрачервоному спектрі, а реєстрацію світлих очей - у видимому діапазоні. Схема процесу отримання зображення ока наведена на рис. 3.2 [17].

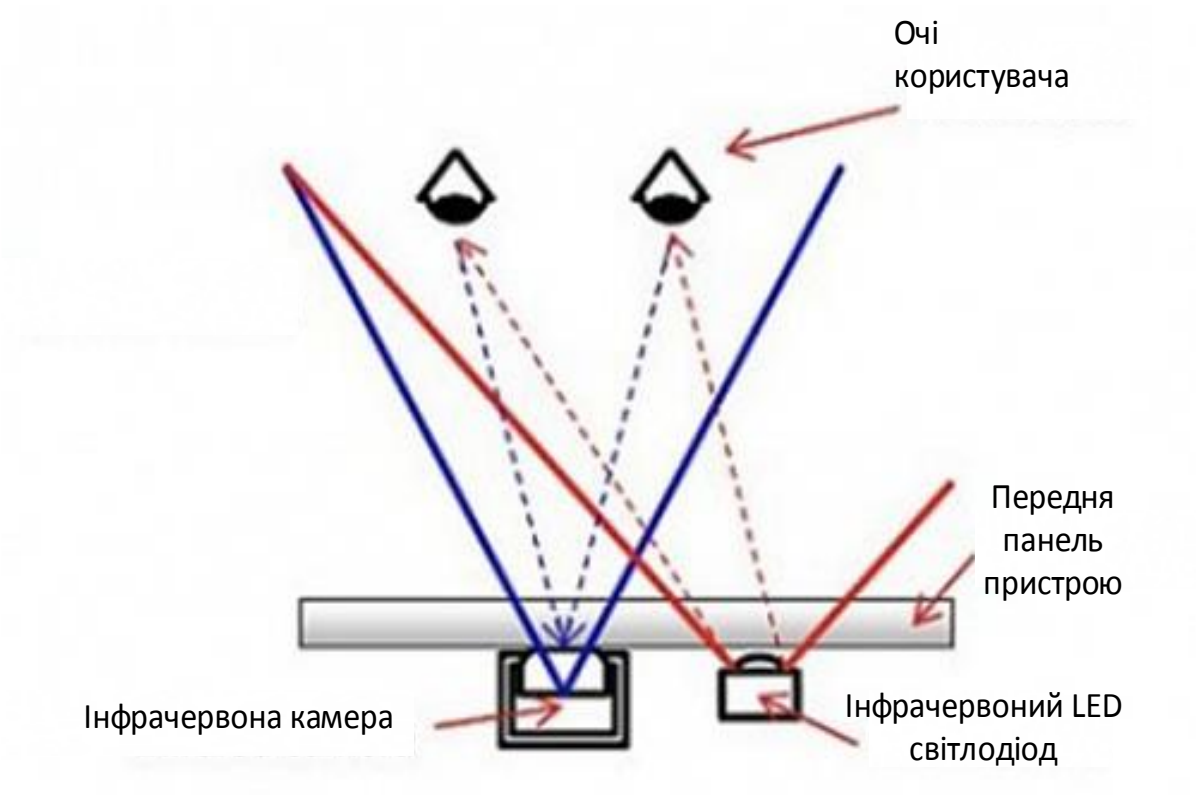

Рисунок 3.2 – Процес отримання зображення ока

Завдяки ретельному розташуванню джерела світла можна уникнути відбитків точкового джерела від окулярів у зображеній райдужній оболонці.

Деякі системи вимагають від користувача самостійно розташувати область очей перед камерою. Інші забезпечують відео-зворотний зв'язок з користувачем у прямому ефірі за допомогою мініатюрного рідкокристалічного дисплея, розміщеного у відповідності з оптикою камери. Це дозволяє користувачу бачити, що фотокамера захоплює, і відповідно регулювати його положення. Під час цього процесу система постійно набуває зображення. Після отримання серії зображень достатньої якості одне автоматично передається для подальшої обробки. Якість зображення оцінюється шляхом пошуку крайових контрастних країв, що позначають межу між райдужною оболонкою та склерою. Слід відзначити, що камера повинна мати дуже невеликий кут огляду. Це необхідно для концентрування на конкретній точці. Зазвичай, процес розпізнавання по райдужній оболонці ока триває до тридцяти секунд [18].

На даний момент не існує єдиного стандартизованого алгоритму біометричної автентифікації по райдужній оболонці ока, тому питання вибору найбільш оптимального є достатньо актуальним.

3.2 Райдужна оболонка ока як біометричний параметр

Для розроблення системи біометричної автентифікації по райдужній оболонці ока необхідно визначити, що саме робить райдужку ока унікальною і особливості її функціонування в організмі людини, щоб знати яким чином слід отримувати її індивідуальні характеристики, не зашкодивши її роботі та комфорту користувача.

Райдужна оболонка ока людини знаходиться між передньою та задньою камерами ока. Вона починає формуватися на третьому місяці вагітності. Формування структури райдужки, але завершується до восьмого місяця вагітності, але пігментація продовжується ще в перший рік після народження. Райдужна оболонка виростає з циліарного тіла, її колір визначається кількістю пігменту і щільністю тканини райдужної оболонки, тобто від синього до чорного. Найважливіша функція райдужної оболонки - контроль розміру зіниці. Освітлення, яке потрапляє в зіницю і потрапляє на сітківку ока, контролюється м’язами райдужної оболонки. Вони регулюють розмір зіниці, і саме це дозволяє райдужній оболонці контролювати кількість світла, що потрапляє до зіниці. Зміна розміру зіниці не знаходиться під усвідомленим контролем людини. Сама тканина

райдужної оболонки, яка виступає у якості біометричного шаблону для автентифікації, називається «trabecular meshwork». Шари райдужної оболонки мають як ектодермальне, так і мезодермальне ембріологічне походження. Видимим є передній шар, який несе рельєфно-кольоровий колір, і він має легку пігментацію завдяки генетично обумовленій щільності пігментних гранул меланіну. Невидимим є задній шар, який дуже темно пігментований, всупереч передньому шару. Пігментна оболонка є межею між зіницею та райдужною оболонкою людини. Весь передній шар складається із зіницької ділянки та циліарної області, а їх межа називається коллатером. Циліарна ділянка поділяється на внутрішню зону, яка є відносно гладкою і несе радіальні борозни, які є унікальними у кожної людини.

Наступні видимі риси райдужної оболонки людини важливі для біометричної ідентифікації людини: особливості, пов’язані з пігментом; особливості, що контролюють розмір зіниці; видимі рідкісні аномалії; пігментна оболонку та комір. Одними з пігментних ознак є крипти, які зображені на рис. 3.3 [19].

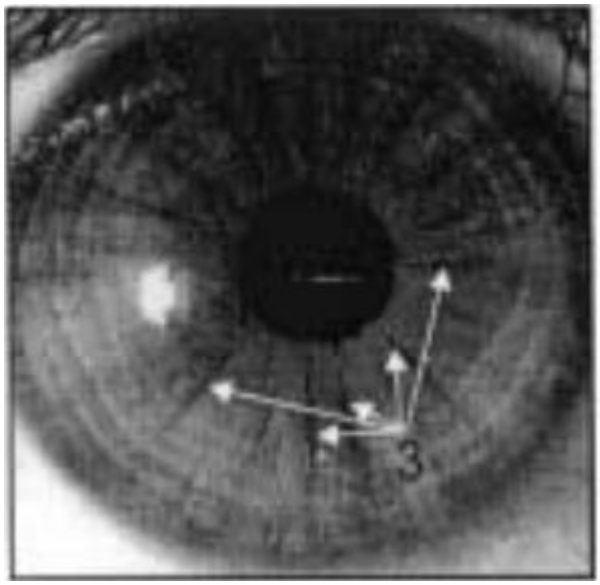

Рисунок 3.3 – Крипти на райдужній оболонці ока

Криптами є ділянки, в яких райдужна оболонка порівняно тонка. На рис. 3.3 крипти виділені стрілками та позначені номером три. Вони мають дуже темний колір через темний колір задньої частини шару. Крипти з’являються біля коміра, або на периферії райдужної оболонки.

Другими пігментними ознаками є пігментні плями. Пігментні плями є випадковими концентраціями пігментних клітин у видимій поверхні райдужної оболонки і, як правило, з’являються в області циліар. Вони відомі як родимки та веснянки майже чорного кольору. Пігментні плями на райдужній оболонці ока зображені на рис. 3.4 та позначені цифрою чотири [19].

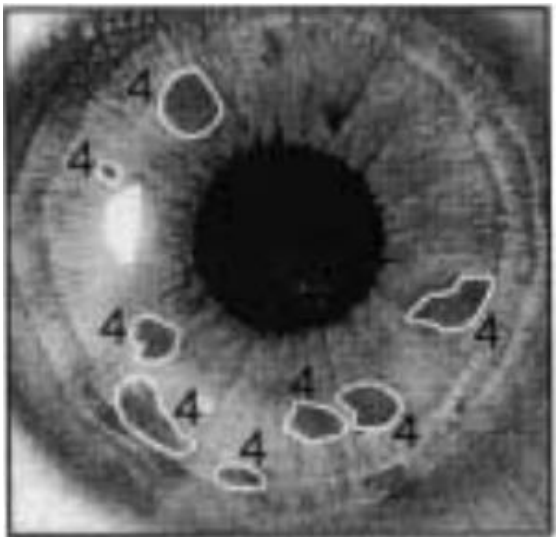

Рисунок 3.4 – Пігментні плями на райдужній оболонці ока

Особливостями, що контролюють розмір зіниці, є радіальні та концентричні борозни. Їх також називають скорочувальними борознами. Радіальні та концентричні борозни зображені на рис. 3.5 цифрами 5 та 6 відповідно [19].

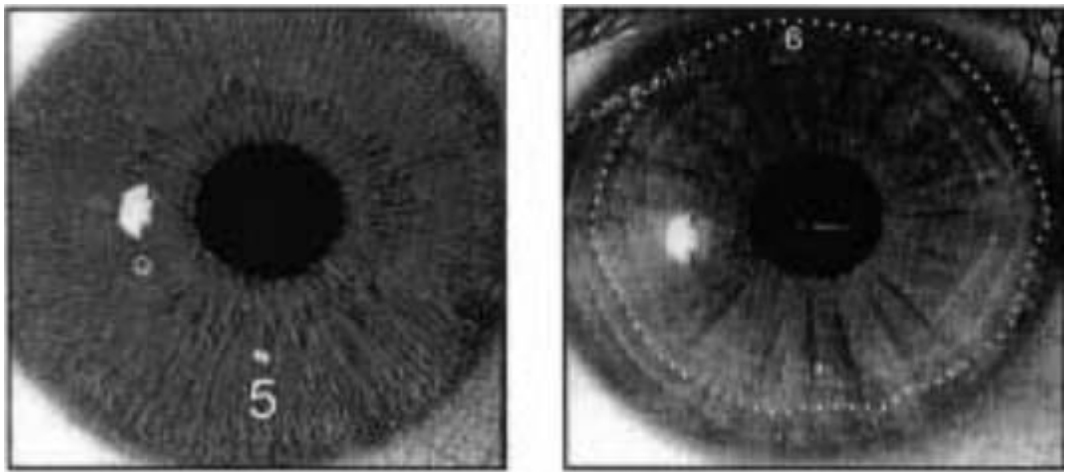

Рисунок 3.5 – Радіальні та концентричні борозни на райдужній оболонці ока

Радіальні борозни укладаються в передньому шарі райдужної оболонки, з якого пухка тканина може випинатися назовні, і саме це дозволяє райдужній

оболонці змінювати розмір зіниці. Концентричні борозни, як правило, круглі та концентричні зі зірочкою. Вони зазвичай з'являються в області циліар, поблизу периферії райдужної оболонки і дозволяють випинати пухку тканину назовні в іншому напрямку, ніж променеві борозни. Райдужна оболонка ока людини може мати декілька рідкісних аномальних видимих рис. Через старіння або травми на райдужній оболонці можуть з’являтися атрофічні ділянки, що призводить до зміни текстури райдужки. На райдужній оболонці можуть зростати пухлини, або можуть виникати вроджені ридання, що з'єднують райдужну оболонку з кришталиком ока.

Таким чином, завдяки великій кількості зазначених вище складових, райдужна оболонка ока має високу унікальність. Згідно з дослідженнями з три-чотири біти інформації на один квадратний міліметр площі можна отримати з одинадцяти міліметрового діаметру райдужної оболонки.

3.3 Загальний алгоритм розпізнавання по райдужній оболонці

Біометрична система автентифікації по райдужній оболонці ока складається з апаратної та програмної складових. В даній роботі досліджуються третій та четвертий етапи моделі системи віддаленої біометричної автентифікації, схема якої зображена на рис. 3.1, - формування біометричного шаблону та формування біохешу [20].

Формування біометричного шаблону райдужної оболонки ока людини відбувається вже після отримання чіткого зображення ока біометричними датчиками і поєднує в собі наступні етапи:

- обробка зображення ока;
- накладання фільтру для виділення важливих характеристик;
- генерація коду райдужної оболонки.

Далі починається формування біохешу на основі згенерованого коду райдужної оболонки. Після цього відбувається занесення біохешу в базу даних. Перше отримання коду райдужної оболонки та занесення його до бази, як еталону, називається реєстрацією користувача. При наступному розпізнаванні користувача відбуваються зазначені вище етапи формування біометричного шаблону та накладання біохешу. Більш детальний алгоритм формування

біометричного шаблону та біохешу при процесі автентифікації користувача наведений на рис. 3.6.

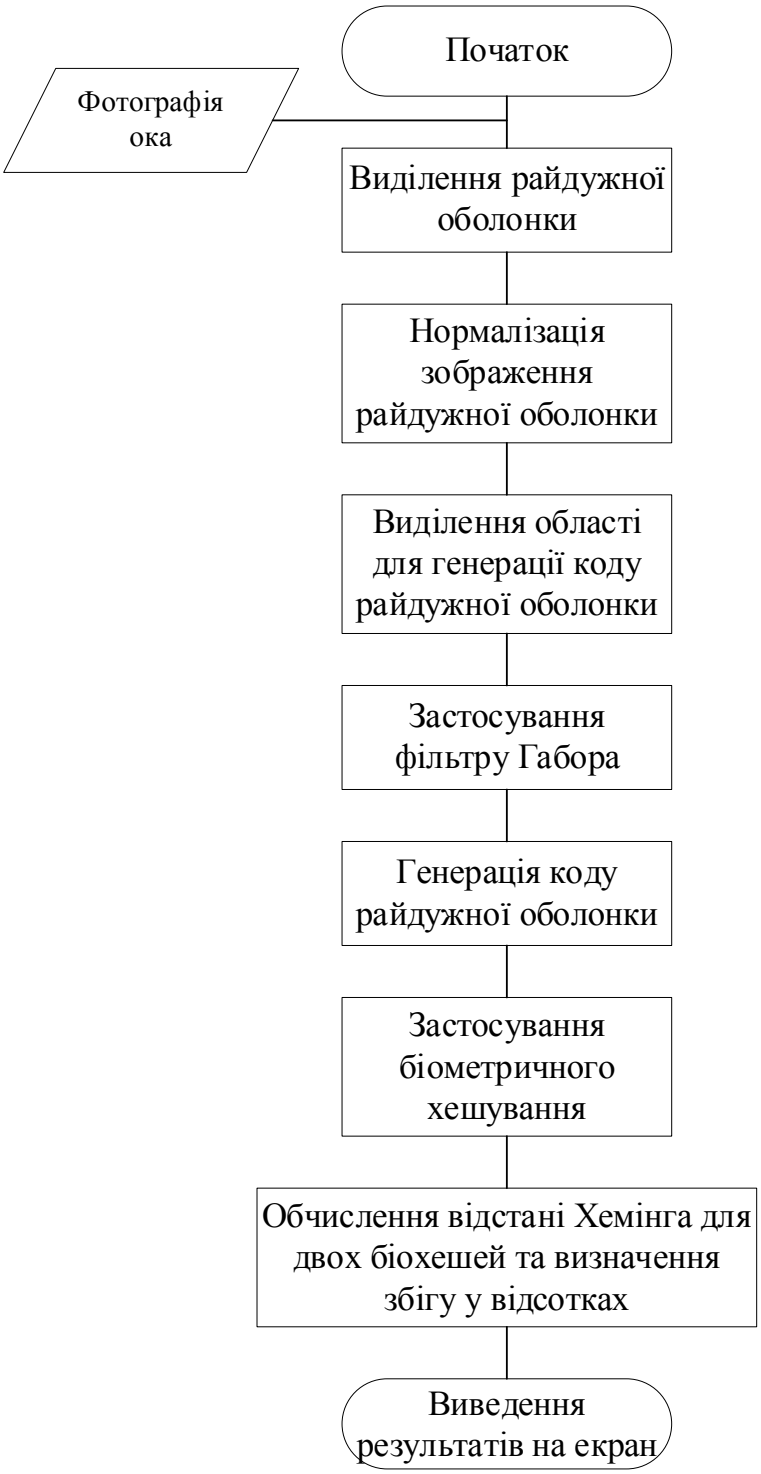

Рисунок 3.6 – Алгоритм розпізнавання по райдужці

Далі відбувається порівняння біохешу із біохешами, які зберігаються у базі. Порівняння може відбуватися за допомогою однієї з двох метрик, які мають назву Hamming distance та Jaccard similarity.

Необхідно відзначити, що порівнюються не зображення, а біохеши, зроблені на основі кодів райдужної оболонки. Такими чином, надійність системи забезпечується завдяки застосуванню фільтру до нормалізованого зображення, тому важливе місце у розробці системи біометричної ідентифікації по райдужці займає вдосконалення способу генерації коду райдужної оболонки.

Збереження коду райдужної оболонки у базі даних не є безпечним, оскільки у разі викрадення коду, людина не зможе згенерувати інший на основі тієї ж самої райдужної оболонки. У зв'язку з цим до схеми біометричної ідентифікації було додано застосування біометричного хешування до згенерованого коду райдужної оболонки. Зазвичай біохеш поєднує набір випадкових векторів, характерних для користувача, з біометричними ознаками. Було досліджено, що деякі алгоритми біохешу мають надзвичайно низькі показники помилок порівняно з єдиним біометричним підходом, коли використовується справжній маркер. Таким чином, у випадку викрадення біометричного коду, може бути згенеровано новий на основі тих же біометричних даних, але із застосуванням іншого кодування або вектору. Також, розміри біохешу та звичайного коду, згенерованого з біометричного параметри, відрізняються. Біохеш є значно меншим, що може позитивно вплинути на швидкість роботи програми при порівнянні та при збереженні їх у базі.

В даній роботі досліджується декілька алгоритмів біохешу, а також порівнюється їх ефективність один з одним та їх показники помилок. Зазначені вище алгоритми досліджуються в умовах генерації коду райдужної оболонки за єдиним алгоритмом, етапи якого наведені на рис. 3.6. У наступному розділі буде детально розглянуто процес обробки зображення ока, вилучення важливих для розпізнавання характеристик райдужної оболонки ока та процес генерації біометричного коду.

4 ДОСЛІДЖЕННЯ АЛГОРИТМУ РОЗПІЗНАВАННЯ ПО РАЙДУЖНІЙ ОБОЛОНЦІ

Враховуючи швидкий розвиток технологій для отримання зображення райдужної оболонки, очікується, що розпізнавання по райдужній оболонці набуде більшої популярності та стане фундаментальним компонентом для забезпечення доступу у багатьох сферах життєдіяльності людини. Однак продуктивність систем розпізнавання райдужної оболонки в не обмежених умовах все ще далеко не ідеальна. Локалізація райдужної оболонки, нелінійна нормалізація, сегментація оклюзії, виявлення живості, масштабна ідентифікація та багато інших проблем дослідження потребують подальшого дослідження. Успіх досліджень таких питань часто залежить від наявності ретельно розроблених баз зображень райдужної оболонки достатнього розміру.

В даному розділі розглядається формування біометричного шаблону райдужної оболонки ока [20]. Даний етап поділяється на наступні складові:

- виділення зовнішніх та внутрішніх кордонів райдужної оболонки;
- нормалізація зображення;
- виділення найбільш інформативної частини зображення;
- накладання фільтру для виділення важливих характеристик;
- генерація коду райдужної оболонки ока.

Далі буде детально описана кожна із зазначених складових та її програмна реалізація на мові програмування Java. Програма може порівнювати між собою біохеши райдужних оболонок отриманих з двох зображень та біохеш, згенерований з щойно отриманого зображення, із біохешем, який знаходиться у базі. Схеми обох варіантів реалізацій наведені на рис. 4.1 та рис. 4.2 відповідно.

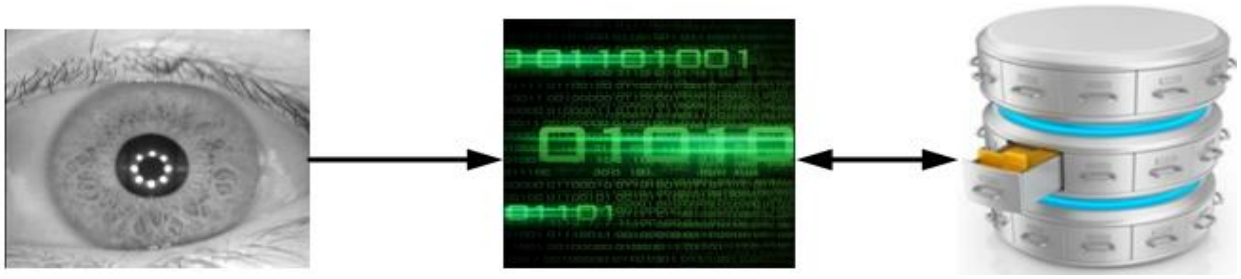

Рисунок 4.1 – Занесення та порівняння біометричного шаблону з шаблонами з бази

Рисунок 4.2 – Порівняння біометричних шаблонів райдужки з двох зображень очей

Для дослідження ефективності програмної реалізації розпізнавання по райдужній оболонці ока біли обрані зображення з бази CASIA-Iris-Interval. Зображення були зроблені за допомогою спеціальної камери з круговим світлодіодним масивом ближнього інфрачервоного спектру з відповідним світловим потоком для зображення райдужної оболонки. Завдяки такому дизайну, ця камера райдужної оболонки може знімати дуже чіткі зображення райдужки. Таким чином, зображення з цієї бази добре підходять для вивчення детальних текстурних особливостей зображень райдужної оболонки. Роздільна здатність таких зображень становить 320 × 280 пікселів. Приклад одного з них наведений на рис. 4.3.

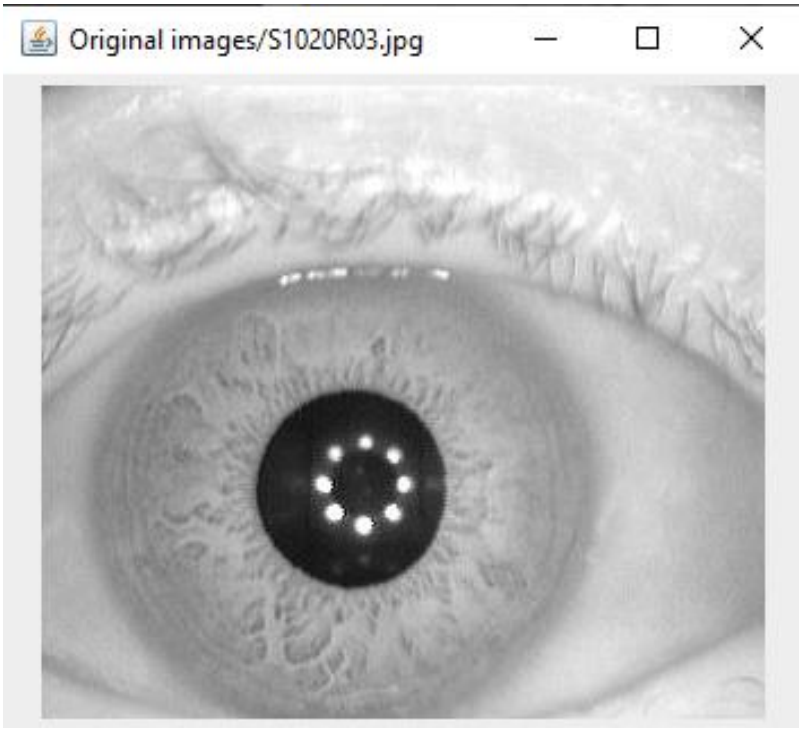

Рисунок 4.3 – Оригінальне зображення

Ідентифікація користувача відбувається на основі таких характеристик райдужної оболонки ока, як борозни, веснянки, кріпти та пігментні плями. Інформація про колір очей не є важливою для розпізнавання. Таким чином, усі зображення мають бути надані у градаціях сірого. Зазначена вище програма була протестована на десяти зображеннях з бази CASIA-Iris-Interval.

Локалізація райдужної оболонки виявляє внутрішні та зовнішні межі райдужної оболонки. І внутрішню, і зовнішню межі райдужні оболонки можна приблизно моделювати як кола. Центр райдужної оболонки не обов'язково має співпадати з центром зіниці. Локалізація райдужної оболонки важлива, оскільки потрібна правильна область райдужки для створення шаблонів для точного узгодження [20].

Оскільки фотографія ока зазвичай має багато чітких контурів, їх слід «розмити» аби чітко виділити коло зіниці та коло, що є межею між райдужкою та склерою. Завдяки такому «розмиттю» лінії контурів будуть значно збільшені, що допоможе виділити більш великі об’єкти на зображенні. Для цього використовується фільтр Гауса. Він представляє собою фільтр імпульсна характеристика якого є функцією Гауса, наведена у формулі:

$$g(x) = a \cdot e^{-\frac{(x-b)^2}{2 \cdot c^2}}, \qquad (4.1)$$

де a – дійсне число, яке є висотою піку кривої;

b – дійсне число, яке є позицією центру;

c – дійсне число, яке контролює ширину «дзвону»;

e – число Ейлера.

Гаусові фільтри мають властивості не мати перекриття на вхід крокової функції, мінімізуючи час підйому та падіння. Така поведінка тісно пов'язана з тим, що фільтр Гауса має мінімально можливу групову затримку. Зазвичай такий фільтр використовується з метою зниження рівня шуму на зображенні [20]. Результат накладання фільтру Гауса на фотографію ока, наведену на рис. 4.3, зображений на рис. 4.4.

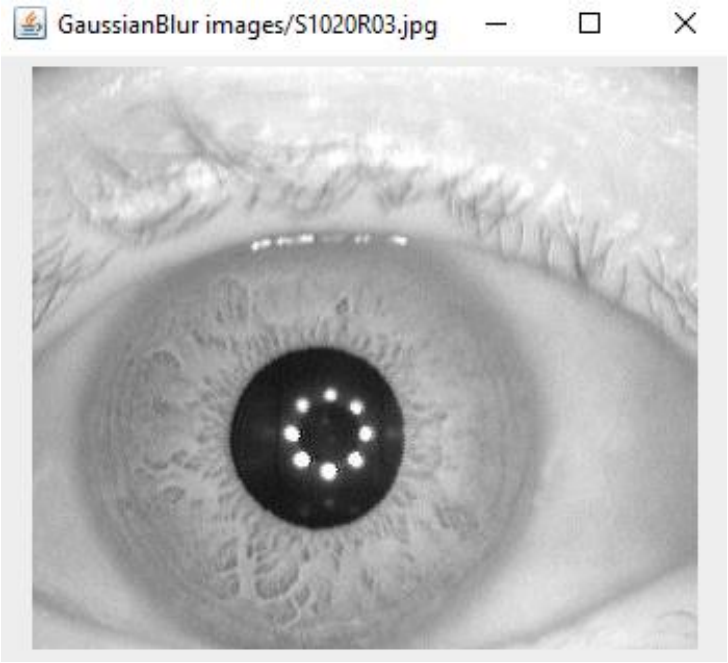

Рисунок 4.4 – Приклад зображення після застосування фільтра Гауса

Для виділення кола зіниці використовується детектор Кенні. Детектор Кенні представляє собою оператор виявлення країв, який використовує багатоступеневий алгоритм для виявлення широкого діапазону країв у зображеннях. Він був розроблений Джоном Ф. Канні в 1986 році. Алгоритм дії детектора Кенні складається з наступних етапів:

- застосування фільтру Гауса, щоб згладити зображення та зняти шум;
- знаходження градієнту інтенсивності зображення;
- застосування подвійного порог для визначення потенційних ребер;
- відстеження краю за допомогою гістерезису;
- придушення усіх інших ребер, які слабкі та не з'єднані із сильними краями.

Алгоритм Кенні містить декілька параметрів, які можна регулювати. Вони можуть впливати на час обчислення та ефективність алгоритму. До них відносять розмір фільтру Гауса та порогові значення.

Серед розроблених до цього часу методів виявлення ребер алгоритм Кенні є одним із найбільш точним серед визначених методів і забезпечує хороше і надійне виявлення. Завдяки своїй оптимальності він відповідає багатьом критеріям виявлення ребер та має простий процес впровадження. На даний час він є одним із найпопулярніших алгоритмів виявлення країв. Результат дії детектору Кенні наведений на рис. 4.5.

Рисунок 4.5 – Зображення після застосування детектора Кенні

Для визначення кругів використовується перетворення Хафа. Перетворення Хаффа є техніка вилучення особливостей, яка використовується в аналізі зображення, комп'ютерному зорі та цифровій обробці зображень. Мета перетворення є виявлення недосконалих екземпляри предметів у межах певного класу фігур процедурою голосування. Класичне перетворення Хоффа найчастіше використовується для виявлення регулярних кривих, таких як лінії, кола та еліпси. Після застосування перетворення Хафа до зображення, наведеного на рис. 4.5, було визначено координати центру та радіус окружності зіниці [20]. Результати визначення наведені на рис. 4.6.

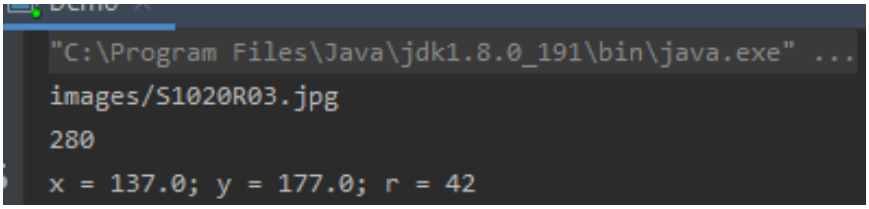

Рисунок 4.6 – Радіуси та центр окружності після перетворення Хафа

Згідно із дослідженнями діаметр райдужної оболонки зазвичай має розмір від десяти до тринадцяти міліметрів. Було визначено, що для досліджуваних

зображень ця відстань відповідає ста пікселям. На рис. 4.7 виділено зовнішні та внутрішні межі райдужної оболонки.

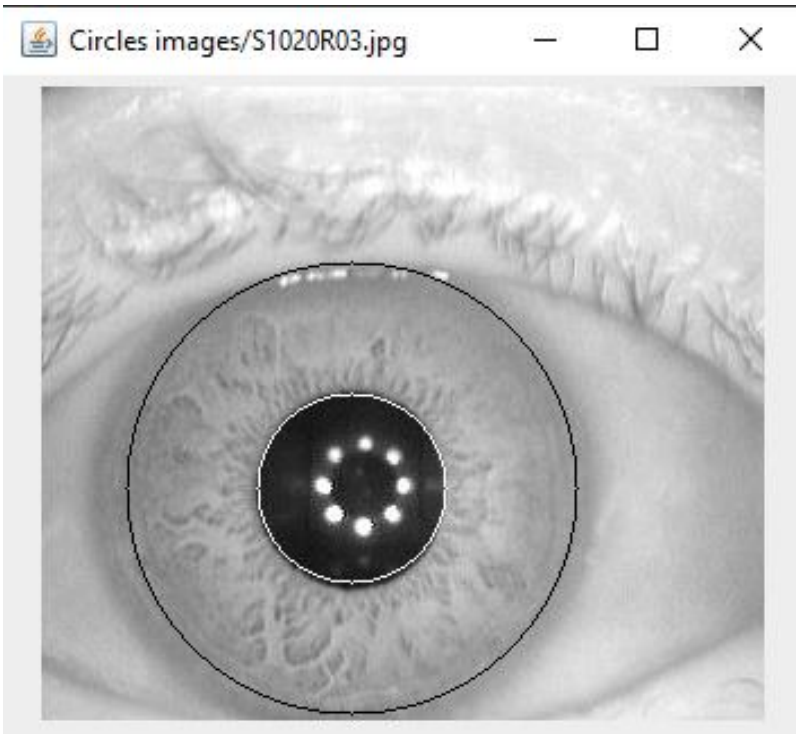

Рисунок 4.7 – Виділення зовнішнього та внутрішнього контурів райдужки

Для виділення меж райдужної оболонки виконувалися умови, наведені у зазначених нижче формулах:

$$(x - a_p)^2 + (y - b_p)^2 > r_p^2, \tag{4.2}$$

де x – координата пікселя на осі абсцис;

y – координата пікселя на осі ординат;

a_p – координата пікселя центру зіниці на осі абсцис;

b_p – координата пікселя центру зіниці на осі ординат;

r_p – радіус зіниці.

$$(x - a_i)^2 + (y - b_i)^2 < r_i^2, \tag{4.3}$$

де x – координата пікселя на осі абсцис;

y – координата пікселя на осі ординат;

a_i – координата пікселя центру райдужки на осі абсцис;

b_i – координата пікселя центру райдужки на осі ординат;

r_i – радіус райдужки.

Наступним етапом обробки зображення є його нормалізація. Етап нормалізації використовує геометричну схему нормалізації для перетворення виділеного зображення райдужної оболонки з декартової системи координат у полярну. Результатом цього є прямокутне зображення, яке використовується для подальшої обробки [20]. Нормалізація зображення має наступні переваги.

1) Вона пояснює зміни в розмірах зіниці через зміни зовнішньої освітленості, які можуть впливати на розмір райдужної оболонки.

2) Вона забезпечує, що райдужки різних осіб не відображаються на загальній області зображення, незважаючи на варіації розмірів зіниці.

3) Вона дозволяє реєстрацію райдужної оболонки під час відповідного етапу за допомогою простої операції перекладу, яка може враховувати обертання очей та голови в площині.

Знаходження x та y у полярній системі координат відбувається за наступними формулами:

$$x = r \cdot \left(x_0 + R \cdot \cos(\alpha)\right), \tag{4.4}$$

$$y = r \cdot \left(y_0 + R \cdot \sin(\alpha)\right), \tag{4.5}$$

де x_0 та y_0 – координати центру райдужної оболонки;

R – радіус райдужної оболонки;

r – розраховується за формулою (4.6);

α – кутова координата, що розраховується за формулою (4.7).

$$r = \sum_{j=0}^{n} \frac{j}{n}, \tag{4.6}$$

де n – висота нормалізованого зображення;

j – значення координати ординати у пікселях нормалізованого зображення.

$$\alpha = \sum_{i=0}^{\theta} \frac{2 \cdot \pi \cdot i}{\theta}, \tag{4.7}$$

де θ – ширина нормалізованого зображення;

і – значення координати абсциси у пікселях нормалізованого зображення.

Результат перетворення досліджуваного зображення райдужної оболонки в полярну систему координат наведено на рис. 4.8.

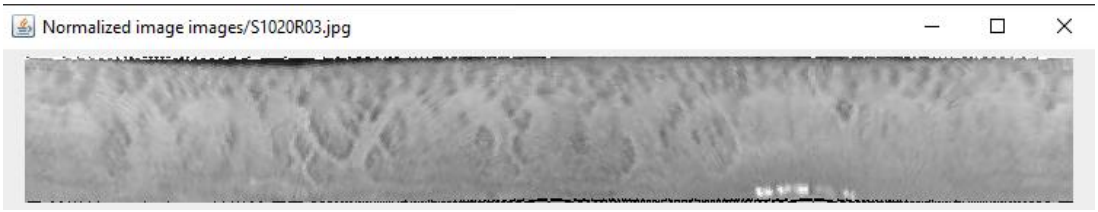

Рисунок 4.8 – Зображення після нормалізації

Вії, верхня та нижня повіки не несуть важливої інформації, тому для подальшого накладання фільтру для виділення важливих характеристик слід вибрати ділянку, яка містить лише рисунок райдужної оболонки. На рис. 4.9 наведене зображення із урахуванням зазначеної вище вимоги.

Рисунок 4.9 – Досліджувана частина райдужки

Як було зазначено у третьому розділі механізмом, який відповідає за різноманітність та складність коду райдужної оболонки, є фільтр, який «підсилює» характеристики райдужної оболонки ока людини. Одним із найефективніших таких механізмів є фільтр Габора.

Фільтр Габора був названий на честь Денніса Габора. Він представляє собою лінійний фільтр, який використовується для аналізу текстури. Фільтр Габора аналізує, чи є якийсь певний вміст частоти в зображенні в конкретних напрямках в локалізованій області навколо точки або області аналізу. Деякі науковці стверджують, що фільтр Габора подібний до візуальної системи людини. Вони були визнані особливо доречними для представлення текстури. В основі

фільтру Габора знаходиться функція ядра Гауса, модульована синусоїдальною плоскою хвилею. Це відображено у наступній формулі:

$$g(x, y, \lambda, \theta, \sigma, \psi, \gamma) = e^{-\frac{x'^2 + y^2 \cdot y'^2}{2 \cdot \sigma^2}} \cdot \cos(2 \cdot \pi \cdot \frac{x'}{\lambda} + \psi), \quad (4.8)$$

де λ – довжина хвилі множника косинуса;

ψ – зсув фаз в градусах;

γ – коефіцієнт стиснення, що характеризує еліптичність функції Габора;

σ – параметр, від якого залежать розміри ядра;

x' – визначається за формулою (4.9);

y' – визначається за формулою (4.10).

$$x' = x \cdot \cos\theta + y \cdot \sin\theta, \quad (4.9)$$

$$y' = -x \cdot \sin\theta + y \cdot \cos\theta, \quad (4.10)$$

де x – рядок у матриці ядра;

y – стовпець у матриці ядра;

θ – орієнтація нормалі паралельних смуг функції Габора в градусах.

Результат накладання фільтру Габора наведений на рис. 4.10.

Рисунок 4.11 – Зображення пісня застосування фільтру Габора

Наступним етапом біометричної автентифікації по райдужці є генерація коду райдужної оболонки ока. У ході генерації коду аналізується значення кожного пікселя, і, в залежності від цього, визначається значення у коді: 0 або1 [20]. На цьому етап формування біометричного шаблону закінчується. У наступному розділі розглядаються методи захисту біометричного шаблону та описується їх програмна реалізація.

5 ДОСЛІДЖЕННЯ АЛГОРИТМІВ БІОХЕШУ

Наприкінці етапу формування біометричного шаблону було отримано код райдужної оболонки, який складався із 17600 біт. Після цього його було конвертовано до цілочисельного типу. У зв’язку з цим кількість елементів зменшилась до 560. Після цього етапу можливе збереження згенерованого коду райдужної оболонки до бази, але це не є безпечним. Згідно з цим для захисту біометричного коду було використано засоби скасовуваної біометрії. Як було зазначено у попередніх розділах, скасовувана біометрія забезпечує спосіб автентифікації навіть тоді, коли біометричний шаблон був викрадений. Вона представляє механізм захисту шаблонів, де оригінальний біометричний зразок спотворюється навмисно для реєстрації в системі ідентифікації. Коли застосовується скасовувана біометрична схема, замість початкового біометричного шаблону зберігається деформована версія шаблону [21]. У випадку звичайної біометричної системи більшість людей виявляють небажання надавати свої біометричні ознаки, оскільки вони стурбовані своєю приватністю. Скасовувана біометрія вирішує такі проблеми, пов’язані з конфіденційністю, оскільки заважає системі зберігати оригінальні біометричні ознаки користувача. Методи захисту біометричного шаблону можна поділити на зворотні та незворотні перетворення. До перших методів можна віднести такі методи, як BIN-SALT та GREY-SALT, що представляють собою біометричне засолювання, до других – BIN-COMBO та GREY-COMBO.

У біометричному засолюванні незалежні допоміжні дані, такі як визначений користувачем пароль або маркер, поєднуються з біометричними даними для надання спотвореної версії біометричного шаблону. Приклад схеми засолювання коду райдужної оболонки був запропонований С. Чонгом. Запропоновано метод засолювання, який можна застосувати як до звичайних значень, так і до двійкових моделей райдужної оболонки, отримав назви GREY-SALT і BIN-SALT відповідно. У GREY-SALT до шаблону райдужки було додано випадково згенерований вектор або помножено на нього. У BIN-SALT для коду райдужної оболонки ока та випадково згенерованого бінарного ключа була застосована операція XOR. І для GREY-SALT, і для BIN-SALT інформація про шаблон райдужної оболонки ока приховується за допомогою допоміжних даних. У

досліджуваній програмі біометричне засолювання коду райдужної оболонки було реалізовано шляхом BIN-SALT методу. До коду райдужної оболонки ока було згенеровано бінарний ключ за допомогою генератору випадкових чисел. Довжина ключа дорівнювала довжині коду райдужки зазначеного вище. Бінарний ключ був згенерований лише один раз і є спільним для всіх біометричних шаблонів. Програма передбачає генерацію нового ключа у разі викрадення біохешу одного з користувачів. Варто зазначити, що існують інші схеми біометричного засолювання. На відміну від описаного варіанту у якості ключа також може використовуватися модифікований пароль користувача. Така схема може виконуватися у системах двох факторної автентифікації. Недоліком усіх варіацій методів біометричного засолювання є те, що у разі отримання бінарного ключа або секретного вектору зловмисник зможе легко відновити код райдужної оболонки користувача.

Недоліку біометричного засолювання позбавлені методи незворотного перетворення. Незворотна трансформація є концептуально привабливою для схем захисту шаблонів. У незворотному перетворенні для трансформації шаблону райдужної оболонки використовується функція одностороннього перетворення. Таким чином, у разі викрадення неможливо відновити оригінальний код райдужної оболонки ока.

Для незворотного перетворення коду райдужної оболонки ока було запропоновано два методи: GREY-COMBO та BIN-COMBO. У GREY-COMBO переставляються елементи коду райдужки за допомогою випадкової комбінації, після чого виконуються операції додавання, або множення для двох випадково вибраних рядків. У BIN-COMBO та сама процедура виконується для коду райдужної оболонки ока, але з операцією XOR або XNOR. Таким чином, вихідні дані коду райдужки були спотворені, змінені операціями додавання або множення між двома випадково обраними рядками. Таким чином виконується критерій незворотності [22].

У досліджуваній програмі було реалізовано метод незворотного перетворення BIN-COMBO. Цей метод бува реалізований наступним чином. За допомогою генератора випадкових чисел було створено послідовність, кількість елементів в якій дорівнювала кількості рядків в оригінальному коді райдужної оболонки, тобто 40. Кожне значення згенерованої послідовності визначало кількість елементів, на які слід обернути елементи рядка. Після цього за

допомогою генератору випадкових чисел було обрано одне просте число. Усі рядки, порядкові номера яких ділилися на це число були з’єднані з наступними за ними рядками за допомогою операції XOR. Недоліком даного методу є те, що у зв’язку із скороченням коду райдужної оболонки після модифікацій ефективність системи розпізнавання погіршилася.

Зазначені вище методи захисту біометричного шаблону не є єдиними. Ще одним методом для змінення коду райдужної оболонки є Min-Hashing. Min-Hashing спочатку використовувався в пошуковій системі для виявлення дублікатів веб-сторінок та видалення їх з результатів пошуку, а також у великих масштабних проблемах кластеризації. У процесі Min-Hashing записується індекс першої зустрічі біту, який дорівнює 1, для ряду двійкових векторів, рядки яких були перемішані. Нехай A і B - два індексні вектори, породжені з двійкового вектора, h - хеш-функція, яка рахує хеші для елементів цих множин. Далі, слід визначити функцію hmin (S), яка обчислює функцію h для всіх членів будь-якого безлічі S і повертає найменше її значення. Після цього необхідно обчислити hmin (A) і hmin (B). Порівняння значень hmin (A) і hmin (B) нічого не дасть, оскільки ймовірність того, що вони будуть стовідсотково рівні дуже низька. Вирішити цю проблему можна за допомогою коефіцієнту подібності Жакарда. Коефіцієнт подібності Жакарда, був придуманий Полом Жакардом у 1902 році. Коефіцієнт вимірює подібність між множинами. Він визначається як розмір перетину, поділений на величину з'єднання двох множин і наведений у наступній формулі:

$$J(A,B) = \frac{|A \cap B|}{|A \cup B|} = \frac{|A \cap B|}{|A| + |B| - |A \cap B|}, \tag{5.1}$$

де A – перша множина;

B – друга множина.

За описаним алгоритмом Min-Hashing була зроблена програмна реалізація третього зазначеного методу захисту біометричних шаблонів. Для знаходження коефіцієнт подібності Жакарда у програмній реалізації була запрограмована наступна формула, яка відображає формулу 5.1:

$$J(a,b) = \frac{c}{a + b - c}, \tag{5.2}$$

де a – кількість елементів у першому біохеші;

b – кількість елементів у другому біохеші;

c – кількість елементів, яка знаходиться в обох біохешах.

Коефіцієнт подібності Жакарда також може використовуватися для порівняння біохешей, які були згенеровані за допомогою перших двох методів.

Варто зазначити, що коефіцієнт Жакарда не є єдиною мірою знайдення подібності хешованих кодів райдужної оболонки ока. Знайти міру подібності можна також за допомогою відстані Хемінга [20]. Вона представляє собою кількість бітових позицій, в яких два біта різні, і розраховується за наступною формулою:

$$d_{ij} = \sum_{k=1}^{p} \left| x_{ik} - x_{jk} \right|, \tag{5.3}$$

де d_{ij} – відстань Хемінга для послідовностей i та j;

p – довжина послідовностей;

k – номер елементу;

x – елемент.

Далі знаходиться відсоток подібності двох біохешей, оскільки кількість елементів є достатньо великою і може змінюватися при зміні розміру частини райдужної оболонки ока, яка використовується для аналізу.

Після результатів порівняння біохешей одним із зазначених методів програма аналізує чи є достатнім результат подібності, щоб допустити користувача далі. Даний поріг для обох методів був визначений за допомогою експериментальних досліджень. У наступному розділі порівнюються усі зазначені методи біометричного захисту шаблону у використанні із різними методами знаходження подібності, а також визначається ймовірність кожного до помилок у відхиленні доступу зареєстрованому користувачу чи його наданні зловмиснику.

6 ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ МЕТОДІВ ЗАХИСТУ БІОМЕТРИЧНОГО ШАБЛОНУ

Описані у попередньому розділі методи захисту біометричного шаблону райдужної оболонки ока були протестовані на десяти зображеннях з бази CASIA-Iris-Interval . Ефективність та якість роботи програмної реалізації зазначених вище алгоритмів була перевірена рядом наступних досліджень. Також було оцінено на скільки використанні методів захисту біометричних шаблонів впливає на ефективність розпізнавання.

Для усіх методів захисту біометричного шаблону та для незахищеного коду райдужки було обране порогове значення для відстані Хемінга або для коефіцієнту подібності Жакарда, порівняння з яким визначає надавати доступ користувачу чи відхиляти його. Даний параметр був визначений експериментальним шляхом. Для цього було підраховано значення відстані Хемінга або коефіцієнту подібності Жакарда, порівнюючи кожний біометричний шаблон з кожним. Для незахищених кодів райдужної оболонки зазначення відстані Хемінга у відсотках наведені у таблиці 6.1.

Таблиця 6.1 – Значення відстані Хемінга у відсотках між незахищеними кодами райдужної оболонки

Номер зображення	1	2	3	4	5	6	7	8	9	10
01	100	72	79	59	67	70	75	75	70	69
02	-	100	71	58	65	68	71	69	65	65
03	-	-	100	60	70	70	75	74	71	71
04	-	-	-	100	57	57	59	60	58	57
05	-	-	-	-	100	63	66	66	62	62
06	-	-	-	-	-	100	69	69	65	64
07	-	-	-	-	-	-	100	71	68	68
08	-	-	-	-	-	-	-	100	68	67
09	-	-	-	-	-	-	-	-	100	64
10	-	-	-	-	-	-	-	-	-	100

Згідно з таблицею 6.1 найменше значення відстані Хемінга у відсотках становить 57, а найбільше - 79 між першим та третім кодами райдужних

оболонок. У зв’язку з цим порогове значення відстані Хемінга для незахищеного шаблону райдужної оболонки ока було обрано рівним 80 відсоткам.

Аналогічним чином було встановлено порогові значення відстані Хемінга у разі використання методів захисту біометричного шаблону, описані у попередньому розділі, а саме таких, як BIN-SALT та BIN-COMBO. Біометричне засолювання лише змінює біти, довжина біометричного шаблону залишається рівною довжині незахищеного коду райдужної оболонки.

Результати порівняння біометричних шаблонів зображень райдужних оболонок, які були захищені за допомогою біометричного засолювання, наведені у таблиці 6.2.

Таблиця 6.2 – Значення відстані Хемінга у відсотках між захищеними кодами райдужок за допомогою біометричного засолювання

Номер зображення	1	2	3	4	5	6	7	8	9	10
01	100	73	77	60	67	71	75	75	71	70
02	-	100	71	58	65	68	72	69	66	66
03	-	-	100	60	70	71	75	75	71	71
04	-	-	-	100	58	58	59	60	59	58
05	-	-	-	-	100	63	67	66	63	63
06	-	-	-	-	-	100	70	70	66	64
07	-	-	-	-	-	-	100	72	69	68
08	-	-	-	-	-	-	-	100	68	68
09	-	-	-	-	-	-	-	-	100	64
10	-	-	-	-	-	-	-	-	-	100

Виходячи з даних таблиці 6.2 можна виділити найменшу та найбільшу відстані Хемінга. Після використання BIN-SALT методу для захисту біометричного шаблона найменше значення відстані Хемінга збільшилося і стало дорівнювати 58 відсоткам, а найбільше значення зменшилося і почало дорівнювати 78 відсоткам. Таким чином, порогове значення відстані Хемінга у разі використання біометричного засолювання було обране 78.

Результати порівнянь кодів райдужних оболонок після застосування до них незворотної трансформації із використанням методу BIN-COMBO за допомогою відстані Хемінга наведені у таблиці 6.3.

Таблиця 6.3 – Значення відстані Хемінга у відсотках між захищеними кодами райдужок за допомогою методу BIN-COMBO

Номер зображення	1	2	3	4	5	6	7	8	9	10
01	100	71	76	60	67	70	73	73	70	69
02	-	100	70	58	65	68	70	68	65	65
03	-	-	100	60	70	70	74	73	70	70
04	-	-	-	100	58	58	60	59	59	58
05	-	-	-	-	100	63	66	65	62	62
06	-	-	-	-	-	100	69	68	65	64
07	-	-	-	-	-	-	100	70	68	67
08	-	-	-	-	-	-	-	100	67	66
09	-	-	-	-	-	-	-	-	100	64
10	-	-	-	-	-	-	-	-	-	100

Із наведених у таблиці 6.3 даних можна виділити найменшу та найбільшу різниці у відстані Хемінга для досліджуваних шаблонів райдужних оболонок. Найменше значення для захищеного коду райдужки за допомогою методу BIN-COMBO становить 58 відсотків, а найбільше - 76 відсотків. У зв’язку цим пороговим значенням було обрано 77.

Для порівняння біохешів у Min-Hashing використовується коефіцієнт подібності Жакарда. Результати порівнянь кодів райдужних оболонок після застосування Min-Hashing для десяти зображень наведені у таблиці 6.4.

Таблиця 6.4 – Значення коефіцієнту подібності Жакарда після застосування Min-Hashing до кодів райдужки

Номер зобр.	1	2	3	4	5	6	7	8	9	10
01	1	0.095	0.1359	0.0504	0.0936	0.0962	0.1210	0.1188	0.0790	0.0907
02	-	1	0.1122	0.0505	0.0883	0.0827	0.1003	0.1068	0.0759	0.0910
03	-	-	1	0.0507	0.1176	0.1105	0.1329	0.1205	0.0928	0.1197
04	-	-	-	1	0.0390	0.0424	0.0531	0.0511	0.0302	0.0516
05	-	-	-	-	1	0.0841	0.0873	0.1019	0.0644	0.0910
06	-	-	-	-	-	1	0.0884	0.0954	0.0725	0.0869
07	-	-	-	-	-	-	1	0.1074	0.0824	0.0939
08	-	-	-	-	-	-	-	1	0.0847	0.1008
09	-	-	-	-	-	-	-	-	1	0.0739
10	-	-	-	-	-	-	-	-	-	1

Виходячи з даних таблиці 6.4 можна виділити найменше та найбільше значення коефіцієнту подібності Жакарда після застосування Min-Hashing до кодів райдужної оболонки ока. Найменше значення становить 0.0302 для біохешей зроблених для четвертого та дев’ятого зображень. Найбільше значення становить 0.1359 для біохешей зроблених для першого та третього зображень. У зв’язку з цим порогове значення коефіцієнту Жакарда для Min-Hashing було обране 0.14.

Для дослідження ефективності та стійкості описаних вище методів захисту біометричних шаблонів у поєднанні з однаковими методами обробки фотографії, зазначеними у другому розділі до зображень було застосовано шум Перліна. В основі цього шуму лежить функція, що має псевдовипадковий вигляд, але всі її візуальні деталі мають однаковий розмір. Ця властивість дозволяє легко контролювати накладання шуму. В математичні вирази можна вставити кілька масштабних копій шуму Перліна, щоб створити велику різноманітність процедурних текстур. Для накладання шуму Перліна на зображення райдужної оболонки ока було розроблено програму на мові програмування Java. Дана програма передбачає накладання шуму на зображення за наданим відсотком. Приклад зображення після накладання шуму Перліна наведений на рис. 6.1.

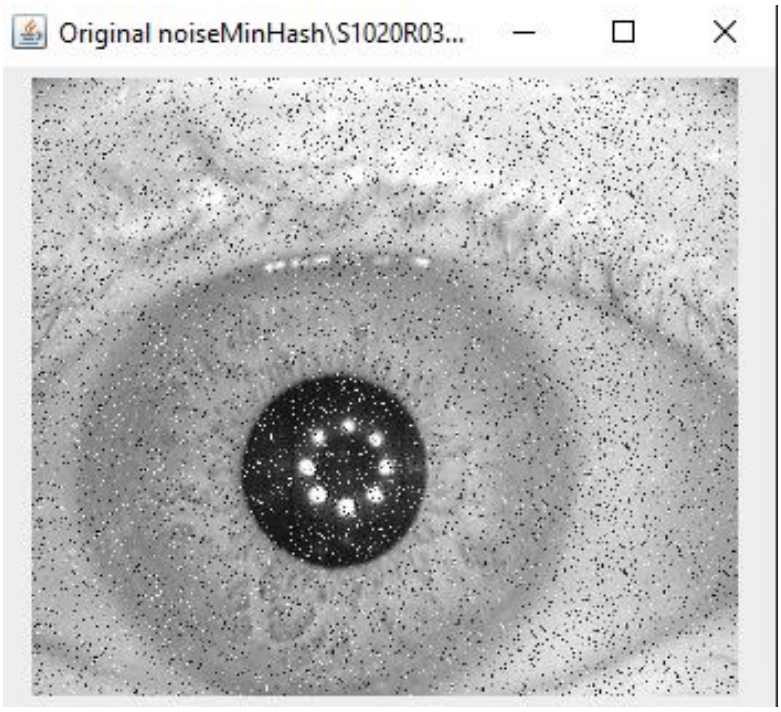

Рисунок 6.1 – Зображення ока після накладання шуму

Зазначений шум був застосований до кожної фотографії ока у різних відсотках. Після чого експериментальним шляхом був визначений відсоток шуму, який відповідає пороговому значенню відстані Хемінга або коефіцієнту подібності Жакарда для кожного з досліджуваних методів захисту біометричного шаблону та оригінального коду райдужної оболонки. Результати досліджень порогового значення шуму для зазначених вище варіантів наведені у таблиці 6.5.

Таблиця 6.5 – Порогові відсотки шуму для кожного з досліджуваних методів захисту біометричного шаблону та незахищеного коду райдужної оболонки

Номер зображення	Пороговий відсоток шуму при незахищеному коді райдужки	Пороговий відсоток шуму при використанні BIN-SALT	Пороговий відсоток шуму при використанні BIN-COMBO	Пороговий відсоток шуму при використанні Min-Hashing
01	1.5	2.8	2.15	0.97
02	1.05	1.1	1.10	3.7
03	0.21	0.85	0.80	0.21
04	0.51	0.52	0.51	0.51
05	0.18	0.16	0.18	0.15
06	0.57	0.55	0.57	0.49
07	0.15	0.17	0.18	0.15
08	0.62	0.62	0.64	0.61
09	0.19	0.19	0.19	0.17
10	0.52	0.52	0.52	0.52

Таким чином відсоток шуму для кожного з зображень у першій колонці відповідає пороговому значенню відстані Хемінга, яка дорівнює 80 відсоткам, у другій колонці – 78 відсотка, у третій – 77 відсотка, у четвертій – коефіцієнту Жакарда, який дорівнює 0,14.

Візуально простежити відмінність та подібність між відсотками шуму для різних методів захисту біометричного шаблону та незахищеного коду райдужної оболонки можна на гістограмі, зображеній на рис. 6.2.

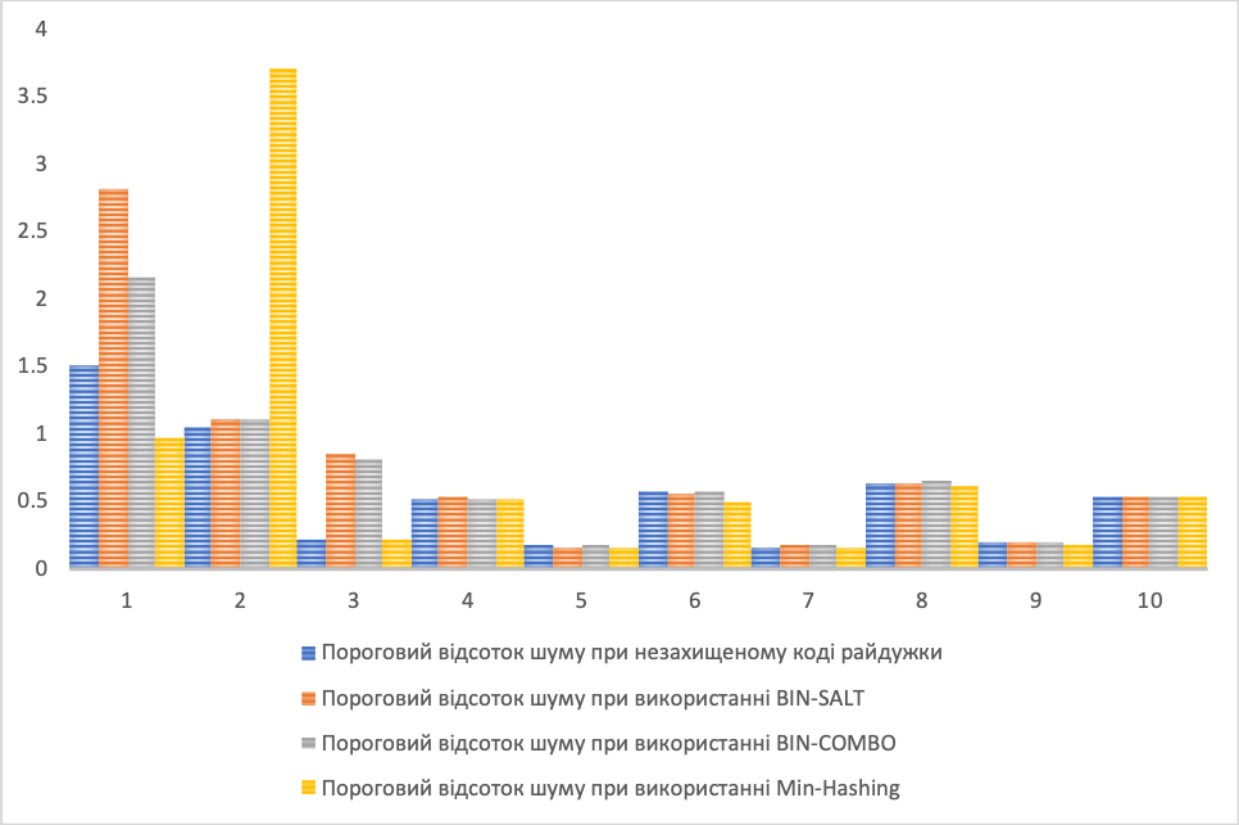

Рисунок 6.2 – Гістограма значень порогів шуму для різних методів захисту біометричного шаблону та незахищеного коду райдужної оболонки ока

Виходячи з результатів, наведених на рис. 6.2, можна зробити висновок, що поріг шуму при незахищеному коді райдужної оболонки є найнижчим серед усіх інших майже для всіх фотографій, в той час, як показники при використанні Min-Hashing є відносно нестабільними.

Для аналізу рівня завад, що був внесений пороговим значенням шуму, було визначено значення «сигнал/шум» (signal to noise ratio SNR) для кожного зображення при використанні різних методів захисту біометричного шаблону та їх відсутності. Також коефіцієнт «сигнал/шум» використовується для визначення характеристики якості зображення [23]. Чутливість системи цифрового зображень зазвичай описується з точки зору рівня сигналу, який дає пороговий рівень SNR. Коефіцієнт «сигнал/шум» розраховується за наступною формулою:

$$\mathrm{SNR} = \frac{\sum_{x,y} (C_{x,y})^2}{\sum_{x,y} (C_{x,y} - S_{x,y})^2}, \qquad (6.1)$$

де x – номер рядка у зображенні;

y – номер стовпця у зображенні;

$C_{x,y}$ – значення пікселя оригінального зображення;

$S_{x,y}$ – значення пікселя зображення, на яке був накладений шум.

Також для кількісної оцінки величини спотворень оригінального зображення було підраховане середньоквадратичне відхилення (mean square error – MSE), що представляє відносний показник розсіювання значень [23]. MSE було розраховано за формулою:

$$MSE = \frac{1}{XY} \cdot \sum_{x,y} (C_{x,y} - S_{x,y})^2, \quad (5.2)$$

де X – кількість рядків пікселів;

Y – кількість стовпців пікселів;

x – номер рядка у зображенні;

y – номер стовпця у зображенні;

$C_{x,y}$ – значення пікселя оригінального зображення;

$S_{x,y}$ – значення пікселя зображення, на яке був накладений шум.

Для розрахунків показників SNR та MSE була розроблена окрема програма. Результати значень SNR та MSE між оригінальними та зашумленими фотографіями, які відповідають порогу шуму для зображень при формуванні незахищеного коду райдужної оболонки, наведеному у таблиці 6.5, занесені у таблицю 6.6.

Таблиця 6.6 – Значення SNR та MSE, які відповідають порогу шуму для зображень при формуванні незахищеного коду райдужної оболонки

Номер зображення	Шум у відсотках	SNR	MSE
1	2	3	4
01	1.5	415.7062	100.4801
02	1.05	544.4697	52.5139
03	0.21	3038.9852	9.3899
04	0.51	1718.9528	15.6271

Продовження таблиці 6.6

1	2	3	4
05	0.18	5146.7746	15.6271
06	0.57	1407.9690	23.8768
07	0.15	4859.4244	7.4757
08	0.62	1193.7185	38.5234
09	0.19	5462.3273	4.9288
10	0.52	1880.4193	14.1280

За формулами 5.1 та 5.2 були підраховані значення SNR та MSE між оригінальними та зашумленими фотографіями, які відповідають порогу шуму для зображень при використанні біометричного засолювання як методу захисту біометричного шаблону райдужної оболонки ока. Результати розрахунків наведені у таблиці 6.7.

Таблиця 6.7 – Значення SNR та MSE, які відповідають порогу шуму для зображень при використанні BIN-SALT для захисту біометричного шаблону

Номер зображення	Шум у відсотках	SNR	MSE
01	2.8	225.66	145.1030
02	1.1	544.47	52.5139
03	0.85	663.47	43.0102
04	0.52	1694.67	15.8510
05	0.16	5146.77	4.8185
06	0.55	1531.09	21.9568
07	0.17	4859.42	7.4757
08	0.62	1193.72	38.5234
09	0.19	5462.32	4.9289
10	0.52	1880.42	14.1279

Аналогічним чином були підраховані SNR та MSE між оригінальними та зашумленими фотографіями, рівень шуму яких становить порогове значення для методу біометричної автентифікації по райдужній оболонці ока із використанням BIN-COMBO, як методу захисту біометричного шаблону. Результати розрахунків занесені у таблицю 6.8.

Таблиця 6.8 – Значення SNR та MSE, які відповідають порогу шуму для зображень при використанні BIN-COMBO для захисту біометричного шаблону

Номер зображення	Шум у відсотках	SNR	MSE
01	2.15	296.49	140.8807
02	1.10	544.46	52.5139
03	0.80	747.67	38.1663
04	0.51	1435.20	18.7167
05	0.18	5146.77	4.8185
06	0.57	1407.97	23.8768
07	0.18	4859.42	7.4757
08	0.64	1115.17	41.2367
09	0.19	5462.32	4.9289
10	0.52	1880.42	14.1280

Використання Min-Hashing для захисту біометричного шаблону було протестованим аналогічним чином. Результати розрахунків SNR та MSE для цього випадку наведені у таблиці 6.9.

Таблиця 6.9 – Значення SNR та MSE, які відповідають порогу шуму для зображень при використанні Min-Hashing для захисту біометричного шаблону

Номер зображення	Шум у відсотках	SNR	MSE
01	0.97	605.91	68.9377
02	3.7	152.58	147.3877
03	0.21	3038.98	9.3899
04	0.51	1718.95	15.6271
05	0.15	5146.77	4.8185
06	0.49	1778.62	18.9011
07	0.15	4859.42	7.4757
08	0.61	1193.72	38.5234
09	0.17	5462.32	4.9289
10	0.52	1880.42	14.1279

Виходячи з результатів показників SNR, наведених у таблицях 6.6, 6.7, 6.8 та 6,9 можна відзначити, що вони мають достатньо великі значення. Із показників, зазначених у вище названих таблицях, можна побачити, що меншому відсотку шуму відповідають більші показники SNR, що є протилежним для показників MSE. Такі показники SNR характеризують низьку кількість завад на зашумлених зображеннях. Таким чином, можна зробити висновок, що усі описані алгоритми є стійкими, оскільки вони чутливі до накладання шуму. Для порівняння значень SNR та виділення найбільш чутливого до завад механізму показники співвідношення «сигнал/шум» для різних методів було зображені гістограмі, наведеній на рис. 6.3.

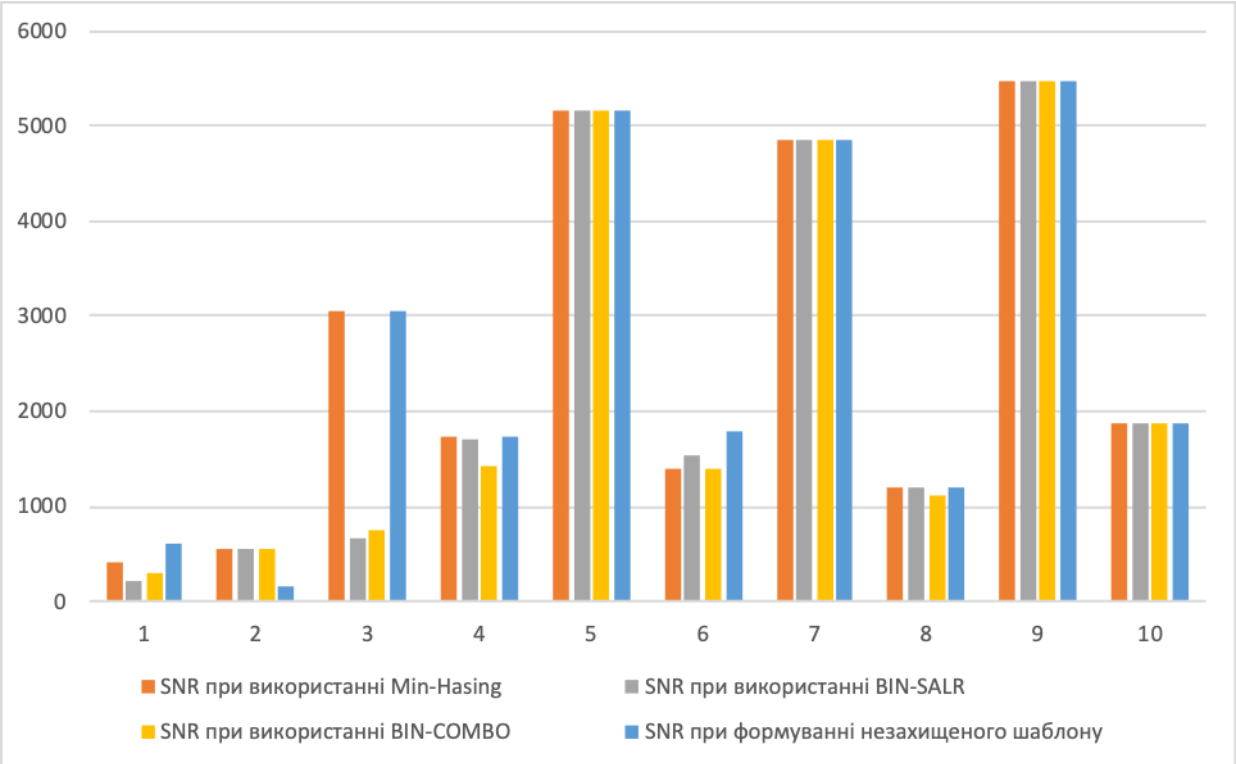

Рисунок 6.3 – Гістограма значень SNR між оригінальними та зашумленими зображеннями для різних методів захисту біометричного шаблону та незахищеного коду райдужної оболонки ока

Виходячи з даних наведених на рис. 6.3 можна зробити висновок, що найбільш чутливими до завад виявилися алгоритм розпізнавання по райдужці із використанням Min-Hashing та алгоритм без використання будь-яких методів захисту біометричного шаблону. Натомість найменш чутливим до завад є алгоритм із використанням BIN-COMBO для захисту коду райдужної оболонки.

Такі показники зумовлені тим, що під час генерації біохешу за цим методом, деяка кількість важливої інформації втрачається під час операції XOR, яка застосована для двох рядків.

Оскільки найближчі показники SNR до показників SNR незахищеного шаблону має алгоритм із використанням Min-Hashing, можна зробити висновок, що даний метод захисту біометричного шаблону менше за інші спотворює важливу інформацію і є найбільш точним у порівнянні з BIN-SALT та BIN-COMBO.

Для кількісної оцінки величин спотворень між десятьма оригінальними зображеннями було підраховане MSE. Дані показники необхідні для визначення мінімальні значення відмінностей між оригінальними зображеннями, щоб на основі цієї інформації підрахувати ймовірність помилок при розпізнаванні. Результати розрахунків MSE між десятьма досліджуваними оригінальними зображеннями наведені у таблиці 6.10.

Таблиця 6.10 – Показники MSE між оригінальними зображеннями

Номер зображення	01	02	03	04	05	06	07	08	09	10
01	0	3427.6	3619.3	5434.2	3845.7	3490.4	2556.8	2278.1	3785.8	4061.5
02	3427.6	0	1643.9	3556.4	1683.4	3930.7	3710.1	4760.2	2108.2	2207.0
03	3619.3	1643.9	0	2670.7	2019.6	2737.3	3031.9	4671.8	1827.7	2130.2
04	5434.2	3556.4	2670.7	0	2609.1	2884.2	4037.5	5289.7	2218.7	2147.6
05	3845.7	1683.4	2019.6	2609.1	0	2952.8	3144.6	4585.4	1228.8	1431.2
06	3490.4	3930.7	2737.3	2884.2	2952.8	0	1573.0	2975.2	2576.6	2940.8
07	2556.8	3710.1	3031.9	4037.5	3144.6	1573.0	0	2768.1	3314.9	3617.1
08	2278.1	4760.2	4671.8	5289.7	4585.4	2975.2	2768.1	0	4350.5	4081.6
09	3785.8	2108.2	1827.7	2218.7	1228.8	2576.6	3314.9	4350.5	0	1650.3
10	4061.5	2207.0	2130.2	2147.6	1431.2	2940.8	3617.1	4081.6	1650.3	0

Із даних, наведених у таблиці 6.10, можна визначити, що найменшу відмінність між один одним маю п’яте та десяте зображення. Найменше значення MSE становить 1431.2. Найбільше значення MSE між першим та четвертим зображеннями. Воно складає 5434.2.

Оцінити ймовірність виникнення помилок при розпізнаванні для кожного алгоритму можна за допомогою наступних показників.

1) Коефіцієнт помилкового пропуску (false acceptance rate – FAR). Даний показник представляє собою процентний поріг, який визначає ймовірність того, що одна людина може бути прийнятий за іншу.

2) Коефіцієнт помилкової відмови в доступі (false rejection rate – FRR). Даний показник представляє собою ймовірність того, що зареєстрована людина може бути не розпізнана системою.

Із зменшенням кількості помилкових пропусків кількість помилкових відхилень буде зростати і навпаки. Точка, в якій перетинаються лінії, також має назву: рівний показник помилок (equal error rate - EER). У цій точці відсоток помилкових акцептів та помилкових відхилень однаковий [24]. Ідеальний графік кореляції коефіцієнту помилкового пропуску та коефіцієнту помилкової відмови в доступі наведений на рис. 6.4.

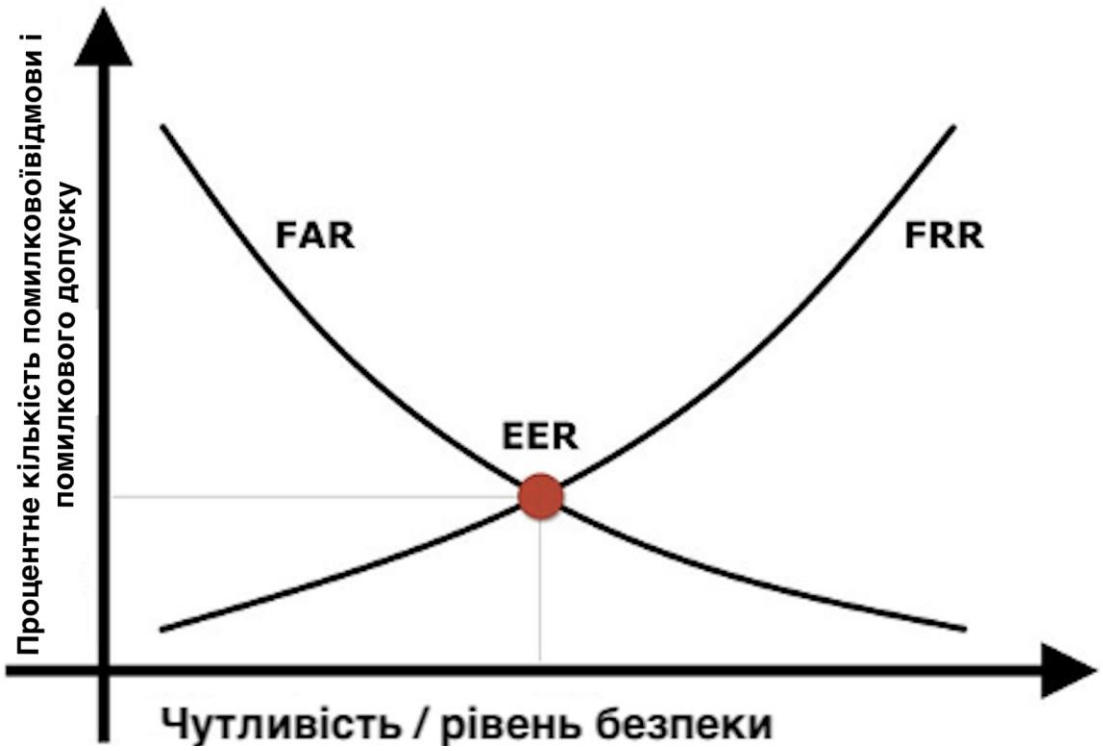

Рисунок 6.4 – Графік кореляції показників FAR та FRR

Зазвичай зниження FAR до найнижчого можливого рівня призведе до різкого збільшення показника FRR. Отже, чим безпечнішим буде контроль доступу у біометричній системі, тим менш зручною вона буде для користувачів, оскільки ймовірність того, що вони будуть помилково відхилені системою буде значно більшою. Зазвичай FAR та FRR можуть бути налаштовані в програмному забезпеченні системи безпеки шляхом коригування відповідних критеріїв. У досліджуваній програмі по розпізнаванню по райдужній оболонці ока людини це можна зробити за допомогою коригування порогу допуску, який був вище визначений експериментальним шляхом для кожного із методів захисту біометричного шаблону та для незахищеного коду райдужки. Далі розглядається процес підрахунків показників FAR та FRR для досліджуваної програми.

Враховуючи, що мінімальне значення MSE між оригінальними зображеннями складає 1431.2, а максимальне значення MSE при впливі шумів у системі із використанням усіх варіантів алгоритмів значно менше, то можна зробити висновок, що зашумлення зображення може призводити до неспрацьовування сканера, а не до прийняття зображення за інше з бази.

Для підрахунку коефіцієнту помилкового пропуску було обране найбільше значення MSE з усіх зашумлених зображень для кожного варіанту алгоритму та знайдено кількість показників MSE між оригінальними зображеннями, які є меншими за це найбільше значення помножене на коефіцієнт. Після цього кількість таких значень було поділено на 90, що складає кількість усіх можливих пар різних зображень, окрім пари з однаковими зображеннями. У результаті таких розрахунків були отримані значення FAR для усіх варіантів алгоритмів.

Для підрахунку коефіцієнту помилкової відмови в доступі кожне значення MSE для зашумлених зображень для кожного варіанту алгоритму було помножене на коефіцієнт, а саме збільшено у стократному розмірі. Після цього була знайдена кількість показників відмінності для кожного конкретного зображення між усіма іншими, які менше значення MSE для конкретного зображення між відповідним йому зашумленим зображенням. Далі була знайдена сума кількості таких показників для кожного зображення, яка була поділена на 90. У результаті таких розрахунків були отримані значення FRR для усіх варіантів алгоритмів. Підраховані за зазначеними вище алгоритмами показники FAR та FRR наведені у таблиці 6.11.

Таблиця 6.11 – Значення показників FAR та FRR для досліджуваних методів

Характеристика алгоритму	FRR	FAR
Незахищений біометричний шаблон	0.26	0.15
Використання BIN-SALT для створення біохешу	0.33	0.46
Використання BIN-COMBO для створення біохешу	0.34	0.42
Використання Min-Hashing для створення біохешу	0.24	0.46

Отже, виходячи з показників FAR та FRR, наведених у таблиці 6.11, можна зробити висновок що найближчу до ідеалу ймовірність помилок має алгоритм розпізнавання по райдужній оболонці ока, у якому не застосований жодний із методів захисту біометричного шаблону. Але використання такого алгоритму у системі біометричної автентифікації, оскільки, у разі викрадення незахищеного шаблону райдужки, згенерувати новий буде неможливо. Серед алгоритмів із захистом біометричного шаблону найбільш близькі до ідеалу показники має алгоритм із використанням BIN-COMBO для створення біохешу. Натомість найкращий показник FRR серед усіх алгоритмів має алгоритм із використанням Min-Hashing для створення біохешу. Це зумовлює найбільше значення показника FAR для цього алгоритму. Виходячи з цього можна зробити висновок, що система із використанням Min-Hashing буде достатньо зручною для користувача. Показники FAR серед алгоритмів із використанням методів біометричного шаблону мають не значні відмінності, а для Min-Hashing та BIN-COMBO є рівними. В той же час показник FRR є значно кращим для алгоритму із використанням Min-Hashing для створення біохешу. Таким чином, можна зробити висновок, що для забезпечення захищеної біометричної системи зі зручним для користувача використанням краще використовувати алгоритм із використанням Min-Hashing для створення біохешу.

Ефективність роботи алгоритмів та ймовірність виникнення помилок не є єдиними показниками, за якими можна оцінити програму по розпізнаванню по райдужній оболонці ока. Важливим критерієм є швидкість роботи того чи іншого метода захисту біометричного шаблону. Цей параметр є важливим, оскільки довгий час роботи при великій кількості зображень у базі може спричинити

незручність у використанні для користувача. Крім того, цей показник може допомогти визначити обчислювальні потужності для сервера, на якому будуть зберігатися захищені біометричні шаблони та/або буде проходити автентифікація користувачів. Час роботи програми був підрахований для наступних алгоритмів розпізнавання по райдужній оболонці ока:

- незахищений шаблон райдужної оболонки;
- захищений шаблон райдужної оболонки із використанням біометричного засолювання для створення біохешу;
- захищений шаблон райдужної оболонки із використанням BIN-COMBO для створення біохешу;
- захищений шаблон райдужної оболонки із використанням Min-Hashing для створення біохешу.

Кожний з алгоритмів був протестований у сукупності з етапами виділення райдужної оболонки ока, нормалізації зображення, виділення найбільш інформативного фрагменту, накладання фільтру та генерації коду райдужної оболонки, що співпадає з першим алгоритмом. Результати підрахувань часу роботи програми на основі алгоритму розпізнавання по райдужці без використання будь-яких методів захисту біометричного шаблону в залежності від кількості біохешей або кодів райдужок користувачів у базі наведені у таблиці 6.12.

Таблиця 6.12 – Час роботи програми на основі алгоритму без використання будь-яких методів захисту коду в залежності від кількості шаблонів у базі

Кількість незахищених кодів райдужних оболонок у базі	Час роботи програми(мс)
1	6462
2	6473
3	6546
4	6559
5	6598
6	6617
7	6687
8	6697
9	6764
10	6929

Виходячи з даних, наведених у таблиці 6.12, можна зробити висновок, що збільшення кількості біометричних шаблонів має не значний вплив на час роботи програми, оскільки відмінність між часом при опрацьовані різної кількості зображень становить менше секунди.

У таблиці 6.13 наведені результати підрахувань часу роботи програми на основі алгоритму розпізнавання по райдужці при використанні біометричного засолювання як методу захисту біометричного шаблону в залежності від кількості біохешей користувачів.

Таблиця 6.13 – Час роботи програми на основі алгоритму при використання BIN-SALT для захисту коду райдужки в залежності від кількості шаблонів у базі

Кількість біохешей отриманих за допомогою BIN-SALT у базі	Час роботи програми (мс)
1	7133
2	7190
3	7431
4	7400
5	8131
6	8143
7	8207
8	8302
9	8521
10	8881

Наведені у таблиці 6.13 дані свідчать про те, що час роботи при використанні біометричного засолювання для захисту біометричного шаблону збільшився для усіє кількості зображень у порівнянні із часом роботи алгоритму без використання будь-яких методів захисту коду райдужки. Також слід зауважити, що різниця між часом однієї кількості зображень та наступної зросла у кілька разів.

У таблиці 6.14 наведені результати підрахувань часу роботи програми на основі алгоритму розпізнавання по райдужці при використанні BIN-COMBO, як методу захисту біометричного шаблону в залежності від кількості біохешей користувачів.

Таблиця 6.14 – Час роботи програми на основі алгоритму при використання BIN-COMBO для захисту коду райдужки в залежності від кількості шаблонів у базі

Кількість біохешей отриманих за допомогою BIN-COMBO у базі	Час роботи програми (мс)
1	7207
2	7102
3	7234
4	7294
5	8114
6	8302
7	8549
8	9160
9	10078
10	10440

У порівнянні з попередніми дослідженнями часу роботи програми можна побачити, що час роботи програми при використання BIN-COMBO для захисту біометричного шаблону збільшився. Це може бути аргументовано тим, що кількість операцій для зміни оригінального коду райдужної оболонки більша ніж для біометричного засолювання.

Результати аналогічних досліджень для алгоритму із використанням Min-Hashing для захисту біометричного шаблону наведені у таблиці 6.15.

Таблиця 6.15 – Час роботи програми на основі алгоритму при використання Min-Hashing для захисту коду райдужки в залежності від кількості шаблонів

Кількість біохешей отриманих за допомогою Min-Hashing у базі	Час (мс)
1	7168
2	8457
3	9798
4	12228
5	15490
6	17076
7	20469
8	24973
9	29416
10	33586

Виходячи з даних, наведених у таблиці 6.15, можна зробити висновок, що час роботи програми на основі алгоритму із використанням Min-Hashing для захисту коду райдужки більший у декілька разів. При кожному збільшенні кількості біометричних шаблонів у базі час роботи програми збільшується від двох до чотирьох секунд. У зв'язку з цим велика кількість зображень при малих потужностях облікових машин може змусити користувача чекати, що може позначитися на зручності користування пристроєм.

Для візуального простеження відмінностей між часом роботи програми із використанням різних алгоритмів були побудовані графіки, наведені на рис. 6.5.

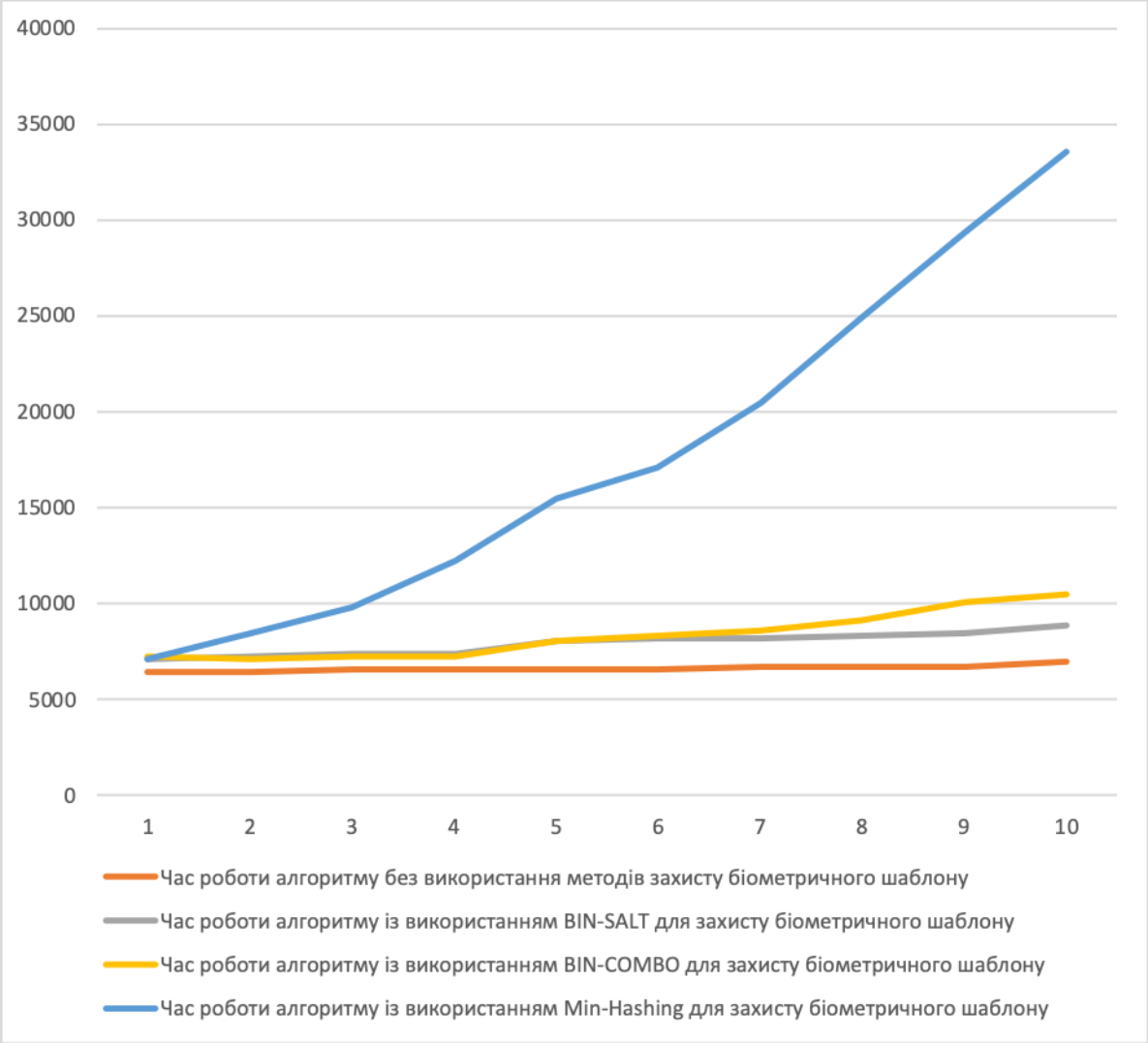

Рисунок 6.5 – Графік залежності часу роботи програми при використанні різних алгоритмів від кількості шаблонів у базі

Таким чином було проведено ряд досліджень на програмою при використанні різних алгоритмів захисту біометричного шаблону або повною їх

відсутністю. Дослідження показали, що найменші ймовірність помилкових відхилень доступу для зареєстрованих користувачів та помилкового надання доступу зловмиснику, які найближчі до ідеалу, час роботи програми має алгоритм без використання жодних методів захисту біометричного шаблону, що не є безпечним, оскільки не можна буде згенерувати нові коди райдужних оболонок з одних й тих самих очей у випадку якщо код райдужної оболонки буде викрадено.

Інші алгоритми, у яких використовується захист біометричного шаблону, мають майже однакові показники коефіцієнту ймовірності надання доступу зловмиснику. Найменші та найкращі значення показнику коефіцієнту ймовірності відмови у доступі зареєстрованому користувачу має алгоритм із використанням Min-Hashing, але він має найгірші показники з часу. Також згідно із дослідженнями SNR алгоритм із використанням Min-Hashing є найбільш чутливим до завад, оскільки має найбільші значення у співвідношенні «сигнал/шум».

Отже, не зважаючи на довгий час роботи, алгоритм із використанням Min-Hashing для захисту біометричного шаблону райдужної оболонки ока люди є найбільш ефективним, оскільки є найбільш зручним для користувачів у зв’язку з найнижчим показником коефіцієнту помилкової відмови зареєстрованому користувачу та найбільш чутливим до завад у порівнянні з іншими методами захисту біометричного шаблону райдужної оболонки ока, які були досліджені у даній роботі.

Даний алгоритм може біти в проваджений у системи розпізнавання по райдужній оболонці разом із етапами виділення райдужної оболонки, нормалізації зображення та іншими етапами обробки зображення, які були розглянуті у п’ятому розділі.

ВИСНОВКИ

У сучасному світі використання паролів відійшло на другий план. Їх місце зайняли унікальні біометричні характеристики людини, відповідальність за автентифікацію яких взяли на себе біометричні системи. Однією із найбільш комфортних та точних систем була визначена біометрична система по розпізнаванню по райдужній оболонці ока. Але точність та комфорт користувачів не можуть вплинути на безпеку системи у разі атак на біометричну систему. У зв'язку з цим у роботі було проаналізовано атаки на біометричні шаблони.

Однією із найсерйозніших проблем було виділено проблему неможливості згенерувати новий код райдужки у рази викрадення біометричного шаблону з бази. Таким чином для вирішення актуальної проблеми захисту біометричного шаблону у роботі було запропоновано три алгоритми з використанням різних методів захисту коду райдужки у комбінації з методами обробки зображення. У роботі були розглянуті такі методу захисту біометричного шаблону, як BIN-SALT, BIN-COMBO та Min-Hashing. На основі запропонованих алгоритмів було проведене програмне та математичне моделювання створення коду райдужки та його біохешу і порівняння з еталоном. Зазначені вище алгоритми були програмно реалізовані на мові Java. Програма була протестована на зображеннях з бази CASIA-Iris-Interval. Для дослідження ефективності роботи кожного з алгоритмів були підраховані показники ймовірності помилок FAR та FRR, визначена чутливість кожного алгоритму до рівня завад та визначений час роботи програми в залежності від кількості збережених у базі шаблонів. Кращим майже за усіма показниками було визначено алгоритм з використанням Min-Hashing для захисту біометричного шаблону

Наукова новизна роботи полягає в подальшій модернізації методів захисту біометричного шаблону райдужної оболонки ока та дослідженні ефективності використання методів на тлі завад.

Практична значущість роботи полягає в можливості використання досліджуваних алгоритмів для захисту біометричних шаблонів в системах біометричної автентифікації по райдужній оболонці ока для вирішення проблеми скасовуваності біометричних параметрів. Окремі результати дослідження були опубліковані у [16, 20, 21, 25-27].

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Static vs behavioural: what's the future of biometric authentication? [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: http://www.itproportal.com/features/static-vs-behavioural-whats-the-future-of-biometric-authentication/

2. Dipti S. Iris and Fingerprint Fusion for Biometric Identification / S. Dipti // International Journal of Computer Applications. – 2013. - Vol. 77, No. 11. - P. 975-88.

3. Explainer: Retinal Scan Technology [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.biometricupdate.com/201307/explainer-retinal-scan-technology.

4. Iris Recognition [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.nec.com/en/global/solutions/biometrics/iris/index.html.

5. Facial Recognition [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.biometricupdate.com/biometric-news/facial-recognition-biometric-articles.

6. DNA biometrics [Електронний ресурс]. – 2011. – Режим доступу до ресурсу: https://www.intechopen.com/books/biometrics/dna-biometrics.

7. Behavioral Biometrics: Dynamic Approach to Authentication and Security [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://gomedici.com/behavioral-biometrics-dynamic-approach-to-authentication-and-security.

8. Biometrics Security [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.commoncriteriaportal.org/communities/Bio.cfm.

9. Biometrics and biometric data: What is it and is it secure? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://us.norton.com/internetsecurity-iot-biometrics-how-do-they-work-are-they-safe.html.

10. Biometric data processing and storage system threats [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://securelist.com/biometric-data-processing-and-storage-system-threats/95364/.

11. Practical security and privacy attacks against biometric hashing using sparse recovery [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://asp-eurasipjournals.springeropen.com/articles/10.1186/s-0396-1.

12. Kaur G. Comparative Analysis of Biometric Modalities G. Kaur, Ch. K. Verma // International Journal of Advanced Research in Computer Science and Software Engineering [Електронний ресурс]. – 2014. – Режим доступу до ресурсу: https://www.ijarcsse.com/docs/papers/Volume_4/4_April2014/V4I4-0407.pdf.

13. Iris Recognition Used to Secure Borders [Електронний ресурс]. – 2017. – Режим доступу до ресурсу: https://www.biometricupdate.com/201205/iris-recognition-used-to-secure-borders

14. How is iris recognition changing the world in which we live? [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.nec.co.nz/market-leader ship/publications-media/how-is-iris-recognition-changing-the-world-in-which-we-live/.

15. Biometrics entering a new era in healthcare [Електронний ресурс]. – 2020. – Режим доступу до ресурсу: https://www.healthcareitnews.com/news/ biometrics-entering-new-era-healthcare.

16. Liashenko G. Network Steganography Application for Remote Biometric User Authentication / G.Liashenko, A.Astrakhantsev, V.Chernikova // The 9th IEEE International Conference on Dependable Systems, Services and Technologies, DESSERT'2018. – 2018. – P. 340-344.

17. Iris Recognition Technology [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.irisid.com/productssolutions/technology-2/.

18. Розпізнавання райдужки ока [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://worldvision.com.ua/articles/raspoznavanie-raduzhki-glaz-i-schitivanie-risunka-ven-chto-u-nih-obshchego.

19. Gite H.R. Iris code generation and recognition / H.R. Gite, C.N. Mahender // International Journal of Machine Intelligence. – 2011. - Vol. 3, No. 3. – P. 103-107.

20. Чернікова В. Г. Дослідження характеристик системи біометричної ідентифікації по райдужній оболонці ока / В.Г. Чернікова, А.А. Астраханцев, Г.Є. Ляшенко // Системи озброєння і військова техніка. – 2018. – № 1(53). – С. 195-202. https://doi.org/10.30748/soivt.2018.53.28.

21. Чернікова В.Г. Дослідження методів захисту біометричного шаблону райдужної оболонки ока / В.Г. Чернікова, А.М. Стрілець, С.О Скирда // Матеріали 24-го Міжнародного молодіжного форуму "Радіоелектроніка і молодь в XXI столітті". – Харків: ХНУРЕ, 2020 – С. 179-180.

22. Алгоритми захищеності біометричної верифікації на основі бінарного представлення [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.elibrary.ru/item.asp?id=17788933.

23. Конахович Г.Ф. Цифрова стеганографія / Г.Ф. Конахович, А.Ю.Пузиренко. – К.: МК-Пресс, 2006. – 40 с.

24. FAR and FRR: security level versus user convenience [Електронний ресурс]. – 2015. – Режим доступу до ресурсу: https://www.recogtech.com/en/knowledge-base/security-level-versus-user-convenience.

25. Чернікова В.Г. Дослідження характеристик системи біометричної ідентифікації по райдужній оболонці ока / В.Г. Чернікова, А.М. Стрілець // Матеріали для всеукраїнської науково-практичної конференції здобувачів вищої освіти та молодих учених «Перспективи розвитку інфокомунікацій та інформаційно-вимірювальних технологій». – Харків: ХНУРЕ, 2019 – С. 150-157.

26. Стрілець А. М. Методи тестування засобів захисту інформації / А. М. Стрілець, С.О. Скирда, В.Г. Чернікова // Матеріали 24-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь в XXI столітті». – Харків: ХНУРЕ, 2020 – С. 217-218.

27. Скирда С.О. Аудит інформаційної безпеки телекомунікаційних мереж з хмарною технологією / С.О. Скирда, В.Г. Чернікова, А.М. Стрілець // Матеріали 24-го Міжнародного молодіжного форуму «Радіоелектроніка і молодь в XXI столітті». – Харків: ХНУРЕ, 2020 – С. 160-161.

28. Колешко В.М. Традиційні методи біометричної автентифікації і ідентифікації / В.М. Колешко, Е.А. Воробей, П.М. Азізов. – М. : БНТУ, 2009. – 107 с.