МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Дніпровський національний університет залізничного транспорту імені академіка В. Лазаряна

Кафедра «Електронні обчислювальні машини»

«ДО ЗАХИСТУ»

Завідувач кафедри
Жуковицький І.В.
(підпис) (ПІБ)
«____» _____ 20____р.

ДИПЛОМНА РОБОТА

на здобуття освітнього ступеня «магістр»

Галузь знань 12 Інформаційні технології
(шифр) (назва)

Спеціальність 125 Кібербезпека
(код) (повна назва)

Тема Дослідження та розробка засобів біометричної аутентифікації за відбитками пальців

Theme Research and development of biometric fingerprint authentication tools

Керівник дипломного проекту	_____ (посада)	_____ (підпис)	Остапець Д.О. (ПІБ)
Консультант розділу з БЖД	_____ (посада)	_____ (підпис)	Музикін М. І. (ПІБ)
Нормоконтролер	_____ (посада)	_____ (підпис)	Шаповалов В. О. (ПІБ)
Студент групи	КБ1921 (група)	_____ (підпис)	Сокольський І.О. (ПІБ)
Student	Sokolskyi Ilan (family name)		

Дніпро
2020

Дніпровський національний університет залізничного транспорту імені академіка В.Лазаряна

Факультет Комп'ютерні технології і системи **кафедра** ЕОМ

Спеціальність Кібербезпека

ЗАТВЕРДЖУЮ:
зав. кафедри

_____
'_____' _____**20__ р.**

ЗАВДАННЯ
до дипломної магістерської роботи студента групи КБ1921 (966–М)
Сокольського Ілана Олеговича

1. Тема проекту (роботи) Дослідження та розробка засобів демонстрації біометричної аутентифікації за відбитками пальців

Затверджена наказом по університету № 945 / ст. від '16' грудня 2019 р.

2. Термін подання студентом закінченої роботи –14 грудня 2020р.

3. Вихідні дані до проекту (роботи)

3.1. Методи та засоби біометричної аутентифікації.

3.2. Характеристики алгоритмів порівняння відбитків пальця.

4. Зміст розрахунково-пояснювальної записки (роботи)

4.1. Огляд методів та засобів біометричної ідентифікації та автентифікації.

4.2. Аналіз методів порівняння відбитків пальців.

4.3. Розробка інформаційної та функціональної структури комплексу.

4.4. Розробка програмного забезпечення комплексу.

4.5. Методика використання комплексу.

4.6. Охорона праці та безпека в надзвичайних ситуаціях.

5. Перелік креслень (з переліком обов'язкових креслень)

5.1. Порівняльна характеристика відомих методів та засобів біометрії – 1

5.2. Порівняльна характеристика відомих методів порівняння відбитків – 1

5.3. Організація розроблюваного комплексу – 1-2

5.4. Математична модель процесу порівняння відбитків – 1

5.5. Схеми основних алгоритмів програми – 1-2

5.6. Екранні форми програми – 1-2

5.7. Методика використання розробленої системи в учбовому процесі – 1

6. Консультанти (з назвами розділів)

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Розділ ОП та БНС			

7. Дата видачі завдання -_____« » 20 р._____ .

Керівник роботи _____(доц. Остапець Д.О.)
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва розділів дипломного проекту (роботи)	Термін виконання розділів проекту (роботи)	Примітки
1	Огляд методів та засобів біометричної ідентифікації та автентифікації		15%
2	Аналіз методів порівняння відбитків		20%
3	Розробка інформаційної та функціональної структури комплексу		15%
4	Розробка програмного забезпечення комплексу		40%
5	Методика використання комплексу		5%
6	Розділ ОП та БНС		5%

Студент-дипломник_____

Керівник роботи_____(доц. Остапець Д.О.)

РЕФЕРАТ

Дипломна робота на тему: «Дослідження та розробка засобів біометричної аутентифікації за відбитками пальців» складається зі вступу, розділу 1 «Огляд методів та засобів біометричної ідентифікації та автентифікації», де розкриваються поняття та види біометричної аутентифікації людини, здійснений порівняльний аналіз методів біометричної аутентифікації; розділу 2 «Аналіз методів порівняння відбитків»: обґрунтування ефективності використання різних методів порівняння відбитків пальців; розділу 3 «Розробка інформаційної та функціональної структури комплексу»: архітектура демонстраційного комплексу; розділу 4 «Розробка програмного забезпечення комплексу», розділу 5 «ОП та БНС», а також п’ятьох таблиць та тридцяти рисунків, загальних висновків; переліку посилань (20 джерел). Загальний обсяг роботи – 63 сторінки.

Об’єкт дослідження - біометрична автентифікація.

Мета кваліфікаційної роботи – дослідження та розробка програмного забезпечення для біометричної автентифікації особистості.

Галузь застосування – біометрична аутентифікація активно застосовуються в багатьох областях, пов'язаних із забезпеченням безпеки доступу до інформації та матеріальних об'єктах, а також в задачах унікальної ідентифікації особистості: в криміналістиці, медицині, політиці, соціальній сфері, правоохоронних органах, кібербезпеці.

Економічна ефективність – застосування біометричної аутентифікації дає можливість ведення електронного бізнесу і електронних урядових справ, збереження безпеки банківських звернень, інвестування та інших фінансових переміщень, а також роздрібної торгівлі, охорони правопорядку, питання охорони здоров'я, а також в сфері соціальних послуг.

Ключові слова: АУТЕНТИФІКАЦІЯ, БІОМЕТРИЧНІ ДАНІ, МЕТОДИ БІОМЕТРИЧНОЇ АУТЕНТИФІКАЦІЇ, ВІДБИТКИ ПАЛЬЦІВ, МОВА ПРОГРАМУВАННЯ C#, VISUAL STUDIO 2019, ПРОГРАМНИЙ ПРОДУКТ.

ABSTRACT

Graduate work on a theme the "Research and development of biometric fingerprint authentication tools" consists of entry, division a 1 «Review of methods and means of biometric identification and authentication», where a concept and types of biometrical authentication of man open up, the comparative analysis of methods of biometrical authentication is carried out; division 2 «Analysis of fingerprint comparison methods»: ground of efficiency of the use of different methods of comparison of finger-prints; division 3 «Development of information and functional structure of the complex»: architecture of the demonstration complex; division 4 «Complex software development»; division 5 «Occupational health and safety in emergencies» and also five tables and thirty drawings, general conclusions development; list of links (20 sources). General volume of work is 63 pages.

A research object is biometrical authentication.

An aim of qualifying work is research and software development for biometrical authentication of personality. Industry of application is biometrical authentication authentications of personality.

Industry of application is biometrical authentication are actively used in many areas related to providing of safety of access to information and to the material objects, and also in the tasks of unique authentication of personality: in criminalistics, medicine, politics, social sphere, law enforcement authorities, cybersecurity.

Economic efficiency - application of biometrical authentication gives an opportunity of conduct of electronic business and electronic governmental businesses, maintenance of safety of bank appeals, investing and other financial moving, and also retail business, guard of law and order, question of health protection, and also in social service business.

Keywords: AUTHENTIFICATION, BIOMETRICAL DATA, METHODS of BIOMETRICAL AUTHENTIFICATION, FINGER-PRINTS, PROGRAMMING C#, VISUAL STUDIO LANGUAGE 2019, SOFTWARE PRODUCT.

ЗМІСТ

ВСТУП

Системи аутентифікації все більше входять у наше повсякденне життя через стрімкий розвиток інформаційних технологій. Існують наступні основні види систем аутентифікації: парольні, майнові, біометричні.

На сьогодні біометричні системи набули широкого використання. Наразі майже у всіх є смартфони, у яких присутня аутентифікація за відбитком пальця або за обличчям.

Основною перевагою біометричних систем, безперечно, є наявність зразку «з собою». На відмінну від парольних систем, користувачеві не потрібно пам’ятати пароль, який можна забути; на відмінну від майнових систем, не потрібно носити ключи або картки, які можна загубити.

Однією з найпоширеніших біометричних систем аутентифікації є система аутентифікації за відбитками пальців. Вважається, що відбиток є унікальним та незмінюваним упродовж життя.

Біометрична система працює за наступним алгоритмом: спеціальний пристрій зчитує відмінні риси користувача, з яких виділяються необхідні характеристики та зберігаються у базі даних. Для входу у систему користувач знову надає свої дані, з бази даних обирається необхідний еталон і порівнюється з отриманим зразком. Після цього приймається рішення про успішність або невдачу аутентифікації.

Метою дипломного проекту є розробка і дослідження засобів демонстрації аутентифікації за відбитками пальців. Для реалізації цієї задачі була обрана мова програмування C# та IDE Visual Studio 2019.

Поставлена мета досягається розв’язанням таких основних задач:

- огляд та аналіз існуючих методів порівняння відбитків пальців;
- розробка структури демонстраційного комплексу;
- реалізація комплексу на практиці за допомогою C# та його тестування.

1 ОГЛЯД МЕТОДІВ ТА ЗАСОБІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

1.1 Загальні відомості

Аутентифікація – це процес перевірки автентичності (автентичність означає справжність). Аутентифікація – основа безпеки для будь-якої системи, яка полягає в перевірці достовірності даних про користувача[7].

Термін «*аутентифікація*» не тотожний термінам «*ідентифікація*» та «авторизація». Ці три терміни є елементами захисту інформації.

Перша стадія – *ідентифікація*. У рамках ідентифікації відбувається розпізнавання інформації про користувача, зокрема, логін і пароль. Друга стадія – *аутентифікація*. Вона уявляє собою процес перевірки інформації про користувача. На третій стадії відбувається *авторизація*. Тут робиться перевірка прав користувача і визначається можливість доступу.

Виділяють наступні основні групи методів аутентифікації:

- *парольна* – найпоширеніший метод. Аутентифікація може проходити по одноразовим і багаторазовим паролів. Багаторазовий пароль задає користувач, а система зберігає його в базі даних. Він є однаковим для кожної сесії, наприклад, PIN-коди, слова, цифри, графічні ключі. Одноразові паролі – різні для кожної сесії, наприклад, SMS з кодом.
- *майнова* – «те, чим ти володієш». В першу чергу під цим розуміють апаратно-програмні системи ідентифікації і автентифікації або пристрої введення ідентифікаційних ознак. До їх складу входять апаратні ідентифікатори, пристрої введення-виведення (зчитувачі, контактні пристрої, адаптери, роз’єми системної плати та ін.) і відповідне ПО. Ідентифікатори призначені для зберігання унікальних ідентифікаційних ознак, крім цього вони можуть зберігати і обробляти конфіденційні дані. Пристрої введення-виведення і ПО здійснюють обмін даними між ідентифікатором і захищаються системою.

− *біометрична* – вона запобігає витоку або крадіжку персональної інформації. Перевірка проходить по фізіологічним характеристикам користувача.

У будь-якій системі аутентифікації можна виділити кілька елементів:

− суб’єкт, що буде проходити процедуру аутентифікації;

− характеристика суб’єкта – його відмінна риса;

− господар системи аутентифікації, який несе відповідальність і контролює її роботу;

− сам механізм аутентифікації – принцип роботи системи;

− механізм управління доступом, що надає певні права доступу суб’єкта.

Останнім часом все частіше застосовується багатофакторна автентифікація. Вона збудована на спільному використанні декількох факторів автентифікації. Це значно підвищує захищеність системи. Наприклад, в деяких сучасних ноутбуках є сканер відбитка пальця. Для того, щоб увійти в систему, суб’єкт повинен пройти процедуру біометричної автентифікації, а потім ввести пароль.

Обираючи для системи той або інший фактор чи спосіб автентифікації, необхідно відштовхуватися від потрібного ступеня захищеності, вартості побудови системи, а також забезпечення мобільності суб’єкта.

Для наочності вищесказаного можна привести таку порівняльну таблицю (Таблиця 1.1.):

Таблиця 1.1 – Порівняння способів автентифікації в залежності від рівня риску

Рівень ризику	**Вимоги до системи**	**Спосіб аутентифікації**
Низький	Виконати аутентифікацію у системі, причому крадіжка, злом, розголошення конфіденційних даних не матимуть значних наслідків	Рекомендується використання багаторазових паролів
Середній	Виконати аутентифікацію у системі, причому крадіжка, злом, розголошення конфіденційних даних заподіють невеликих збитків	Рекомендується використання одноразових паролів
Високий	Виконати аутентифікацію у системі, причому крадіжка, злом, розголошення конфіденційних даних заподіють великих збитків	Рекомендується використання багатофакторної аутентифікації

У моїй роботі розглядається біометрична автентифікація. У порівнянні з парольною та майновою автентифікацію, можна виділити такі її переваги:

- надійність і швидкість автентифікації: електронно-аналітичні пристрої розпізнають людину протягом 1-2 с;
- високий рівень безпеки: біометричні ознаки людини є неповторними, що зводить до мінімуму кількість можливих помилок при впізнанні;
- дані біометричних характеристик не можна втратити або забути;
- пристрої біометричної автентифікації зручні в користуванні та експлуатації.

1.2 Класифікація методів біометричної аутентифікації

Біометрія – це вимірювання тіла та обчислення, пов'язані з характеристиками людини. Біометрична автентифікація (або реалістична автентифікація) використовується в інформатиці як форма ідентифікації та контролю доступу.

Біометричні ідентифікатори – це відмінні, вимірювані характеристики, що використовуються для маркування та опису людей. Біометричні ідентифікатори часто класифікуються як фізіологічні та поведінкові характеристики. Фізіологічні характеристики пов'язані з формою тіла. Приклади включають, але не обмежуються відбитками пальців, венами долоні, розпізнаванням обличчя, ДНК, геометрією рук, розпізнаванням райдужки, сітківкою та запахом. Поведінкові характеристики пов'язані зі зразком поведінки людини, включаючи, але не обмежуючись, ритмом друку, ходою та голосом. Деякі дослідники ввели термін «*біхевіометрія*» для опису останнього класу біометрії.

Для біометричної автентифікації можна використовувати багато різних аспектів фізіології, хімії чи поведінки людини. Вибір конкретного біометричного методу для використання в конкретному застосуванні включає зважування кількох факторів. Джейн та ін. (1999) визначив сім таких факторів, які слід використовувати при оцінці придатності будь-якої ознаки для використання в біометричній автентифікації:

1) *Універсальність* означає, що кожна людина, яка використовує систему, повинна володіти цією рисою.
2) *Унікальність* означає, що ознака повинна бути достатньо різною для особин відповідної популяції, щоб їх можна було відрізняти один від одного.
3) *Постійність* пов'язана зі способом зміни ознаки з часом. Більш конкретно, ознака з «гарною» стійкістю з часом буде досить незмінною щодо конкретного алгоритму узгодження.

4) *Вимірність* стосується простоти набуття або вимірювання ознаки. Крім того, отримані дані повинні мати форму, яка дозволяє подальшу обробку та вилучення відповідних наборів ознак.
5) *Продуктивність* пов'язана з точністю, швидкістю та надійністю використовуваної технології.
6) *Прийнятність* пов'язана з тим, наскільки добре люди у відповідній популяції сприймають технологію таким чином, що вони готові мати їх біометричні ознаки.
7) *Обхід* стосується легкості імітації ознаки за допомогою артефакту або замінника.

Правильне біометричне використання дуже залежить від застосування. Певні біометричні показники будуть кращими за інші на основі необхідних рівнів зручності та безпеки. Жодна біометрична не відповідає всім вимогам усіх можливих застосувань.

Перший раз, коли людина використовує біометричну систему, відбувається *зарахування*. Під час реєстрації біометрична інформація від особи фіксується та зберігається. При подальшому використанні біометрична інформація виявляється та порівнюється з інформацією, що зберіглася під час реєстрації. Дуже важливо, щоб зберігання та пошук таких систем були безпечними, якщо біометрична система має бути надійною.

Перший блок (датчик) – це інтерфейс між реальним світом і системою; він повинен отримати усі необхідні дані. Найчастіше, це система отримання зображень, але вона може змінюватися відповідно до бажаних характеристик. Другий блок виконує всю необхідну попередню обробку: він повинен видалити артефакти з датчика, посилити вхід (наприклад, видалити фоновий шум), використовувати якусь нормалізацію тощо. У третьому блоці витягуються необхідні функції. Цей крок є важливим кроком, оскільки правильні функції потрібно витягувати оптимальним способом. Для створення шаблону використовується вектор чисел або зображення з певними

властивостями. Шаблон – це синтез відповідних характеристик, вилучених із джерела. Елементи біометричного вимірювання, які не використовуються в алгоритмі порівняння, відкидаються в шаблоні, щоб зменшити розмір файлу та захистити ідентифікацію учасника.

На етапі реєстрації шаблон просто зберігається десь (на картці або в базі даних, або в обох). На етапі узгодження отриманий шаблон передається збігу, який порівнює його з іншими існуючими шаблонами, оцінюючи відстань між ними за допомогою будь-якого алгоритму (наприклад, відстань Хеммінга). Програма відповідності проаналізує шаблон із введеними даними. Потім це буде виведено для певного використання або цілі (наприклад, вхід в обмежену зону), хоча існує побоювання, що використання біометричних даних може зіткнутися з повзучим завданням [7] [8]. При виборі конкретного біометричного фактору слід враховувати фактори, ефективність, соціальну прийнятність, простоту обходу та / або підробки, надійність, охоплення населення, розмір необхідного обладнання та запобігання крадіжці особистих даних. Вибір біометричного методу базується на вимогах користувача та враховує доступність датчика та пристрою, обчислювальний час та надійність, вартість, розмір датчика та енергоспоживання.

1.2.1 Аутентифікація по райдужній оболонці ока

Ця технологія біометричної автентифікації особистості використовує унікальність ознак і особливостей райдужної оболонки ока. Ця оболонка – тонка рухома діафрагма очі у хребетних з отвором (зіницею) в центрі; розташована за рогівкою, між передньою і задньою камерами ока, перед кришталиком. Вона утворюється ще до народження людини, і не змінюється протягом усього життя. За текстурою райдужна оболонка нагадує мережу з великою кількістю оточуючих кіл і малюнків, що можуть бути виміряні комп’ютером, при цьому малюнок райдужної оболонки дуже складний, що дозволяє відібрати близько 200 точок, використовуючи які можна домогтися

високої ступені надійності автентифікації. Для порівняння, найкращі системи ідентифікації за відбитками пальців використовують для цього 60-70 точок.

Технології розпізнавання райдужної оболонки ока були розроблені для того, щоб звести нанівець незручність сканування сітківки ока, при якому застосовуються інфрачервоні промені або яскраве світло. Учені також провели ряд досліджень, які засвідчили, що сітківка ока людини може змінюватися з часом, в той час як райдужна оболонка ока залишається незмінною. І головне, – неможливо знайти два абсолютно ідентичних рисунки райдужної оболонки ока, навіть у близнюків. Для отримання індивідуальних даних про райдужну оболонку ока чорно-білою камерою здійснюють 30 записів на секунду. Ледве помітне світло висвітлює райдужну оболонку, і це дозволяє відеокамері сфокусуватися на ній. Потім записи оцифровуються та зберігається в базі даних зареєстрованих користувачів. Уся процедура займає кілька секунд, і вона може бути повністю комп'ютеризована та автоматизована за допомогою голосових вказівок і автофокусування. Камера може бути установлена на відстані від 10 см до одного метра, в залежності від обладнання. Термін «сканування» може бути оманливим, позаяк в процесі отримання зображення проходить не сканування, а просте фотографування. Далі отримане зображення райдужної оболонки перетворюється в спрощену форму, записується і зберігається для подальшого порівняння. Окуляри й контактні лінзи, навіть кольорові, не впливають на якість автентифікації.

1.2.2 Аутентифікація за сітківкою ока

Метод автентифікації по сітківці ока отримав практичне застосування приблизно в середині 50-х років XX століття. Саме тоді було встановлено унікальність малюнка кровоносних судин очного дна (у близнюків дані малюнки також не збігаються). Для сканування сітківки використовують інфрачервоне випромінювання низької інтенсивності, що спрямоване через зіницю до кровоносних судин, розташованих на задній стінці ока. З отриманих

даних виділяють кілька сотень особливих точок, інформація про яких зберігається в шаблоні.

До недоліків подібних систем слід в першу чергу віднести психологічний фактор: не всякому людині приємно дивитися в незрозуміле темний отвір, де щось світить в око. До того ж, подібні системи вимагають чіткого зображення і, як правило, чутливі до некоректної орієнтації сітківки. Тому потрібно дивитися акуратно, а наявність деяких захворювань (наприклад, катаракти) може погано впливати на використання даного методу. Сканери для сітківки ока набули поширення для доступу до надсекретних об'єктів, позаяк забезпечують одну з найнижчих ймовірностей помилки першого роду (відмова в доступі для зареєстрованого користувача) і майже нульовий відсоток помилок другого роду [10].

1.2.3 Аутентифікація по геометрії руки

У цьому методі для біометричної автентифікації особистості використовують форму кисті руки. Через те, що окремі параметри геометрії руки не є чимось унікальним, доводиться використовувати кілька характеристик. Зокрема, скануються такі параметри руки, як вигини пальців, їх довжина і товщина, ширина і товщина тильного боку руки, відстані між суглобами і структура кістки. Також геометрія руки включає в себе дрібні деталі (зокрема, зморшки на шкірі). Хоча структура суглобів і кісток є відносно сталими ознаками, проте розпухання тканин чи удари руки можуть спотворити вихідну структуру. Технологія має й інші проблеми: навіть без урахування можливості ампутації, захворювання на артрит може сильно перешкоджати застосуванню сканерів.

За допомогою сканера, що складається з камери і підсвічувати діодів (при скануванні кисті руки, діоди вмикаються по черзі, що дозволяє отримати різні проекції руки), завдяки чому будується тривимірний образ пензля руки.

Надійність автентифікації по геометрії руки порівнянна з автентифікацією за відбитком пальця.

Системи автентифікації по геометрії руки широко поширені, що є доказом їх зручності для користувачів. Використання цього параметра привабливо по ряду причин. Процедура отримання зразка досить проста і не пред'являє високих вимог до зображення. Розміри отриманого шаблону дуже малі, кілька байт. На процес автентифікації не впливають ані температура, ані вологість, ані забрудненість. Підрахунки, вироблені при порівнянні з еталоном, дуже прості і можуть бути легко автоматизовані. Системи автентифікації, засновані на геометрії руки, почали використовуватися в світі на початку 70-х років [10].

1.2.4 Аутентифікація за геометрію обличчя

Біометрична автентифікація людей за допомогою геометрії обличчя – широко використовуваний метод ідентифікації та автентифікації. Технічна реалізація є складним математичним завданням. Широке використання мультимедійних технологій дозволяє використовувати достатню кількість відеокамер на залізничних і автовокзалах, в аеропортах, на площах, вулицях, шляхах та в інших людних місцях. Це стало вирішальним для бурхливого розвитку даного напрямку.

Щоб зробити тривимірну модель людського обличчя, фіксують контури очей, брів, носа, губ та інших елементів обличчя та вираховують відстань між ними та будують тривимірну модель. Аби побудувати унікальний шаблон, за яким можна ідентифікувати конкретну людину, знадобиться від 12 до 40 відмінних елементів. Шаблон має враховувати багато варіацій зображення з точки зору повороту обличчя, нахилу, зміни освітлення, виразу обличчя тощо.

Діапазон таких варіантів варіюється в залежності від цілей застосування цього способу (для ідентифікації, автентифікації, віддаленого пошуку на великих територіях тощо). Деякі алгоритми дозволяють компенсувати наявність у людини очок, капелюхи, вусів і бороди.

1.2.5 Аутентифікація по термограмі обличчя

Спосіб заснований на дослідженнях, які засвідчили, що термограма обличчя унікальна для кожної людини. Термограма отримується за допомогою камер ІЧ діапазону. На відміну від автентифікації по геометрії особи, цей метод розрізняє близнюків. Використання спеціальних масок, проведення пластичних операцій, температура тіла, старіння організму людини, охолодження шкіри обличчя в морозну погоду не впливають на точність термограми. Через невисоку якість автентифікації, метод наразі не має широкого поширення.

1.2.6 Аутентифікація за голосом

Біометричний метод автентифікації за голосом характеризується простотою в застосуванні. Даному методу не потрібна дорога апаратура, досить мікрофона і звукової плати. В даний час дана технологія швидко розвивається, позаяк цей метод автентифікації широко використовується в сучасних бізнес-центрах. Існує чимало способів побудови шаблону по голосу. Зазвичай, це різні комбінації частотних і статистичних характеристик голосу людини. Можуть розглядатися такі параметри, як модуляція, інтонація, висота тону, і т. п.

Основним і визначальним недоліком методу автентифікації по голосу – низька точність методу. Наприклад, людину з застудою система може не упізнати. Важливу проблему становить різноманіття проявів голосу в однієї людини: голос здатний змінюватися в залежності від стану здоров’я, віку, настрою і т. д. Це різноманіття зумовлює серйозні труднощі при виділенні властивостей голосу у людини. Крім того, врахування шумових компонентів є ще однією важливою і невирішеною проблемою в практичному використанні автентифікації по голосу. Так як ймовірність помилок другого роду при використанні цього методу велика (близько одного відсотка), автентифікація по голосу застосовується для управління доступом в приміщеннях середнього

рівня безпеки, такі як комп'ютерні класи, лабораторії виробничих компаній і т. ін. [4].

1.2.7 Аутентифікація за рукописним почерком

Метод біометричної автентифікації по рукописному почерку ґрунтується на специфічному русі людської руки під час написання документів. Для збереження підпису з метою подальшого його аналізу використовують спеціальні ручки чи сприйнятливі до тиску поверхні. Цей вид автентифікації людини використовує його підпис. Шаблон створюється в залежності від необхідного рівня захисту. Як правило, виділяють два способи обробки даних щодо підписів:

- Аналіз самого підпису, тобто використовується ступінь збігу двох картинок підпису.
- Аналіз динамічних характеристик написання, тобто для автентифікації будується згортка, в яку входить інформація по підпис, часові і статистичні характеристики його виконання.

1.2.8 Аутентифікація за відбитком пальця

Використання автентифікації за відбитками пальців – найпоширеніша біометрична технологія автентифікації користувачів. Метод використовує унікальність рисунка папілярних візерунків на пальцях людей. Відбиток отримується за допомогою сканера та перетворюється на цифровий код, а потім порівнюється з раніше введеними наборами еталонів. Переваги використання цього методу – легкість у використанні, зручність і надійність. Універсальність цієї технології дозволяє застосовувати її в будь-яких сферах і для вирішення будь-яких і найрізноманітніших завдань, де необхідна достовірна і досить точна ідентифікація користувачів.

Для отримання даних про відбитки пальців застосовуються спеціальні сканери. Щоб отримати виразне електронне подання відбитків пальців,

використовують досить специфічні методи, так як відбиток пальця занадто малий, і дуже важко отримати добре помітні папілярні візерунки.

Зазвичай застосовуються три типи сканерів відбитків пальців, а саме: ємнісні, прокатні, оптичні. Найпоширеніші і широко використовувані це оптичні сканери, але вони мають один серйозний недолік. Оптичні сканери нестійкі до муляжів і мертвим пальцях, а це значить, що вони не настільки ефективні, як інші типи сканерів. Так само в деяких джерелах сканери відбитків пальців ділять на 3 класу за їхніми фізичними принципам: оптичні, кремнієві, ультразвукові.

1.3 Порівняльний аналіз характеристик методів біометричної аутентифікації

Для порівняння відносних характеристик, а саме: стійкості до фальсифікації даних, швидкості автентифікації, можливості суворої автентифікації, незмінності біометричних характеристик, вартості реалізації наведено Таблицю 1.2.

Таблиця 1.2 – Порівняльний аналіз характеристик методів біометричної автентифікації

Біометричний метод	**Стійкість до фальсифікації даних**	**Швидкість аутентифікації**	**Можливість суворої аутентифікації**	**Незмінність біометричних характеристик**	**Вартість реалізації**
Відбиток пальця	Низька	Висока	Можлива	Низька	Низька
Розпізнавання обличчя 2D	Низька	Середня	Ні	Низька	Середня
Розпізнавання обличчя 3D	Середня	Низька	Ні	Висока	Висока
Райдужна оболонка ока	Висока	Висока	Можлива	Висока	Висока
Сітківка ока	Дуже висока	Низька	Можлива	Середня	Висока
Малюнок вен	Дуже висока	Висока	Можлива	Середня	Середня

1.4 Висновки за розділом

В першому розділі розглянуто поняття біометричної автентифікації, класифікацію методів біометричної автентифікації та проведено порівняльний аналіз методів біометричної автентифікації. Результати показують, що найбільш вдалим є варіант біометричної автентифікації за відбитком пальцю, що пов’язано зі співвідношенням переваг і недоліків і їх якісною оцінкою.

Серед основних переваг біометричної автентифікації за відбитками пальців можна виділити: швидкість автентифікації, можливість суворої автентифікації, вартість та відносну простоту реалізації. Проте, такий метод можна назвати найбільш оптимальним лише відкинувши можливі зовнішні фактори, наприклад, підвищену вологість повітря приміщення, де буде встановлено сканер, яка буде перешкоджати нормальній роботі деяких видів сканерів відбитку пальця.

2 АНАЛІЗ МЕТОДІВ ПОРІВНЯННЯ ВІДБИТКІВ

2.1 Характеристики відбитків пальців

У кожному відбитку пальця людини можна визначити два типи ознак – глобальні й локальні.

Глобальні ознаки (Рис.2.1) – ті, які людина можна побачити неозброєним оком:

- Папілярний візерунок
- Область візерунка – виділений фрагмент відбитка, в якому локалізовані всі глобальні ознаки.
- Ядро або центр – точка, локалізована в середині відбитка або певної виділеної області.
- Пункт «дельта» – початкова точка. Це місце, в якому відбувається поділ або поєднання борозенок папілярних ліній, чи дуже коротка борозенка (може доходити до крапки).
- Тип лінії – дві найбільші лінії, що починаються як паралельні, а потім розходяться і огинають всю область образу.
- Лічильник ліній – це число ліній на області образу, чи між ядром і пунктом «дельта».

Є наступні типи папілярних візерунків:

- візерунки типу «петля» (права, ліва, подвійна, центральна);
- візерунки типу «дельта» чи «дуга» (проста і гостра);
- візерунки типу «спіраль» (центральна і змішана).

Інший тип ознак – локальні ознаки. Їх називають *мінуції* (Рис.2.2) (особливостями або особливими точками) – унікальні для кожного відбитку пальця ознаки, які визначають пункти зміни структури папілярних ліній (роздвоєння, закінчення, розрив тощо), орієнтацію папілярних ліній і координати в цих пунктах. Кожен відбиток може містити до 70 і більше мінуцій.

Рисунок 2.1 – Глобальні ознаки відбитку пальця

Рисунок 2.2 – Локальні ознаки відбитку пальця (мінуції)

Практика показує, що відбитки пальців у різних людей можуть мати окремі однакові глобальні ознаки, проте абсолютно неможливо наявність однакових мікровізерунків мінуцій. Тому глобальні ознаки використовують з метою поділу бази даних на класи і на етапі автентифікації. На другому етапі розпізнавання користуються вже локальними ознаками.

2.2 Стандарти в сфері дактилоскопії

Зараз в основному використовуються стандарти ANSI і ФБР США. У них визначені такі вимоги до образу відбитка:

- кожен образ представлено у форматі нестислого TIFF;
- образ повинен мати дозвіл не менше 500 dpi;
- образ має бути напівтоновим з 256 рівнями яскравості;

− максимальний кут повороту для відбитка від вертикалі – не більше 15 град.;

− основні типи мінуцій – закінчення і роздвоєння.

Зазвичай в базі даних зберігають більше одного способу. Це дозволяє поліпшити якість розпізнавання та ідентифікації. Образи можуть відрізнятися зрушенням і поворотом. Масштаб не змінюється, так як всі відбитки отримують з одного пристрою.

2.3 Методи порівняння відбитків пальців

2.3.1 Порівняння за локальними ознаками

− Етап 1. Покрашення якості вихідного зображення відбитка. Збільшується різкість меж папілярних ліній.

− Етап 2. Обчислення поля для орієнтації папілярних ліній відбитка пальців. Зображення розбивають на квадратні блоки, зі сторонами більше 4 пікселів і по градієнтам яскравості обчислюють кут t орієнтації ліній фрагмента відбитка пальця.

− Етап 3. Бінаризація зображення відбитка пальця. Приведення до чорно-білого зображення (1 bit) пороговою обробкою.

− Етап 4. Витончення ліній в зображенні відбитка. Потоншення робиться доти, поки лінії не будуть шириною 1 px.

− Етап 5. Виділення мінуцій. Зображення розбивають на блоки 3x3 пікселів. Після цього підраховують число чорних (ненульових) пікселів, що знаходяться біля центру. Піксель в центрі вважається мінуцією, якщо він сам ненульовий, і сусідніх ненульових пікселів один (минуція «закінчення») чи три (мінуція «розгалуження»). Координати виявлених мінуцій і їх кути орієнтації записуються в вектор: **W (p) = [(x1, y1, t1), (x2, y2, t2) ... (xp, yp, tp)] (p – число мінуцій)**. При реєстрації користувачів такий вектор вважається еталоном і записується в базу даних. При розпізнаванні вектор визначає відбиток.

− Етап 6. Зіставлення мінуцій.

Два відбитка з одного пальця будуть відрізнятися поворотом, зміщенням, зміною масштабу і / або площею дотику в залежності від того, як користувач прикладає палець до сканера. Тож не можна сказати, чи належить відбиток певній людині чи ні на підставі простого їх порівняння (вектори еталона і поточного відбитка можуть відрізнятися по довжині, містити невідповідні мінуцій і т. д.). Через це процес зіставлення має бути зроблений для кожної мінуції.

Етапи порівняння включають в себе:

- Реєстрацію даних;
- Пошук пар відповідних мінуцій;
- Оцінку відповідності відбитків.

При реєстрації визначають параметри афінних перетворень (кут повороту, масштаб і зрушення), при яких деяка мінуція з одного вектора є певною мінуцією з іншого.

При пошуку для кожної мінуції слід перебрати до 30 значень повороту (починаючи від -15 градусів до +15), 0,5 тис. значень зсуву (в інтервалі -250 ПКС … +250 ПКС – хоча іноді вибирають і менші кордону) і 10 значень масштабу (0,5…1,5 з кроком 0,1). Разом до 150 тис. кроків для кожної з 70 можливих мінуцій. На практиці усі можливі варіанти не перебираються – після підбору значень для однієї мінуції їх же намагаються підставити і до інших мінуцій, інакше було б важко зіставити практично будь-які відбитки між собою.

Оцінку відповідності відбитків виконують за формулою:

$$\boldsymbol{K = \frac{D^2}{pq} \cdot 100\%,}$$

де D – кількість мінуцій, які збігаються, p – кількість мінуцій еталону, q – кількість мінуцій впізнаваного відбитка. В разі, якщо результат перевищує

65%, відбитки вважають ідентичними (поріг можна знизити виставлянням іншого рівня пильності).

Якщо виконувалася автентифікація, то на цьому все і закінчується. Для впізнання необхідно повторити цей процес для усіх відбитків в базі даних (потім вибирається користувач, у якого найбільший рівень відповідності).

2.3.2 Порівняння на основі глобальних ознак

Виконується визначення глобальних ознак (ядро, дельта). Кількість таких ознак і їх взаємне розташування дозволяє отримати класифікацію типу візерунку. Остаточне розпізнавання виконують на основі локальних ознак (число порівнянь буває на кілька порядків нижче для бази даних великих розмірів). Цей метод можна використовувати і в цілях, відмінних від впізнання або автентифікації.

2.3.3 Метод на основі графів

Початкове зображення відбитка пальця перетворюється в зображення поля орієнтації папілярних ліній. На ньому помітні області з однаковою орієнтацією ліній, тож можна провести кордони між зазначеними областями. Потім визначають центри цих областей і виходить граф. Подальші дії схожі на попередній метод – порівняння за локальними ознаками.

2.4 Порівняльний аналіз методів порівняння відбитків

Виходячи з вищесказаного, для порівняльного аналізу методів порівняння відбитків складена Таблиця 2.1, у якій наведено переваги та недоліки кожного з методів.

Таблиця 2.1 – Порівняльний аналіз методів порівняння відбитків

Метод	**Переваги**	**Недоліки**
Локальні ознаки	Чіткість алгоритму, однозначність результату, велика варіативність, різноманіття характеристик	Час виконання алгоритму, складність з точки зору створення робочого алгоритму
Глобальні ознаки	Простота використання, можливість використання без спеціального обладнання, «на око»	Є «передмовою» для першого методу, без нього може бути неоднозначним
Метод графів	Проста і зрозуміла математична модель, однозначність результатів	Мала варіативність, дуже багато часу на обробку

2.5 Висновки за розділом

В другому розділі розглянуто основні дактилоскопічні характеристики відбитків пальців, стандарти в сфері дактилоскопії. Окрім цього, проаналізовано відомі методи порівняння відбитків пальців, виявлено їх переваги і недоліки, на базі яких було проведено порівняльний аналіз методів порівняння відбитків пальців в дактилоскопії.

Виходячи з аналізу, можна зробити висновок, що найбільш оптимальним є найбільш розповсюджений метод порівняння за локальними ознаками. Такий висновок слідує з того, що даний метод має велику варіативність і велику кількість однозначних характеристик для порівняння, які можна комбінувати, створюючи власний, кастомізований алгоритм порівняння.

3 РОЗРОБКА ІНФОРМАЦІЙНОЇ ТА ФУНКЦІОНАЛЬНОЇ СТРУКТУРИ КОМПЛЕКСУ

3.1 Загальна структура комплексу

Демонстраційний комплекс біометричної аутентифікації за відбитками пальців було вирішено організувати наступним чином: три незалежних один від одного режими, кожний із яких виконує свої функції (Рис.3.1).

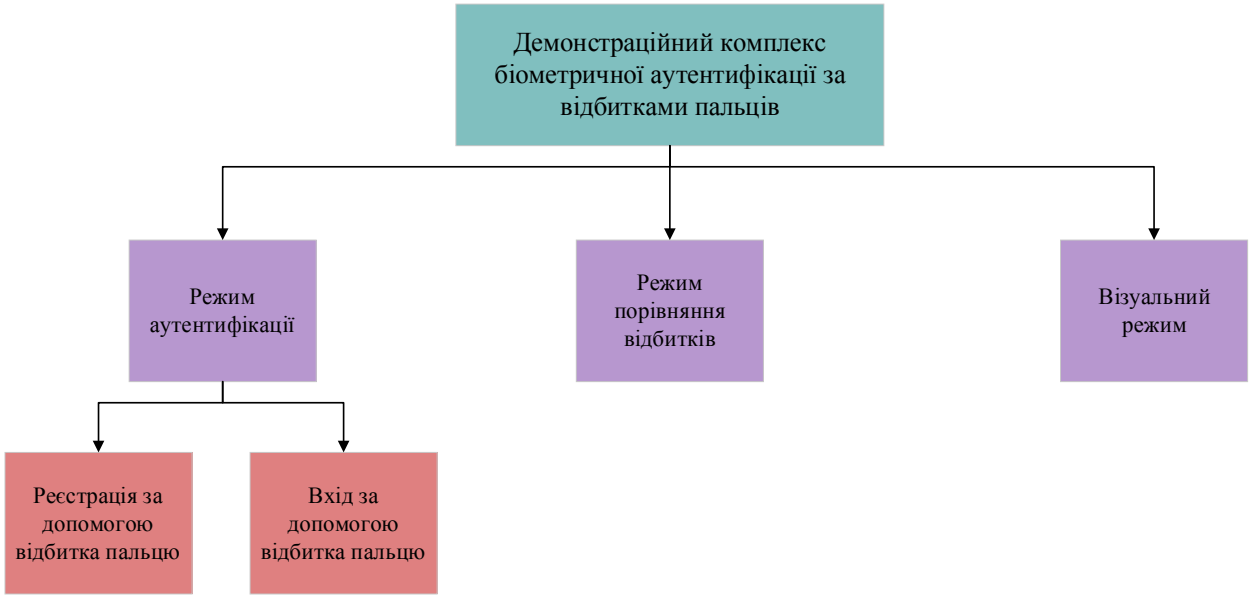

Рисунок 3.1 – Загальна структура демонстраційного комплексу

Як можна побачити з Рис.3.1, в комплексі присутні наступні режими: режим аутентифікації (до якого входять реєстрація за відбитком пальця та вхід за відбитком пальця), режим порівняння відбитків та візуальний режим. Для кращого розуміння розглянемо кожен із них більш детально.

3.2 Структура режиму аутентифікації

До основних елементів комплексу біометричної аутентифікації, що розроблюється, віднесено:

- зразок біометричної характеристики;
- блок обробки знятих біометричних даних;
- контрольний шаблон біометричної характеристики користувача (КШ);

- база даних еталонних шаблонів користувачів системи;
- еталонний шаблон біометричної характеристики користувача (ЕШ);
- блок порівняння контрольного та еталонного зразків.

Опис основних компонентів системи представлено в Таблиці 3.1

Таблиця 3.1 - Опис елементів комплексу

№	Елемент комплексу	Опис елементу
1	2	3
1	Зразок характеристики	Являє собою логін користувача системи і зображення відбитку пальця.
2	Обробка	Виконує формування контрольного шаблону користувачів із отриманого зразка біометричної характеристики і логіну – реалізується програмно, як частина програмного комплексу системи.
3	Контрольний шаблон (КШ)	Контрольним шаблоном є логін користувача та хеш відбитку пальця.
4	База даних	Базою даних є текстовий файл «dataBase.txt», у якому зберігаються логіни користувачів системи та відповідні їм відбитки у хешованому вигляді.
5	Еталонний шаблон (ЕШ)	Відповідає контрольному шаблону.
6	Порівняння	Являє собою реалізацію порівняння логінів та хешованих відбитків пальцю, на підставі якого виноситься рішення про вдалу або невдалу аутентифікацію.

Інформаційна структура системи аутентифікації на основі відбитку пальця представлена на Рис.3.2.

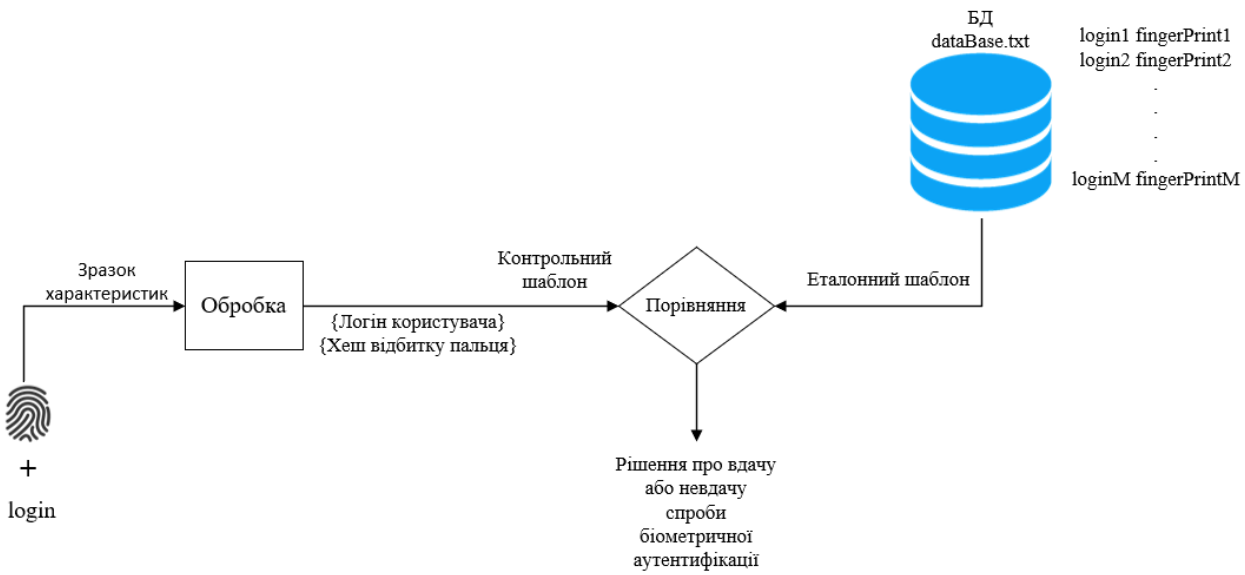

Рисунок 3.2 - Інформаційна структура режиму аутентифікації

Файл «dataBase.txt» - база даних системи. Містить перелік логінів користувачів, які зареєструвались у системі, використовуючи логін і відбиток пальця, та відповідний логіну відбиток пальця у вигляді хеша. Розглядаються системою, як легітимні.

Структуру файлу «dataBase.txt» представлено на Рис.3.3.

dataBase.txt

```
1  "login", "fingerPrint"
2
3  "ilan","B05F170CB19F7A135CB58989C540EA43"
4  "vika","99D360E90228E8227388B75CBF67B96E"
5  "denis","21423DD3E58D1E7CE095DD4D371CE4EC"
6  "pugna2000","CC22BF2CE601EEA30A899CA9417768E7"
7  "rexxar","95664F21A80CA32469A96119398F7C10"
```

Рисунок 3.3 – Структура файлу бази даних «dataBase.txt»

При реєстрації у системі за відбитком пальця для кожного користувача створюється пара “login”-“fingerPrint”. Призначенням даного файлу є

збереження еталонного шаблону користувача для можливості подальшого використання при проходженні аутентифікації.

Функціональна структура системи - це сукупність стійких операцій і процедур, що циклічно повторюються, а також їх зв'язків, орієнтованих на кінцевий результат роботи системи. Послідовність типових операцій і процедур при аутентифікації по відбитку пальця представлена на Рис. 3.4.

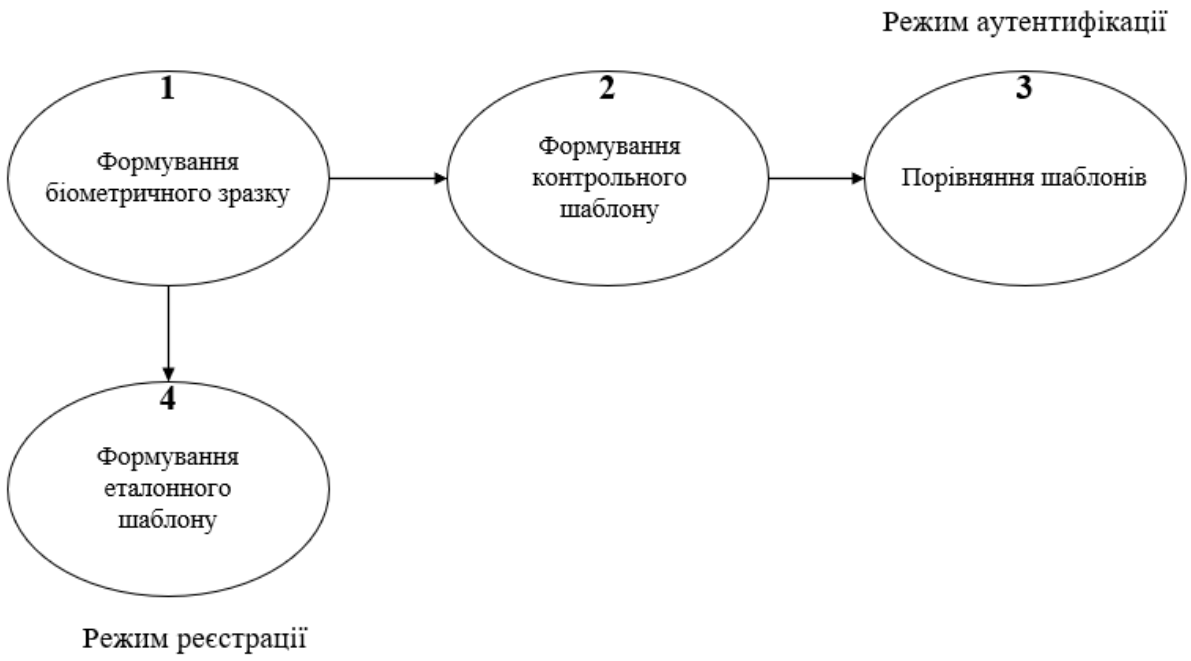

Рисунок 3.4 - Послідовність типових процедур при аутентифікації за відбитком пальця

Перелік процедур, які мають бути у системі для її функціонування (див. Рис. 3.4).

1 – Формування зразку біометричних характеристик:

Вхідні дані: логін користувача системи, відбиток пальцю у форматі *.tif.

Вихідні дані: логін користувача системи, хешований відбиток пальцю.

2 – Обробка сформованого зразка для формування контрольного шаблону користувача:

Вхідні дані: зразок біометричної характеристики.

Вихідні дані: контрольний шаблон користувача.

3 – Порівняння контрольного та еталонного шаблонів:

Вхідні дані: контрольний та еталонний шаблони користувача.

Вихідні дані: рішення про вдалу або невдалу спробу аутентифікації.

4 – Формування еталонного шаблону та збереження його у файл БД:

Вхідні дані: логін користувача системи, відбиток пальцю у форматі *.tif.

Вихідні дані: еталонний шаблон користувача.

3.3 Структура режиму порівняння відбитків

У цьому режимі реалізовано порівняння двох відбитків пальцю по особливих точках (мінуціях). Структура цього режиму зображена на Рис.3.5.

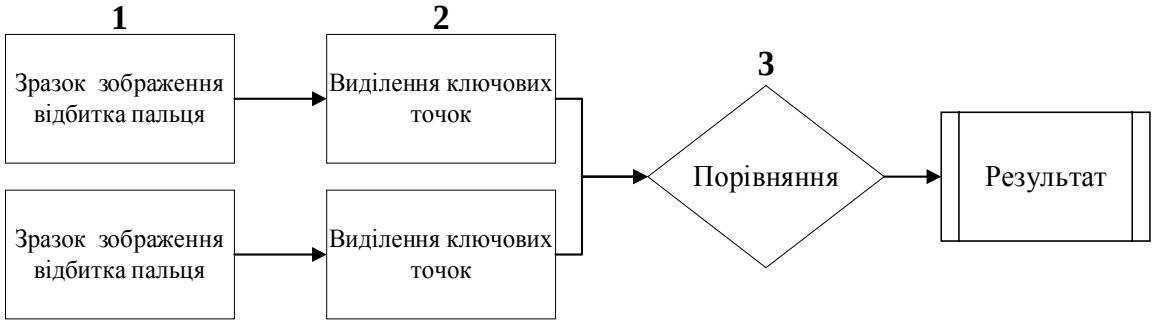

Рисунок 3.5 – Структура режиму порівняння відбитків

Перелік процедур у режиму порівняння відбитків (див. рис.3.5)

1 – Формування зразку біометричних характеристик:

Вхідні дані: відбиток пальцю у форматі *.tif.

Вихідні дані: зразок біометричних характеристик.

2 – Виділення ключових точок:

Вхідні дані: зразок біометричних характеристик.

Вихідні дані: виділені ключові точки (мінуції).

3 – Порівняння двох відбитків:

Вхідні дані: ключові точки (мінуції) двох відбитків пальців.

Вихідні дані: відсоток збігу мінуцій двох відбитків пальців.

3.4 Структура візуального режиму

Візуальний режим дозволяє з зображення відбитка пальцю виділити ключові точки і за допомогою графіки вималювати їх. Структура візуального режиму зображена на Рис.3.6.

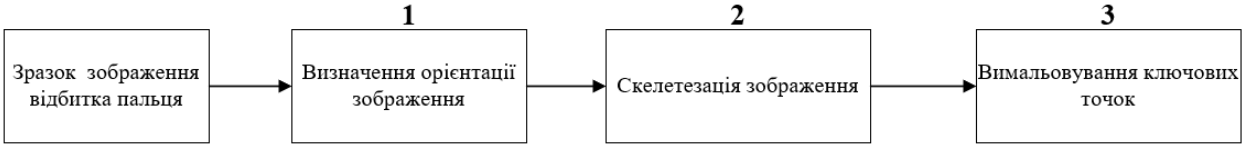

Рисунок 3.6 – Структура візуального режиму

Перелік процедур у візуальному режимі (див. рис.3.6)

1 – Визначення орієнтації зображення:

Вхідні дані: відбиток пальцю у форматі *.tif.

Вихідні дані: зображення із визначеною орієнтацію зображення.

2 – Скелетезація зображення:

Вхідні дані: зображення із визначеною орієнтацію зображення.

Вихідні дані: скелетезоване зображення відбитку пальця.

3 – Вимальовування ключових точок:

Вхідні дані: скелетезоване зображення відбитку пальця.

Вихідні дані: зображення ключових точок на відбитку пальця.

3.5 Висновки за розділом

В даному розділі було представлено структуру демонстраційного комплексу, що розробляється. Він складається із трьох незалежних один від одного режимів, кожен із яких реалізує в собі окремі функції. Окрім цього, були приведені інформаційна структура комплексу, опис елементів демонстраційного комплексу, функціональні структури кожного з режимів та структура файлу бази даних, описані вхідні і вихідні дані окремо для кожного з режимів.

4 РОЗРОБКА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ КОМПЛЕКСУ

4.1 Вибір засобів реалізації демонстраційного комплексу

Для реалізації засобу демонстрації біометричної аутентифікації за відбитками пальців мною вибрана середа розробки Visual Studio 2019, мова програмування C#, тип проекту WinForms.

Середовище розробки Visual Studio 2019 було обрано по декількох критеріях:

- підтримка мови C#;
- інтуїтивно зрозумілий інтерфейс;
- можливості графічного редактору, який підходить до задачі.

Так як усі критерії задовільнено — середовищем розробки було обрано саме Visual Studio 2019.

Мова програмування C# була обрана основною мовою розробки даного проекту з огляду на функціонал, який підтримує дана мова, операційні системи, які підтримуються та простоту вивчення.

Загалом — функціонал C# найкраще підходить під дану розробку, за рахунок простої реалізації основних принципів ООП роботи з аналізом зображень та функцій роботи з базами даних.

Для реалізації функцій виділення ключових точок і порівняння відбитків за ними був використаний фреймворк Fingerprint Recognition Framework для C#, який поширюється за ліцензією The Code Project Open License (CPOL).

4.2 Діаграма компонентів

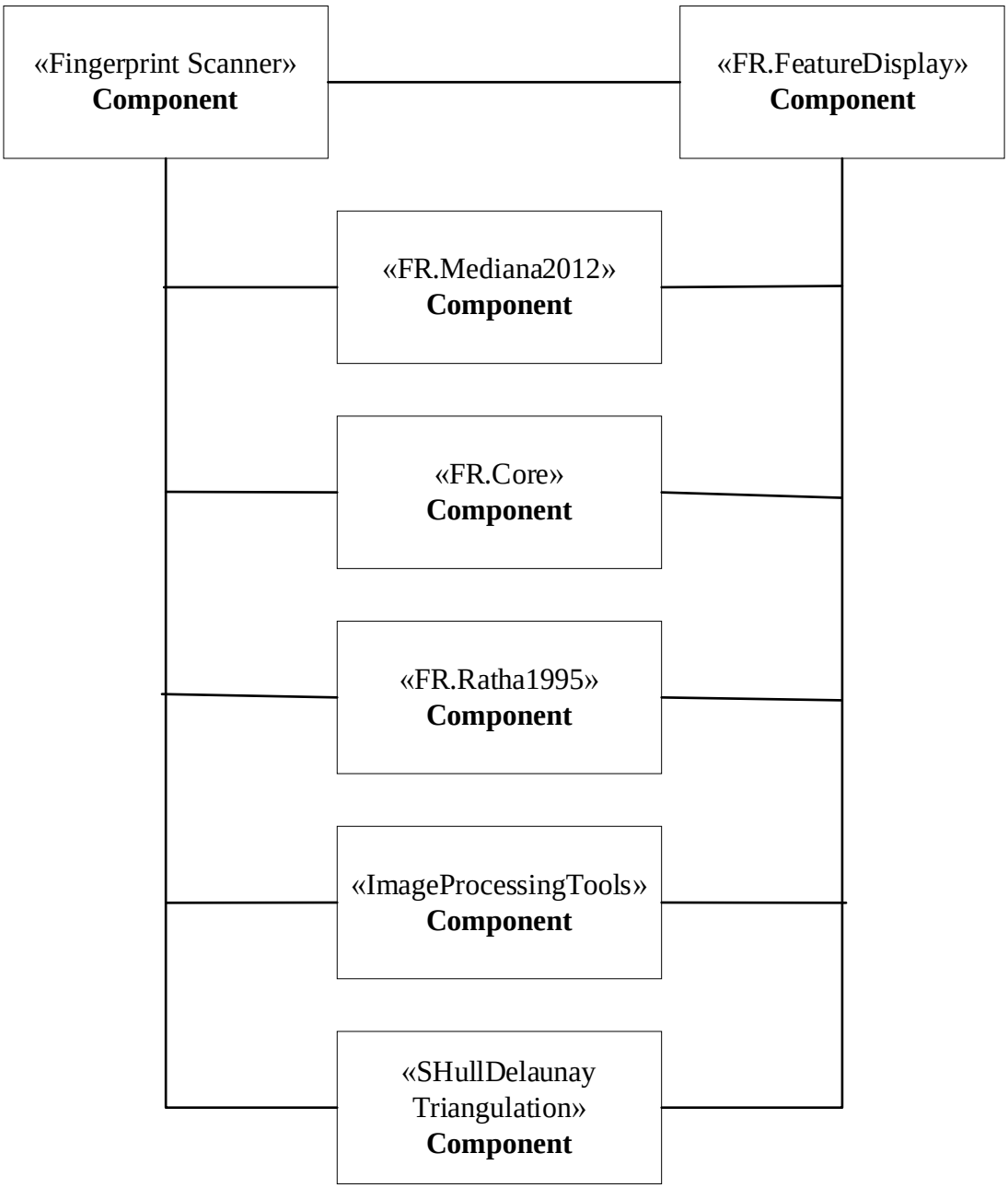

Рисунок 4.1 - Діаграма компонентів програмного продукту

Як видно з Рис. 4.1., програмний продукт складається з 7 компонентів, кожний з яких представлений окремим проектом. Для більш детального розуміння слід опуститися на рівень глибше і розглянути кожний проект окремо, а точніше спроектувати та розробити діаграму класів для кожного проекту, аби отримати розуміння про внутрішню структуру програмного забезпечення для порівняння відбитків пальців.

4.3. Діаграми класів

4.3.1 Діаграма класів проекту fingerprintScaner

Класи проекту **fingerprintScaner** представлені у Таблиці 4.1.

Таблиця 4.1 – Класи проекту **fingerprintScaner**

Назва класу	**Призначення класу**
MainApp	Головна форма додатку
authentication	Форма вибору реєстрації або входу до системи за відбитком пальця
registration	Форма реєстрації за відбитком пальця
enter	Форма входу до системи за відбитком пальця
match	Форма порівняння двох відбитків пальця за особливими точками

Діаграма класів проекту **fingerprintScaner** представлена нижче (Рис.4.2).

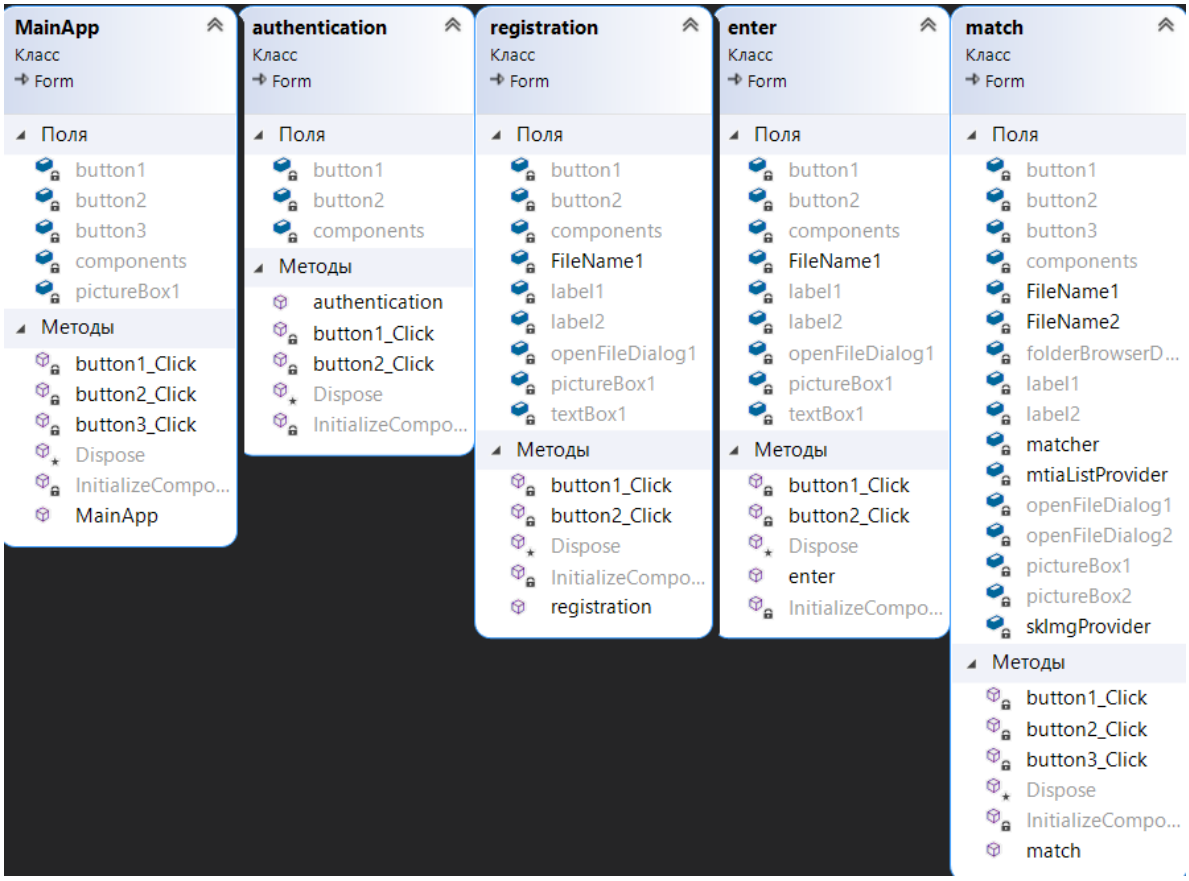

Рисунок 4.2 - Діаграма класів проекту **fingerprintScaner**

4.3.2 Діаграма класів проекту FR.FeatureDisplay

Проект складається з одного класу-форми, який несе в собі функціонал виділення графічного зображення особливих точок на зображенні відбитка пальця (Рис.4.3).

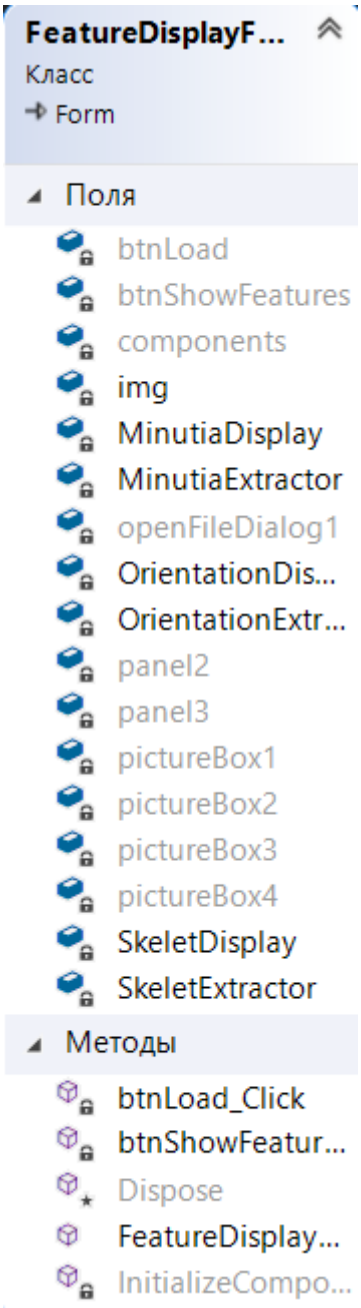

Рисунок 4.3 - Діаграма класів проекту FR.FeatureDisplay

4.3.3 Діаграма класів проекту FR.Medina2012

Проект складається з семи класів, які несуть в собі функціонал порівняння двох відбитків пальців, пошуків точок порівняння, тощо (Рис.4.4).

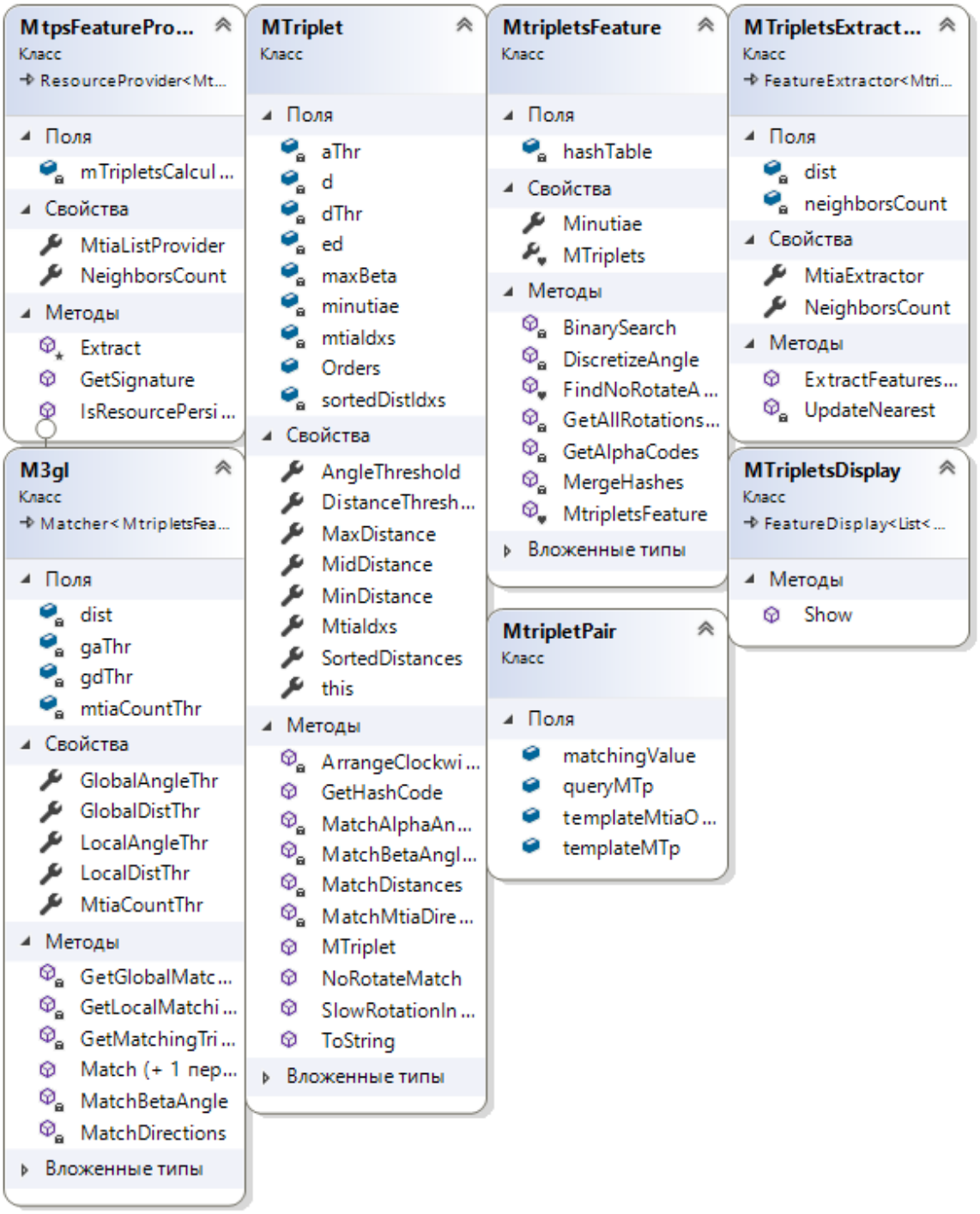

Рисунок 4.4 - Діаграма класів проекту FR.Mediana2012

4.3.4 Діаграма класів проекту FR.Core

Проект складається з двадцяти дев’яти класів і 12 інтерфейсів (Рис.4.5).

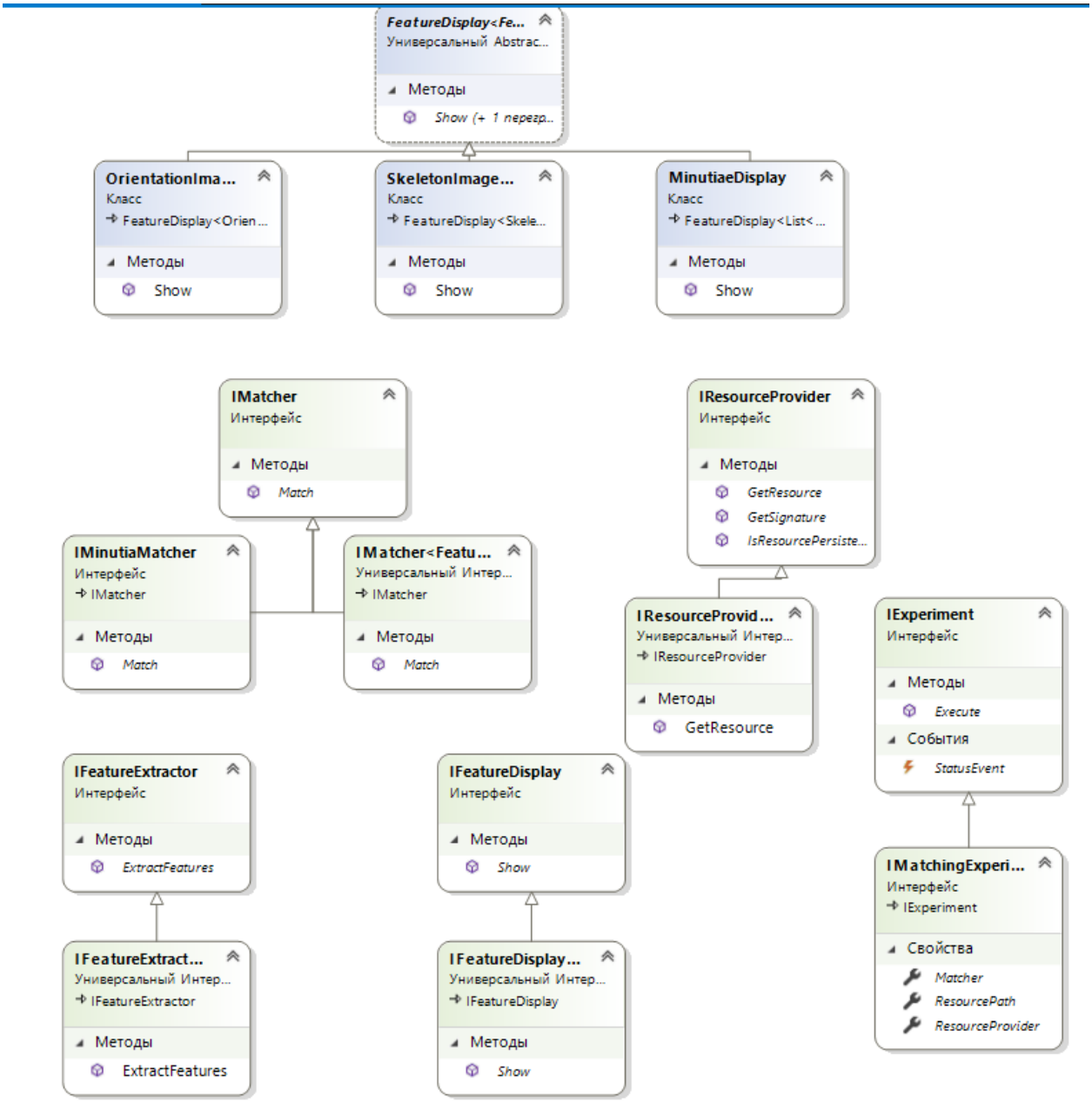

Рисунок 4.5 - Часткова діаграма класів FR.Core

4.3.5 Діаграма класів проекту FR.Ratha1995

Проект складається з трьох класів, які реалізують функціонал екстракторів ключових точок (Рис.4.6).

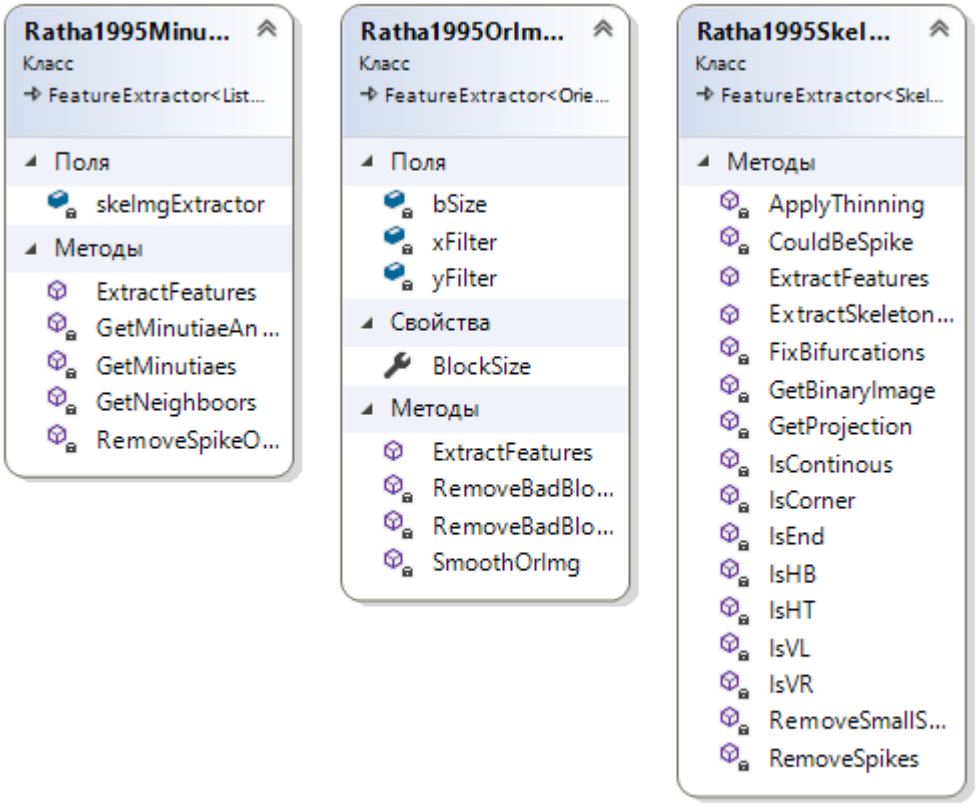

Рисунок 4.6 - Діаграма класів FR.Ratha1995

4.3.6 Діаграма класів проекту FR.ImageProcessingTools

Проект складається з шести класів, які реалізують функціонал роботи з зображеннями (Рис.4.7).

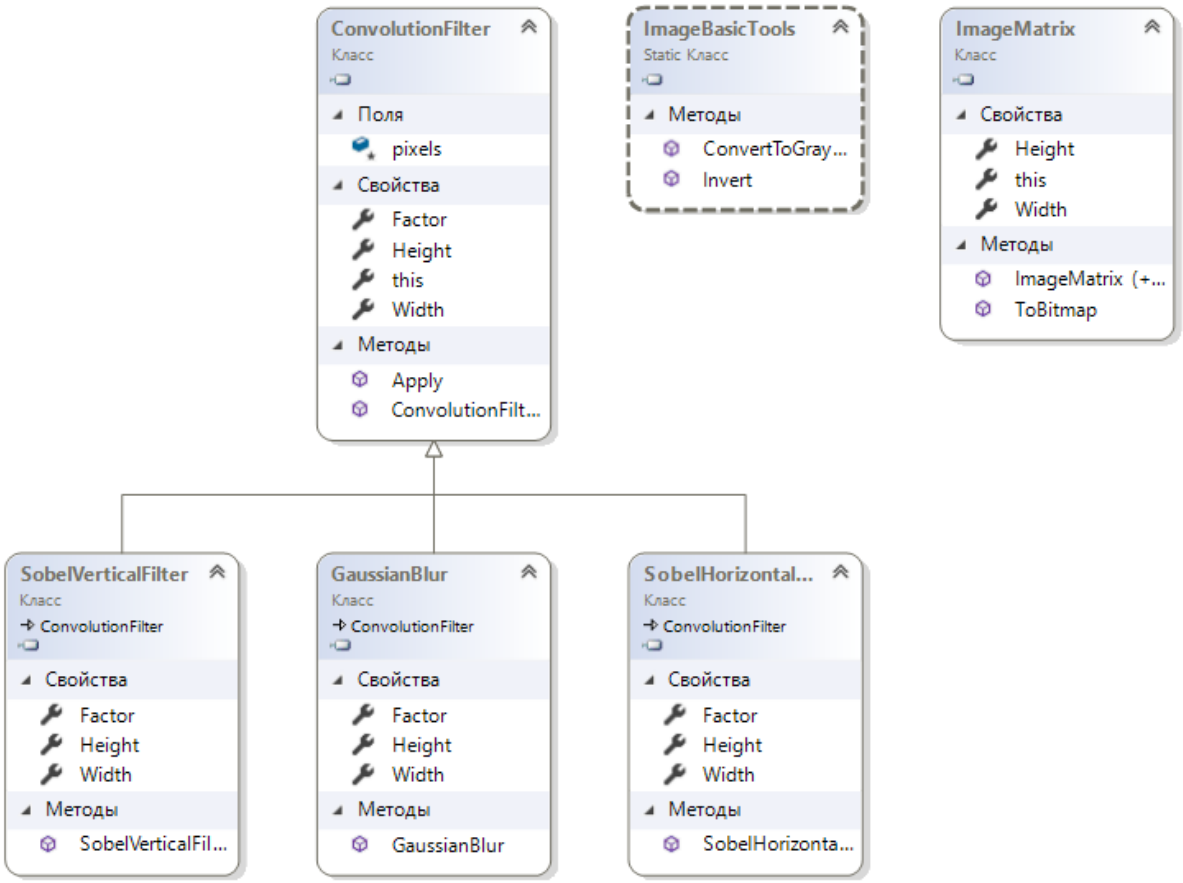

Рисунок 4.7 - Діаграма класів FR.ImageProcessingTools

4.3.7 Діаграма класів проекту FR. SHullDelaunayTriangulation

Проект складається з шести класів (Рис.4.8).

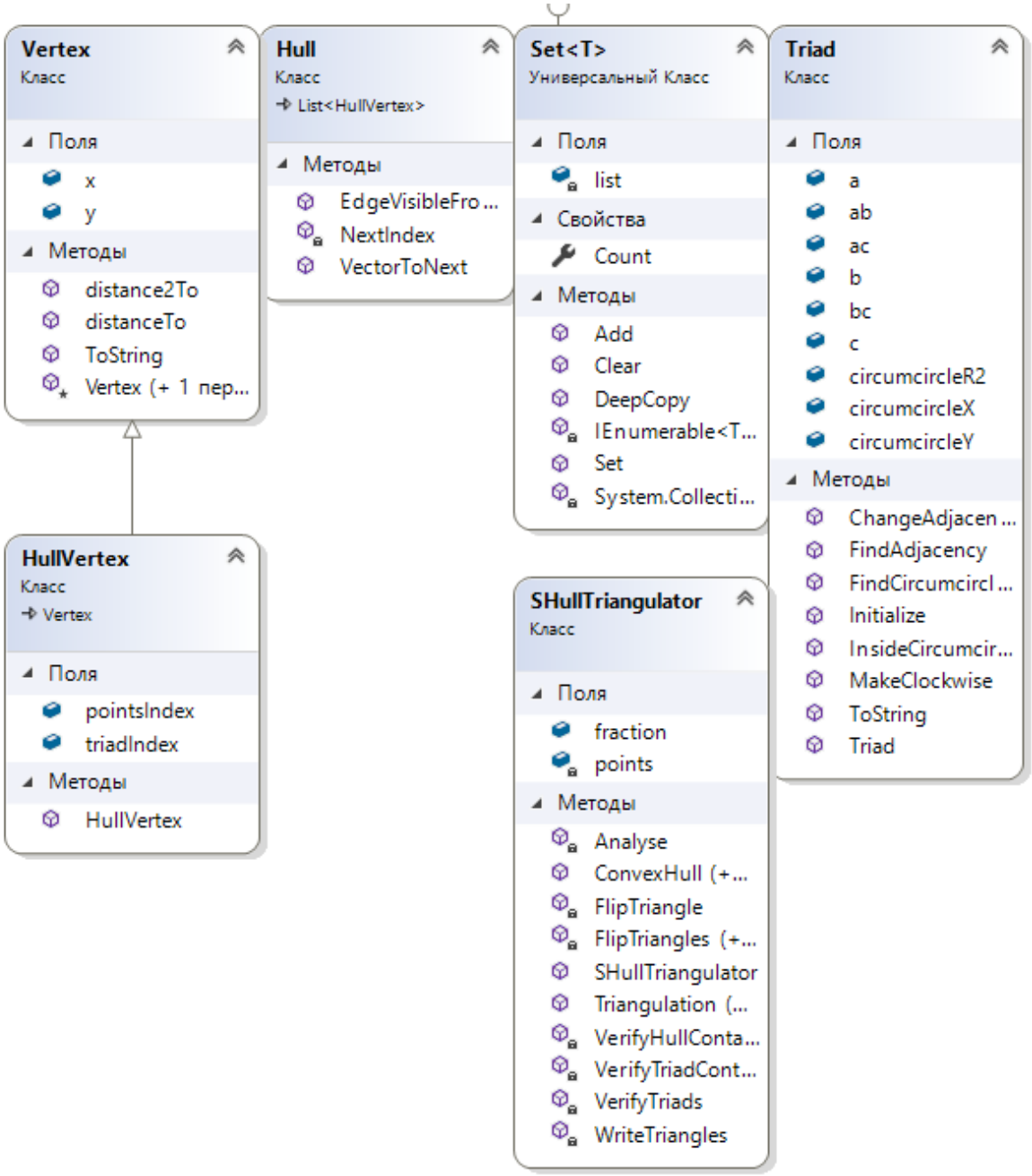

Рисунок 4.8 - Діаграма класів FR. SHullDelaunayTriangulation

4.4. Тестування ПЗ

4.4.1 Тестування режиму біометричної аутентифікації

Так як демонстраційний комплекс містить у собі три режиму (Рис.4.9), кожен з яких реалізує в собі різний функціонал, було вирішено протестувати кожен режим окремо.

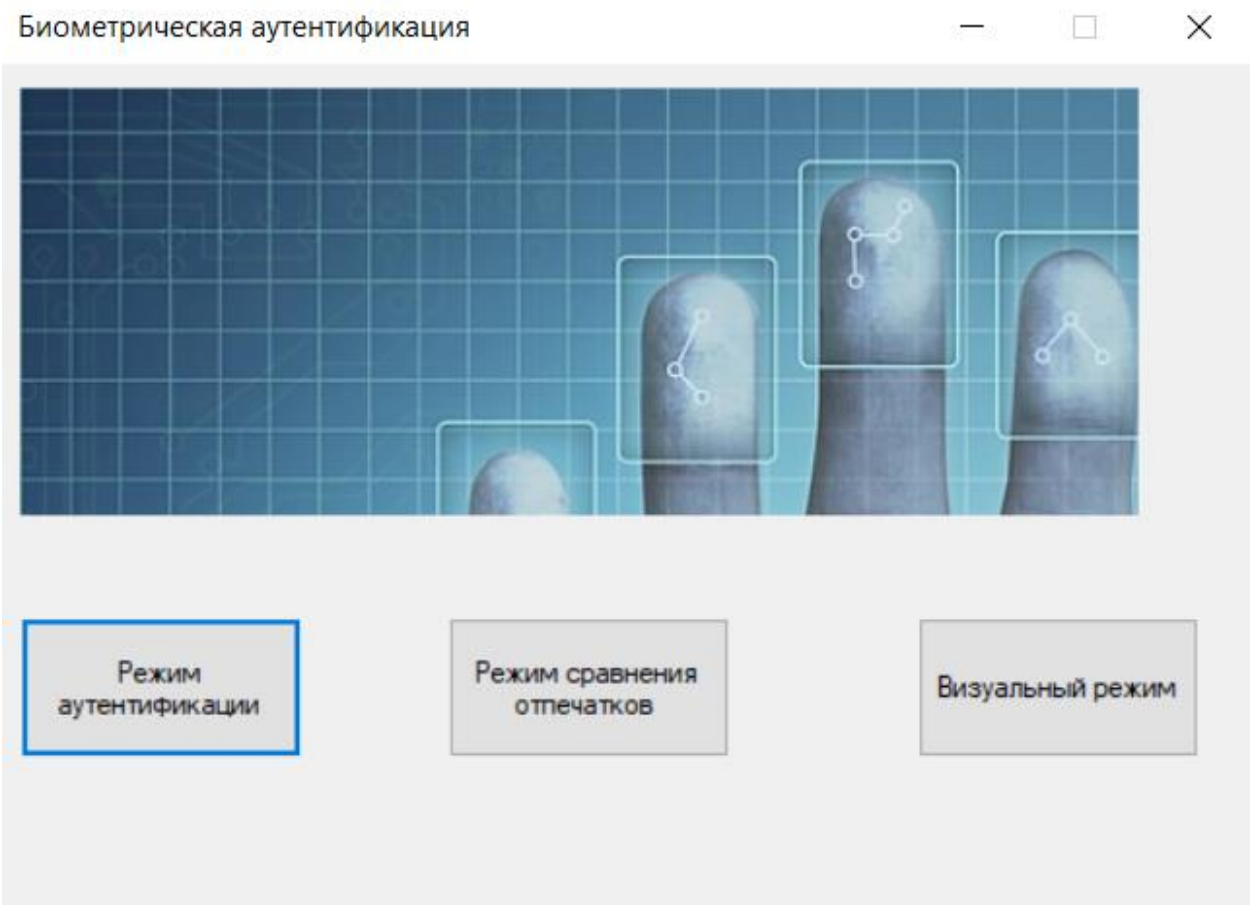

Рисунок 4.9 – Головна форма демонстраційного комплексу

Перейшовши до режиму аутентифікації, побачимо форму із двома кнопками: «Реєстрація за допомогою відбитка пальцю» та «Вхід за допомогою відбитка пальцю» (Рис.4.10).

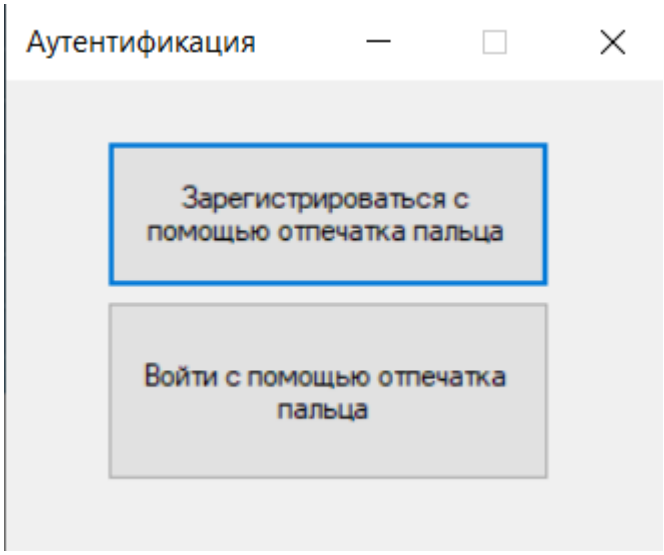

Рисунок 4.10 – Форма вибору реєстрації або входу за відбитком пальцю

Для початку треба зареєструватися у системі. Для цього необхідно ввести свій логін та обрати відбиток пальцю (Рис.4.11). Після цього обліковий запис буде зареєстровано та додано до бази даних (Рис.4.12). Зазначмо, що не можна зареєструватися, якщо не введено логін або не обрано відбиток пальця (Рис.4.13). Також не можна використовувати логін, котрий вже існує (Рис.4.14).

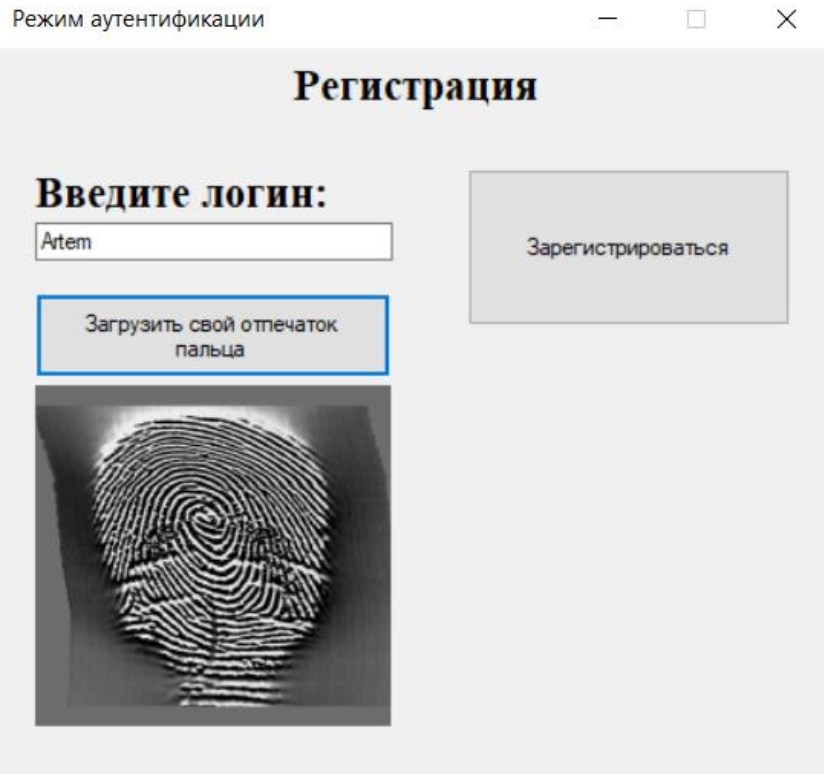

Рисунок 4.11 – Вибір логіну та відбитку пальця для реєстрації

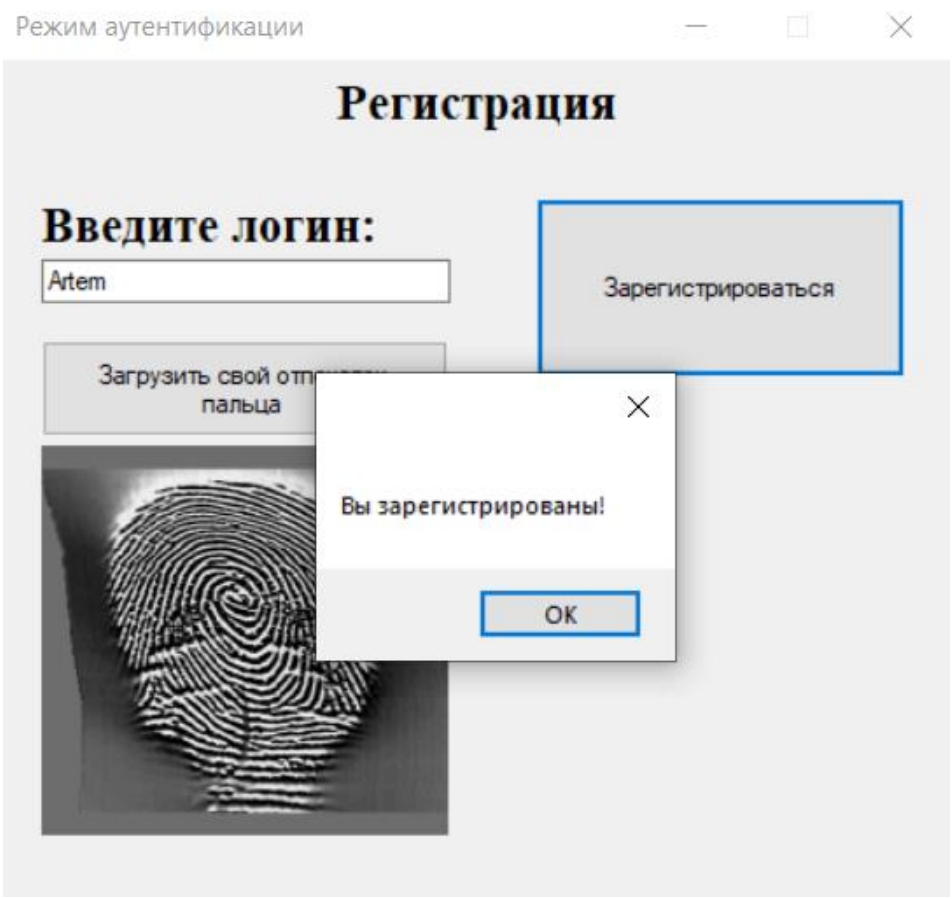

Рисунок 4.12 – Інформація про успішну реєстрацію у системі

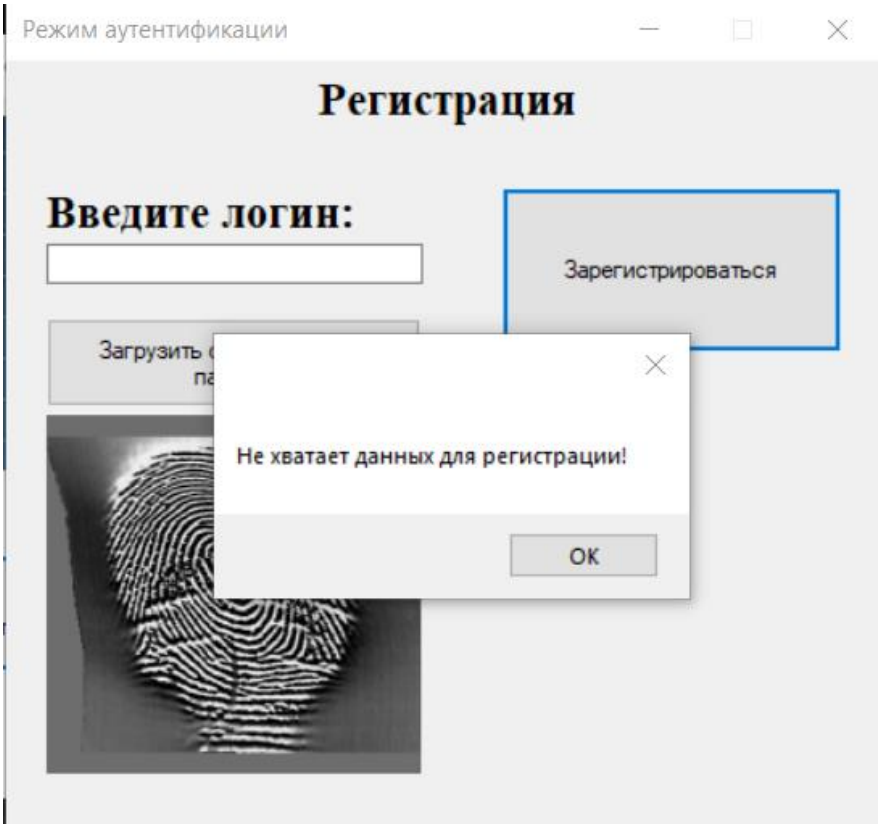

Рисунок 4.13 – Інформація про відмову реєстрації у системі через відсутність даних користувача

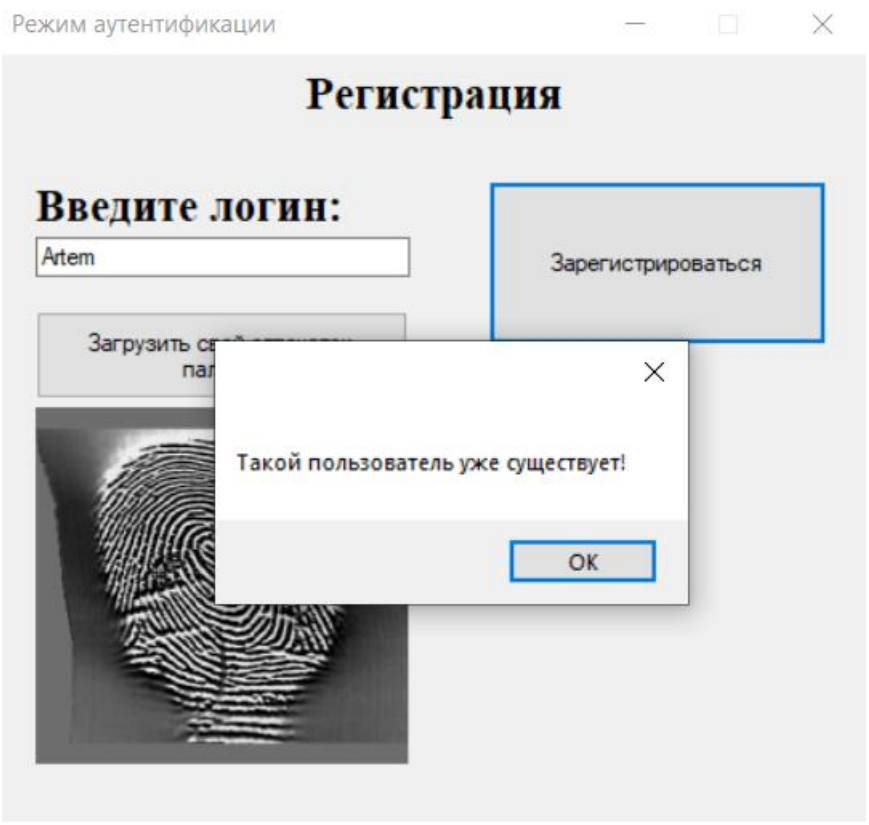

Рисунок 4.14 – Інформація про відмову реєстрації у системі через існуючий логін користувача

Після реєстрації можна входити до системи, використовуючи свій логін та відповідний йому відбиток пальця. Для цього необхідно вказати свої дані для входу, а саме логін та відбиток пальця, які використовувались для реєстрації у системі (Рис.4.15). Після перевірки коректності введених даних буде отримано повідомлення про успішну аутентифікацію у системі (Рис.4.16). Відмову у вході до системи можна отримати або через некоректні дані (Рис.4.17), або через відсутність даних користувача (Рис.4.18).

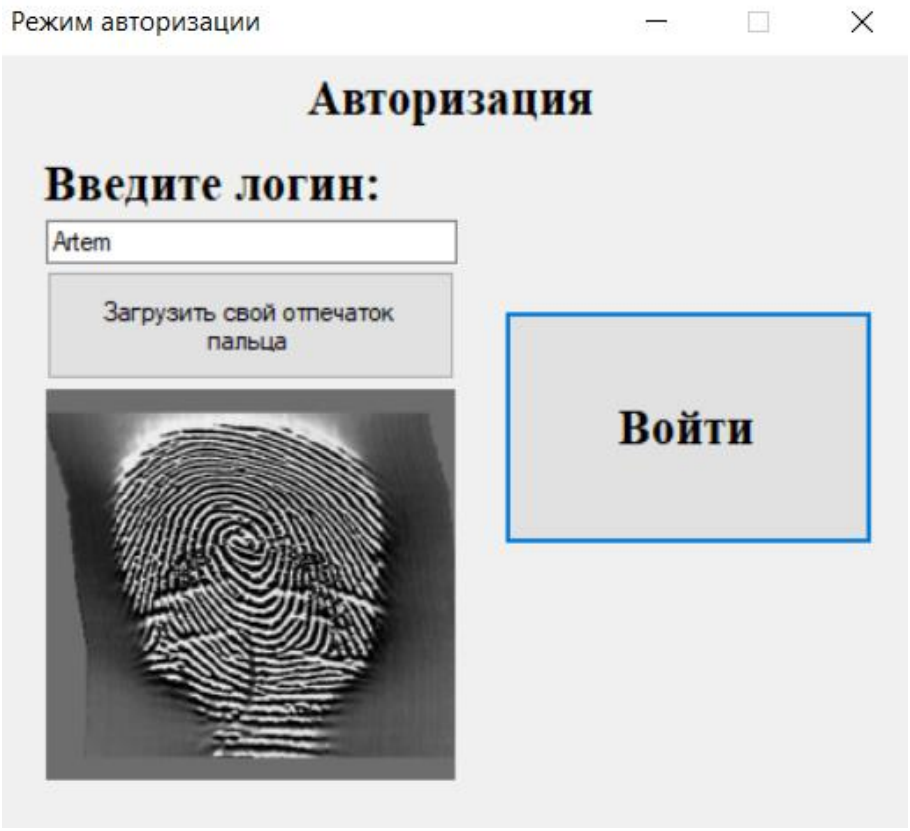

Рисунок 4.15 – Вхід до системи за логіном і відбитком пальця, які вказувалися при реєстрації

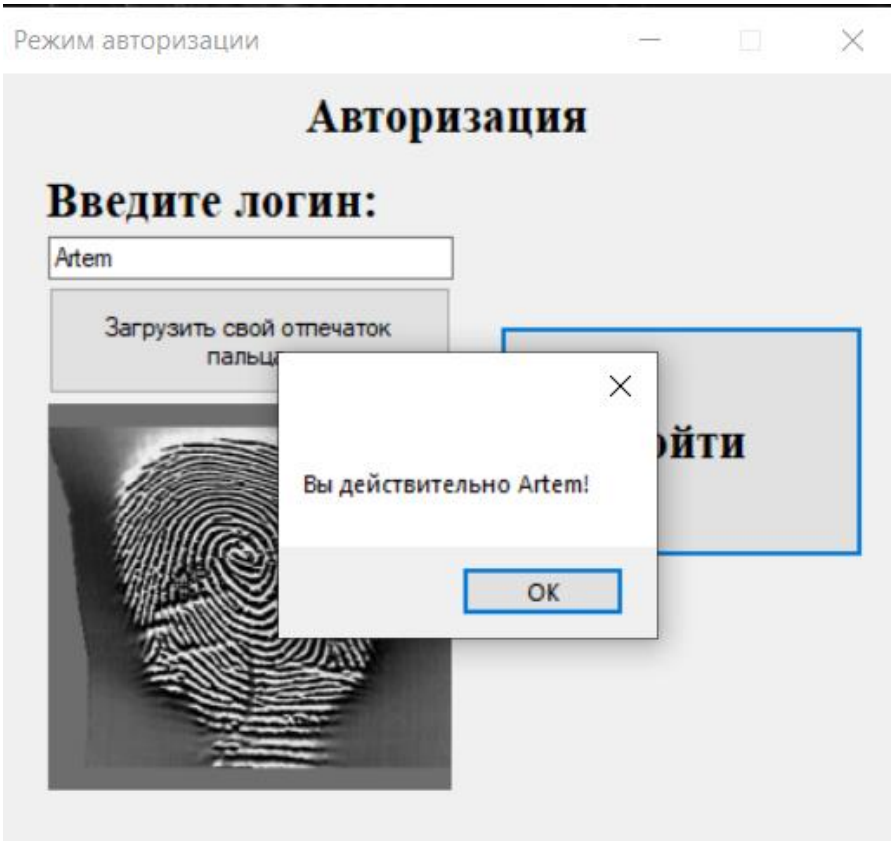

Рисунок 4.16 – Повідомлення про успішну аутентифікацію у системі

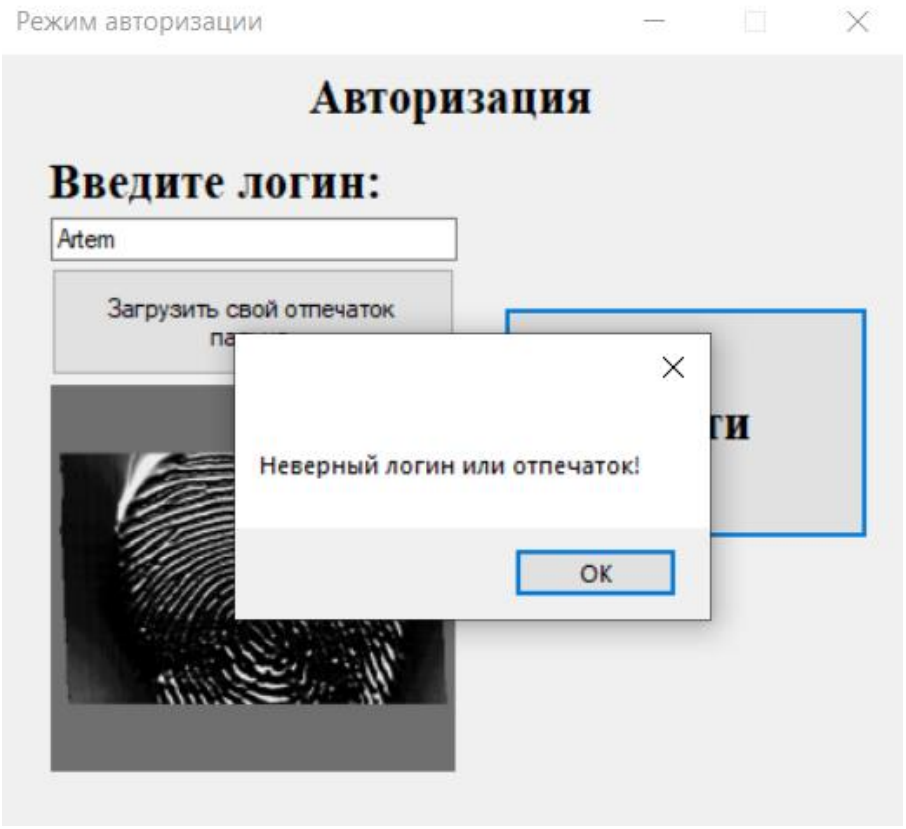

Рисунок 4.17 – Повідомлення про невдалу аутентифікацію у системі через некоректні дані

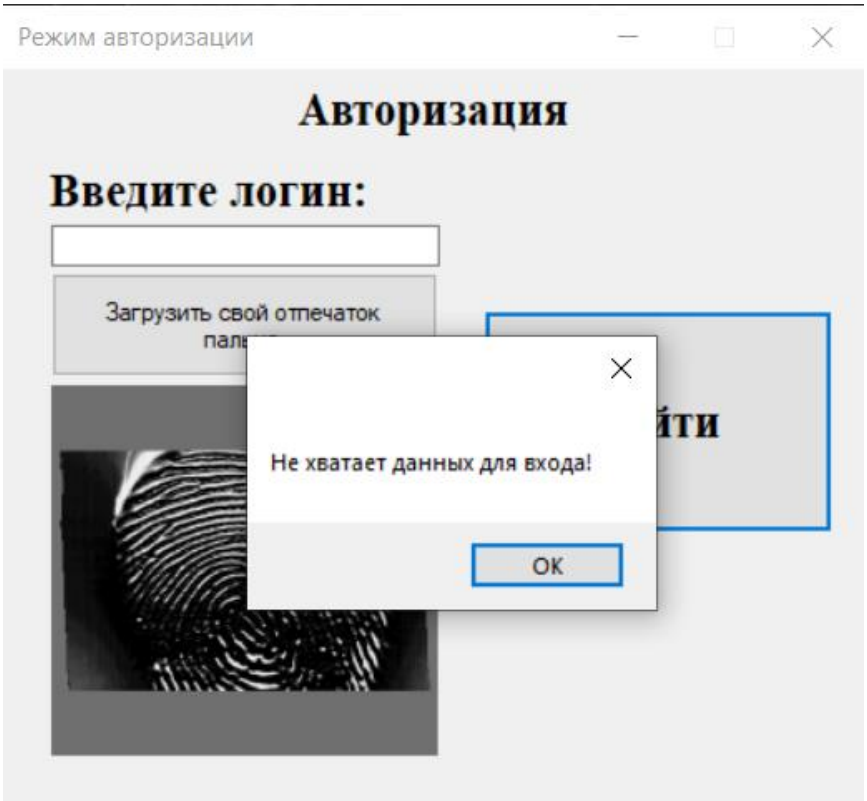

Рисунок 4.18 – Повідомлення про невдалу аутентифікацію у системі через відсутність даних

4.4.2 Тестування режиму порівняння відбитків

У режимі порівняння відбитків реалізовано функціонал порівняння двох відбитків пальця за особливими точками (мінуціями) (Рис.4.19). Для цього необхідно завантажити два зображення відбитка (Рис.4.20), та натиснути кнопку «Порівняти». Після цього буде показано відсоток збігу мінуцій двох відбитків пальцю (Рис.4.21).

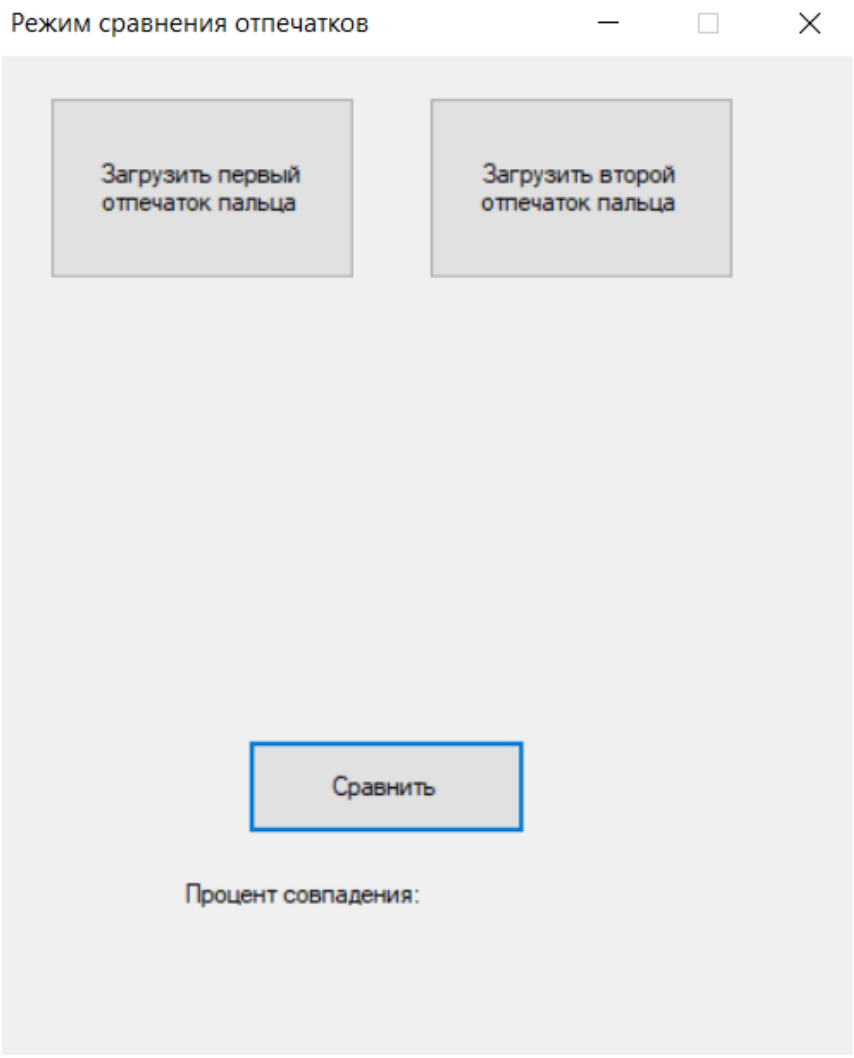

Рисунок 4.19 – Форма режиму порівняння відбитків

Рисунок 4.20 – Відбитки пальців для порівняння

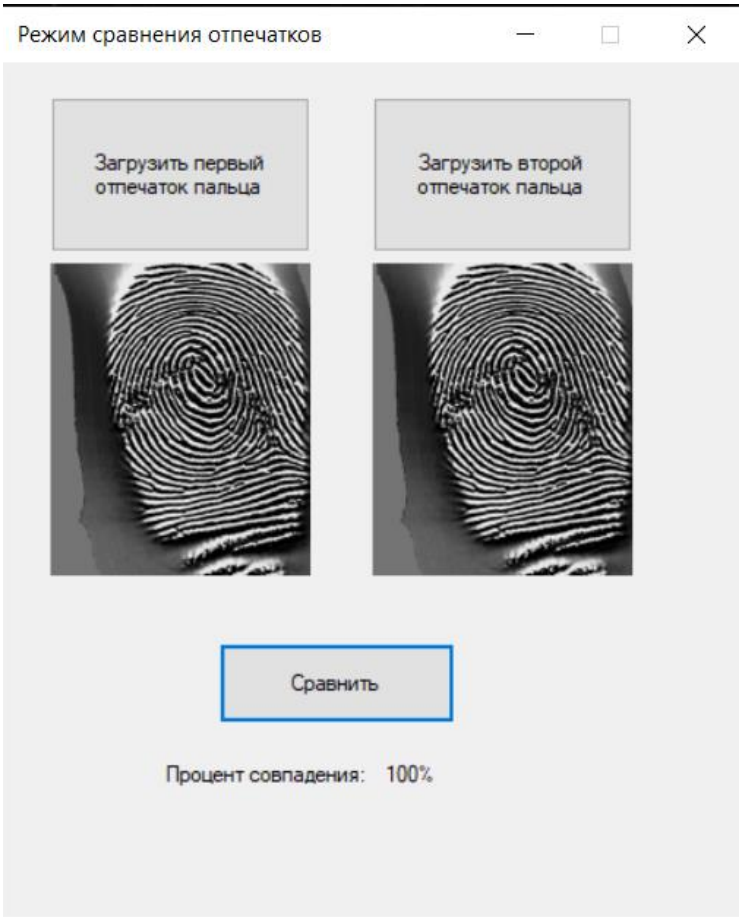

Рисунок 4.21 – Відсоток збігу мінуцій двох відбитків

4.4.3 Тестування візуального режиму

У візуальному режимі реалізований функціонал зображення особливих точок за допомогою графіки. Для завантаженого зображення визначається його орієнтація, скелетезація та виділення особливих точок (мінуцій) (Рис.4.22).

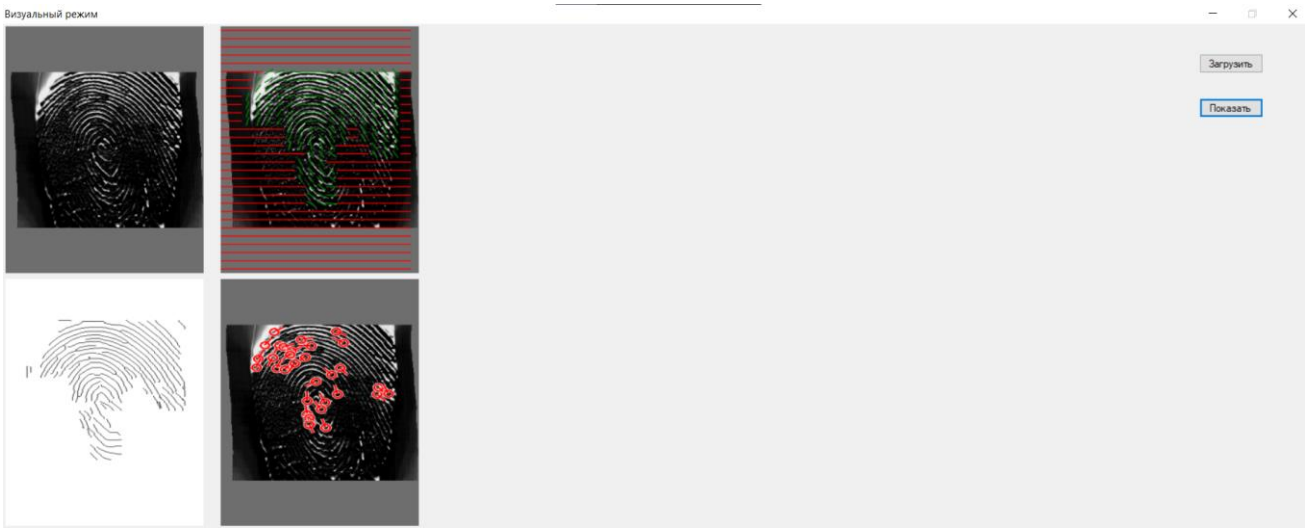

Рисунок 4.22 – Візуальний режим

4.5 Висновки за розділом

В даному розділі був описаний вибір засобів для програмної реалізації демонстраційного комплексу аутентифікації та його розробка, були представлені діаграми класів, які застосовувались для реалізації програмного продукту.

Демонстраційний комплекс був реалізований мовою C# у Visual Studio 2019 та представляє собою три незалежних один від одного режиму: режим аутентифікації, режим порівняння відбитків та візуальний режим. Програмний продукт було протестовано на коректність виконуваних ним функцій окремо за кожним режимом.

5. ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

5.1 Вимоги безпеки при виконанні робіт на робочому місці

Розділ розроблений на підставі Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями (далі – Вимоги), затверджених наказом Міністерства соціальної політики України від 14.02.2018 № 207, зареєстрованим в Міністерстві юстиції України 25.04.2018 за №508/31960 [11].

Розділ встановлює мінімальні вимоги безпеки та захисту здоров'я, яких необхідно дотримуватись під час здійснення роботи, пов'язаної з використанням екранних пристроїв, чиї робочі місця обладнані екранними пристроями незалежно від їхнього типу та моделі.

До роботи з екранними пристроями допускаються особи (для персоналу, робочі місця яких обладнані екранними пристроями (відеодисплейними терміналами, далі – ВДТ) на основі електронно–променевих трубок), які пройшли медичний огляд відповідно до вимог «Порядку проведення медичних оглядів працівників певних категорій», затвердженого наказом Міністерства охорони здоров'я України від 21.05.2007 №246 [12], зареєстрованого в Міністерстві юстиції України 23.07.2007 за №846/14113, а також навчання і перевірку знань з питань охорони праці та безпечного використання екранних пристроїв відповідно до вимог Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці, затвердженого наказом Державного комітету України з нагляду за охороною праці від 26.01.2005 №15 [13], зареєстрованого в Міністерстві юстиції України 15.02.2005 за №231/10511.

Екранний пристрій може обладнуватись периферійними пристроями, що можуть включати модеми, сканери, друкувальні пристрої, багатофункціональні пристрої офісного (настільного) типу та іншим обладнання. Мінімальні заходи безпеки щодо експлуатації вказаного обладнанням також встановлюються цим

розділом. За умови дотримання Вимог та цього розділу робота з екранними пристроями, не належить до категорії із шкідливими та небезпечними умовами праці.

В окремих випадках, у разі наявності в експлуатації копіювально-розмножувальної техніки промислового типу, до роботи на такому обладнанні допускається персонал, який має відповідну професійну підготовку, після попереднього медогляду, навчання та перевірки знань з питань охорони праці. Вказана професія, відповідно до п.114 «Переліку робіт з підвищеною небезпекою» [14], затвердженого наказом Держнаглядохоронпраці України 26.01.2005 №15, відноситься до категорії робіт з підвищеною небезпекою. Заходи безпеки під час роботи на вказаній категорії обладнання обумовлюється окремою інструкцією для професії та виду робіт на конкретному обладнанні.

Вимоги безпеки до робочих місць працівників з екранними пристроями:

- Робочі місця працівників з екранними пристроями повинні мати такі розміри, щоб працівники мали простір для зміни робочого положення та рухів;
- Освітлення робочого місця працівника з екранними пристроями має бути організовано таким чином, щоб створювався контраст відповідно до ДСП 3.3.2.007-98 [15].
- Мікроклімат на робочих місцях повинен підтримуватися відповідно до «Санітарних норм мікроклімату виробничих приміщень» ДСН 3.3.6.042-99 [16].
- Рівні шуму на робочих місцях осіб, які працюють з екранними пристроями, мають відповідати вимогам «Санітарних норм виробничого шуму, ультразвуку та інфразвуку» ДСН 3.3.6.037-99 [17], затверджених постановою Головного державного санітарного лікаря України від 01 грудня 1999 року № 37.
- Робочий стіл або робоча поверхня повинні бути достатнього розміру та мати поверхню з низькою відбивною здатністю, допускати гнучкість під

час розміщення екрана, клавіатури, документів і відповідного устаткування. Висота робочої поверхні столу має бути в межах 680 – 800 мм, а ширина – забезпечувати можливість виконання операцій в зоні досяжності моторного поля. За необхідності може використовуватись окрема підставка або регульований стіл для розміщення екрана.

- Робоче крісло має бути стійким і дозволяти працівнику з екранними пристроями легко рухатися та займати зручне положення.

При користуванні екранними пристроями, є неприпустимим:

- виконувати ремонт або налагодження пристроїв під час роботи з ними;

- відключати захисні пристрої, самочинно проводити зміни у конструкції та складі екранних пристроїв або їх технічне налагодження;

- працювати з екранними пристроями, у яких є ознаки поламки;

- розташовувати екранні пристрої біля обігрівачів та предметів або обладнання з магнітними властивостями;

- самостійно усувати будь-які несправності;

- відкривати захисні кожухи і панелі пристроїв, роз'єднувати кабельні шнури.

Перед початком роботи працівник повинен:

- оглянути і привести в порядок робоче місце;

- відрегулювати місцеве освітлення так, щоб робоча зона була достатньо освітлена;

- встановити сидіння в положення, зручне для роботи, щоб при виконанні робочих операцій не приходилось робити зайвих рухів;

- перед включенням екранного пристрою необхідно зовнішнім оглядом переконатися в справності електрообладнання. Кабель не повинен мати пошкоджень ізоляції. Вилка і розетка повинні мати заземлення, розетка щільно укріплена на стіні, а кришка не повинна мати тріщин, підпалин.

У разі виявлення несправності обладнання, пристрою, засобів захисту тощо повідомити про це безпосереднього керівника та викликати ремонтну службу.

Під час роботи з екранними пристроями та їх периферійними пристроями можуть бути наступні небезпечні відхилення від їх нормального режиму роботи, а саме:

- нестабільне зображення на екрані, наявні миготіння;
- символи на екранних пристроях нечіткі, невідповідного розміру;
- устаткування, яке входить до робочої станції, виділяє надлишкове тепло;
- з’являється дим чи відчувається сильний запах.

Працівник повинен вимкнути комп’ютер, повідомити керівника і звернутися до фахівця з технічного обслуговування у таких випадках:

- при вмиканні на екрані не з’являється жодної інформації (екран порожній) або висвічуються нехарактерні символи, смуги тощо;
- при нагріві, появі нехарактерного шуму, запаху горіння в екранних пристроях та периферійних пристроях;
- при наявності електроструму на корпусі (різке пощипування на кінцях пальців).

Необхідно негайно повідомляти безпосереднього керівника про кожну виявлену серйозну та безпосередню небезпеку, будь-яке пошкодження захисних пристроїв, про несправності устаткування. Викликати ремонтну службу.

Під час роботи у положенні сидячи треба час від часу змінювати фіксовані робочі пози, робити короткочасні перерви. Щогодини необхідно робити перерву на 5-10 хв., а через 2 години - на 15 хв. Для підтримки тонусу м'язів рук, під час перерви рекомендується проводити гімнастичні вправи. Періодично рекомендується виконувати комплекс вправ для очей.

При завершенні роботи користувач повинен:

- завершити працюючі програми;
- ввійти в режим закінчення роботи;
- вимкнути екранний пристрій, системний блок, периферійне обладнання (за допомогою перемикача на корпусі обладнання);
- вимкнути стабілізатор напруги, якщо екранний пристрій підключається через стабілізатор;
- прибрати робоче місце;
- повідомити безпосереднього керівника про усі недоліки під час роботи з екранними пристроями, що були виявлені у процесі роботи;

5.2 Шкідливі виробничі фактори на робочому місці

Професійні захворювання - захворювання, у розвитку яких переважну роль відіграють несприятливі умови праці — професійні шкідливості. Характер професійних хвороб визначається особливостями механізму дії шкідливих виробничих факторів та їх поєднань на організм людини, а також сила і тривалість дії.

Згідно до «Порядка проведення медичних оглядів працівників певних категорій» [12]:

Програмісти повинні проходити медичний огляд 1 раз на рік лікарями невропатологом, офтальмологом та оториноларингологом, при цьому перевіряти загальні аналізи крові, Hb, тромбоцити, визначення гостроти зору, характер зору.

До професійних захворювань програмістів відносять:

- Виражені нейроциркуляторні порушення;
- Передпухлинний стан, схильний до переродження і рецидиву;
- Гострота зору с корекцією не менш як 0,5 на одному оці і 0,2 на другому;
- Аномалії рефракції: міопія 6,0 Д; гітерметропія більше 4,0 Д; астигматизм більше 2,0 Д;

- Глаукома;
- Відсутність бінокулярного зору;
- Виразний ністагм;
- Лагофтальм;
- Хронічні захворювання повік, кон’юктиви, рогівки, сльозовивідних шляхів;
- Захворювання зорового нерву, сіткивки.

Нажаль, повністю уникнути професійних захворювань можно лише одним кардинальним шляхом-перестати працювати. Однак, зменшити ризик появи таких хвороб, можна за допомогою оздоровчої фізкультури, мануальних терапій, а також ведення здорового способу життя. Потрібно завжди чітко дотримуватися режиму чергування праці і відпочинку, не допускати перевтоми, ефективно використовувати паузи в роботі для зміни роду діяльності.

Згідно до ДСН 3.3.6.042-99 [16], фізичні роботи порозділяють на легкі фізичні роботи (категорія Іа та Іб), фізичні роботи середньої важкості (ІІа та ІІб категорія) та важкі фізичні роботи (категорія ІІІ).

У своїй роботі я досліджую аутентифікацію за відбитками пальців, тому було проведено дослідження щодо стану відбитків пальців у працівників різних професій та встановлено залежність невдалих спроб біометричної аутентифікації в залежності від різновиду професії.

Зокрема, були проаналізовані наступні професії: категорії ІІб – професії зварювальника та ливарника; категорії ІІІ-професії коваля з ручним куванням та ливарника з ручним набиванням.

Як показав аналіз, чим вища категорія виконуваної роботи, тим більше навантаження на опорно-рухову, дихальну,серцево-судинну системи, шкіру.

Простежується пряма залежність: чим вище категорія виконуваної роботи, тим вищий відсоток невдалих спроб біометричної аутентифікації. Пов'язано це з тим, що пошкоджена важкою роботою шкіра читається комп’ютером гірше.

Наприклад, професія зварювальника, яка відноситься до категорії IIб, менш негативно вливає на папілярний візерунок пальців, ніж професія коваля з ручним куванням (категорія III), де приходиться мати справу з постійним стиранням шкіри рук, зокрема і папілярного візерунка, за котрим і проводиться біометрична аутентифікація.

5.3 Дії працівників в надзвичайних ситуаціях

Дії при пожежі регулює наказ «Про затвердження Правил пожежної безпеки в Україні» [18] 30.12.2014 № 1417 МВС.

У разі ознак горіння (диму, запаху гару, відчуття електричної напруги тощо), припиненні подачі електроенергії або виявленні будь-яких несправностей необхідно негайно відключити екранний пристрій від електричної мережі. Повідомити про те, що сталося безпосереднього керівника.

При виникненні небезпеки пожежі:

- усі споживачі електроенергії відключіть і вживайте заходів по запобіганню аварійній ситуації;

- негайно повідомте про це по телефону 101 пожежну охорону. При цьому назвіть місце виникнення пожежі, обстановку на пожежі, наявність людей, а також повідомте своє прізвище;

- повідомте про пожежу керівника чи відповідну компетентну посадову особу;

- якомога швидше почніть евакуацію людей;

- при можливості розпочніть гасіння пожежі наявними первинними засобами пожежогасіння, дотримуючись заходів безпеки гасіння;

- зустріньте підрозділи пожежної охорони, надайте їм допомогу у виборі найкоротшого шляху для під'їзду до осередку пожежі та до установки для підключення до водних джерел.

У разі пожежі безпосередній керівник зобов'язаний повідомити про те, що сталося, роботодавця. Якщо є потерпілі – надавати їм першу медичну допомогу, викликати швидку допомогу за телефоном 103.

При відсутності у потерпілих в пожежі дихання і пульсу необхідно робити йому штучне дихання і непрямий (зовнішній) масаж серця, звернувши увагу на зіниці. Розширені зіниці свідчать про різке погіршення кровообігу мозку. При такому стані необхідно негайно приступити до оживлення, після чого викликати швидку медичну допомогу.

При наданні домедичної допомоги розрізняють опіки чотирьох ступенів:

1) I ступінь (еритема) - почервоніння шкіри, набряклість і біль;

2) II ступінь (утворення пухирів) - сильний біль із інтенсивним почервонінням, відшаруванням епідермісу з утворенням міхурів, наповнених прозорою або каламутною рідиною;

3) III ступінь - некроз всієї товщі шкіри з утворенням щільного струпу, під яким перебувають ушкоджені тканини;

4) IV ступінь - обвуглення: виникає при впливі на тканини дуже високих температур (полум’я, розплавлений метал тощо); частіше при пожежах та аваріях на автотранспорті (ДТП), в літаках, нещасні випадки на шахтах; результат таких опіків – ушкодження м’язів, сухожилля, кісток.

ВИСНОВКИ

В магістерській дипломній роботі були розглянуті види аутентифікації, зокрема біометрична аутентифікація. Після порівняльного аналізу методів біометричної аутентифікації прийшли до висновку, що найоптимальнішим методом біометричної аутентифікації є аутентифікація за відбитками пальців.

Було досліджено та проаналізовано біометричну аутентифікацію за відбитками пальців. Проведено класифікацію і порівняльний аналіз методів порівняння відбитків пальців. Також були розглянути стандарти у сфері дактилоскопії.

Був спроектований демонстраційний комплекс аутентифікації за відбитками пальців,. Демонстраційний комплекс був спроектований на мові C# у середовищі Visual Studio з використанням фреймворку Fingerprint Recognition Framework для C#, який поширюється за ліцензією The Code Project Open License (CPOL), було зроблено тестування його функцій. Комплекс може працювати у трьох режимах: режимі аутентифікації, режимі порівняння відбитків пальців та у візуальному режимі.

В усіх цих режимах відбитки пальців порівнюються за локальними ознаками – мінуціями. Такий вибір було здійснено через те, що практика показує – відбитки пальців у різних людей можуть мати окремі однакові глобальні ознаки, проте абсолютно неможливо наявність однакових мікровізерунків мінуцій.

Таким чином, можна зробити висновок, що комплекс має готовий функціонал та готовий за використанням у навчальному процесі.

Результати дипломної роботи були опробовані на двох конференціях [19, 20].

ПЕРЕЛІК ПОСИЛАНЬ

1. Бастрикін А. І. Дактилоскопія. Знаки руки. / Бастрикін А. І., 2004.
2. Девід Ліон. Товариство спостереження: Моніторинг повсякденного життя / Девід Ліон. – Філадельфія, 2001.
3. Туляков С. Симетричні хеш-функції для мініцій відбитків пальців / С. Туляков, Ф. Фарук, Г. В.., 2005.
4. Хагхигат М. Дискриминантний кореляційний аналіз: Fusion в режимі реального часу для мультимодального біометричного розпізнавання / М. Хагхигат, М. Абдель-Мотталеб, В. Аналлабі., 2016.
5. Science Daily. Запитання, що виникли про системи Розпізнавання Іриси. – 12.
6. N. K. Ratha. Enhancing security and privacy in biometrics-based authentication systems, IBM systems Journal / N. K. Ratha, J. H. Connell, R. M. Bolle. – №40.
7. Шаров В. Біометричні методи комп'ютерної безпеки/ Владислав Шаров // ByteMag. – 2005. [Електронний ресурс] – Режим доступу: https://www.bytemag.ru/articles/detail.php?ID=6719
8. Попов М. Біометричні системи безпеки / Попов М.., 2011.
9. Клімакін С.П. Ера біометрії / Клімакін С.П, Петруненко А.А., Черномордик О.М.., 2006.
10. Задорожний В. Ідентифікація за відбитками пальців. Частина 1 / Задорожний В. // PC Magazine. – 2004. [Електронний ресурс] – Режим доступу: https://bms.ucoz.ru/statii/identifikacija_po_otpechatkam_palcev.pdf
11. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями» від 14.02.2018 № 207, затверджені наказом Міністерства соціальної політики України
12. «Про затвердження Порядку проведення медичних оглядів працівників певних категорій» від 21.05.2007 №246, затверджено наказом

Міністерства охорони здоров'я України
13. «Про затвердження Типового положення про порядок проведення навчання і перевірки знань з питань охорони праці та Переліку робіт з підвищеною небезпекою» від 26.01.2005 №15, затверджено наказом Міністерства соціальної політики України
14. НПАОП 0.00-4.12-2005 «Перелік робіт з підвищеною небезпекою» від 26.01.2005 №15, затверджено наказом Держнаглядохоронпраці України
15. ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми роботи з візуальними дисплейними терміналами електронно-обчислювальних машин» від 10.12.1998 №7, затверджено постановою Головного державного санітарного лікаря України
16. ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень» від 01.12.1999 №42, затверджено наказом Міністерства охорони здоров'я України
17. ДСН 3.3.6.037-99 «Санітарні норми виробничого шуму, ультразвуку та інфразвуку» від 01.12.1999 №37, затверджено постановою Міністерства охорони здоров'я України
18. «Про затвердження Правил пожежної безпеки в Україні» від 30.12.2014 №1417, затверджено наказом Міністерства внутрішніх справ України
19. Сокольський І.О. Дослідження та розробка засобів демонстрації аутентифікації за відбитками пальців / І.О. Сокольський // Всеукраїнська конференція студентів та молодих вчених. – 2020. – С. 24.
20. Сокольський І.О. Дослідження та розробка засобів демонстрації аутентифікації за відбитками пальців / І.О. Сокольский // XIV Міжнародна науково-практична конференція. – 2020.