

Міністерство освіти і науки України

Луцький національний технічний університет
(повне найменування вищого навчального закладу)

Факультет транспорту та механічної інженерії
(повне найменування факультету)

Кафедра прикладної механіки та мехатроніки
(повна найменування кафедри)

**КВАЛІФІКАЦІЙНА РОБОТА
ЗА СТУПЕНЕМ ВИЩОЇ ОСВІТИ «МАГІСТР»**

**ЗАСТОСУВАННЯ КОМП'ЮТЕРНО-
ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ОБРОБКИ
ЗОБРАЖЕНЬ ВІДБИТКІВ ПАЛЬЦІВ**

спеціальність 131 Прикладна механіка
(шифр і назва спеціальності)

освітня програма «Прикладна механіка»
(назва освітньої програми)

Виконав: здобувач вищої освіти
групи ІМм-21
Гончар Віталій Васильович

(підпис)

Керівник:
д.т.н., професор
Повстяной Олександр Юрійович

(підпис)

Кваліфікаційну роботу
допущено до захисту
«__» _____ 2025 р.
Гарант освітньої програми:
к.т.н., доцент
Четвержук Тарас Іванович

(підпис)

Луцьк – 2025 року

ЛУЦЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

Факультет *транспорту та механічної інженерії*

Кафедра *прикладної механіки та мехатроніки*

Ступінь вищої освіти: *магістр*

Галузь знань: *13 Механічна інженерія*

Спеціальність: *131 Прикладна механіка*

Освітня програма: *«Прикладна механіка»*

ЗАТВЕРДЖУЮ

Завідувач кафедри

Р. Г. Редько

« ___ » _____ 2025 р.

ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ ЗДОБУВАЧА ДРУГОГО (МАГІСТЕРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ

Гончара Віталія Васильовича

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи: *Застосування комп'ютерно-інформаційних технологій для*

обробки зображень відбитків пальців

Керівник роботи: *д.т.н., професор Повстяной Олександр Юрійович*

затверджені наказом закладу вищої освіти від «14» червня 2025 року №391/01-07

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи: «1» грудня 2025 року

3. Вихідні дані до роботи: *комп'ютерно-інформаційні технології обробки зображень,*

спеціалізована програма AVIZO, алгоритми обробки

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

1. Аналітичний огляд предметної області щодо обробки зображень.

2. Теоретична частина.

3. Практична частина.

4. Програмна частина.

5. Висновки.

5. Перелік графічного матеріалу :

графічний матеріал виконано у вигляді презентації, яка складається з 10 слайдів

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
<i>Розділ 1</i>	<i>Повстяной О.Ю.</i>		
<i>Розділ 2</i>	<i>Повстяной О.Ю.</i>		
<i>Розділ 3</i>	<i>Повстяной О.Ю.</i>		
<i>Розділ 4</i>	<i>Повстяной О.Ю.</i>		
<i>Нормоконтроль</i>			
<i>Показник запозичень тексту</i>			
<i>Академічна доброчесність</i>	<i>Полінкевич Р.М.</i>		

7. Дата видачі завдання 14.06.2025 р.

КАЛЕНДАРНИЙ ПЛАН

N з/п	Назва етапів кваліфікаційної роботи магістра	Строк виконання етапів роботи	Примітка
1	<i>Аналіз проблеми за темою роботи та постановка задач</i>	<i>01.09.2025 р.</i>	<i>виконав</i>
2	<i>Аналіз і вибір напрямків дослідження</i>	<i>10.09.2025 р.</i>	<i>виконав</i>
3	<i>Теоретичне дослідження та практична реалізація</i>	<i>20.09.2025 р.</i>	<i>виконав</i>
4	<i>Опис засобів розробки об'єкта проєктування</i>	<i>01.10.2025 р.</i>	<i>виконав</i>
5	<i>Загальні висновки та рекомендації</i>	<i>20.10.2025 р.</i>	<i>виконав</i>
6	<i>Оформлення роботи</i>	<i>10.11.2025 р.</i>	<i>виконав</i>
7	<i>Оформлення презентації</i>	<i>20.11.2025 р.</i>	<i>виконав</i>
8	<i>Здача чистового варіанту кваліфікаційної роботи на кафедру</i>	<i>01.12.2025 р.</i>	<i>виконав</i>

Здобувач вищої освіти _____
(підпис)

Гончар В. В.
(прізвище та ініціали)

Керівник кваліфікаційної роботи _____
(підпис)

Повстяной О. Ю.
(прізвище та ініціали)

АНОТАЦІЯ

Гончар В. В. Застосування комп'ютерно-інформаційних технологій для обробки зображень відбитків пальців. Рукопис.

Кваліфікаційна робота магістра ОП «Прикладна механіка» спеціальності 131 Прикладна механіка. Луцький національний технічний університет. Луцьк, 2025.

Кваліфікаційна робота магістра складається із вступу, 4 розділів, висновків, списку використаних джерел.

Кваліфікаційна робота присвячена розробці програмно-апаратного комплексу для ідентифікації особи за відбитками пальців, що дозволить підвищити якість та швидкість роботи систем доступу на основі сканування відбитків пальців. Даний розроблений програмно-апаратний комплекс для ідентифікації осіб за зображеннями їх відбитків зі спеціалізованим сканером і програми написаної на мові програмування Delphi, здійснює виконання наступних функцій: знаходження реєстраційних крапок на зображенні; їх сполучення у трикутники з наступним обрахунком сумарного вектору кожного з них; визначення кількості співпадаючих точок; виділення центру на термо картині; визначення матриці значень тепловіддачі секторів навколо нього. Використання даного програмно-апаратного комплексу скорочує затрати часу на обробку до 47,3 %.

Ключові слова: програмно-апаратний комплекс, автоматизована система керування, механізм, відбиток, вектор напрямний.

ABSTRACT

Gonchar V. Application of computer and information technologies for processing fingerprint images. Manuscript.

Master's qualification work OP «Applied Mechanics» specialty 131 Applied Mechanics. Lutsk National Technical University. Lutsk, 2025.

Master's qualification work consists of an introduction, 4 chapters, conclusions, list of sources used.

The qualification work is devoted to the development of a software and hardware complex for identifying a person by fingerprints, which will allow to improve the quality and speed of access systems based on fingerprint scanning. This developed software and hardware complex for identifying persons by images of their prints with a specialized scanner and a program written in the Delphi programming language, performs the following functions: finding registration points in the image; combining them into triangles with the subsequent calculation of the total vector of each of them; determining the number of matching points; highlighting the center on the thermal image; determination of the matrix of heat transfer values of the sectors around it. The use of this software and hardware complex reduces processing time by 47.3%.

Keywords: software and hardware complex, automated control system, mechanism, imprint, directional vector.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1 АНАЛІТИЧНИЙ ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ ЩОДО ОБРОБКИ ЗОБРАЖЕНЬ.....	10
1.1 Огляд існуючих методик обробки зображень відбитків пальців.....	10
1.2 Огляд існуючих програмних та апаратно-програмних комплексів для аналізу і обробки дактилоскопічних зображень.....	24
1.3 Поставка завдань на кваліфікаційну роботу.....	31
РОЗДІЛ 2 ТЕОРЕТИЧНА ЧАСТИНА.....	32
2.1 Реалізація програмно-апаратного комплексу і розроблення структури програми.....	32
2.2 Розроблення структури програми термального відбитка пальця.....	38
РОЗДІЛ 3 ПРАКТИЧНА ЧАСТИНА.....	43
3.1 Вибір обладнання для ідентифікації.....	43
3.2 Технічні передумови створення програмного забезпечення.....	46
РОЗДІЛ 4 ПРОГРАМНА ЧАСТИНА.....	48
4.1 Опис проекту програмного забезпечення.....	48
4.2 Графічний інтерфейс користувача програми.....	56
4.3 Інтерфейс та специфікація програми установки.....	60
ВИСНОВКИ.....	63
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	64
ДОДАТКИ.....	70

ВСТУП

Актуальність дослідження. На сучасному етапі розвитку інформаційних технологій спостерігається формування єдиного інформаційного простору, що інтегрує всю накопичену та використовувану інформацію. Однією з ключових проблем створення такого простору є забезпечення розмежування доступу до інформаційних систем, а також диференціація інформаційних ресурсів відповідно до прав і потреб конкретних користувачів. Центральним аспектом розв'язання цієї проблеми стає надійна ідентифікація суб'єктів доступу.

Одним із найдавніших і водночас найбільш поширених підходів до розв'язання задачі ідентифікації є біометрична ідентифікація. Згідно з визначенням, наведеним в Українській енциклопедії, біометрія являє собою сукупність методів математичної обробки даних, отриманих у результаті вимірювання параметрів тіла або окремих органів живих організмів. Біометричні методи, що ґрунтуються на положеннях теорії ймовірностей, дозволяють кількісно охарактеризувати значення досліджуваних ознак та їх мінливість, оцінити ймовірність подібності або відмінності відповідних характеристик у різних групах осіб, а також встановити взаємозалежність між змінами окремих ознак.

У цьому контексті постає науково-практична задача вибору найбільш зручного та ефективного методу ідентифікації особи за певною метричною та індивідуально унікальною біологічною ознакою. Сучасні дослідження пропонують два основні напрями її розв'язання: ідентифікацію за зображенням сітківки ока та ідентифікацію за відбитками пальців. Оскільки методи розпізнавання сітківки ока потребують значних матеріально-технічних витрат і характеризуються тривалим часом обробки даних, у даній роботі основну увагу приділено біометричній ідентифікації за відбитками пальців.

Метою даного кваліфікаційної роботи є розробка програмно-апаратного комплексу для ідентифікації особи за відбитками пальців, що дозволить підвищити швидкодію та надійність функціонування систем контролю доступу на основі дактилоскопічного сканування.

Об'єктом дослідження є сучасні методи біометричної ідентифікації та апаратні засоби, що застосовуються для їх реалізації.

Відповідно до поставленої мети в роботі передбачено розв'язання таких основних задач:

- аналіз існуючих методів і методик ідентифікації та обробки зображень з подальшим порівнянням їх за основними показниками ефективності та визначенням найбільш результативних елементів;
- дослідження програмних і програмно-апаратних комплексів для аналізу та обробки дактилоскопічних зображень із виявленням їх основних недоліків;
- розробка нового принципу обробки та аналізу зображень відбитків пальців;
- створення ергономічного, зручного та швидкодіючого користувацького програмного інтерфейсу і відповідної бази даних.

У процесі **дослідження** застосовувалися такі **методи**: теоретичний аналіз і систематизація наукових та методичних джерел; кореляційний аналіз; методи обробки даних; методи програмування з використанням мови Object Pascal у середовищі Delphi.

Наукова новизна дослідження полягає в удосконаленні підходів до біометричної ідентифікації за відбитками пальців.

Практичне значення отриманих результатів полягає у можливості використання розробленого програмно-апаратного комплексу в системах цивільної та криміналістичної ідентифікації, а також у широкомасштабних комерційних застосуваннях, що потребують надійних і швидкодіючих засобів контролю доступу.

Особистий внесок магістранта. Висновки, основні результати, виклад матеріалу у високій презентаційній формі, а також рекомендації щодо подальшого впровадження отримані автором самостійно з відповідним консультуванням простого наукового керівника.

РОЗДІЛ 1

АНАЛІТИЧНИЙ ОГЛЯД ПРЕДМЕТНОЇ ОБЛАСТІ ЩОДО ОБРОБКИ ЗОБРАЖЕНЬ

1.1 Огляд існуючих методик обробки зображень відбитків пальців

На сучасному етапі розвитку біометричних технологій сформовано та практично застосовуються три базові методичні підходи до ідентифікації особи за відбитками пальців. Кожен із відомих дактилоскопічних і цифро-аналітичних методів характеризується специфічними особливостями, що визначаються властивостями, структурними параметрами та якісними характеристиками зображень папілярних візерунків.

Ключовою концепцією досліджень у даній галузі є пошук оптимального компромісу між мінімізацією матеріальних, технічних і часових витрат на процедуру ідентифікації та максимізацією точності, надійності й якості розпізнавання. Основним завданням даного дослідження є аналіз та оцінювання найбільш поширених методів ідентифікації особи за відбитками пальців з точки зору їх ефективності та практичної реалізації.

Алгоритми даного класу функціонують за наступною узагальненою схемою. Цифрове зображення відбитка пальця, отримане за допомогою сканувального пристрою, у оперативній пам'яті комп'ютера або спеціалізованого автоматизованого процесора розбивається на множину локальних елементів (прямокутних або трикутних сегментів). При цьому зменшення геометричних розмірів окремих сегментів, як правило, призводить до підвищення точності подальшого розпізнавання.

У межах кожного сегмента просторове розташування папілярних ліній — мікроскопічних каналів на поверхні шкіри, конфігурація яких визначає унікальність біометричних характеристик відбитка пальця (рис. 1.1) — апроксимується синусоїдальною функцією, що описується параметрами початкового фазового зсуву та напрямку поширення.

На наступному етапі виконується порівняння хвильового представлення відповідних сегментів еталонного шаблону, що зберігається в базі даних (рис.

1.2, рис. 1.3), із поточним відсканованим зображенням, розміщеним у пам'яті системи.

Конфігурація папілярних ліній у кожному локальному осередку описується параметрами синусоїдальної хвилі, а саме: початковим фазовим зсувом δ , довжиною хвилі λ та кутом нахилу її поширення θ .

Перевагою алгоритмів цього класу є відсутність жорстких вимог до високої якості вхідного зображення, що дозволяє ефективно застосовувати їх за умов обмежених технічних можливостей сканування.

Разом із тим у процесі автоматизованої біометричної ідентифікації існує низка проблем, пов'язаних зі складністю сканування та розпізнавання окремих типів відбитків пальців. Зокрема, це стосується відбитків пальців дітей молодшого віку, розміри яких є недостатніми для отримання зображень з рівнем деталізації, необхідним для надійного розпізнавання навіть за використання високоточних сканувальних пристроїв. Крім того, приблизно у 1 % дорослого населення спостерігаються настільки специфічні особливості папілярного візерунка, що для їх коректної ідентифікації виникає необхідність розроблення спеціалізованих алгоритмів обробки або застосування альтернативних методів ідентифікації з повною чи частковою відмовою від біометричних процедур.

Слід також зазначити, що папілярний візерунок відбитка пальця характеризується високою структурною складністю. Збереження його повного цифрового представлення потребує значних обсягів пам'яті, що негативно впливає на швидкодію системи та збільшує тривалість процедури ідентифікації. Крім того, порівняння повних відбитків часто супроводжується зростанням ймовірності помилок, зумовлених похибками сканування, варіативністю стану шкірного покриву, силою притискання пальця до робочої поверхні та іншими випадковими факторами, які впливають на якість отриманого зображення.



Рисунок 1.1 – Схема ключових елементів відбитку: 1 – точка утворення гілок, розгалуження; 2 зона поділу гребеня на три лінії з подальшим сходженням в одній точці (форма трикутника); 3 – точки закінчення лінії гребеня; 4 – точка (зона) найбільшої кривизни спіралі гребеня; 5 – одиничний короткий обмежений гребінь, в більшості у вигляді короткого прямого відрізка

У багатьох методиках ідентифікації використовується не повний відбиток пальця, а тільки перелік певних крапок. У більшості сучасних технологій застосовуються два різних підходи – перший використовується в тому випадку, якщо сканування здійснюється з досить низькою або середньою якістю. При цьому на одержуваному відбитку можна розібрати багато дрібних деталей.

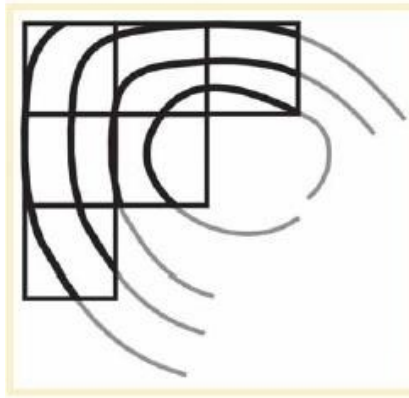


Рисунок 1.2 – Розбиття папілярного візерунка на секції



Рисунок 1.3 – Хвильове представлення в секції

Переважає більшість сучасних дактилоскопічних технологій ідентифікації ґрунтується на аналізі так званих мінуцій — характерних локальних елементів папілярного візерунка, до яких належать кінцеві точки та точки розгалуження папілярних ліній. Кінцеві точки відповідають місцям припинення папілярних гребенів, тоді як у точках розгалуження спостерігається їх роздвоєння або, навпаки, злиття, залежно від напрямку аналізу візерунка. Вибір саме цих структурних елементів як базових ознак ідентифікації зумовлений двома основними чинниками. По-перше, кінцеві точки та точки розгалуження, як правило, чітко виявляються на зображеннях відбитків пальців навіть за середньої якості сканування. По-друге, їх кількісна насиченість є достатньою для формування унікального набору ознак, що забезпечує однозначну ідентифікацію особи.

У межах альтернативного підходу застосовуються сканувальні пристрої, здатні забезпечувати отримання високоякісних зображень відбитків пальців з

розподільною здатністю не нижче 1000 dpi. За таких умов на цифровому зображенні папілярного візерунка стають доступними для аналізу не лише зовнішні морфологічні ознаки, але й елементи його внутрішньої мікроструктури. Зокрема, в окремих перспективних технологіях біометричної ідентифікації розглядається можливість використання пор потових залоз як додаткових інформативних ознак.

Водночас слід зазначити, що подібні методи наразі перебувають на стадії наукових і експериментальних досліджень. Основним обмежувальним фактором їх практичного впровадження є необхідність отримання зображень з надвисокою розподільною здатністю, що вимагає застосування складних і вартісних сканувальних систем, доступних переважно у спеціалізованих лабораторіях.

Дані даного класу базуються на безпосередньому кореляційному аналізі цифрових зображень відбитків пальців. Сутність підходу полягає у накладанні двох зображень одне на одне з подальшим обчисленням коефіцієнта кореляції між відповідними пікселями.

Кореляційне порівняння (рис. 1.4) передбачає використання зображень відбитків пальців з високою розподільною здатністю, як правило не нижче 800 dpi. У процесі аналізу здійснюється поетапне вирівнювання зображень шляхом взаємних зсувів і поворотів, після чого визначається рівень кореляції між інтенсивностями відповідних пікселів або напіввпадин папілярного візерунка. На основі отриманого значення кореляційного коефіцієнта формується рішення щодо ідентичності або відмінності порівнюваних відбитків.

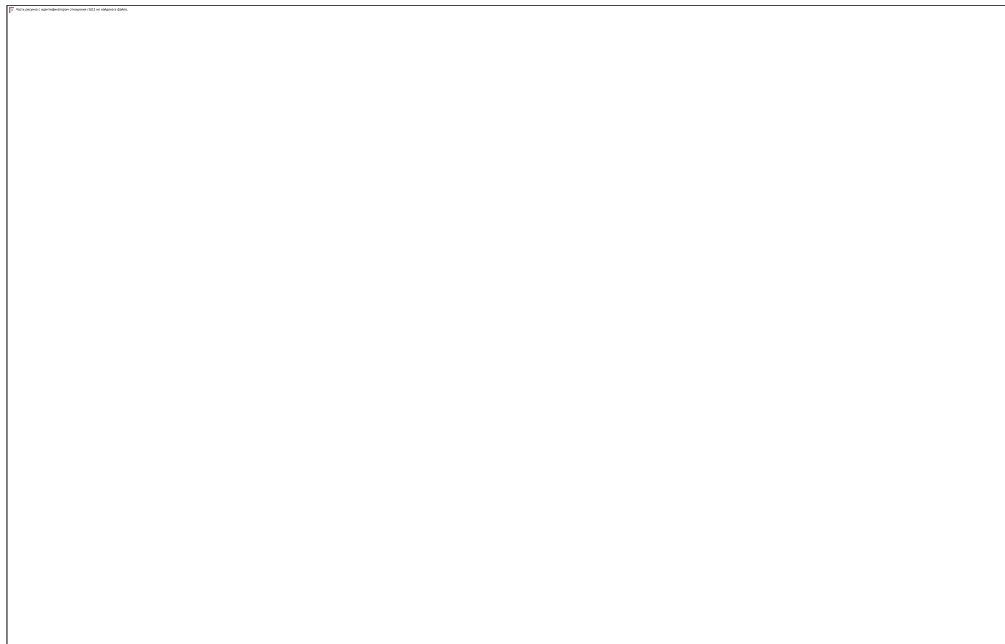


Рисунок 1.4 – Кореляція зображення відбитку по відповідним пікселям

Через складність даного алгоритму, особливо при рішенні завдань ідентифікації системи на його основі, зараз практично не використовуються в звичайних системах ідентифікації. Тому через надзвичайно велику ймовірність вірного відповідними пікселями (до 96 %), цей метод знайшов застосування у об'єктах підвищеної захищеності. При цьому порівняння йде лише з декількома відбитками людей, що мають таке право доступу (здебільшого їх кількість не перевищує 2–5 чоловік).

Під час реєстрації користувача в інформаційній системі цифрове зображення відбитка його пальця піддається послідовній обробці за визначеним алгоритмом. На початковому етапі виконується виявлення множини особливих точок папілярного візерунка (рис. 1.5). Для кожної з виявлених точок визначається набір метричних характеристик, які подаються у числовій формі. У результаті формується структурований масив даних, що кількісно описує сукупність особливих точок конкретного відбитка пальця.

У подальшому зазначена процедура повторюється кожного разу під час проходження користувачем процесу аутентифікації. Отриманий числовий опис особливих точок послідовно порівнюється з відповідними записами, що зберігаються в базі даних системи. При цьому досягнення повного збігу

параметрів, як правило, є неможливим унаслідок варіативності умов сканування та природних змін характеристик зображення. Тому в практичних реалізаціях застосовується пороговий підхід, згідно з яким встановлюється мінімально допустима кількість або частка співпадаючих особливих точок, достатня для прийняття рішення щодо ідентифікації користувача.

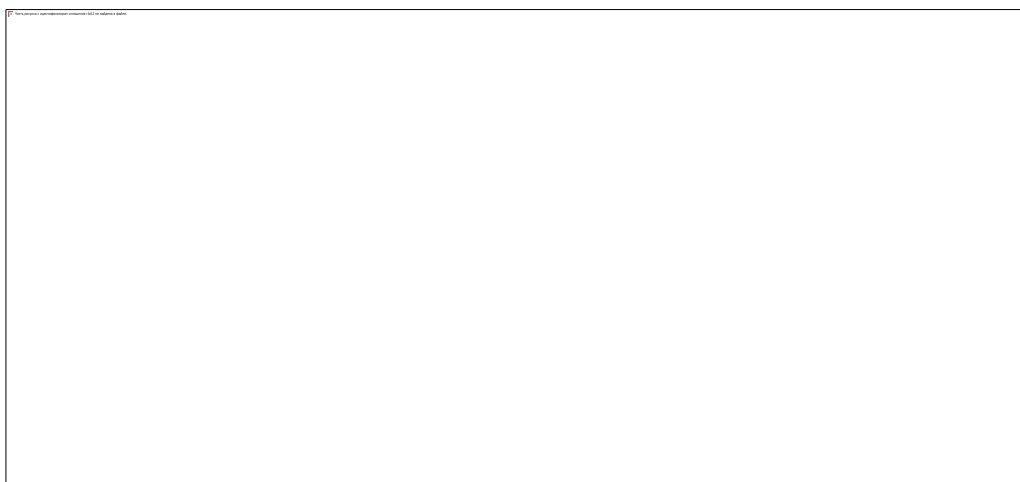


Рисунок 1.5 – Циклічний аналіз корельованих сигналів

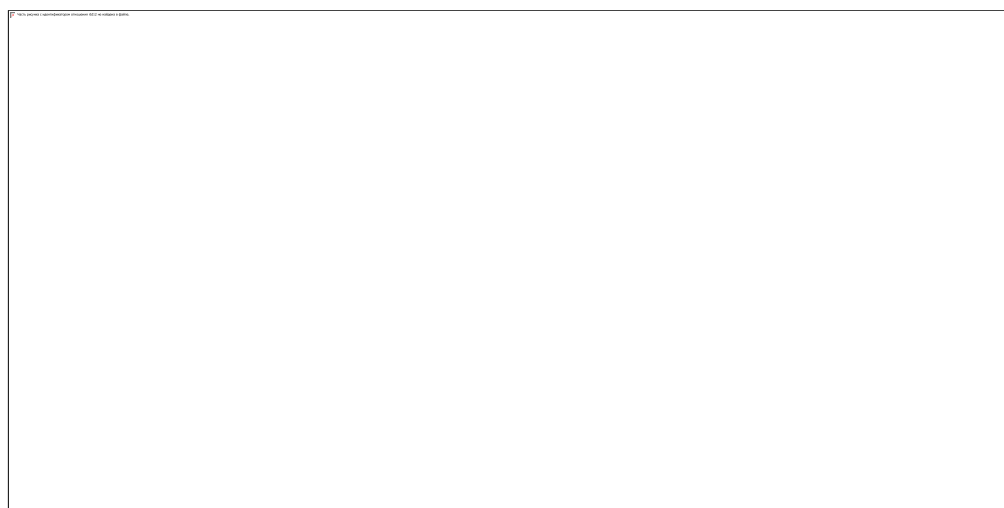
Розглянутий підхід характеризується наявністю низки суттєвих переваг. По-перше, метод ідентифікації за відбитками пальців на основі аналізу особливих точок є одним із найраніше розроблених у дактилоскопії, у зв'язку з чим він достатньо ґрунтовно теоретично обґрунтований та добре апробований у практичних реалізаціях. По-друге, даний метод є ефективним для задач порівняння типу «один до багатьох», що забезпечує високу швидкодію процедури зіставлення отриманого цифрового шаблону відбитка пальця з великою кількістю записів, які зберігаються в базі даних, під час пошуку конкретної особи.

Водночас зазначена технологія має і низку обмежень. По-перше, вона характеризується підвищеними вимогами до апаратного забезпечення, насамперед до сканувальних пристроїв, що використовуються для отримання зображень відбитків пальців.

На сьогодні відомо значну кількість різних методів формування зображень папілярного візерунка, проте не всі з них забезпечують параметри якості,

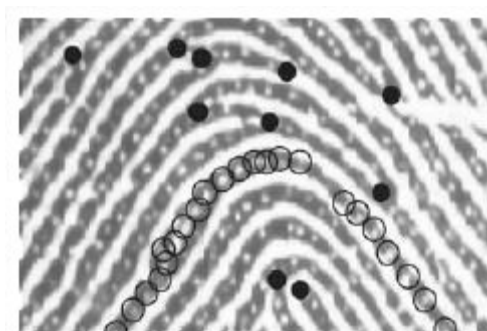
необхідні для коректної роботи даного алгоритму. Додатковими обмежувальними факторами є розподільна здатність та геометричні розміри сенсора. Недостатня якість отриманого зображення відбитка пальця призводить до істотного зниження ефективності процесу розпізнавання (рис. 1.6).

По-друге, ще одним недоліком методу є обмежений рівень криптобіометричної стійкості алгоритму, що визначається кількістю та інформативністю використовуваних особливих точок. За недостатньої кількості таких ознак знижується рівень захищеності системи та зростає ймовірність помилкових рішень під час ідентифікації.



а)

б)



в)

Рисунок 1.6 – Зображення відбитку з виділеними особливими точками:
а) відбиток ідентифікованої особи; б) еталон відбитку з БД; в) зразок з виділеними точками певного типу

Нижче наведені етапи аналізу та обробки зображення при використанні даного методу (рис.1.7.).

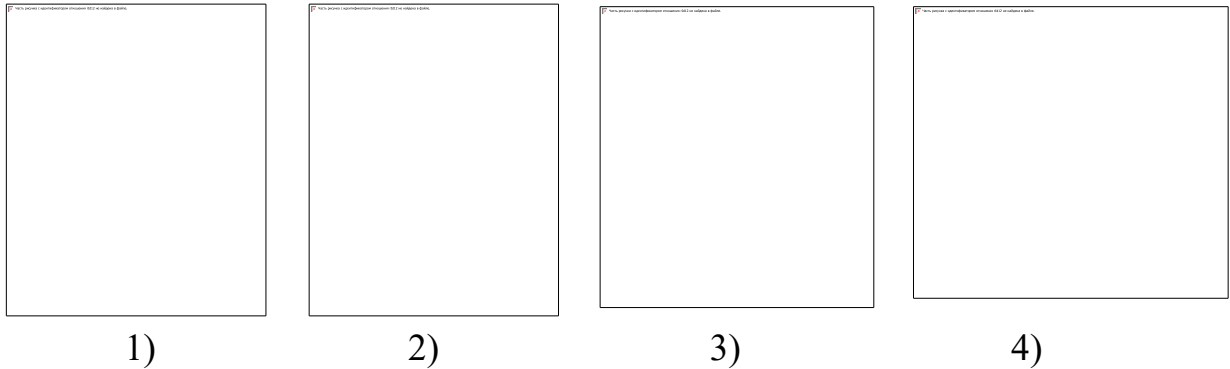


Рисунок 1.7 – Етапи аналізу зображення відбитку:

1. Отримання зображення зі скануючого пристрою спеціального типу
2. Виявлення програмою спеціальних точок на поверхні зображення
3. Відокремлення крапок від усього зображення
4. Формування метричних характеристик точок та порівняння з занесеними у базу

Розглянемо загальну схему алгоритму розпізнання відбитків (рис. 1.8).

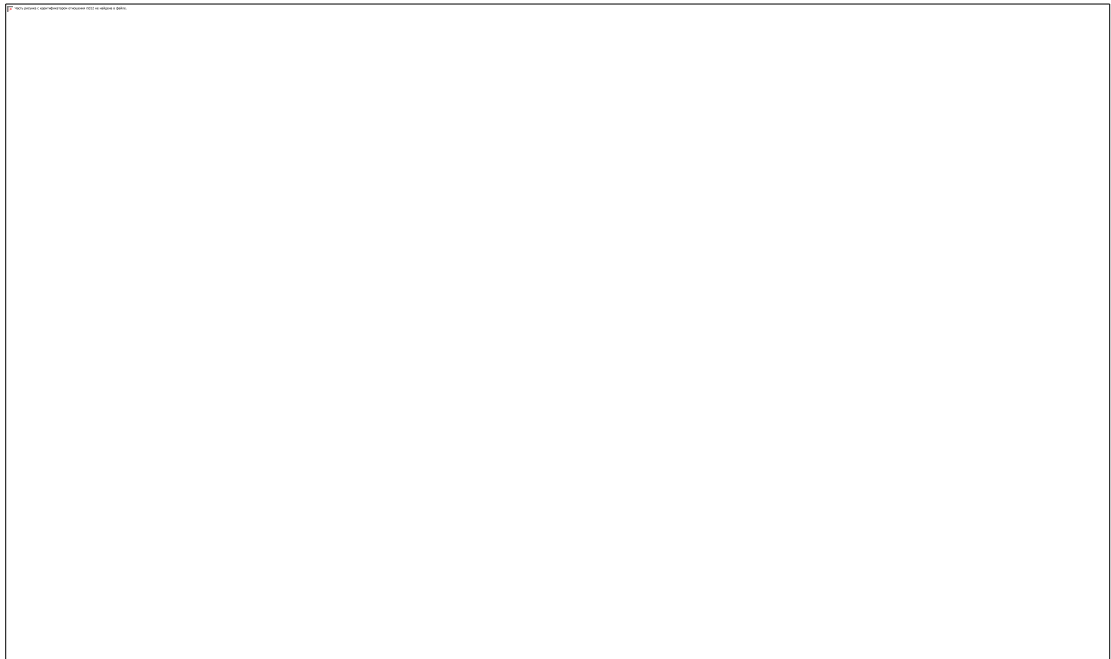


Рисунок 1.8 – Алгоритмічна схема процесу ідентифікації

Функціонування автоматизованої біометричної системи (рис. 1.8) здійснюється в одному з двох основних режимів: режимі ідентифікації або режимі верифікації. В обох режимах початковий етап обробки інформації, що відповідає процедурі реєстрації, є практично ідентичним і значною мірою визначається коректністю введення первинних даних.

Процес реєстрації полягає у введенні та налаштуванні базових параметрів системи і включає п'ять послідовних етапів:

1. Завантаження біометричних даних. Під час внесення біометричних характеристик до бази даних, як правило, реєструється декілька зразків, що належать одній і тій самій особі, з метою врахування можливих варіацій умов зняття відбитків. У результаті в базі даних зберігається декілька відбитків пальців однієї особи.

2. Фіксація даних. Здійснюється вимірювання та фіксація базової біометричної інформації, що відповідає конкретному біометричному зразку.

3. Обробка даних. Зафіксовані біометричні параметри перетворюються у цифрову форму з формуванням цифрового еквівалента відбитка пальця.

4. Верифікація оброблених даних з первинною інформацією. Даний етап виконується з метою підтвердження коректності обробки та правильності розпізнавання введених даних біометричною системою.

5. Збереження підтверджених біометричних даних. Після перевірки цифрові біометричні шаблони зберігаються у відповідних носіях інформації.

Результатом процедури реєстрації є формування електронного набору біометричних даних у форматі, придатному для зберігання, передачі та подальшого використання. Такі дані можуть розміщуватися у централізованій базі даних, у спеціалізованих файлах-ключах (зазвичай із застосуванням криптографічних методів, зокрема RSA-шифрування), на ідентифікаційних магнітних носіях типу смарт-карт або на захищених оптичних носіях.

Етап реєстрації є критично важливим з точки зору надійності функціонування біометричної системи, оскільки саме на цьому етапі забезпечується коректна взаємодія між користувачами та системою і

зкладається основа для подальшої працездатності та точності процесів ідентифікації та верифікації.

Одним із ключових питань, що вирішується на етапі реєстрації, є визначення призначення біометричної системи – для задач ідентифікації або для задач верифікації. У режимі ідентифікації система здійснює пошук особи, якій належить поданий біометричний зразок, шляхом його порівняння з усією множиною записів у базі даних з метою знаходження найбільш імовірного збігу. Даний процес також відомий як порівняння типу «один до багатьох».

Режим верифікації, у свою чергу, передбачає підтвердження заявленої особистості користувача. У цьому випадку новий біометричний зразок порівнюється з раніше збереженим еталонним шаблоном конкретної особи. За результатами такого порівняння система приймає рішення щодо відповідності особи заявленій ідентичності. Таким чином, у режимі ідентифікації здійснюється порівняння одного зразка з багатьма, тоді як у режимі верифікації або аутентифікації виконується зіставлення одного зразка з одним.

Для реалізації режиму ідентифікації необхідною є наявність централізованої бази даних біометричної інформації, з якою здійснюється порівняння поточного зразка. У режимі верифікації біометричні дані особи можуть перевірятися на відповідність електронним шаблонам, що зберігаються на персональних носіях, наприклад на експрес-картах пам'яті або МС-картах.

Важливим етапом обробки є класифікація отриманого зображення відбитка пальця. Застосування процедури класифікації є необхідним для істотного скорочення часу ідентифікації, особливо у випадках, коли поточний зразок порівнюється з великою кількістю записів у базі даних, кількість яких може змінюватися від десятків і сотень до мільйонів і навіть десятків мільйонів, як, наприклад, у базах даних правоохоронних органів.

З цією метою отримане зображення відбитка пальця на початковому етапі відноситься до певного класу або підкласу на основі набору характерних ознак. Подальше порівняння виконується лише в межах визначеного класу, що дозволяє скоротити загальний час роботи системи в декілька разів. При цьому первинна оцінка класу відбитка, на відміну від повноцінного процесу

розпізнавання, реалізується на відносно простому техніко-математичному рівні, що не потребує значних обчислювальних ресурсів.

На сьогодні з метою уніфікації баз даних відбитків (fingerprints datas) прийнято виділяти 5 основних класів відбитків – відповідно до моделі розробленою в Відділенні розробки методів біометричної ідентифікації Мічиганського державного університету, Biometrics Researches of MSU (рис. 1.9.):

- завиток або тип W;
- права котушка або тип R;
- ліва котушка або тип L;
- арковий тип або тип A;
- плоска арка або тип T.

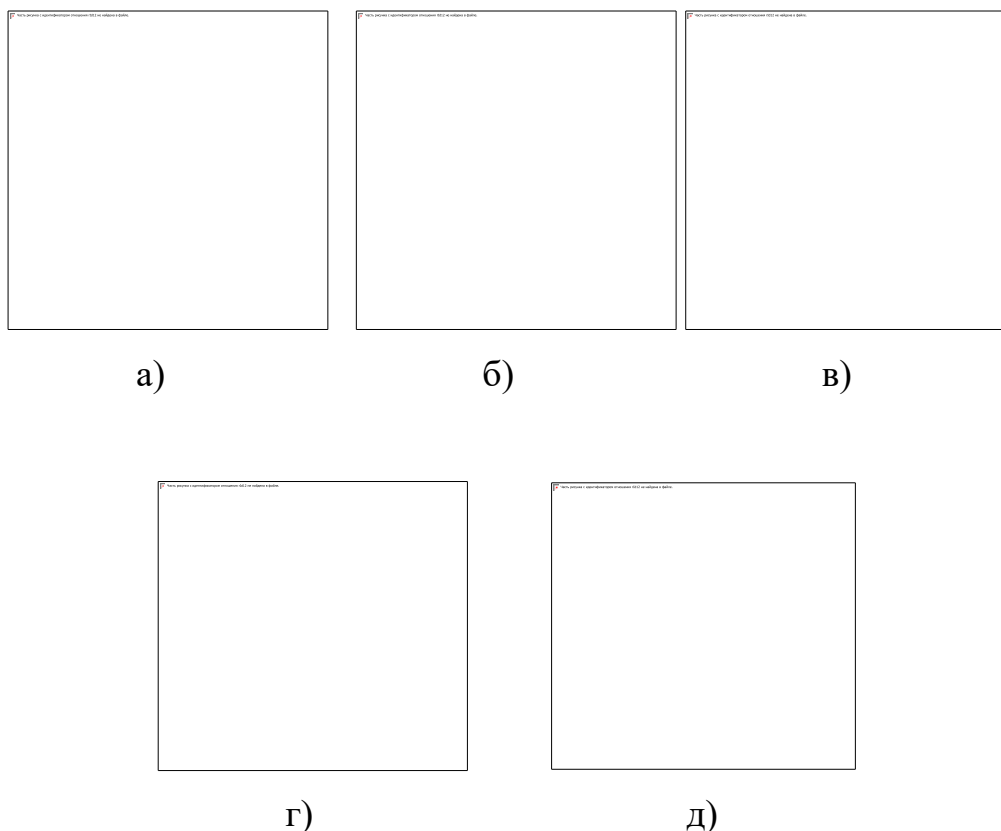


Рисунок 1.9 – Основні класи відбитків по класифікації MSU:
 а) арка (A); б) котушка (R); в) завиток (W); г) плоска арка (T);
 д) котушка (L).

Класифікатор, який наведений на рисунку 1.10, приводить до точності 85,4% для завдання розгляду 10 найближчих сусідів ($K=10$) при виборі між 5 основними класами. Метод «найближчого сусіда» відноситься до класу методів, робота яких ґрунтується на зберіганні даних у пам'яті. З появою нового запису для прогнозування знаходяться відхилення між цим записом і подібними наборами даних.

Точність класифікації не завжди збільшується зі збільшенням K , бо не існує оптимальне значення K для кінцевих навчальних завдань класифікації розміру моделі.

Для завдання класифікації чотирьох з п'яти класів досягнута точність 91,5%. Змішана матриця для класифікатора показана в таблиці 1.1.

Таблиця 1.1 – Змішана матриця для класифікатора K -найближчого сусіда

Справжній клас	Заданий клас				
	W	R	L	A	T
W	320	38	31	6	0
R	1	368	2	10	21
L	0	1	359	13	8
A	1	3	7	422	20
T	0	15	16	95	208

Діагональні записи в цій матриці показують число тестових моделей від різних класів, які правильно класифіковані.

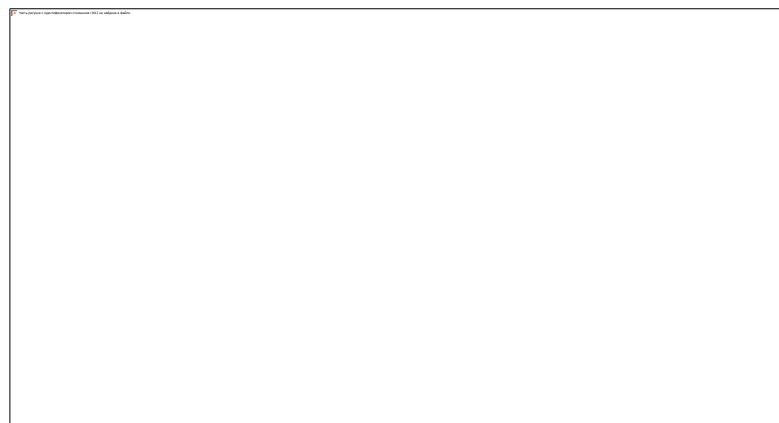


Рисунок 1.10. Знаходження найближчих сусідів

Другий класифікатор – це для для Байесовської мережі. Це імовірнісна модель, що представляє собою безліч змінних . Байесовська мережа – це спрямований граф, вершини якого представляють змінні, а ребра кодують умовні залежності між змінними. Вершини можуть представляти змінні будь-яких типів, бути схованими змінними або гіпотезами.

Існують ефективні методи, які використовуються для обчислень таких мереж. Байесовські мережі ще називають динамічними байесовськими мережами. Цей підхід гарантує якісну класифікацію завдяки глибокій математичній моделі аналізу, який підходить для розпізнавання образів та успішному повному застосуванню розпізнавання мови й інших завдань.

Ці моделі здатні класифікувати дані, які засновані на великій кількості ознак, число яких є змінним і має певні типи основної структури.

У відбитку пальця, основна інформація класу може бути виведена із синтаксичного аналізу особливих крапок. Щоб знаходити місця розташування виступів, використовується безліч методів обробки зображення.

У вибіркового відхиленні для запобігання виникнення метричних та аналітичних помилок частину зображення відхиляють на першому ж етапі ідентифікації. Категорії таких зображень – забруднені відбитки, зображення низької якості. Залежність між кількістю відхилень та якістю подальшого процесу розпізнавання наведена у таблиці 1.2

Таблиця 1.2 – Співвідношення між вибіркового відхиленням і позитивною ідентифікацією

Норма відхилення	1,80%	8,50%	19,50%	32,50%
Помилки 5 класу	10%	8,80%	6,50%	1%
Помилки 4 класу	5,20%	4,50%	3,40%	2,20%

Існує ще близько десятка класифікаторів нижчої точності та ефективності, хоча навіть деякі з них сьогодні успішно реалізовані у портативних системах ідентифікації. Найпоширеніші з них – метод дерева рішень, двухетапний класифікатор – гібрид на основі двох з вище перерахованих методів,

класифікатор на основі одно- або багат шарової нейронної мережі.

1.2 Огляд існуючих програмних та апаратно-програмних комплексів для аналізу і обробки дактилоскопічних зображень

На сучасному етапі розвитку інформаційних технологій апаратні та програмні засоби для аналізу й обробки дактилоскопічних зображень набули широкого поширення. В умовах глобалізації та інтенсивної інформатизації суспільства задача надійної ідентифікації особи постає практично в усіх сферах життєдіяльності, зокрема у системах контролю доступу, інформаційній безпеці, правоохоронній діяльності та фінансовому секторі.

Розглянемо декілька найбільш поширених автономних ідентифікуючих пристроїв, по одному представнику для кожного з основних класів, що використовуються у сучасних біометричних системах.

1. Універсальний сканер відбитків пальців Sagem MSO300 (рис. 1. 11).

Сканер відбитків пальців MSO300 виробництва компанії Sagem є компактним автономним пристроєм, призначеним для зчитування та цифрового перетворення зображень папілярного візерунка пальця з подальшим автоматизованим занесенням отриманих даних до бази біометричної інформації. Час ідентифікації за допомогою даного пристрою не перевищує 2 с, що забезпечує можливість його ефективного використання в системах з підвищеними вимогами до швидкодії.

Пристрій оснащений оптичним сенсором з площею активного сканування 21×21 мм та розподільною здатністю 500 dpi, що відповідає стандартним вимогам до якості зображень папілярних візерунків. Наявність вбудованих програмних модулів попередньої обробки зображень дозволяє виконувати первинну фільтрацію та нормалізацію даних безпосередньо на рівні пристрою, що істотно скорочує тривалість процедури реєстрації нових користувачів у біометричній системі.

Підключення сканера MSO300 до центрального комп'ютера системи контролю доступу здійснюється через інтерфейс USB, що забезпечує простоту

інтеграції пристрою у складі автоматизованих інформаційних систем організацій різного призначення.

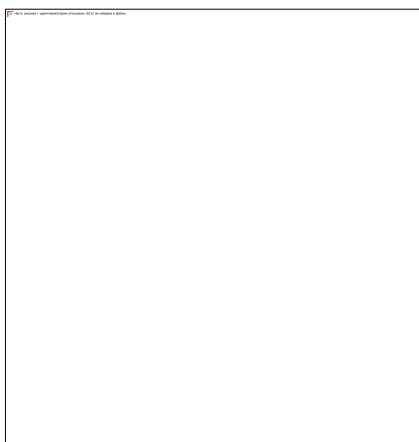


Рисунок 1.11 – Сканер відбитків пальців Sagem MSO300

Таблиця 1.3 – Технічні характеристики сканера відбитків пальця MSO300

Ідентифікація:	1:2000(2пальці)<2сек
Розп.здатність сканера:	500 крапок на дюйм
Градації кольорів:	8рівнівсірого
Розп.здатність відбитка:	4lppm для контрасту>25%
Активна площа:	21x21мм
Інтерфейс:	USB1.1
Електроживлення:	5У,500ма
Робоча температура:	0°...+40°З
Припустима вологість:	10–80%безконденсату
Вага сканера:	300м
Габарити:	80x92x57мм

Даний пристрій є представником класу несаможіючих сканерів для централізованої і комп'ютеризованої системи контролю доступу.

2. BioLink U–Match Mouse.

BioLink Umatch® Mouse – це пристрій, що сполучає в єдиному корпусі двокнопковий маніпулятор «миша» з ролером прокручування (рис.1.12).



Рисунок 1.12 – BioLink U–Match Mouse

Пристрій розроблений з метою сполучити біометричний сканер у стандартному пристрої введення. Не вимагає застосування додаткових роз'ємів, працює через стандартний інтерфейс USB або RS–232C.

Таблиця 1.4 – Технічні характеристики BioLink U–Match Mouse

Ідентифікація:	0,2 с
Розп.здатність сканера:	284 x 400 крапок
Градації кольорів:	8рівнівсірого
Активна площа:	18 x 28 мм
Інтерфейс:	USB1.1, USB 2.0, RS232
Електроживлення:	RS232
Імовірність помилкової відмови системи	1% (10–2)
Імовірність помилкової ідентифікації	<0.1%
Вага сканера:	300м
Габарити:	80x92x57мм

Даний пристрій – інтегрований несаможіючий сканер, які набули великого поширення в останні три роки. Вони забезпечують відповідний рівень доступу до інтелектуальних та інформаційних систем, комп'ютерних мереж, для роботи потребують додаткового програмного забезпечення.

3. Пристрій контролю доступу по відбитках пальців IDTECK STAR FGR007A

FGR007A доступний за ціною й робить можливість установки й модернізації систем контролю доступу в бік дактилоскопічної біометрії цілком реальною (1.13).

Маючи механізм швидко й точної персональної ідентифікації з ємністю користувальницької бази до 4000 записів, він є закінченим рішенням безпеки.

Області застосування – особливо охоронювані зони, системи обліку відвідуваності й робочого часу, сполучені із системами контролю доступу в офісах і на виробництві

Основні характеристики – швидка ідентифікація, компактна конструкція – передбачається вбудовування у дверні рами будь-якого типу; можливість об'єднання в мережу – до 256 пристроїв на одному шлейфі; точна ідентифікація – відсоток помилкового надання доступу 0.0001%; автоматизований алгоритм розпізнання.

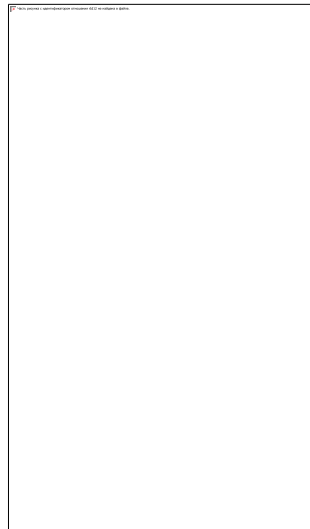


Рисунок 1.13 – IDTECK STAR FGR007A

4. Температурні датчики відбитків пальців із сімейства FingerChip (AT77C102B) – представник сімейства датчиків відбитка пальців Atmel FingerChip, які не вимагають застосування оптики, призми і джерел світла (рис 1.14.). Це є однокристальний, високоякісний і недорогий датчик відбитка пальців, що використовує для визначення відбитка пальця теплові фізичні ефекти.

AT77C102B характеризується лінійною формою, що захоплює зображення відбитка пальця переміщенням пальця поперек чутливої поверхні. Після захвату декількох зображень може відновити повне 8 бітне зображення відбитка пальця.

Датчик характеризується програмувальною частотою знімання зображення й інтегрує аналогово–цифровий перетворювач, цифровий вихід якого сполучимо з паралельним портом EPP, USB–мікроконтролером або шиною мікропроцесора.

Для передачі кадрів немає необхідності застосування механізму захвата кадру або інтерфейсу, що погоджує. Дані особливості роблять AT77C102B простим для застосування пристроєм у будь–якій системі для виконання функцій ідентифікації або верифікації.

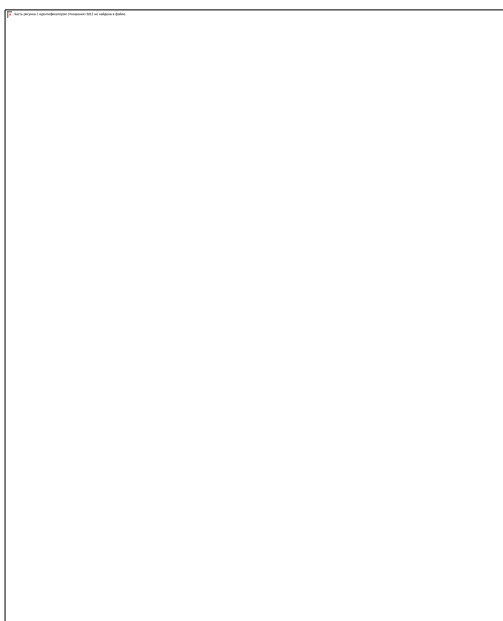


Рисунок 1.14 – AT77C102B

Таблиця 1.5 – Технічні характеристики AT77C102B

Чутливий шар	на основі 0,35 мкм–ої КМОП–матриці
Зона зображення:	0.4 x 14 мм = 0.02" x 0.55"
Матриця зображення:	8 x 280 = 2240 пікселів
Крок пікселів:	50 мкм x 50 мкм = 500 dpi
Синхронізація пікселів:	до 2 МГц (відповідає 1780 кадрам у сек.)
Розмір кристала:	1.64 x 17.46 мм
Робоча напруга:	3У...3.6В
Ефективний захист від електростатичних розрядів:	> 16 кВ грозового розряду
Споживана потужність:	16 мВт при 3.3В, 1 МГц, 25°C
Робочий температурний діапазон:	–40°C...+85°C

Пристрій є представником нового класу напівавтоматичних датчиків з вбудованим АЦП на основі термального аналізу.

5. Пакет FingerCell 2.0 (рис 1.15) спроможний зіставляти із шаблонами, що зберігаються в базі, до 700 відбитків пальців у секунду й може використатися для перевірконої ідентифікації або для встановлення особистості по базі інтегрованих додатках. Тут присутні системи контролю доступу, робочого часу й присутності на робочих місцях, а також безпеки апаратних засобів.

Розроблений в системі VeriFinger алгоритм FingerCell 2.0 модернізований для забезпечення більше високих швидкостей обробки зображень і виділення характерних їхніх зон на пристроях з відносно низькими енергоспоживанням.

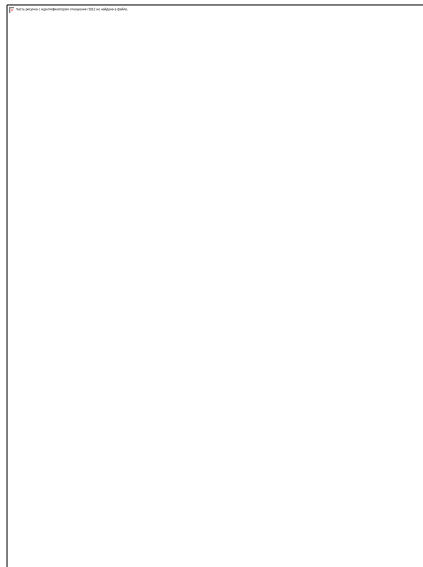


Рисунок 1.15 – FingerCell 2.0

6. VeriFinger 5.0 Standard SDK. Даний алгоритм та ПЗ на його основі (рис. 1.16) є одним з найбільш використовуваних на сьогодні завдяки низькій вартості, невисоким вимогам до апаратного забезпечення та досить високими показниками розпізнання. Алгоритм VeriFinger в модифікованому чи повному вигляді застосовують сьогодні в різноманітних автономних та комп'ютеризованих системах доступу по всьому світі.

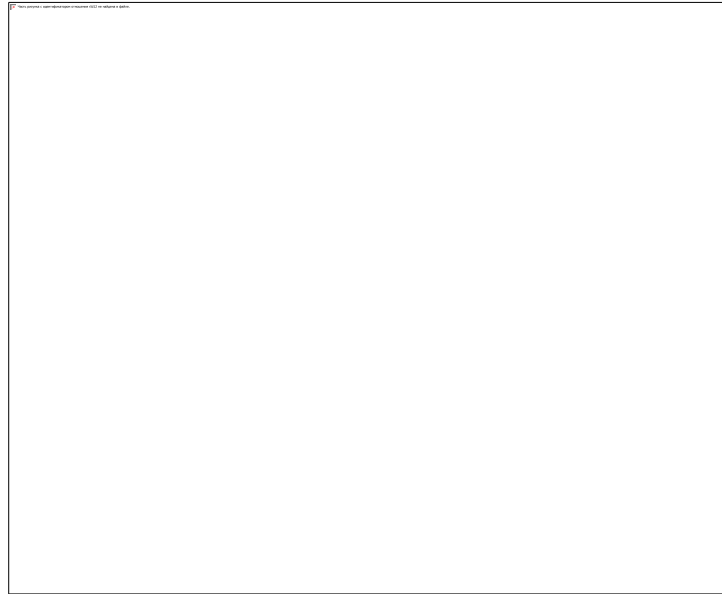


Рисунок 1.16 – VeriFinger 5.0 Standard SDK

7. IBM ThinkVantage Fingerprint Software - досить нове програмне забезпечення (рис 1.17), яке отримало акредитацію Ibm kbit минулого року. Використовує гібридну математичну модель аналізу та криптографічні системи захисту бази даних. На сьогодні застосовується в різноманітних портативних пристроях, хоча сам алгоритм дозволяє досить широке використання. З відомих технічних характеристик: швидкість розпізнання одного відбитку – менше 1 секунди. Вірогідність успішного підтвердження особи – 96,67 %.



Рисунок 1.18 – IBM ThinkVantage Fingerprint Software

1.3 Постановка задачі на кваліфікаційну роботу

Завданням даної кваліфікаційної роботи є розробка програмно–апаратного комплексу з новим гібридним алгоритмом, який автоматично отримує зі спеціального сканера відбиток пальця та обробляє скановане зображення. Далі відбувається процес ідентифікації особи:

- визначення таблиці параметрів порівняння;
- віднесення відбитка до певного класу;
- порівняння параметрів з існуючими шаблонами;
- визначення особи чи відхилення відбитку.

РОЗДІЛ 2

ТЕОРЕТИЧНА ЧАСТИНА

2.1 Реалізація програмно-апаратного комплексу

Програма, що розробляється для даного програмно-апаратного комплексу повинна виконувати наступні функції:

- задання чорно-білого режиму сканування зображення для основного сканера та 64-ти бітного кольорування для термального сканера;
- задання роздільної здатності;
- сканування зображення;
- відображення сканованого зображення у вікні програми;
- відкриття зображення з файлу;
- автоматична очистка зображення від шумів;
- фільтрування зображення спеціальним програмним фільтром;
- визначення об'єктів та їх координат;
- визначення співвідношень між об'єктами;
- створення матриці даних об'єкта;
- визначення параметрів рівномірності об'єктів по площі;
- остаточне підрахування вірогідності співпадань суб'єкта;
- визначення автентичності особи відповідно до заданої вірогідності.

Фактичний математичний алгоритм моделі складається з наступних етапів:

1. Сканування поверхні пальця спеціальним комбінованим сканером, що забезпечує подвійне сканування: верхній блок здійснює оптичне сканування на основі відбиття світла від поверхні пальця; нижній блок за допомогою спеціального термального барабанного датчика здійснює сканування термальної «карти» капілярів пальця.

Передбачається, що сканер буде напряму під'єднаний до комп'ютера – для можливості зміни попередніх параметрів сканування оператором системи.

Всі ці опції доступні завдяки графічному інтерфейсу користувача. Керування сканером відбувається завдяки його драйверу та через систему команд API.

2. Зображення завжди сканується у формат RAW, а потім конвертується у звичайний графічний формат із застосуванням поточних налаштувань яскравості, контрастності і т.д.

Ця конвертація здійснюється або в самому сканері, або в комп'ютері – залежно від моделі конкретного сканера. В нашому випадку конвертацію буде здійснюватися безпосередньо на комп'ютері. На параметри і якість RAW–даних впливають такі апаратні налаштування сканера, як час експозиції матриці, рівні калібрування білого й чорного тощо.

RAW – формат даних, що не має чіткої специфікації. Файли цього формату містять у собі неопрацьовані дані, що дозволяє уникнути втрат інформації. У таких файлах утримується багато надлишкової інформації, тому RAW використовують набагато більшу кількість дискового простору.

3. Отримані зображення потребують обробки, очищення від зайвих шумів, та виділенні необхідних у подальшій обробці елементів. Існує надзвичайно багато різноманітних програмованих фільтрів та алгоритмів – як самостійних, так і інтегрованих у відомі графічні пакети. Найкраще для вирішення математичних та кореляційних задач запропонував себе з математичним алгоритмом класування відбитку. Саме цим фільтром буде відбуватися опрацьовування обох зображень, однак з різними налаштуваннями.

Головні кроки цього етапу алгоритму:

- 1) знайти спеціальну крапку (крапку центра) і визначити просторову складову мозаїки місця зображення навколо неї (представлене сукупністю секторів);
- 2) розкласти вхідне зображення в ряд складових зображень;
- 3) обчислити оцінку стандартного відхилення, щоб сформувані вектор ознак або код пальця.

У даному алгоритмі використовуються шість концентричних смуг навколо пункту центра (рис. 2.8). Кожна смуга з 20 пікселями шириною ($b = 20$), і сегментованим у вісім секторів ($k = 8$). Сама внутрішня смуга не використовується для добування ознак, тому що в області біля центра містять дуже небагато пікселів. Таким чином, у цілому $8 \times 6 = 48$ секторів.



Рисунок 2.1 – Відбиток пальця із крапкою центра (x), ядром (o) і відзначеними 48 секторами.

Головні кроки алгоритму класифікації наступні (рис. 2.1) - визначити місцезнаходження реєстраційних крапок у вхідному зображенні й визначити просторову складову мозаїки області навколо реєстраційної крапки.

Центр, знайдений вище, переміщений на 40 пікселів униз для подальшої обробки тому, що більшість інформацій у відбитку пальця перебуває в більшій низькій частині відбитка пальця. Ця значення було дослідним шляхом визначено.

Зображення відбитка пальця умовно розділяємо на чотири складові зображення, що відповідають чотирьом різним значенням θ (0° , 45° , 90° , і 135°) щодо осі X (рис. 2.2). Зображення відбитка пальця згорнуте з кожним із чотирьох фільтрів Габора, щоб зробити чотири складові зображення.

Перед розкладанням зображення відбитка пальця, ми нормалізуємо необхідну область у кожному секторі окремо до постійного середнього. Нормалізація зроблена, щоб видалити ефекти шуму датчика й розходжень тиску пальця.

Нехай $I(x, y)$ позначають сіре значення в пікселя (x, y), M_i й V_i , передбачуваному середньому й різниці сектора S_i , відповідно, і $N_i(x, y)$, нормалізоване значення сірого рівня в пікселя (x, y).



Рисунок 2.2 – Застосування фільтрів Габора: а) – орієнтація 00; б) – орієнтація 450; с) – орієнтація 900; d) – орієнтація 1350

Нормалізація – піксельна операція, що не змінює чіткість структур виступів. Для наших експериментів, ми встановлюємо обоє значень M_0 , і V_0 рівними 100.

Нормалізовані, фільтровані і відновлені зображення для відбитка пальця, показані на рисунку 2.3.

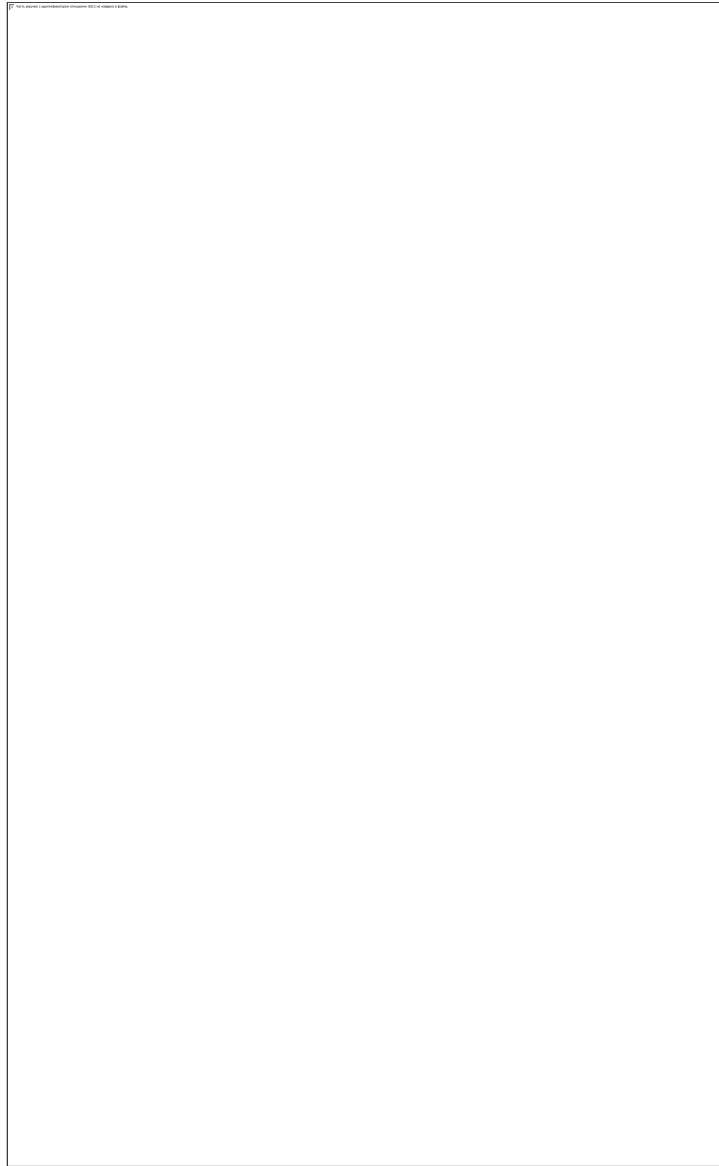


Рисунок 2.3 – Нормалізоване, фільтроване, і відновлене зображення відбитка пальця: а) – нормалізоване зображення, б), с) ,d), е) – фільтроване (00, 450, 900, 1350), ф) – відновлене зображення

У даному алгоритмі застосовується дворівнева схема класифікації. На першому етапі використовується класифікатор типу k найближчих сусідів (k -Nearest Neighbors, k -NN), тоді як на другому етапі залучається сукупність класифікаторів на основі штучних нейронних мереж. Така комбінація дозволяє здійснювати класифікацію вектора ознак відбитка пальця до одного з п'яти визначених класів папілярних візерунків.

У кожному складовому фрагменті зображення локальне оточення папілярних гребенів і борозен, орієнтованих паралельно напрямку відповідного

фільтра, характеризується підвищеним рівнем варіації інтенсивності. Натомість локальні області, у яких гребені та борозни не є паралельними напрямку фільтра, зазнають більшого пригнічення внаслідок фільтрації, що призводить до зниження рівня варіації сигналу.

У межах запропонованого алгоритму числовий вектор ознак формується на основі значень стандартного відхилення інтенсивності, обчислених у межах відповідних секторів зображення. Отриманий вектор ознак використовується як вхідна інформація для дворівневої процедури класифікації.

Тестова модель – права петля (рис. 2.4). Кожен диск відповідає одному специфічному фільтру з 48 ознаками (показані як сірі значення). Кожен диск ($8 \times 6 = 48$ секторів) для в цілому 192 (48×4) ознак : а) тестова модель, b) завитушка, c) права петля, d) ліва петля, e) арка, f) півсфера.

Отже, загальний алгоритм віднесення до класу буде мати такий вигляд, який представлено на рисунку 2.5.

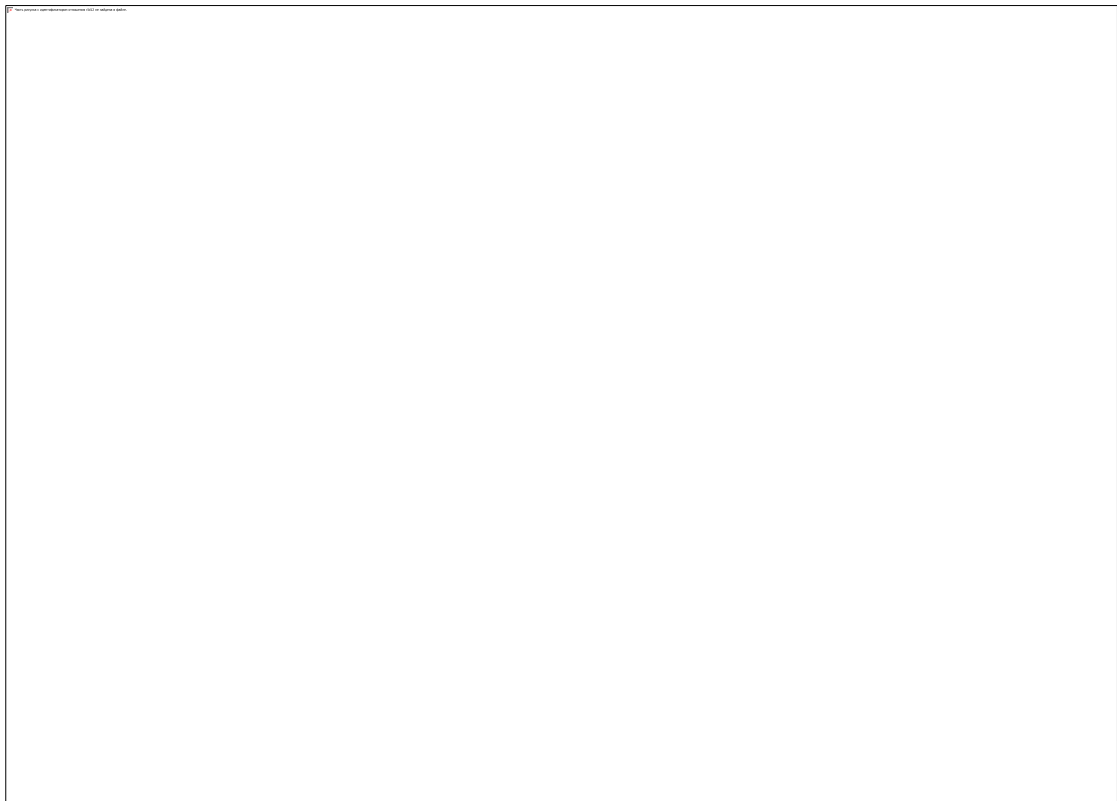


Рисунок 2.4 – 192-мірні вектори ознак

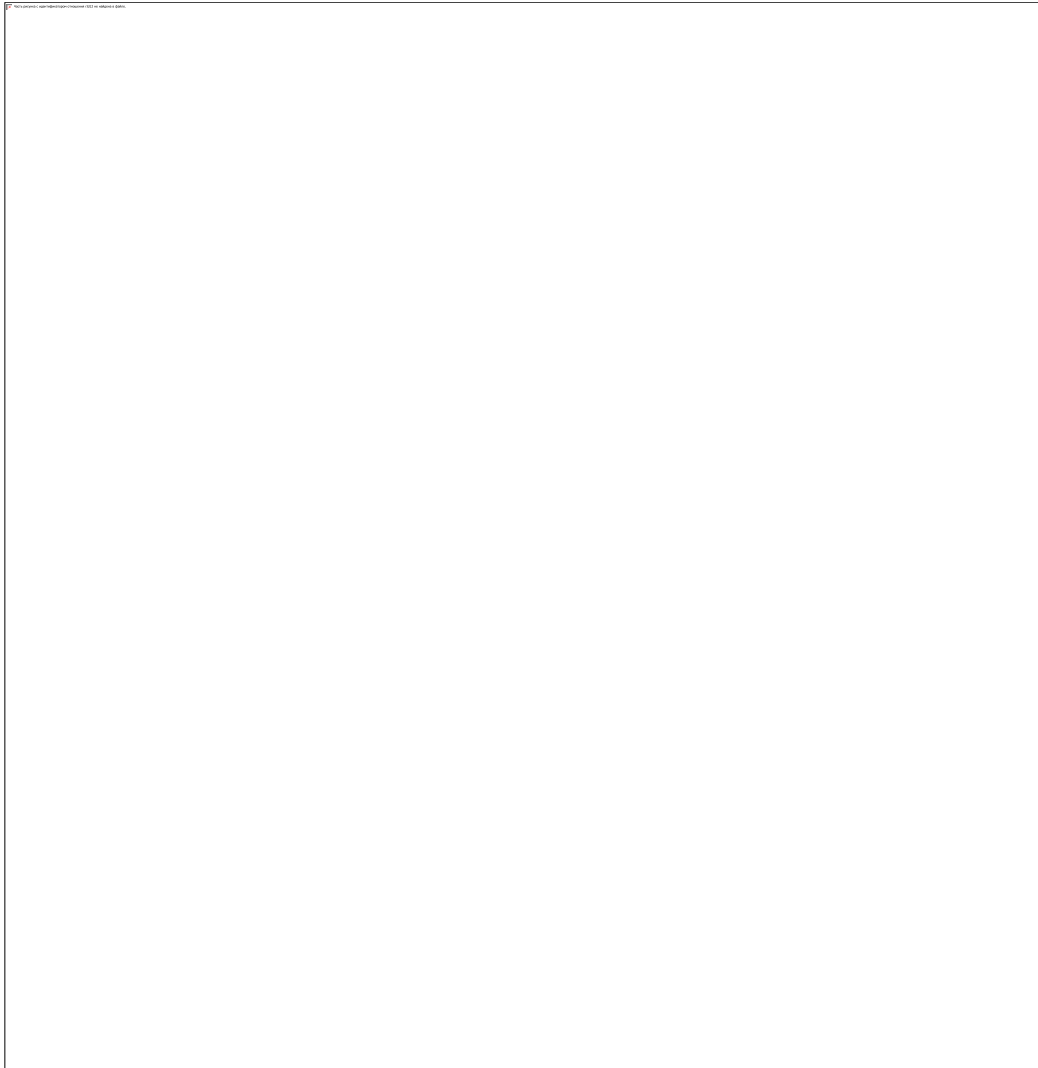


Рисунок 2.5 – Загальна схема алгоритму

Зауважимо, що дана схема (рис. 2.5) застосовується для зображення 1.

2.2 Розроблення структури програми термального відбитка пальця

Наступна дія – визначити розподіл тепла навколо центру і порівняння з існуючим в базі. Для цього використовується вбудовані у середовище Delphi засоби визначення розподілу спектру або автоматизовані фільтри для середовища Adobe.

У випадку використання термального відбитка пальця спільним початковим етапом обробки є визначення центру відбитка. Подальша процедура передбачає аналіз просторового розподілу теплового випромінювання (теплової карти) у околі визначеного центру з наступним порівнянням отриманих

характеристик з еталонними даними, що зберігаються в базі даних. Для реалізації даного етапу можуть застосовуватися інструменти аналізу спектрального розподілу по окремих точках, а також автоматизовані фільтри для програмного середовища Adobe, які поширюються на вільній основі.

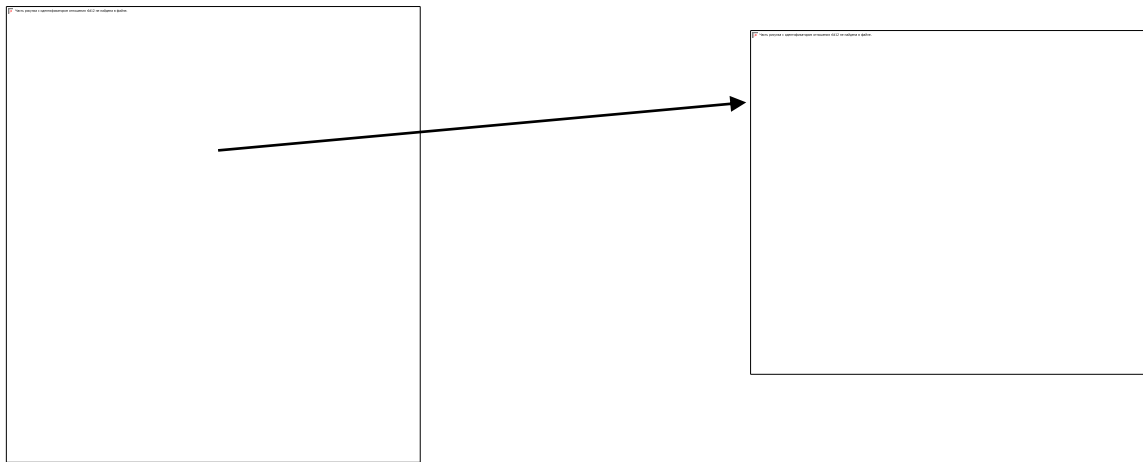
Визначений на первинному зображенні центр відбитка використовується як початкова точка відліку. Навколо нього в межах радіуса 0,5 см формується уявна кругова область, яка автоматизовано поділяється на матрицю секторів однакової площі розміром 10×10 . Після цього функція оцінювання інтенсивності забарвлення, що фактично відповідає інтенсивності тепловіддачі, присвоює кожному сектору числове значення у діапазоні від 0 до 10, яке характеризує теплову активність відповідної ділянки відбитка пальця.

На основі отриманих значень формується числова матриця, яка зберігається в базі даних як компактне представлення термального відбитка. При цьому слід зазначити, що під час порівняння термальних відбитків аналізуються не абсолютні значення інтенсивності, а їх відносні співвідношення. Зокрема, для послідовності значень у суміжних комірках матриці, наприклад 5-3-7, не вимагається точного відтворення цих чисел у порівнюваному зразку; достатньою умовою є збереження пропорційного співвідношення 5:3:7 з допустимою похибкою до 0,3. Схематичне представлення матричної структури наведено на рисунку 2.6.

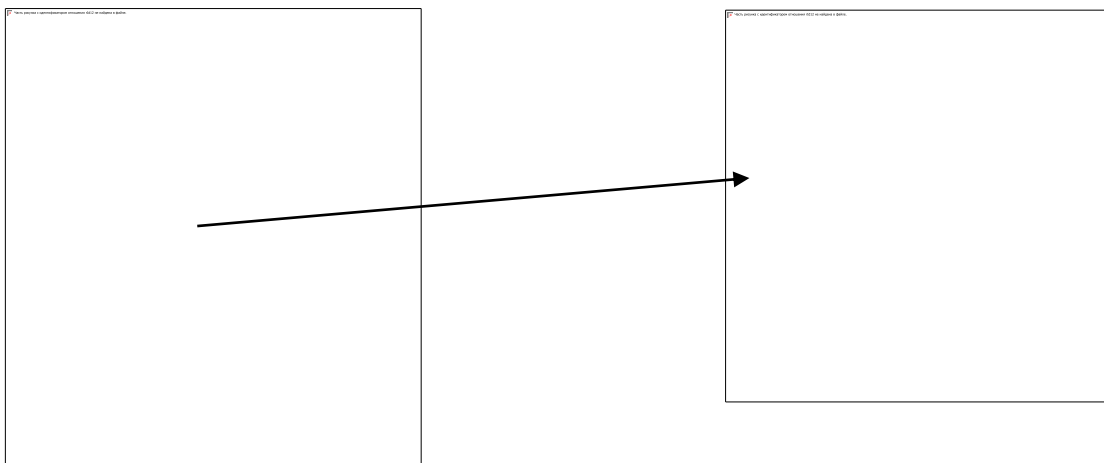
На завершальному етапі отримані дані для обох зображень у вигляді числових матриць (які можуть мати різну розмірність залежно від кількості визначених та отриманих параметрів) порівнюються з відповідними записами, що містяться в базі даних. Водночас для зображення №1, яке є висококонтрастним чорно-білим зображенням, перед безпосереднім порівнянням необхідно виконати додаткову процедуру попередньої обробки.

Оскільки пряме порівняння координат кількох десятків або навіть сотень реєстраційних точок потребувало б значних обчислювальних ресурсів і часу, застосовується метод структурної інваріантності. Згідно з цим підходом кожна з виявлених після обробки характерних точок з'єднується умовними лініями з двома найближчими сусідніми точками, у результаті чого формується множина

трикутників. Надалі отримані трикутні конфігурації корелюються з еталонними даними бази за просторовим розміщенням у двовимірній координатній системі. Такий спосіб порівняння забезпечує інваріантність до повороту зображення, оскільки зіставлення виконується не за абсолютними координатами точок, а за взаємним розташуванням геометричних фігур.



а)



б)

Рисунок 2.6 – Знаходження центра та сегментація оброблюваної області навколо нього на другому етапі ідентифікації:

- а) для первинного (чорно–білого зображення поверхні) зображення;
- б) для вторинного (кольорового зображення тепловіддачі) зображення.

Сумарний коефіцієнт відповідності результатів порівняння зіставляється з наперед заданим пороговим значенням. У випадку, коли величина відхилення не

перевищує 06 %, приймається рішення про відповідність аналізованого відбитка еталонному шаблону. Результат ідентифікації або верифікації може відображатися на дисплеї системи або безпосередньо передаватися на виконавчий інтерфейс, наприклад, керування механізмом відкривання дверей.

Перехресний коефіцієнт визначається як точка, у якій значення коефіцієнта помилкового допуску (FAR) дорівнює значенню коефіцієнта помилкової відмови (FRR) за змінного порогового рівня відповідності. Графічно перехресний коефіцієнт відповідає точці перетину відповідних кривих залежності FAR та FRR від порогового параметра.

Усі системи розпізнавання відбитків пальців орієнтовані на мінімізацію значень коефіцієнтів помилкового допуску та помилкової відмови. Однак на практиці між цими показниками існує компромісна залежність: зменшення одного з них неминуче призводить до зростання іншого. У зв'язку з цим пороговий рівень відповідності повинен підбиратися таким чином, щоб мінімізувати негативні наслідки можливих помилок для конкретної сфери застосування біометричної системи.

У більшості практичних випадків більш критичними є помилкові допуски, оскільки за таких умов несанкціонований користувач може успішно подолати систему контролю доступу, що потенційно призводить до значних негативних наслідків. Водночас наслідки помилкової відмови можуть варіюватися від незначних незручностей до загрози життю людини, залежно від умов експлуатації системи, особливо у разі відсутності резервних або альтернативних механізмів доступу.

Окремі сучасні біометричні системи характеризуються підвищеним рівнем інтелектуальності та, окрім стандартних рішень «допуск» або «відмова», передбачають третій варіант реагування. У таких випадках від користувача може вимагатися надання додаткової інформації або виконання повторної дії, зокрема повторне сканування того самого пальця або сканування іншого пальця за наявності резервного біометричного шаблону в системі.

Процедура порівняння біометричного зразка з еталонним шаблоном реалізується повністю програмними засобами та не залежить від конкретної

технології отримання зображення відбитка пальця. Водночас ключовим чинником зниження ймовірності помилок є забезпечення високої розподільної здатності вхідного зображення, що дозволяє підвищити достовірність виділення ознак та точність подальшого аналізу.

РОЗДІЛ 3

ПРАКТИЧНА ЧАСТИНА

3.1 Вибір обладнання для ідентифікації

В основу нашої розробки програмно-апаратного комплексу для ідентифікації особи покладена модель FingerChip AT77C101B. Вона підтримуються поширеними апаратними платформами, включаючи ARM, STRONGARM, INTEL XScaleT і Texas INSTRUMENTSR, і операційними системами WINDOWS CE і LINUX.

Спеціальне програмне забезпечення розроблене для ідентифікації особи за відбитками пальців, є одним з основних компонентів такого комплексу, бо дозволяє клієнтам отримувати продуктивність та надійність і низьку вартість.

З метою забезпечити велику безпеку в смарт-карту може бути завантажений еталон відбитку пальця її власника. При використанні смарт-карти власник надає зразок відбитку пальця считувачу смарт-карти для аутентифікації. Всі інтегральні схеми, які використовуються як в самій смарт-карті, є у вигляді ASSP або стандартних продуктів. Вони показані на блок-схемі (рис. 3.1).

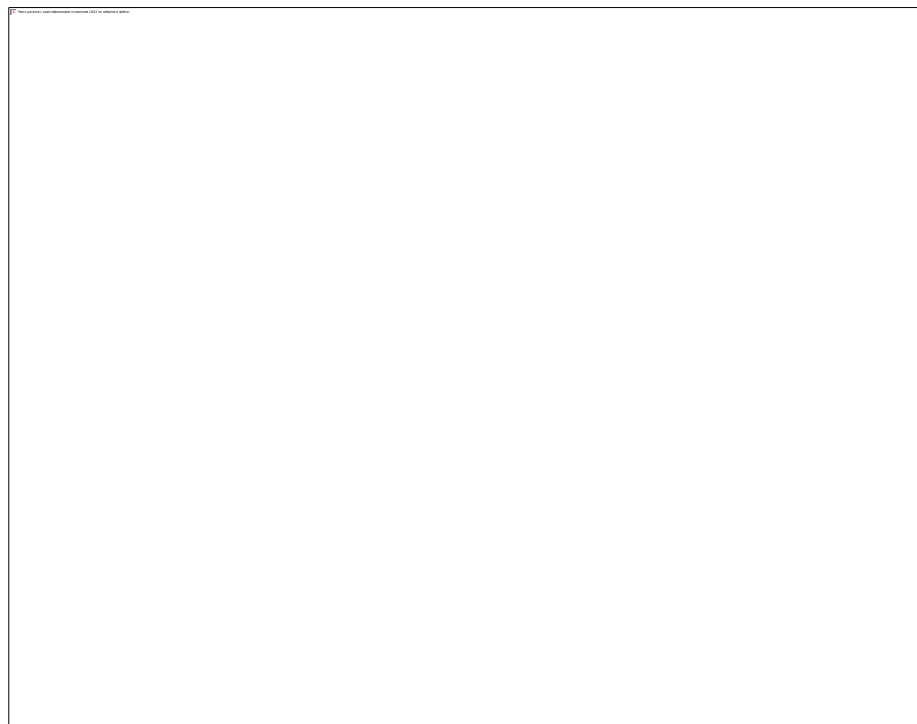


Рисунок 3.1 – Зчитувач смарт-карт з аутентифікацією за відбитком пальця

Перспективи продуктів FingerChip будуються на принципі температурного отримання зображення з подальшою передачею по швидкісних інтерфейсах, таким як USB і SPI. Бо тут досягається вживання продукту в широкому спектрі пристроїв. Одним з таких пристроїв є старт-карта.

Смарт-карта містить захищений 8-розрядний мікроконтролер AT90SC з інтегрованою flash-пам'яттю. Окрім програмного коду та службових даних, у цій пам'яті зберігається зашифрований біометричний еталон відбитка пальця, який записується під час процедури реєстрації власника смарт-карти. Зчитувальний пристрій смарт-карти реалізовано на базі 32-розрядного мікроконтролера AT91 ARM, оснащеного flash-пам'яттю AT49BV, призначеною для зберігання програмного забезпечення та робочих даних. Обмін інформацією між мікроконтролерами AT90SC та AT91 здійснюється через інтерфейс промислового стандарту ISO 7816. Формування та оцифрування зображення відбитка пальця виконується за допомогою спеціалізованої інтегральної схеми AT77C101B FingerChip.

На початковому етапі процедури аутентифікації зчитувальний пристрій на базі мікроконтролера AT91 ініціює активацію мікроконтролера AT90SC, розміщеного у смарт-карті, після чого здійснюється стандартна процедура введення та перевірки персонального ідентифікаційного номера (PIN-коду) через інтерфейс ISO 7816. Даний етап забезпечує базовий рівень підтвердження заявленої особистості користувача.

Після успішної перевірки PIN-коду відбиток пальця особи, яка претендує на роль власника смарт-карти, зчитується за допомогою сенсора FingerChip, оцифровується та передається до мікроконтролера AT91. На цьому етапі AT91 виконує реконструкцію зображення з послідовності кадрів та здійснює виділення біометричного зразка. Отриманий зразок підлягає криптографічному перетворенню, після чого у зашифрованому вигляді передається до мікроконтролера AT90SC, розміщеного у смарт-карті.

Мікроконтролер AT90SC виконує порівняння зашифрованого біометричного зразка, отриманого від зчитувача, з еталонним зашифрованим шаблоном, що зберігається у його захищеній пам'яті. У разі перевищення рівня

відповідності наперед заданого порогового значення формується сигнал підтвердження, який передається до мікроконтролера AT91. За результатами успішного порівняння особистість користувача вважається підтвердженою, після чого виконується відповідна транзакція або надається доступ до ресурсів системи.

Описана процедура аутентифікації відома як режим «збіг з картою». Її ключовою перевагою є те, що зашифрований еталон біометричних даних ніколи не передається за межі смарт-карти, а біометричний зразок надходить на порівняння виключно у зашифрованому вигляді, що істотно підвищує рівень інформаційної безпеки системи.

Як зазначалося вище, реалізація процедур виділення біометричного шаблону та його порівняння з еталоном потребує спеціалізованого програмного забезпечення, яке може бути як придбане у сторонніх розробників, так і створене самостійно. У зв'язку з цим застосування окремих біометричних сенсорів є економічно доцільним переважно у випадках великосерійного виробництва, зокрема у мобільних терміналах та стільникових телефонах.

Для використання зчитувачів відбитків пальців у дрібносерійному та середньосерійному виробництві доцільним є застосування готових біометричних модулів, зокрема модуля AT77SM0101BCB02VKE (рис. 3.2), побудованого на базі 32-розрядного мікроконтролера Atmel AT91RM9200, який інтегрує апаратні та програмні засоби для реалізації повного циклу біометричної аутентифікації.

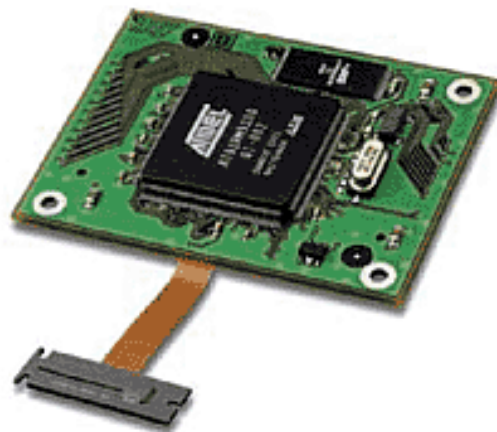


Рисунок 3.2 – Модуль біометрії AT77SM0101BCB02VKE

Модуль AT77SM0101BCB02VKE дозволяє реалізувати наступні функції:

- покадрове прочитування відбитку пальця;
- відновлення картини відбитку пальця;
- ідентифікацію за алгоритмом наведеним вище;
- роботу з базою даних відбитків пальців;
- передачу даних по інтерфейсах RS-232/485, USB, EBI.

До складу такого комплексу біометрії входить считувач AT77C101V-CB02V, модуль біометрії, гнучкий кабель для з'єднання считувача і модуля, програмне забезпечення.

3.2 Технічні передумови створення програмного забезпечення

Завдання створення програмного забезпечення при використанні набору біометрії полягає в написанні програми, що приведена на функціональній схемі програмної частки (рис. 3.3).

Для оцінки можливості модуля AT77SM0101BCB02VKE і розробки програмного забезпечення нижнього рівня випускається набір AT77SM0101BCB02VEK (рис. 3.4), який складається з модуля біометрії AT77SM0101BCB02VKE, базової плати з блоком живлення і роз'ємами (Ethernet, USB, RS232, зовнішньої Flash-пам'яті CompactFlash, SmartMedia, NAND Flash, смарт-карти ISO7816), комутаційних кабелів, документації, демонстраційного ПО для Windows і Linux, SDK для Linux.

Такий налагоджувальний набір здійснює демонстрацію можливостей модуля біометрії та розробку програмного забезпечення верхнього і нижнього рівня.

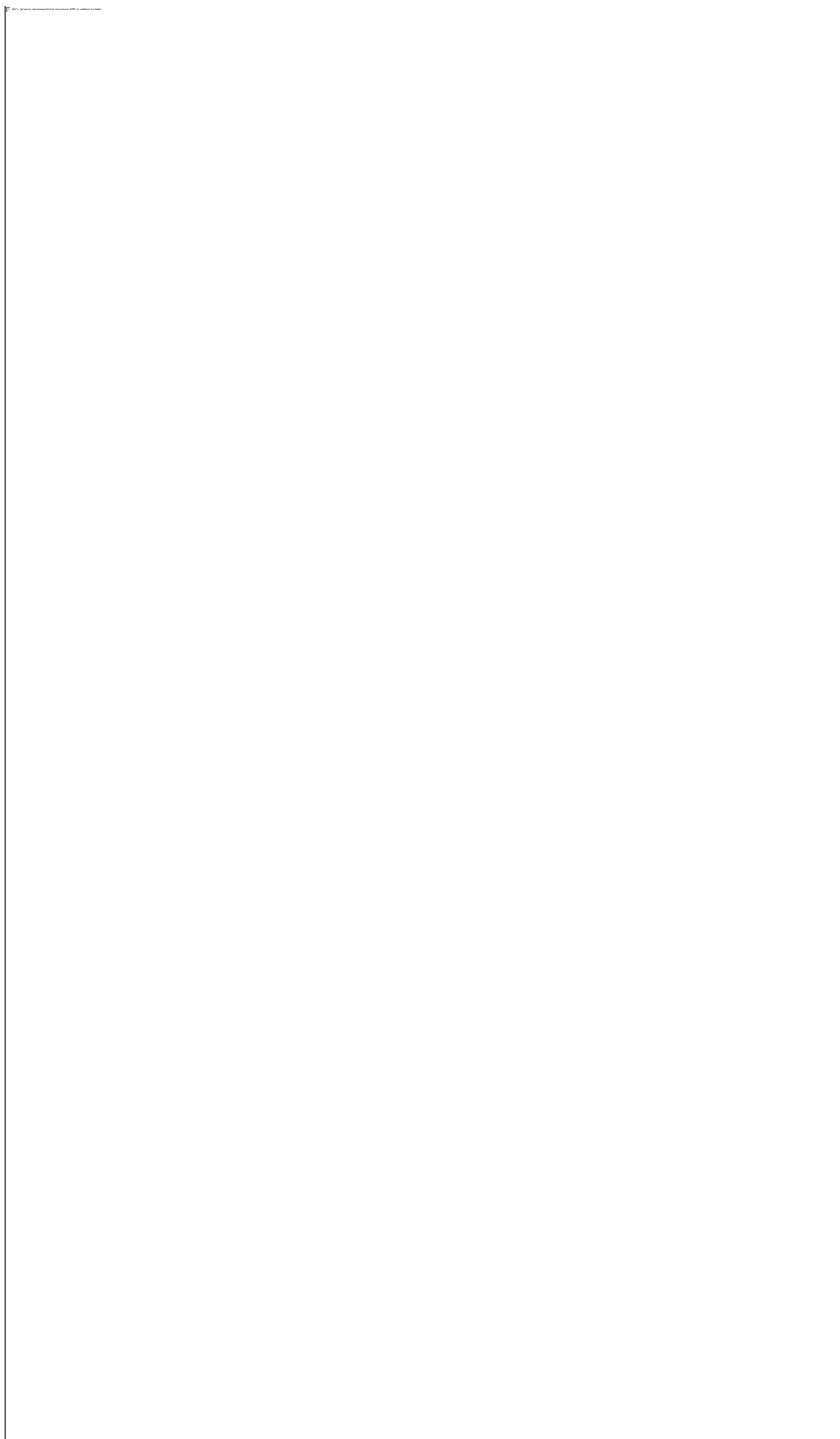


Рисунок 3.3 – Функціональна схема считувача FingerChip



Рисунок 3.4 – Модуль біометрії AT77SM0101BCB02VEK

РОЗДІЛ 4

ПРОГРАМНА ЧАСТИНА

4.1 Опис проекту програмного забезпечення

Проект розроблений за допомогою мови програмування Object Pascal.

На екрані розміщені:

1. Головне вікно Delphi.
2. Вікно форми розробленого проекту.
3. Вікно редактора властивостей об'єктів.
4. Вікно перегляду списку об'єктів.
5. Вікно редактора кода.

У режимі редагування коду та форми проект має наступний вигляд, як показано на рисунку 4.1.

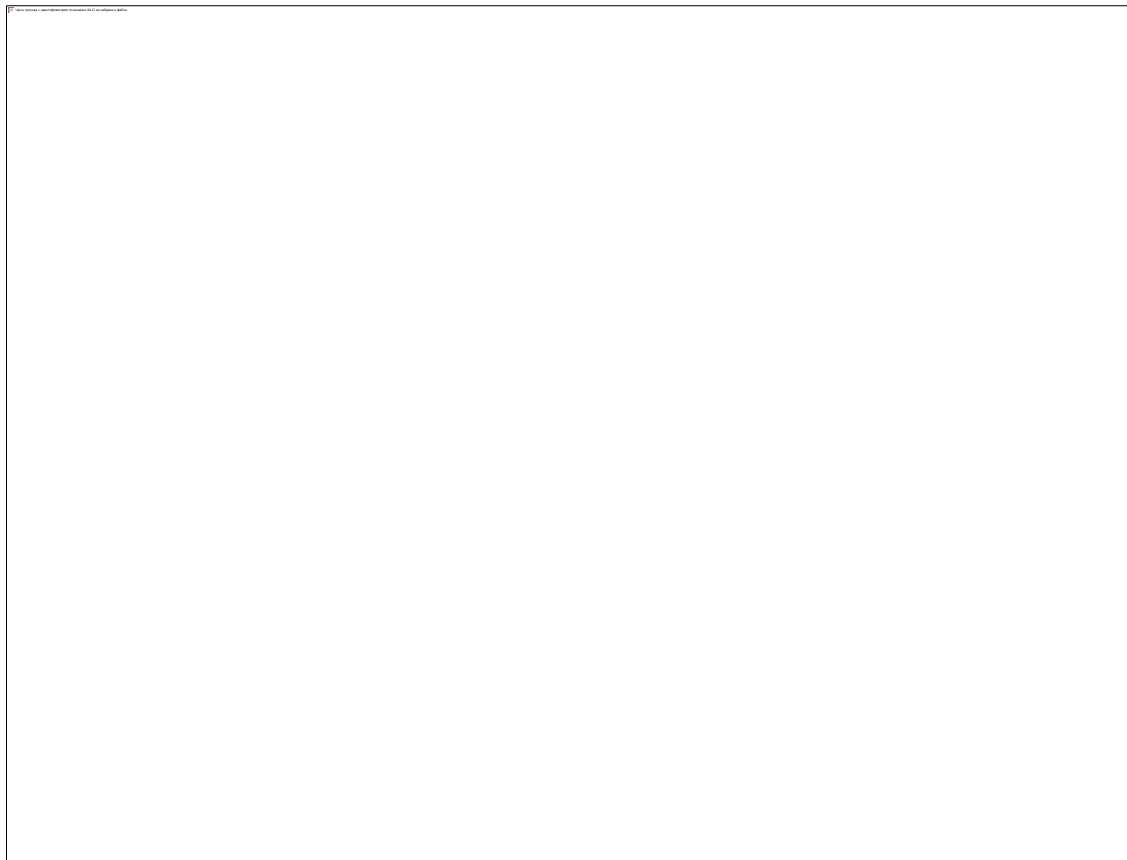


Рисунок 4.1 - Головне вікно з відкритим проектом

При створенні проекту використовувалися стандартні інструменти, які розміщені на палітрі компонентів.

Були використані інструменти з вкладок Standart, Additional, System, Win 32, Samples, Win 3.1, Dialogs (рис. 4.2).

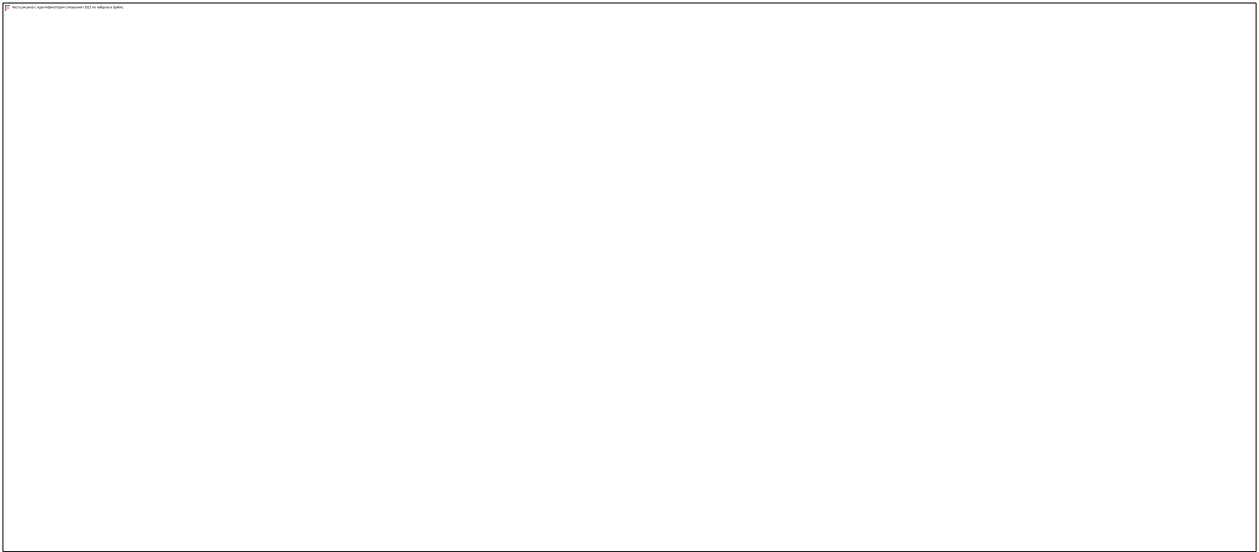


Рисунок 4.2 – Інструменти використані при створенні проекту

Інспектор об'єктів (рис. 4.3) дозволяє регулювати опції, зовнішній вигляд та інші параметри та властивості усіх елементів проекту. Він дозволяє автоматично формувати процедури подій, які можливі для обраного компонента.

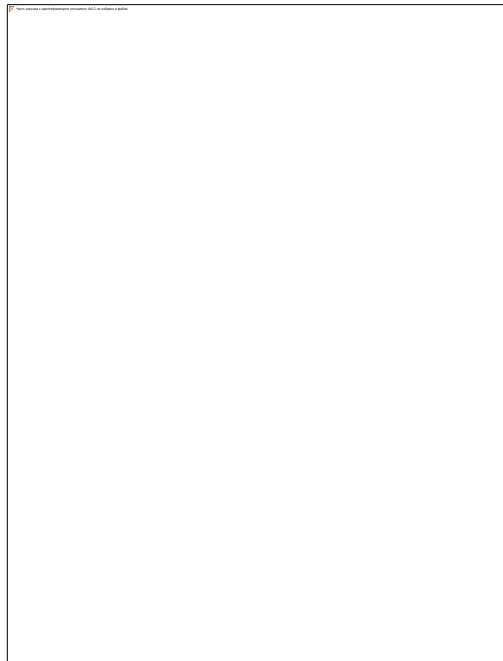


Рисунок 4.3 – Інспектор об'єктів

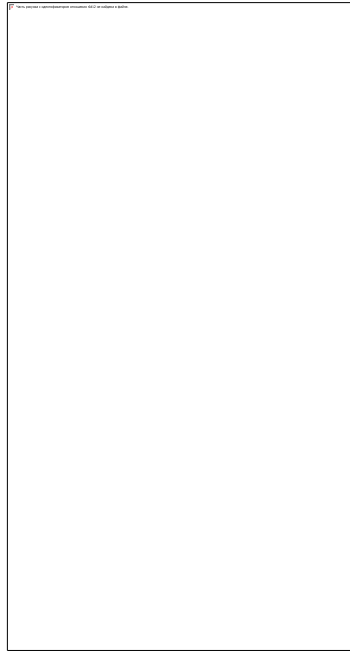


Рисунок 4.4 – Перегляду списку об’єктів

Список об’єктів (рис. 4.4) – це інструмент, що дозволяє легко керувати усім проектом, або окремими його компонентами.

Форма об’єкту (рис. 4.5) використовується для визначення вигляду програми і для розташування невидимих користувачеві елементів. Вона надає користувачу доступ до розробки об’єктів візуально, що є дуже зручним і позбавляє користувача необхідності шукати елемент по назві.

Головна форма проекту містить порядку багато елементів, необхідних для функціонування програми, управління нею та візуалізації роботи.

Серед них:

- Bevel1. Використані для забезпечення кращого естетичного сприйняття форми і візуального відокремлення об’єктів на формі. Відповідно усі фаски застосовані у двох виглядах – `bsLowered` (утоплена) і `bsRaised` (опукла).
- Button. Ними здійснюється основне управління програмою задля оптимізації роботи програми та зменшення кількості візуалізації, що призводить до додаткового непотрібного навантаження на систему.
- GroupBox – компонент, який містить в собі групу певних пов’язаних компонентів.

- Label – компонент, що дозволяє розміщувати надписи на самій формі, а також на будь-якому її елементі.
- Image – елемент, для візуалізації обробки зображення. Показує користувачеві зображення (RAW), з яким і працює алгоритм обробки
- Memo – компонент, який виводить текстовий результат окремих етапів роботи алгоритму. Його зміст можливо зберігати у звичайний текстовий файл.
- Main Menu – компонент, що створює головне меню програми.
- OpenFileDialog – компонент, що викликає стандартний діалог операційної системи.
- SaveFileDialog – компонент, що викликає стандартний діалог операційної системи.
- SaveDialog – компонент, що викликає стандартний діалог операційної системи для збереження повідомлень алгоритму.
- Timer – компоненту відліку часу.
- StaticText – компонент, який використаний для підпису груп кнопок на формі.
- CheckBox – компонент, що використовується для попереднього визначення певних подій.

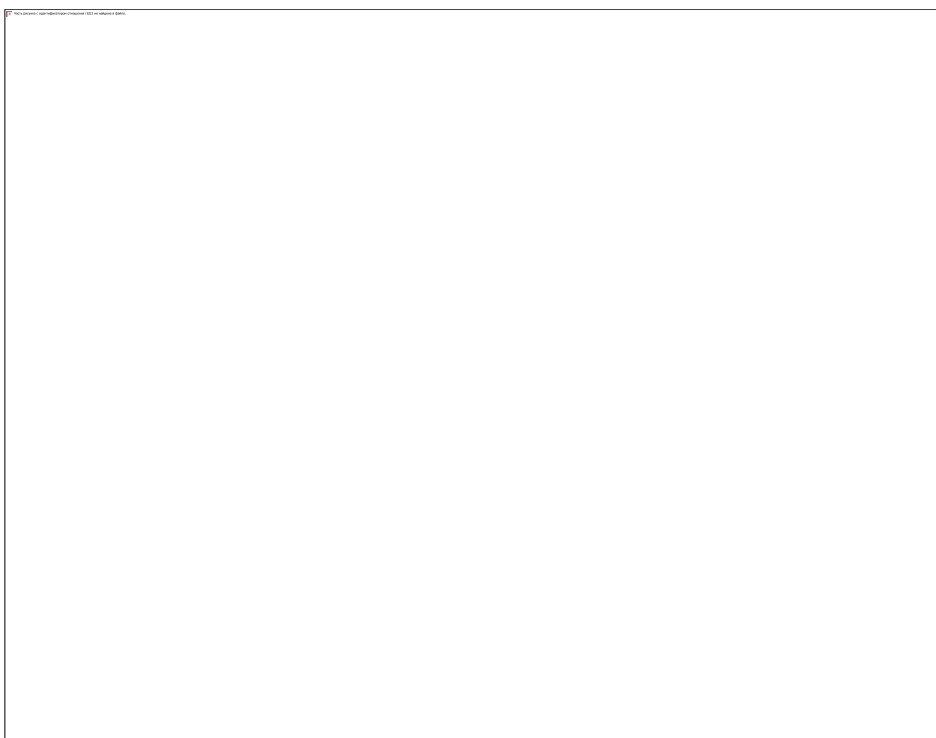


Рисунок 4.5 – Форма проекту

Розроблений проект `Fingers` складається з програмних одиниць – модулів (рис. 4.6):

1. Головний модуль, який містить інструкції з яких починається виконання програми і зв'язки з бібліотеками;
2. Модуль головної форми `uMain.pas`, який містить опис форми додатку і процедури, які підтримують її роботу.

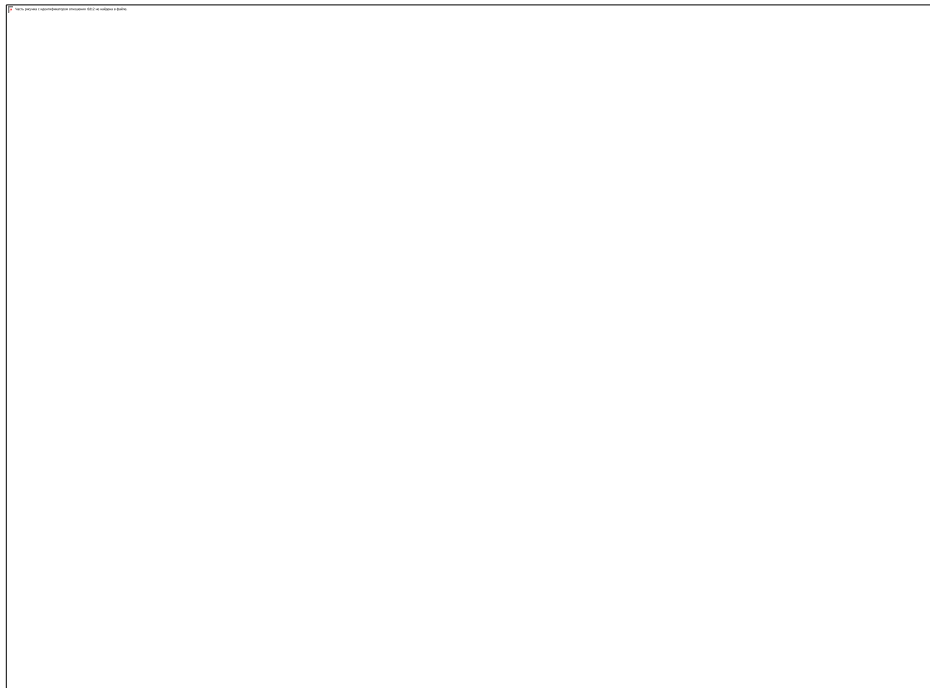


Рисунок 4.6 – Редактор коду з відкритим проектом

Крім того тут присутні додаткові модулі та бібліотеки, що забезпечують роботу алгоритму, а також містять усі необхідні для його роботи елементи.

- Для написання проекту були створені наступні процедури користувача у головному модулі:
- процедура додавання нового відбитку в базу;
- процедура запуску процесу ідентифікації відбитку;
- процедура запуску процесу верифікації відбитку;
- процедура створення тимчасового зображення для обробки відбитку і визначення якості вхідного зображення;

- процедура очистки бази даних відбитків;
- процедура очистки поля звіту роботи програми;
- процедура збереження відкритого в програмі зображення;
- процедура завантаження зображення з графічного файлу;
- процедура показує повідомлення з версією програми;
- ряд дублюючих функцій, що повторюють функції пунктів головного меню на кнопках у формі (procedure TFormMain.Button4Click, procedure TFormMain.Button5Click, procedure TFormMain.Button2Click і тд.);
- викликає модуль налаштування зображення uOptions;
- процедура викликає діалог операційної системи для збереження змісту текстового поля звіту.

А також деякі функції і процедури додаткових модулів:

- функція звернення до бібліотеки обробки зображення;
- процедура перезапуску звіту програми;
- процедура перезапуску циклу обробки зображення;
- процедура перезапуску циклу роботи програми після завантаження нового зображення;
- функція зв'язку з базою даних;
- процедура закриття зв'язку;
- процедура очистки тимчасового звіту;
- функція додавання тимчасового зображення в базу даних;
- процедура виклику зображення з бази для порівняння
- процедура встановлення значень функцій змінних алгоритму;
- процедура визначення подій алгоритму та їх повідомлень;
- процедура визначення помилкових дій алгоритму та їх повідомлень;
- функція перевірки параметрів тимчасового зображення;
- процедура фіналізації роботи програми та закриття усіх з'єднань;
- процедура відображення відбитку на екрані.

Лістинг використуваних бібліотек та додаткових модулів можна знайти на диску з програмою.

Зв'язок між програмною оболонкою та базою здійснюється за допомогою open-source компонента Microsoft Jet.OLEDB.4.0. Компонент забезпечує захищений двосторонній зв'язок, створює закритий mdb-файл бази. При цьому наявність додаткового програмного забезпечення не потрібна.

З міркувань безпеки його розміщують на окремому спеціалізованому сервері з розмежованим доступом, що забезпечує надійність та доступ до запису-читання бази.

Приклад коду додавання запису в базу:

```
function TDBClass.addTemplate(template: TTemplate): Integer;
var
  rs: TADODataset;
  tptStream: TMemoryStream;
  id: Integer;
begin

  rs := TADODataset.Create(nil);
  rs.Connection := connection;
  rs.CursorType := ctStatic;
  rs.LockType := ltOptimistic;
  rs.CommandText := 'SELECT * FROM enroll';
  rs.Open();
  rs.Append();
  tptStream := TMemoryStream.Create();
  tptStream.write(template.tpt^, template.size);
  (rs.FieldByName('template') as TBlobField).LoadFromStream(tptStream);
  rs.post();
  id := rs.FieldByName('ID').AsInteger;
  tptStream.Free();
  rs.Close();
  rs.Free();
  addTemplate := id;
end;
```

Існує можливість шифрування інформації, що передається з бази та надходить в базу за допомогою методу дільників надвеликих чисел. Найпростіший ключ в 64 біта довжиною, генерація якого займає близько 1,5-2 секунд володіє криптографічною стійкістю в мінімум п'ять років.

4.2 Графічний інтерфейс користувача програми

При запуску виконавчого файлу проекту Fingers.exe користувач бачить на екрані робочу оболонку програми, яка має наступний вигляд (рис. 4.7).

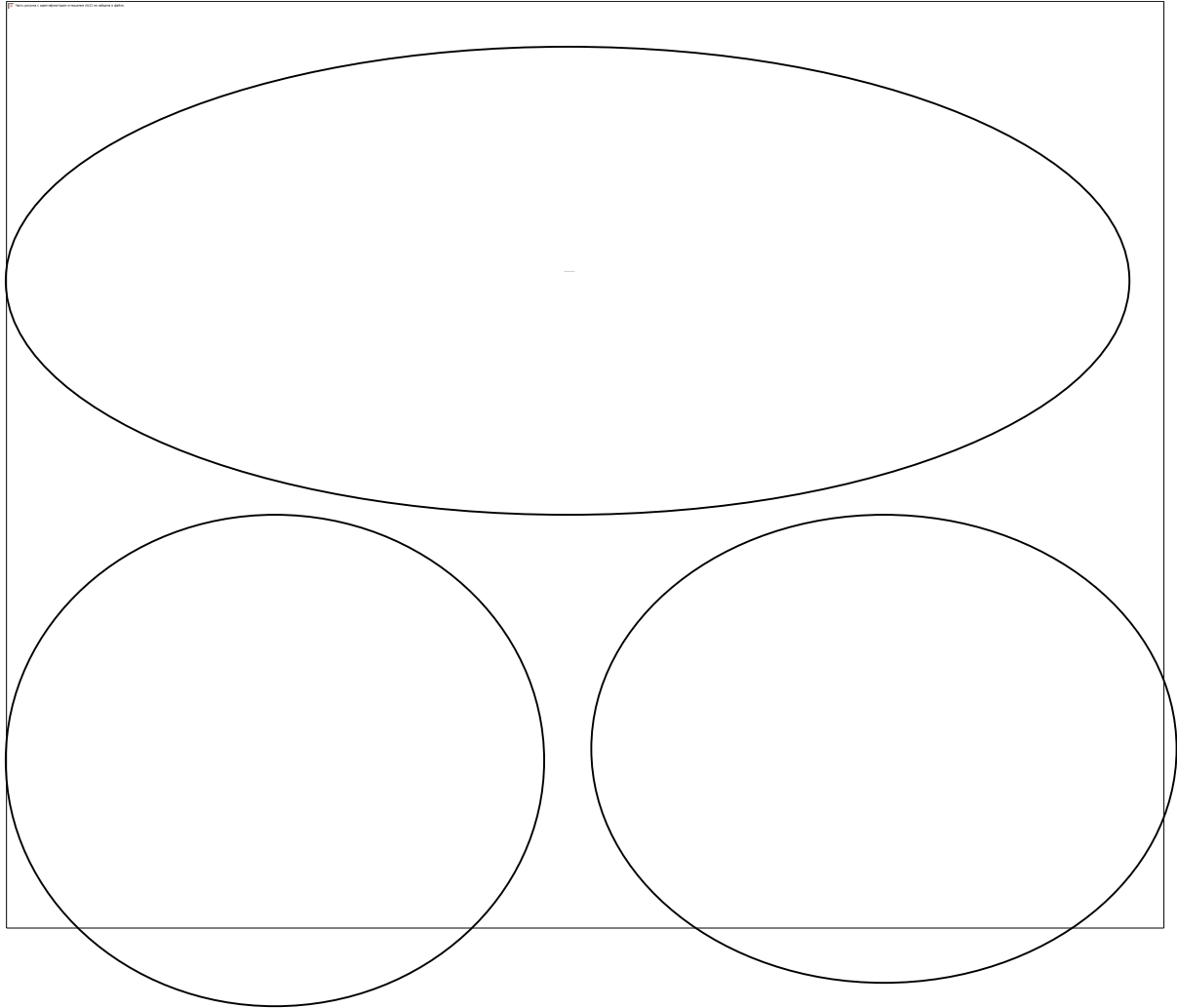


Рисунок 4.7 – Робоча оболонка програми

Як видно з рисунку 4.7, робоча область поділена на 3 сектори відповідно до функціонального призначення. Також присутнє головне меню програми.

Сектор I надає користувачеві варіанти дій та опцій алгоритму обробки, а також реалізує функції роботи з файлом, що повторюють елементи головного меню. Тут є наступні кнопки керування:

— «Опції» – кнопка виклику модуля опцій відображення (рис. 4.8).

- «Обробка» – пошук та виділення спеціальних точок на зображенні, їх сполучення у трикутники.
- «Ідентифікація» – порівняння отриманих даних із присутніми в базі даних та виявлення співпадань.
- «Додати» – додавання нового відбитку в базу даних (при невизначені попередніми діями).

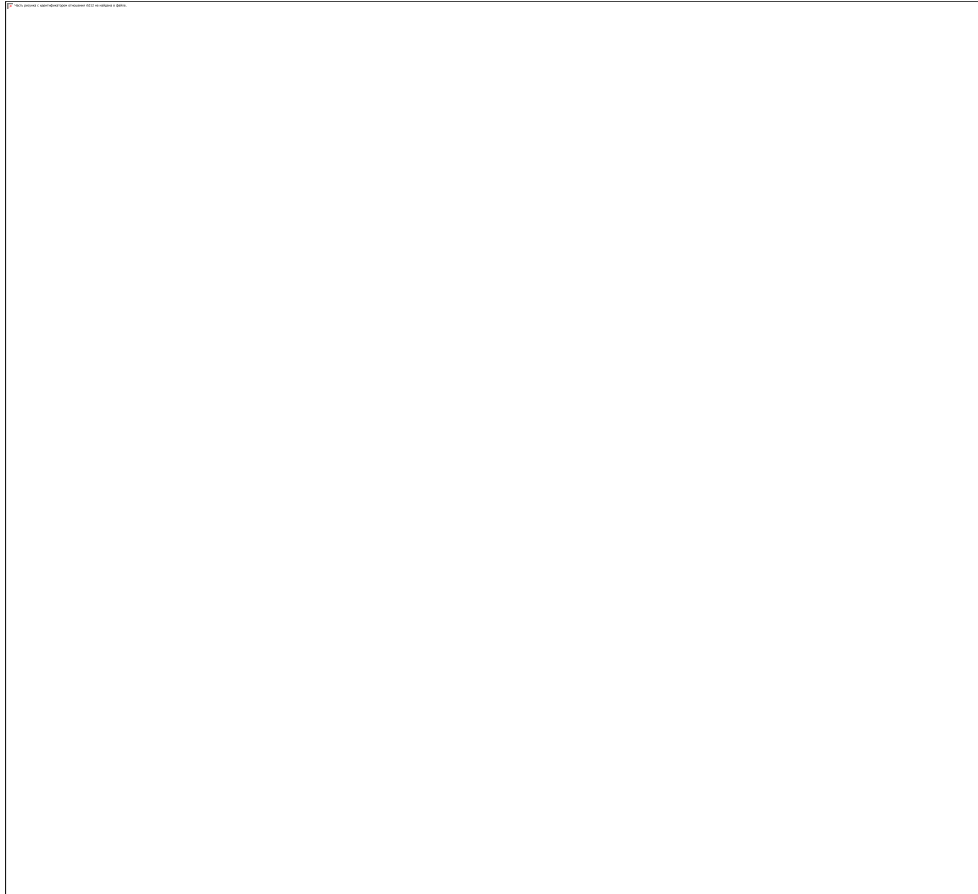


Рисунок 4.8 – Модуль опцій відображення

- «Верифікація» – порівняння вхідного зображення з конкретним із бази даних на відповідність (верифікація особистості).
- Група опцій автоматичної обробки та ідентифікації зображення при відкритті – «Авто-обробка» і «Автоматом?» (рис. 4.9)

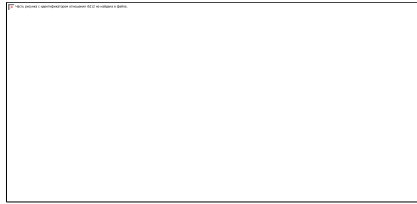


Рисунок 4.9 – Група опцій автоматичної обробки

- «Вихід» – закриття програми та фіналізація роботи алгоритму;
- «Обробка» (з фаски групи функцій для роботи з термо-картиною) – первинна обробка зображення. Поділ на сектори.
- «Ідентифікація» - співставлення визначеною матриці насиченості з існуючими в базі і визначення додаткового коефіцієнту відповідності після першого етапу роботи алгоритму.
- «Відкрити» – завантаження зображення із графічного файлу;
- «Зберегти» – збереження відкритого зображення;
- «Зберегти звіт» – збереження вмісту текстового поля звіту роботи алгоритму в текстовий файл.

Сектор II (рис. 4.10) являє собою 2 фаски, на яких, при завантаженні, відображається зображення відбитку (область малюнку зліва), а також тимчасове зображення після обробки (область малюнку справа).

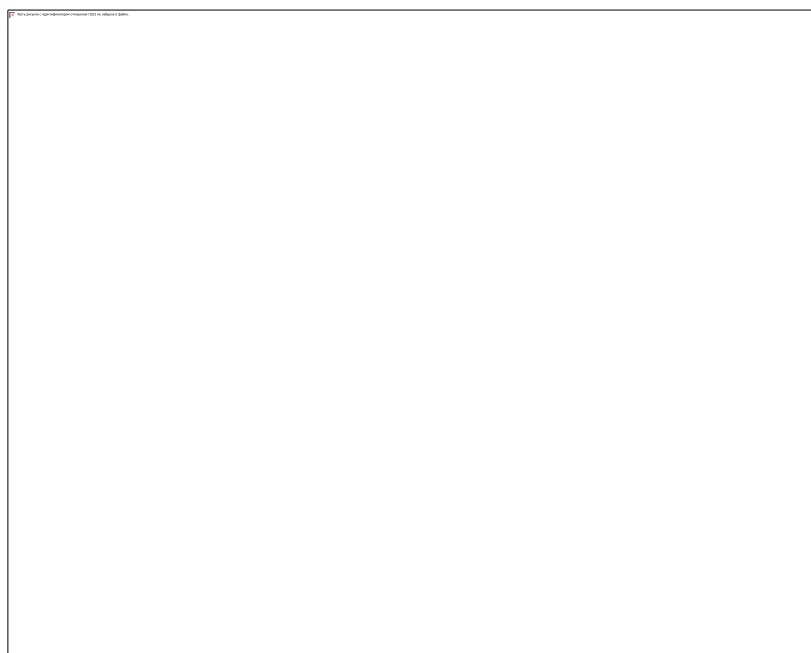


Рисунок 4.10 – Вікно програми після виконання обробки

Сектор III являє собою текстове поле звітування роботи програми (рис. 4.11).

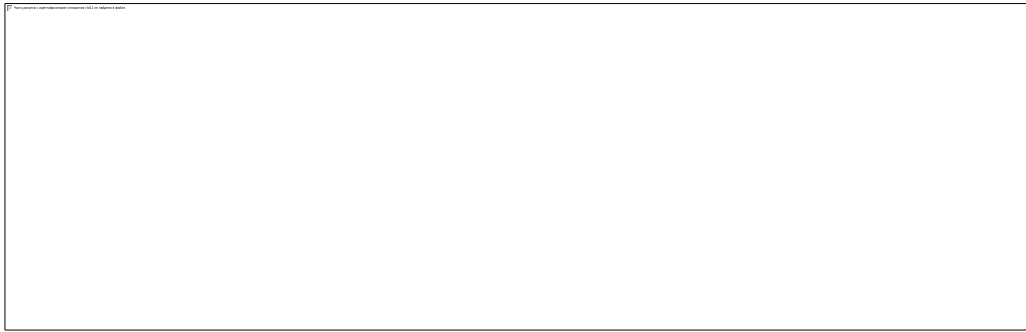


Рисунок 4.11 – Область звітування

- «Очистити базу даних» – видалення з бази наявних відбитків;
- «Очистка логу» – очищення поля виводу повідомлень роботи алгоритму;
- «Поточна дата і час».

При натисканні на елемент головного меню «Про продукт» користувач отримує наступне повідомлення (рис. 4.12):



Рисунок 4.12 – Повідомлення «про продукт»

4.3 Інтерфейс та специфікація програми установки

Програмний продукт є засобом безпеки – встановлення повинне бути захищене від зловмисників. Програма працює з динамічними бібліотеками, що вимагає додаткового їх пропису у реєстрі операційної системи. Виходячи з цих вимог, був обраний пакет для створення установочних файлів та скриптів Inno Setup Compiler, що розповсюджується на безплатно та надає надзвичайно широкі можливості по створенню, налагодженню та конфігурації установки.

Робота з Inno Setup Compiler проста і не вимагає додаткових знань мови скриптування.

Головне вікно програми являє собою простий на вигляд редактор скрипту, усі додаткові функції якого реалізуються через головне меню (рис. 4.13).

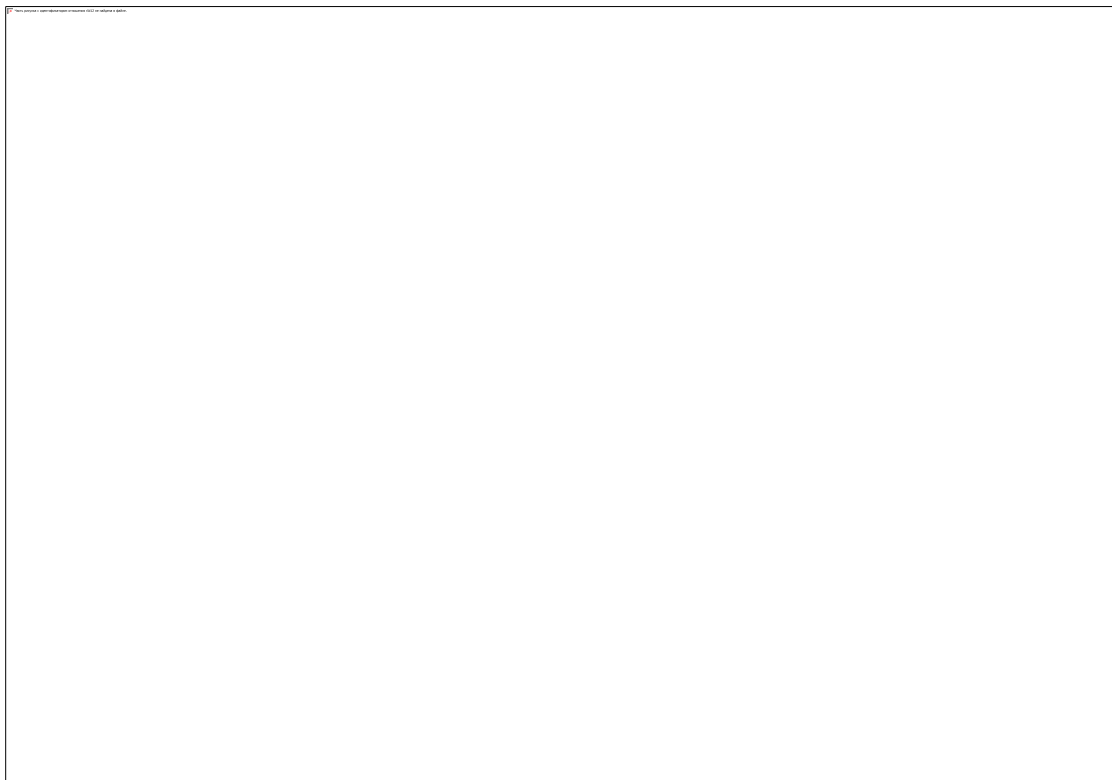


Рисунок 4.13 – Головне вікно пакету Inno Setup Compiler

Розділ Sections – список модулів, що будуть задіяні в майбутній установці.
Розділ Script – вікно безпосереднього редагування скрипту.

Приклад частини скрипту установки:

[Setup]

```
AppName=Fingerprint
AppVerName=Fingerprint v 1.2.2.
DefaultDirName={pf}\Presston\Fingerprint
OutputBaseFilename=Fingerprint
Compression=lzma
```

[Files]

```
Source: "{app}\samples\FingerSample.mdb"; DestDir: "{app}\samples"; Flags: ignoreversion
Source: "{app}\bin\GrFinger,1.dll"; DestDir: "{app}\bin"; DestName: "GrFinger.dll"; Flags: ignoreversion
Source: "{app}\Delphi\Fingers\bin\Fingers.exe"; DestDir: "{app}\Delphi\Fingers\bin"; Flags: ignoreversion
....
```

[Icons]

```
Name: "{group}\Delphi\Fingerprints"; Filename: "{app}\Delphi\Fingers\bin\Fingers.exe"; WorkingDir:
"{app}\Delphi\Fingers\bin";
```

[Components]

```
Name: "full"; Description: "Fingerprint v 1.2.2."; Types: "fulltype";
```

[Types]

```
Name: "fulltype"; Description: "Fingerprint v 1.2.2.";
```

[CustomMessages]

[Languages]

Скрипт дозволяє включати додаткові налаштування для майбутньої встановленої програми:

- ярлики та групи ярликів в Головному меню;
- ярлики на Робочому столі;
- типи установки програмного продукту (повна, часткова та ін.)
- компоненти для установки;
- вибір зображення та написів для демонстрації під час установки;
- додаткові файли ліцензії, ліцензійних умов і тд;
- додаткова перевірки цілісності файлів;
- додаткова перевірка версії файлів;
- додаткові мови установки.

Після перевірки та виконання написаного скрипту Inno Setup Compiler компіює виконуючий exe-файл. Це буде здійснювати саму установку. Виконання цього файлу не вимагає ніяких додаткових встановлених програмних продуктів

у системі (рис. 4.14). Сам файл установки компілюється в захищеному режимі, тому змінити його після створення неможливо.

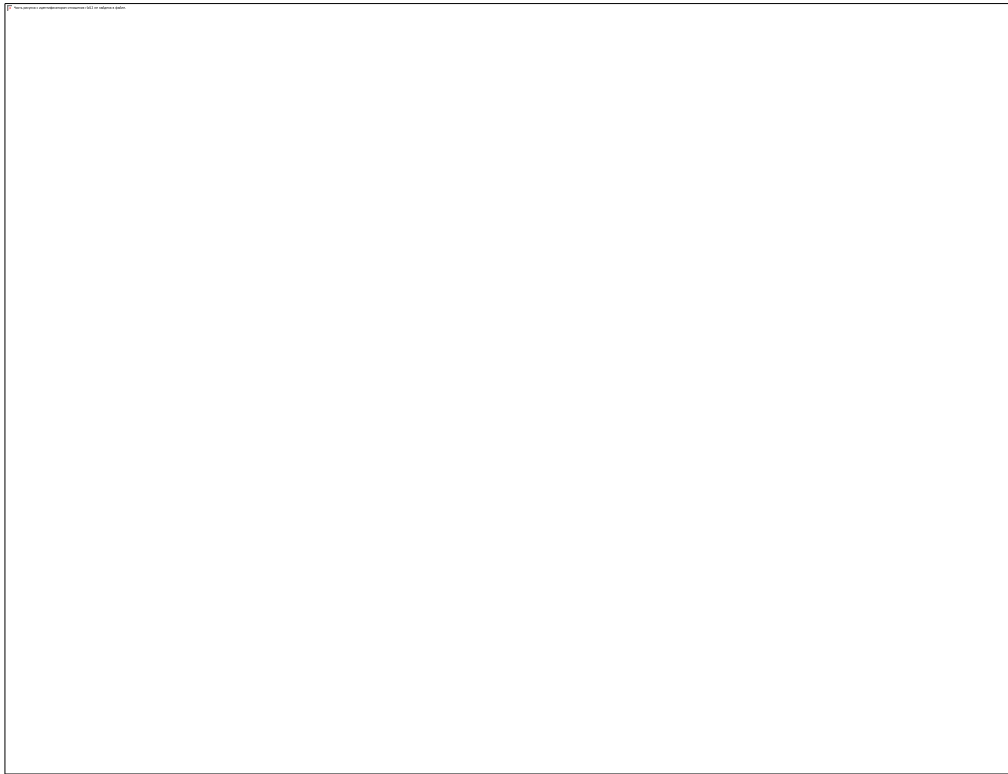


Рисунок 4.14 – Вигляд вікна програми установки

Створена програма установки (рис. 4.14) є зручною та легкою у використанні. Це вимагає від недосвідченого користувача лише три натискання кнопки «Next». Після цього наш програмний продукт буде встановлено у визначеному наперед місці, а його компоненти автоматично зареєстровані.

ВИСНОВКИ

У ході виконання даної кваліфікаційної роботи магістра на підставі аналізу та узагальнення існуючих методик та методів ідентифікації особи було розроблено комбінований програмно-апаратний комплекс, який призначений для визначення відповідності поточних біометричних даних записам суб'єктів доступу, що зберігаються у базі даних.

У процесі огляду сучасних програмних і програмно-апаратних засобів для обробки та ідентифікації зображень відбитків пальців виявлено низку характерних недоліків, серед яких: недостатня швидкодія обробки зображень, низька ефективність використовуваних алгоритмів, значне математичне навантаження на обчислювальні ресурси системи, а також обмежена доступність технічної та експлуатаційної документації різними мовами.

Розроблений програмно-апаратний комплекс ідентифікації осіб за зображеннями відбитків пальців, що реалізується із застосуванням персонального комп'ютера, спеціалізованого сканера та програмного забезпечення забезпечує виконання таких основних функцій:

- виявлення характерних точок на цифровому зображенні відбитка пальця;
- об'єднання виявлених точок у трикутні структури з подальшим обчисленням узагальненого векторного опису кожної з них;
- визначення кількості співпадаючих ознак під час порівняння біометричних зразків;
- локалізацію центру термального зображення відбитка;
- формування матриці значень тепловіддачі (інтенсивності забарвлення) секторів, розташованих у околі визначеного центру.

За результатами проведених розрахунків та експериментальних досліджень встановлено, що застосування розробленого програмно-апаратного комплексу дозволяє істотно скоротити часові витрати на обробку біометричної інформації, а досягнутий рівень економічної ефективності впровадження системи становить 47,3 %.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. A.D.Kuo, An optimal control model for analyzing human postural balance, - IEEE Transactions on biomedical engineering. Vol.42. №1, 2005. Pp.87-102.
2. Masaki Oshita and Akifumi Makinouchi A Dynamic Motion Control Technique for Human-like Articulated Figures EUROGRAPHICS 2001 / A. Chalmers and T.-M. Rhyne (Guest Editors), Volume 20, 2021. №3.
3. Jerzy Mrozowski, Jan Awrejcewicz Changes in the gait characteristics caused by external load, ground slope and velocity variation. Commun Nonlinear Sci Numer Simulat 16, 2021. Pp. 2313–2318.
4. Taku Komura, Yoshihisa Shinagawa and Tosiyasu L. Kunii Calculation and Visualization of the Dynamic Ability of the Human Body The journal of visualization and computer animation J. Visual. Comput. Animat.10, 2020. Pp. 57–78.
5. Povstianoi O., Markina L., Denysiuk V., Lapchenko Y., Satsyk V., Pylypets M. Automated smart humanoid robot arm on the arduino platform V. 129, Issue 4. 2025, P.43-53. <https://doi.org/10.7862/tiam.2025.4.4>
6. Jerzy Mrozowski, Jan Awrejcewicz, Piotr Bammerski. Analysis of stability of the human gait. Journal of theoretical and applied mechanics 45 (1), 2021, pp. 91-98.
7. Korzhyk O., Morenko O., Morenko A., Kotsan I. Gender features of brain processes during inhibition of manual movements' program. Annals of Neurosciences. 2019. Vol. 26, No 1. P. 4–9. <https://doi.org/10.5214/ans.0972.7531.260103> Scopus (Q3), Web of Science/
8. Кваліфікаційна робота: методичні вказівки до оформлення кваліфікаційних робіт для здобувачів першого (бакалаврського) та другого (магістерського) рівнів вищої освіти всіх освітніх програм денної та заочної форм навчання / уклад. Н.В. Ковальчук, Ю.Г. Фесіна, І.Л.Заблоцька Луцьк : ЛНТУ, 2023. 46 с.
9. Інноваційні підходи в підготовці магістрів з прикладної механіки : навч. посіб. / Т. Є. Божко, Б. П. Валецький, Л. М. Самчук, Т. І. Четвержук. Луцьк : Вежа-Друк, 2024. – 324 с.

10. Методичні рекомендації до написання кваліфікаційної роботи за ступенем вищої освіти «магістр» : метод. рекомендації для здобувачів другого (магістерського) рівня вищої освіти освітньої програми «Прикладна механіка», спец. 131 Прикладна механіка, галузі знань 13 Механічна інженерія денної та заоч. форм навч. / уклад.: Т. І. Четвержук, Р. М. Полінкевич. Луцьк: ЛНТУ, 2024. 48 с.

11. Дмитрієв Д.О. Кінетостатичний аналіз каркасних компоновок верстатів з механізмами паралельної структури // Науковий журнал "Технологічні комплекси" №2, 2020. С. 40=45.

12. Бороzeneць Г.М., Павлов В.М., Семак І. В. Деталі машин : Навчальний посібник. – К.: Видавничий дім «Кондор», 2021. 220 с.

13. Головня В.Д. САПР технологічних процесів : конспект лекцій / В.Д. Головня. Житомир : Житомирська політехніка, 2019. 200 с.

14. Morenko A., Morenko O., Dmytrotsa O., Poruchynsky A., Korzhyk O. Changes in electroencephalogram (EEG) power during subdominant (left) hand finger movements in females with different alpha rhythm characteristics. Health Problems of Civilization. 2020. Vol 14, No 1. P. 63–69. 15. <https://doi.org/10.5114/hpc.2020.93295> [Web of Science/](#)

15. Korzhyk O. V., Dmytrotsa O. R., Poruchynskyi A. I., Morenko A. H. Event-related potentials during contralateral switching over motor programs in humans. Regulatory Mechanisms in Biosystems. 2020. Vol. 11, No 1. P. 110–115. <https://doi.org/10.15421/022016> Scopus (Q4), Web of Science.

16. Чех О., Моренко О., Титюк О., Коржик О., Моренко А. ЕМГ – активність м'язів верхньої кінцівки людини при патології нервово-м'язового проведення. Науковий вісник Східноєвропейського національного університету імені Лесі Українки. Біологічні науки. 2019. № 4(388). С. 168–178. <https://doi.org/10.29038/2617-4723-2019-388-4-168-178>

17. Korzhyk O., Morenko A., Poruchynskyi A., Dmytrotsa O. Event-Related Potentials under Condition of Switching over of the Programs of Manual Movements in Humans. NEURONUS 2020 IBRO Neuroscience Forum (December 8-11 2020). Online, 2020.

18. Korzhyk O., Morenko A. Event-related potentials under conditions of cessation of the motor programs in humans. FENS Regional Meeting: Book of Abstracts (Krakow, August 25-27 2021). Krakow, 2021. P.182.

19. Дмитроца О. Р., Коржик О. В., Журавльов О. А. Функціональний стан опорно-рухового апарату сучасних школярів. Перспективи розвитку фізичної культури і спорту у закладах освіти : матеріали Всеукр. онлайн наук. конф. з міжнародною участю (м. Луцьк, 19-20 травня 2022 р.). Луцьк, 2022. С. 52-54.

20. Korzhyk O., Morenko A. Cortical sources of electrical activity, related to the cessation of a prepared motor reaction in humans. *Acta Neurobiologiae Experimentalis NEURONUS* 2022. 2022. P. LXXXIII (85). Scopus, Web of Science <https://ane.pl/index.php/ane/issue/view/260>

21. Korzhyk O., Morenko A. Cortical sources of electrical activity, related to the switching to an alternative motor program in humans. *Acta Neurobiologiae Experimentalis*. VIth International Congress of the Polish Neuroscience Society (Torun, 20-23.09.2023). 2023. Vol. 83, No Supl 1. P. 91-92. <https://ane.pl/index.php/ane/issue/archive> Scopus (Q3), Web of Science Core Collection

22. Коржик О. В., Моренко А. Г., Дмитроца О. Р. Статеві особливості викликаної активності кори головноо мозку за умов зупинки запущеної моторної програми мануального руху. *Фізіологічний журнал (НАН України, Інститут фізіології ім. О. О. Богомольця, 25-27 липня 2022 р.)*. 2022. Т. 68, № 3S. С. 55. Scopus.

23. Cyr, K. M., Segal, A. D., Neptune, R. R., & Klute, G. K. Biomechanical responses of individuals with transtibial amputation stepping on a coronally uneven and unpredictable surface. *Journal of Biomechanics*. 2023. Vol. 155. DOI: 10.1016/j.jbiomech.2023.111622.

24. The Evolution of Prosthetic Limbs. URL: <https://www.sutori.com/en/story/the-evolution-of-prosthetic-limbs-WHf39iforVcK1V7rueghYRxN> (Last accessed: 10.06.2024).

25. Bertelson, S., Molina, L., Neptune, R. R., Djurdjanovic, D. System-based monitoring of muscular fatigue in lower-extremity movement. Annual Conference of

the Prognostics and Health Management Society. 2023. Vol. 15. No. 1. P. 1–9. DOI: 10.36001/phmconf.2023.v15i1.3551.

26. Panhelleux, B., Shalhoub, J., Silverman, A. K., McGregor, A. H. A review of through-knee amputation. *Vascular*. 2022. Vol. 30. No. 6. P. 1149-1159 DOI: 10.1177/17085381211045183.

27. Crouch, D. L., Hall, P. T., Stubbs, C., Stephenson, S. M., Anderson, D. E. Feasibility of implanting a foot–ankle endoprosthesis within skin in a rabbit model of transtibial amputation. *Bioengineering*. 2022. Vol. 9. No. 8. P. 348. DOI:10.3390/bioengineering9080348.

28. Hall, P. T., Bratcher, S. Z., Stubbs, C., Anderson, D. E., Crouch, D. L. Fully Implanted Prostheses for Musculoskeletal Limb Reconstruction After Amputation: An In Vivo Feasibility Study. *Annals of Biomedical Engineering*. 2021. Vol. 49. No.3. P. 1012-1021. DOI:10.1007/s10439-021-02741-z.

29. Kowalski, N., Zhu, X., Crouch, D. L. Using the Intact Human Hand to Benchmark Real-Time Myoelectric Control Performance for Robotic Interfaces. *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*. 2021. P. 6524-6527.

30. Hussain Z., Azlan N. Z. 3-D Dynamic Modeling and Validation of Human Arm for Torque Determination During Eating Activity Using Kane’s Method // *In Iranian Journal of Science and Technology Transactions of Mechanical Engineering*. – 2020. – Vol. 44(3). DOI:10.1007/s40997-019-00299-8.

28. Davoudabadi Farahani S., Svinin M., Andersen M. S., de Zee M., Rasmussen J. Prediction of closed-chain human arm dynamics in a crank-rotation task // *Journal of Biomechanics*. 2020. Vol. 49(13). P. 2684–2693. DOI:10.1016/j.jbiomech.2016.05.034.

29. Lemieux P. O., Tétreault P., Hagemester N., Nuno N. Influence of prosthetic humeral head size and medial offset on the mechanics of the shoulder with cuff tear arthropathy: A numerical study // *Journal of Biomechanics*. 2023. Vol. 46(4). P. 806–812. DOI:10.1016/j.jbiomech.2012.11.021.

30. Ali N., Andersen M.S., Rasmussen J., Robertson D.G.E., Rouhi, G. The application of musculoskeletal modeling to investigate gender bias in non-contact ACL

injury rate during single-leg landings / Computer methods in biomechanics and biomedical engineering. 2024. Vol. 17(14). P. 1602-1616.

31. Rasmussen J., Torholm S., de Zee M. Computational analysis of the influence of seat pan inclination and friction on muscle activity and spinal joint forces // International Journal of Industrial Ergonomics. 2020. Vol. 39(1). P. 52-57. DOI:10.1016/j.ergon.2008.07.008

32. Rasmussen J., Holmberg L.J., Sorensen K., Kwan M., Andersen M.S., de Zee M. Performance optimization by Musculoskeletal simulation / Mov. Sport Sci. – 2022. Vol. 1(75). P. 73–83.

33. Ariff F. H. M., Rambely A. S., Ghani N. A. A.Shoulder’s modeling via Kane’s method: Determination of torques in smash activity // IFMBE Proceedings. - 2021. Vol. 35(6). P. 207-209. DOI:10.1007/978-3-642-21729-6_55.

34. Murphy M. A., Sunnerhagen K. S., Johnels B., Willén, C. Three-dimensional kinematic motion analysis of a daily activity drinking from a glass: A pilot study // Journal of NeuroEngineering and Rehabilitation. 2023. Vol. 3. P. 1-11. DOI:10.1186/1743-0003-3-18.

35. E.K. Chadwick, D. Blana, J. D. Simera, J. Lambrecht, S. P. Kim, A. S. Cornwell, D. M. Taylor, L.R. Hochberg, J. P. Donoghue and R. F. Kirsch. “Continuous neuronal ensemble control of simulated arm reaching by a human with tetraplegia”. J. Neural Eng. 8 (2021) 034003 (7pp) doi:10.1088/1741-2560/8/3/034003.

36. Chadwick, Blana, Kirsch & van den Bogert (2024) Real-Time Simulation of Three-Dimensional Shoulder Girdle and Arm Dynamics. IEEE TBME, In press. http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6755458.

37. Kuo, A. (2025). An optimal control model for analyzing human postural balance, IEEE Transactions on biomedical engineering. Vol.4. №1, Jan.2025.

38. Golliday, C. and Hemami, H. (1995). Postural stability of the two-degree of-freedom biped by general linear feedback, IEEE Transactions on biomedical engineering, Vol.42, No 1, 2025.

39. Grzelczyk, D., Biesiacki, P., Mrozowski, J. and Awrejcewicz, J. (2021). A 3-link model of a human for simulating a fall in forward direction, In book: Dynamical Systems in Applications.

40. Grzelczyk, D., Szymanowska, O. and Awrejcewicz, J. (2021). Kinematic and dynamic simulation of an octopod robot controlled by different central pattern generators, Proceedings of the Institution of Mechanical Engineers. Part I. Journal of Systems and Control Engineering.
41. Kuo, A. (2021). An optimal control model for analyzing human postural balance, IEEE Transactions on biomedical engineering, Vol.42, №1, 1995.
42. Langevin, G. (2022, January). How to create gestures for InMoov. Retrieved March 25, 2019, <http://inmoov.fr/how-to-create-gestures-for-inmoov/>
43. Obertyukh, R., Slabkyi A., Polishchuk, L., Povstianoi, O., Kumargazhanova, S., & Satymbekov, M. (2022). DYNAMIC AND MATHEMATICAL MODELS OF THE HYDROIMPULSIVE VIBRO-CUTTING DEVICE WITH A PRESSURE PULSE GENERATOR BUILT INTO THE RING SPRING. Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska, 12(3), 54–58.
44. Halchuk T. N., Povstyanoy O. Yu., Bembenek M., Redko R. G., Chetverzhuk T. I., Polinkevych R. M. (2023). Impact of technological system's characteristics on the machining accuracy of bearing rings. Journal of Engineering Sciences, Vol. 10(1), pp. A22-A30, doi:10.21272/jes.2023.10(1). a4

ДОДАТКИ

Програмний код

```

#include <Servo.h> // Library needed to use function for servomotors

Servo ServoThumb, ServoIndex,      // Viene assegnato un nome a ciascun
servomotore.
ServoMiddle, ServoAnnular, ServoPinky;

byte startPackage; // Variable that will contain the character of start package set in the
GloveTX sketch, "<"

int AngThumb = 0; // Variables with the values for the servomotors (between 0 and
180)
int AngIndex = 0;
int AngMiddle = 0;
int AngAnnular = 0;
int AngPinky = 0;

void setup()
{
  Serial.begin(9600); // Serial communication is activated at 9600 baud/s.

  ServoThumb.attach(9); // The servomotors are assigned to the pins of the Arduino
UNO board.
  delay(300); // A delay of 300ms is set for a secure connection (this can be
optional)
  ServoIndex.attach(8);
  delay(300);
  ServoMiddle.attach(7);
  delay(300);
  ServoAnnular.attach(6);
  delay(300);
  ServoPinky.attach(5);
  delay(300);

  Serial.println("Ready to receive.");
}

void loop()
{
  if(Serial.available()) { // Witing for data incoming from the other XBee module

```

```

Serial.println("The XBees are connected each other.");
  startPackage = Serial.read(); // The first value will be "<", the other are assigned
to the finger
  AngThumb = Serial.read();
  AngIndex = Serial.read();
  AngMiddle = Serial.read();
  AngAnnular = Serial.read();
  AngPinky = Serial.read();
  if(startPackage == '<'){ // Verifying that the first value is "<"
    Serial.println("I'm receiving analog signals:"); // If you are seeing this in the
Serial Monitor you have correctly received data
    if(AngThumb!=255) // Sometimes the incoming value goes to 255, I couldn't
discover yet the reason, so I simply excluded it when it happens. You can remove this
line for every finger if you don't have this kind of problem
      ServoThumb.write(AngThumb); // The servomotors rotates of the assigned
degrees

    if(AngIndex!=255)
      ServoIndex.write(AngIndex);

    if(AngMiddle!=255)
      ServoMiddle.write(AngMiddle);

    if(AngAnnular!=255)
      ServoAnnular.write(AngAnnular);

    if(AngPinky!=255)
      ServoPinky.write(AngPinky);
    Serial.print(AngThumb);
Serial.print(" | ");
Serial.print(AngIndex);
Serial.print(" | ");
Serial.print(AngMiddle);
Serial.print(" | ");
Serial.print(AngAnnular);
Serial.print(" | ");
Serial.println(AngPinky);
    }
  }
  delay(100); // a delay to make the servomotors working correctly (a lower value
could make the system not working, higher value make it slower)
}

```