АНОТАЦІЯ

Кваліфікаційна робота складається з графічної частини і пояснювальної записки.

Об’єм графічної (ілюстративної) частини кваліфікаційної роботи становить 18 слайдів.

Об’єм пояснювальної записки складає 74 друкованих сторінок формату А4 (210×297).

В кваліфікаційній роботі нараховується 31 рисунок. Використано 14 літературних джерела.

Завданням на кваліфікаційну роботу була розробка та дослідження програмно–апаратного комплексу для ідентифікації особи по відбиткам пальців, що дозволить підвищити якість та швидкість роботи систем доступу на основні сканування відбитків пальців.

Наукова новизна роботи полягає в розробці нового гібридного алгоритму обробки та порівняння зображень відбитків, що практично виключає можливість підробки відбитка чи помилки системи ідентифікації.

ЗМІСТ

ВСТУП

В останні десятиліття людство стрімко рухається вперед по шляху науково–технічного прогресу. На наших очах відбувається процес загальної інтеграції, уніфікації усіх, без винятку, сфер життя і суспільства. Як наслідок, на сьогодні ми бачимо процес створення єдиного інформаційного простору, що поєднає в собі всю накопичену і використовувану інформацію.

І головною проблемою створення такого простору – є проблема розмежування доступу до систем, диференціація інформації відповідно до потреб і прав кожного конкретного суб'єкта. Це є проблема ідентифікації користувача.

Одним з самих старих, але в той же час один з найвикористовуваніших методів є біометрична ідентифікація. Перед нами постає задача: знайти найбільш зручний та ефективний метод ідентифікації особи по певній метричній та виключно індивідуальній ознаці його організму, тіла.

Сучасна наука пропонує два шляхи вирішення даної задачі. Перший з них, це ідентифікація суб'єкта по малюнку сітківки ока. Другий – це метод біометрії малюнку пальців руки, тобто, так званих відбитків пальців.

Однак, оскільки діагностування та розпізнання сітківки пов'язане зі значними матеріально–технічними витратами та довгим періодом обробки, ми розглянемо метод біометрії пальців.

Таким чином, метою роботи є розробка програмно–апаратного комплексу для визначення рівномірності розподілу об'єктів по площі.

Усі сучасні методи біометричної ідентифікації по відбиткам пальців базуються на трьох основних принципах роботи: порівняння по умовних точках, кореляційний аналіз зображення і співставлення зображення з існуючим у базі даних. Однак, кожен метод має свої певні плюси і недоліки. Тому нам необхідно, враховуючи усі сучасні методи ідентифікації, порівнявши їх сильні та слабкі

сторони, створити новий метод, що буде на порядок ефективніше та економічніше.

Задачі на дослідження:

- розглянути існуючі методики та методи ідентифікації, обробки зображень, порівняти їх за усіма показниками; визначити найефективніші елементи;
- розглянути програмні та програмно–апаратні комплекси для аналізу і обробки зображень дактилоскопічних досліджень і вказати їх недоліки;
- розробити новий принцип обробки та аналізу зображень відбитків пальців;
- розробити ергономічний, зручний та швидкодійний програмний інтерфейс користувача та базу даних.
- реалізувати виконання таких дій:
    - отримання зображення з цифрового пристрою обробки зображення (сканера)
    - обробка зображення відповідно до розробленого алгоритму
    - порівняння результату обробки із базою існуючих даних та визначення особи
    - провести обробку експериментальних даних і загальну оцінку роботи програмно–апаратного комплексу.

Наукова новизна роботи – полягає у розробці точного та швидкого та ефективного методу оцінки, обробки та ідентифікації зображення відбитків пальців на основі вже існуючих засобів та принципово нових підходів до математичної обробки зображень та реалізації цього методу у програмно–апаратному комплексі.

1 АНАЛІТИЧНА ЧАСТИНА

1.1 Огляд існуючих методик обробки зображень відбитків пальців

На сьогодні існують три основні методи для визначення особи за відбитками пальців, які були розроблені та впроваджені в практику. Кожна з розроблених дактилоскопічних та цифро-аналітичних стратегій має свої характеристики, що базуються на властивостях та особливостях зображень відбитків пальців.

Основна мета полягає в виборі оптимального методу, який б мінімізував матеріальні, технічні та часові витрати ідентифікації, а також максимізував ступінь точності та якості розпізнавання. Головною задачею дослідження є оцінка найпоширеніших методів ідентифікації особи за відбитками пальців.

Алгоритм даного класу працює за наступною схемою. Зображення отримане з цифрового сканеру розбивається у оперативній пам’яті комп’ютера чи автоматизованого процесора на множину прямокутних чи трикутних секцій. При цьому, чим менші фізичні розміри має кожна секція – тим вища точність розпізнання.

Місцезнаходження папілярів (мініатюрних каналів на поверхні шкіри, розташуванням яких і визначається унікальність біометричних характеристик відбитку пальця, рис.1.1) на зображенні відбитку у цій секції описується певною синусоїдальною функцією (початковий зсув фази, напрям поширення). Потім порівнюються хвильове (аналітичне) представлення відповідних секцій шаблону (рис.1.2 і рис.1.3), що зберігається у базі даних, та відсканованого зображення у пам’яті системи.

Розташування ліній у кожному осередку описується параметрами деякої синусоїдальної хвилі, тобто, задається початкове зрушення фази (δ), довжина хвилі (λ) і напрямок її поширення (θ). Параметри хвилі скалатають її рівняння (1.1), по якому пізніше і йде порівняння:

$$A\,\theta = A0 \sin 2\pi(t/T - \theta/cT)\,, \qquad (1.1)$$

де $\lambda = cT$ – довжина хвилі,

T – період коливання хвилі.

Це – рівняння синусоїдальної, або монохроматичної хвилі. Всі крапки хвилі в момент часу t мають різні зсуви. Але ряд крапок, що знаходяться на відстань с одна від іншої (при початковому зрушенні фази коливання δ), у будь–який момент часу зміщені однаково (тому що аргументи синусів у рівнянні відрізняються на 2 π, а отже, їхні значення рівні).

Перевагою алгоритмів цього класу є те, що дані алгоритми порівняння не потребують одержання зображення високої якості.

Окремо варто помітити, що в автоматизованій ідентифікації існує кілька проблем зв'язаних зі складністю сканування й розпізнавання деяких типів відбитків пальців, у першу чергу це стосується маленьких дітей, тому що їхні пальці дуже маленькі, для того, щоб навіть на гарному встаткуванні одержати їхні відбитки пальців з деталізацією, прийнятної для розпізнавання. Крім цього, близько 1% дорослих людей, є власниками настільки унікальних відбитків пальців, що роботи з ними доводиться або розробляти спеціалізовані алгоритми обробки або робити виключення у вигляді персонального для них відмови від біометрії.

Папілярний візерунок дуже складний (рис 1.1). І якщо цифровий образ відбитка пальця буде містити його цілком, те він займе занадто багато місця. Природно, процес ідентифікації в цьому випадку буде тривати відносно довго. І це не враховуючи те, що порівняння по повному відбитку пальця занадто часто може приводити до помилок. Все–таки сканери мають певні погрішності, а отриманий з їхньою допомогою відбиток пальця залежить від стану шкіри, ступеня натискання на робочу поверхню й багатьох інших факторів.

Рисунок 1.1 – Схема ключових елементів відбитку

1 – *точка утворення гілок, розгалуження* (the Bifurcation) – точка розходження гребеня на гілки

2 – *дельта* (the Delta) – зона поділу гребеня на три лінії з подальшим сходженням в одній точці (форма трикутника).

3 – *кінцеві точки* (the Ending points) – точки закінчення лінії гребеня

4 – *центр* або ядро (the Core) – точка (зона) найбільшої кривизни спіралі гребеня

5 – *острів* (the Island) – одиничний короткий обмежений гребінь, в більшості у вигляді короткого прямого відрізку

Для того, щоб уникнути подібних проблем, у багатьох методиках ідентифікації використається не повний відбиток пальця, а тільки перелік певних крапок. При цьому в більшості сучасних технологій застосовуються два різних підходи. Перший використається в тому випадку, якщо сканування здійснюється з досить низькою або середньою якістю (розподільна здатність до 500 dpi). При цьому на одержуваному відбитку можна розібрати багато дрібних деталей. Саме вони й використаються для ідентифікації людини.

Рисунок 1.2 –Розбиття папілярного візерунка на секції (комірки)

Рисунок 1.3 – Хвильове представлення в секції

Переважна більшість технологій ґрунтується на застосуванні кінцевих крапок і крапок розгалуження. Кінцеві крапки – це крапки, у яких зникають горбки папілярного візерунка. Ну а в крапках розгалуження ці горбки роздвоюються (або, навпаки, сходяться – дивлячись звідки дивитися). Рішення про використання саме цих елементів папілярного візерунка прийнято по двох причинах. По–перше, кінцеві крапки й крапки розгалуження добре видні на відбитках. А по–друге, їх число досить велике, що може служити для однозначної ідентифікації особи.

По–іншому обстоять справи при другому підході, коли сканер може забезпечити зняття високоякісного відбитка пальця (розподільна здатність не менше 1000 dpi). У цих випадках на зображенні папілярного візерунка видні не тільки зовнішні елементи, але й деталі його внутрішньої будови. Так, наприклад, у деяких сучасних технологіях для ідентифікації особистості використаються

пори потових залоз. Правда, варто відзначити, що такі розробки – справа майбутнього. Проблема полягає в тому, що одержання зображення відбитка пальця з дозволом в 1000 dpi можливо тільки на дуже дорогих, а тому мало розповсюджених поза спеціальними лабораторіями сканерах.

1.2 Клас методів, що базуються на кореляційному порівнянні зображень

Суть методу така: два відбитки накладаються один на інший та проводиться розрахунок кореляції між відповідними пікселями.

Метод полягає в тому, що два відбитки пальців накладаються один на одного, і потім обчислюється кореляція між відповідними пікселями. Для цього використовуються великорозподільні зображення відбитків пальців з високою роздільною здатністю (не менше 800 dpi).

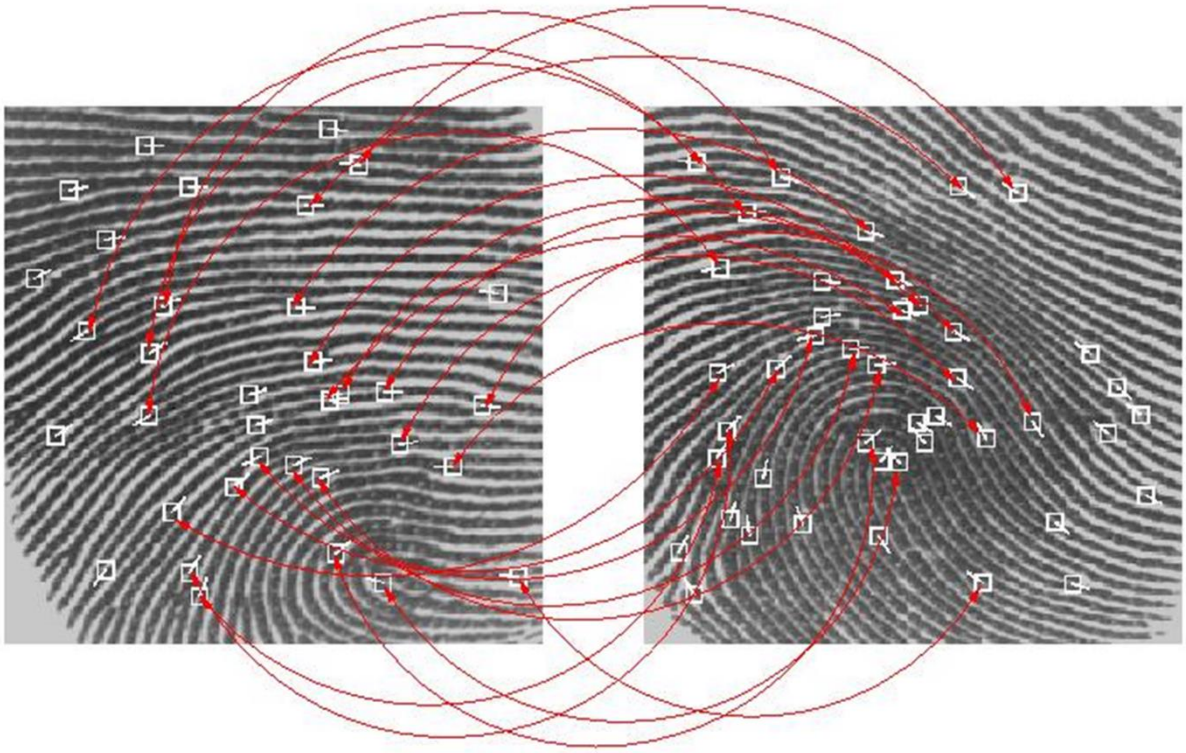


Рисунок 1.4 – Кореляція зображення відбитку по відповідним точкам (пікселям)

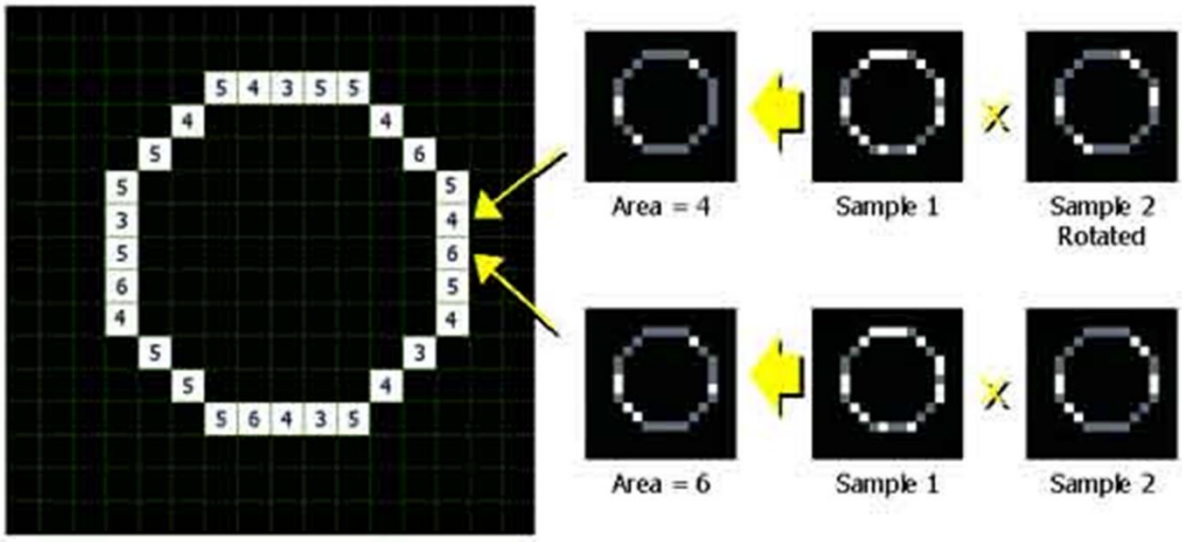


Рисунок 1.5 – Циклічний аналіз корельованих сигналів

Через надзвичайно велику ймовірність вірного відповідними пікселями (до 96%), цей метод знайшов застосування у об’єктах підвищеної захищеності (таких, як різноманітні сховища). При цьому порівняння йде лише з декількома відбитками людей, що мають таке право доступу (здебільшого їх кількість не перевищує 2–5 чоловік).

Загальний алгоритм кореляційного аналізу полягає у використанні двох формул (1.2) і (1.3). Оператор співвідношення, заданий рівнянням (1.2), особливо корисний для знаходження ймовірних проявів одного сигналу в іншому. Коли співвідношення дійсне, сигнал, що утворюється в результаті, визначає величину (коефіцієнт), що залежна від різниці між двома сигналами, які він опрацьовує

$$g(x) = \int_{-\infty}^{\infty} f_1(\alpha) f_2(\alpha + x) \delta\alpha$$

Розмір отриманого коефіцієнта прямо вказує на величину кореляції між двома сигналами, тому що коефіцієнт знаходиться по всій площі роботи двох сигналів (на графіку). Операція порівняння відбувається циклічним методом так, що порівнюваний сигнал повинен ніби «огортати» сигнал–еталон. Ця процедура

показана на рис. 1.5 з даним рівнянням.

$$g_n(i) = \sum_{\alpha=0}^{I_n-i-1} f_{1n}(\alpha) f_{2n}(\alpha+i) + \sum_{\alpha=I_n-i}^{I_n-1} f_{1n}(\alpha) f_{2n}(\alpha-I+i)$$

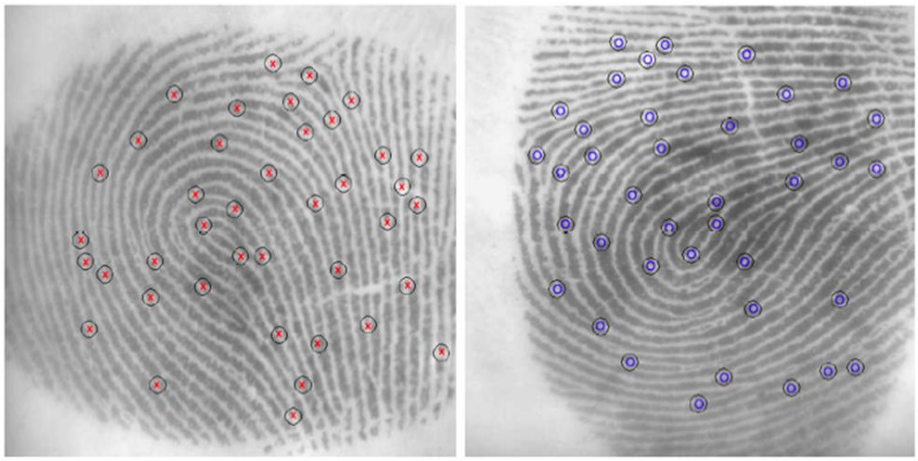
1.3 Клас методів, що базуються на порівнянні по особливим точкам

При реєстрації користувача в інформаційній системі зображення відбитка його пальця обробляється наступним способом. Спочатку знаходиться деяка кількість особливих крапок (рис.1.6). У кожної з них визначаються різні метричні характеристики, що представляють у числовому вигляді. У результаті виходить масив даних, що описують особливі крапки відбитка. У майбутньому цей процес повторюється щоразу, коли хтось хоче пройти процес аутентифікації, і отриманий масив чисел, що описує особливі крапки, по черзі рівняється із записами, що зберігаються в базі даних. При цьому повного збігу домогтися не вдається. Звичайно встановлюється деякий поріг, тобто кількість співпадаючих крапок, достатніх для ідентифікації користувача.

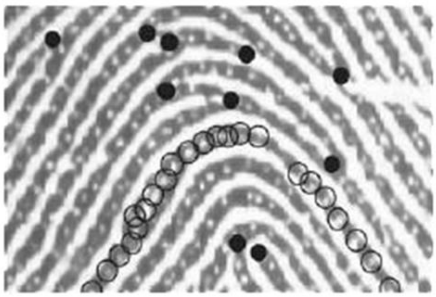
У розглянутого підходу є дві переваги. По–перше, метод порівняння відбитків пальців по особливих крапках розроблений досить давно й тому добре вивчений. По–друге, він добре підходить для порівняння типу "один до багатьох". Інакше кажучи, він забезпечує високу швидкість порівняння отриманого цифрового "відбитка" з усіма записами, що зберігаються в базі даних, при пошуку потрібної людини.

Звичайно, у даної технології є й недоліки. По–перше, вона дуже вимоглива до апаратури – до сканерів, які знімають відбитки. Сьогодні існує не менше десятка різних способів одержання зображень візерунків на пальцях, і не всі вони підходять для роботи в такій системі. Крім того, є серйозні обмеження з дозволу й розміру використовуваного сенсора. Низька якість одержуваного відбитка пальця дуже сильно зменшує ефективність процесу розпізнавання.

По-друге, ще один недолік методу – обмеження безпеки алгоритму кількістю використовуваних особливих крапок.



а) б)



в)

Рисунок 1.6 – Зображення відбитку з виділеними особливими точками:

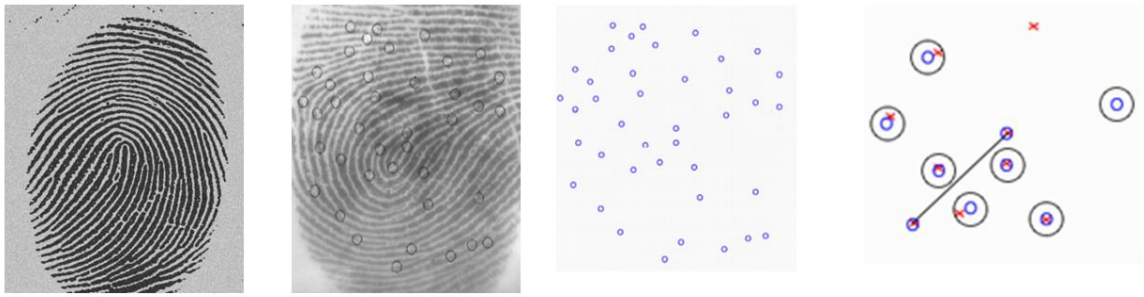
а) Відбиток ідентифікованої особи;

б) Еталон відбитку з БД;

в) Зразок з виділеними точками певного типу (потові залози, пори та кінцеві точки).

Причому варто відзначити, що в деяких випадках (наприклад, при забрудненні пальця, невеликих ушкодженнях шкіри й т.п.) детектування цих крапок сильно ускладнюється. Є й третій недолік: висока ймовірність появи помилок визначення особливих крапок через особливості будови папілярних гребенів у деяких людей.

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



1. 2. 3. 4.

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.

2 ТЕХНОЛОГІЧНА ЧАСТИНА

2.1 Загальні принципи та алгоритми розпізнання відбитків, що використовуються в усіх класах методів

Робота автоматизованої біометричної системи (рис.2.1.) відбувається в одному із двох режимів – ідентифікації (I) або верифікації (II), про які буде розказано нижче. В обох випадках вхідна інформація, або так називана реєстрація, практично однакова і багато в чому залежить від правильного вводу інформації.

Процес реєстрації являє собою введення основних початкових параметрів системи й складається з п'яти етапів:

1. Завантаження біометричних даних. При додаванні в базу даних конкретної біометричної характеристики часто вводиться декілька її варіантів, що відносяться до однієї і тієї ж особи, щоб урахувати можливі зміни. Тому найчастіше в базі даних зберігаються кілька відбитків пальців однієї особи.

2. Фіксування даних. Вимір і фіксація базової біометричної інформації, що відноситься до конкретного образа.

3. Обробка даних. Перевід зафіксованих даних у цифрову форму зі створенням еквівалента відбитку пальця.

4. Звірка оброблених даних з первинною інформацією. Проводиться з метою підтвердження правильності розпізнавання системою введених даних.

5. Збереження підтверджених біометричних даних.

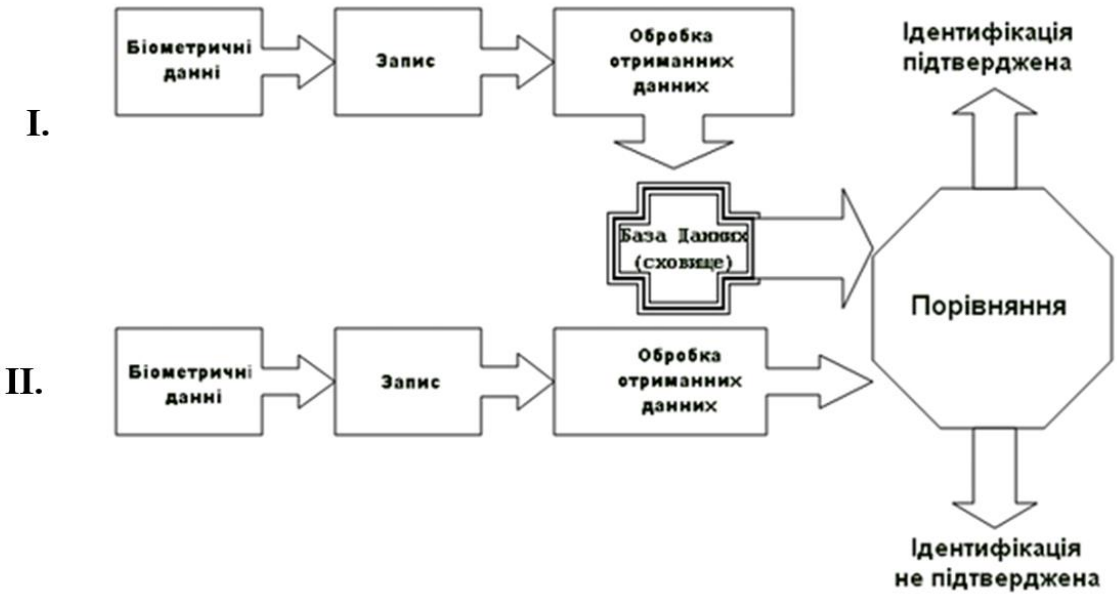


Рисунок 2.1 – Алгоритмічна схема процесу ідентифікації

Результатом реєстрації повинен стати представлений в електронному вигляді об’єм даних, у форматі зручному для використання та пересування, розміщений у базі даних, спеціальному файлі–ключі (зазвичай з використання методу RSA–ключування) або ж на ідентифікаційних магнітних картах (так званих смарт–картах) чи особливих захищених оптичних носіях типу «Zip–drive Protected».

Реєстрація є тим етапом, на якому надзвичайно важливо здобути ефективну взаємодію між всіма користувачами і точне виконання всіх процедур, тому що від цього залежать подальше функціонування, працездатність і точність системи.

Одне з важливих питань, які необхідно вирішити, полягає в цим етапом – для чого планується використати систему – для ідентифікації або верифікації.

2.2 Класифікація отриманого зображення відбитку

Даний метод є край необхідним для пришвидшення процесу ідентифікації. У випадку, якщо отримане зображення порівнюється з багатьма занесеними у базу даних (а таких може бути від декількох десятків до сотень і тисяч, , і навіть десятків мільйонів – як то БД ФБР, що налічує близько 100 млн. відбитків), ми

ризикуємо отримати комплекс з над великим періодом обробки. Тому з самого початку отримане зображення по певних ознаках відносять до вже відомих класів відбитків. В результаті порівняння відбувається лише в рамках класу чи підкласу. Це дозволяє скоротити час роботи установки в декілька разів. Первина оцінка класу, на відміну від самого процесу розпізнання, відбувається на досить примітивному технічно–математичному рівні.

На сьогодні з метою уніфікації баз даних відбитків (fingerprints datas) прийнято виділяти 5 основних класів відбитків – відповідно до моделі розробленою в Відділені розробки методів біометричної ідентифікації Мічиганського державного університету (Рис. 2.2.):

- Завиток або *тип W;*
- Права котушка або *тип R;*
- Ліва котушка або *тип L;*
- Арковий тип або *тип A;*
- Плоска арка або *тип T.*

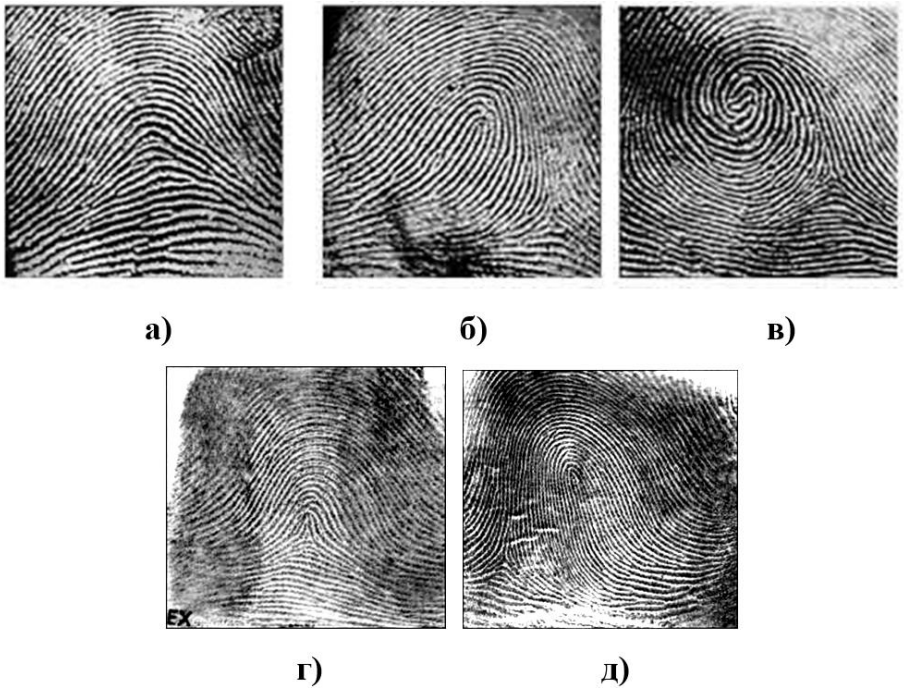


Рисунок 2.2 – Основні класи відбитків по класифікації MSU: а) Арка (A); б) Котушка (R); в) Завиток (W); г) Плоска арка (T); д) Котушка (L);

Алгоритмів класифікації відбитка, тобто віднесення до якогось із вищевказаних класів, також є декілька. Ось короткий опис основних з них.

I. Класифікатор K–найближчий ("k–nearest neighbour").

Класифікатор K–найближчий (рис.2.3) приводить до точності 85.4% для завдання розгляду 10 найближчих сусідів (K=10) при виборі між 5 основними класами. З появою нового запису для прогнозування знаходяться відхилення між цим записом і подібними наборами даних, і найбільш подібна (або ближній сусід) ідентифікується.

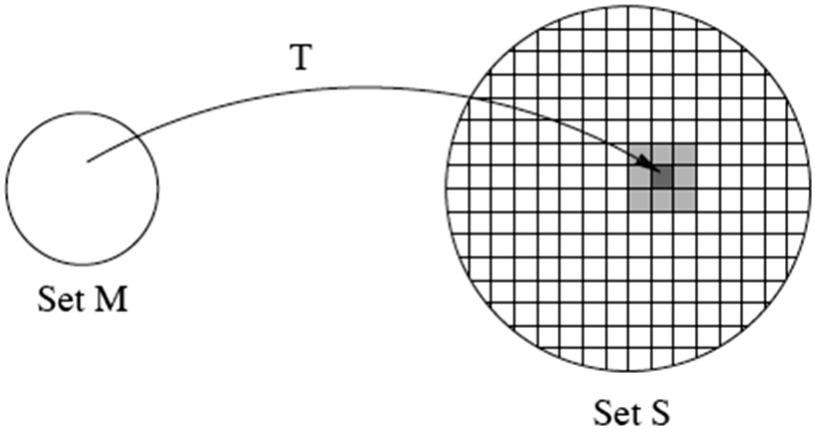


Рисунок 2.3 – Знаходження найближчих сусідів

Точність класифікації не завжди збільшується зі збільшенням K; так існує оптимальне значення K для кінцевих навчальних завдань класифікації розміру моделі. Для завдання класифікації чотирьох з п’яти класів (де класи A й T були об'єднані в один клас), досягнута точність 91.5%. Змішана матриця для класифікатора K– найближчий показана в таблиці 2.1.

Таблиця 2.1 - Змішана матриця для класифікатора K–найближчого сусіда (до K=10)

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.

II. Класифікатор для *Байесовської мережі*

Частковим випадком такого підходу є *прихована марківська модель (ПММ)*. Цей підхід гарантує якісну класифікацію завдяки глибокій математичній моделі аналізу, підходящого для розпізнавання образів та успішному повному застосуванню розпізнавання мови й інших завдань.

Ці моделі здатні класифікувати дані, 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, але може також бути замічена в загальному виді виступів. Пмм у стані статистично моделювати різні структури зразків виступів по цілому відбитку, не ґрунтуючись на добуванні особливих крапок. Щоб знаходити місця розташування виступів, використається безліч методів обробки зображення. Імовірності виділення структури змодельовані з об'єднанням діагональної коваріції, багатомірних Гауссівських розподілів.

III. *Вибіркове відхилення*

Для запобігання виникнення метричних та аналітичних помилок частину зображення відхиляють на першому ж етапі ідентифікації. Категорії таких зображень: забруднені відбитки, зображення низької якості, зображенні отримані з так званим «шумом». Залежність між кількістю відхилень та якістю подальшого процесу розпізнання наведена у таблиці 2.2.

Таблиця 2.2 - Співвідношення між вибірковим відхиленням і позитивною ідентифікацією (класи 4,5 – відповідний поділ на 4 або 5 категорій).

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%

IV. *Інші алгоритми*

Окрім названих вище класифікаторів 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 (не досить вивчений на сьогодні), двухетапний класифікатор–гібрид на основі двох з вище перерахованих методів, класифікатор на основі одно– або багатошарової нейронної мережі (великий плюс такого класифікатора – самонавчання зі збільшенням кількості суб’єктів аналізу).

2.3. Огляд існуючих програмних та апаратно–програмних комплексів для аналізу і обробки дактилоскопічних зображень

На сьогодні апаратні та програмні рішення досить поширені, адже в умовах глобалізації та інформатизації суспільства проблема ідентифікації виникає повсякчас у всіх сферах життя.

Розглянемо декілька широко використовуваних пристроїв, відповідно по одному на кожен існуючий клас.

I. Універсальний сканер відбитків пальців Sagem MSO300 із часом ідентифікації менше 2 секунд.

Малогабаритний сканер відбитків пальця MSO300 компанії Sagem призначений для сканування й перетворення зображення папілярного малюнка пальця з наступним автоматичним занесенням його в базу даних. Цей сканер оснащений оптичним чутливим елементом із площею сканування 21x21 мм і розподільною здатністю 500 крапок на дюйм. Вбудовані в MSO300 програмні модулі для попередньої обробки малюнка пальця дозволяють прискорити процес реєстрації нових користувачів біометричної системи. До центрального комп'ютера системи контролю доступу організації сканер відбитків пальця підключається через USB–порт.

Рисунок 2.4 - сканер відбитків пальців Sagem MSO300

Таблиця 2.3 - Технічні характеристики сканера відбитків пальця MSO300:

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

Даний пристрій є представником класу несамостійних сканерів для централізованої і комп’ютеризованої системи контролю доступу.

II. BioLink U–Match Mouse (біометричний маніпулятор типу «миша»)

BioLink Umatch® Mouse – пристрій, що сполучає в єдиному корпусі двокнопковий маніпулятор«миша» з ролером прокручування й високоточний оптичний сканер відбитка пальця (рис.2.5). Виробництво пристроїв перебуває в США. Не вимагає застосування додаткових роз’ємів, працює через стандартний інтерфейс USB або RS–232C.

Рисунок 2.5 - BioLink U–Match Mouse

Таблиця 2.4 - Технічні характеристики BioLink U–Match Mouse

Ідентифікація:	0,2 с
Розп.здатність сканера:	284 х 400 крапок
Градації кольорів:	8 рівнів сірого
Активна площа:	18 х 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:	80х92х57мм

Даний пристрій є представником класу інтегрованих несамостійних сканерів, які набули великого поширення в останні три роки. Вони покликані забезпечувати відповідний рівень доступу до інтелектуальних та інформаційних систем, комп’ютерних мереж. Для роботи потребують додаткового програмного забезпечення. Сьогодні подібні пристрої інтегрують у наступні види допоміжної та комп’ютерної техніки: флеш–накопичувачі, маніпулятори, мобільні телефони, ноутбуки (портативні комп’ютери різних типів) і тд.

III. Пристрій контролю доступу по відбитках пальців IDTECK STAR FGR007A

Пристрій FGR007A доступно за ціною й робить можливість установки й модернізації систем контролю доступу в бік дактилоскопічної біометрії цілком реальною. Маючи механізм швидко й точної персональної ідентифікації з ємністю користувальницької бази до 4000 записів, він являє собою закінчене рішення безпеки.

Області застосування:

- Особливо охоронювані зони – такі, як науково–дослідні центри, урядові заклади й військові об'єкти

- Системи обліку відвідуваності й робочого часу, сполучені із системами контролю доступу в офісах і на виробництві

Основні характеристики:

- Швидка ідентифікація – менше однієї секунди
- 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
- Вбудований АЦП, та пам’ять на 4000 відбитків

Рисунок 2.6 - IDTECK STAR FGR007A

IV. Температурні датчики відбитків пальців із сімейства FingerChip (AT77C102B)

AT77C102B – представник сімейства датчиків відбитка пальців Atmel FingerChip, які не вимагають застосування оптики, призм 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 шляхом переміщення пальця поперек чутливої поверхні. Після захвата декількох зображень запатентоване програмне забезпечення Atmel 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 відсутня необхідність 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.

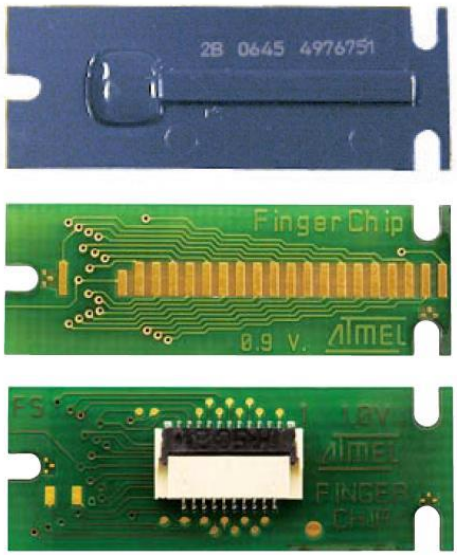


Рисунок 2.7 - AT77C102B

Таблиця 2.5 - 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 в 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°С
Робочий температурний діапазон:	–40°С...+85°С

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

V. Інші

Окрім вищеперерахованих існують декілька інших типів приладів та датчиків для автоматизації дактилоскопічного аналізу. Однак, через не досить широке розповсюдження, ціну чи низькі аналітичні показники, їх сьогодні майже не використовують. Ось їх перелік:

- Оптичні протяжні;
- Роликові;
- Безконтактні;
- Радіочастотні;
- Ультразвукові.

2.4 Автоматизовані програмні комплекси ідентифікації по відбиткам

Програмні комплекси даного спрямування є надзвичайно вигідними, в першу чергу з комерційної точки зору (ціна працюючого алгоритму з відповідною базою даних нерідко сягає ціни автомобіля). Звичайно ж, це викликане складністю розробки оригінального алгоритму та накопиченням бази якісними шаблонами. Отож, найпоширеніші на сьогодні ПК для аналізу зображень відбитків.

I. FingerCell 2.0

Пакет FingerCell 2.0 спроможний зіставляти із шаблонами, що зберігаються в базі, до 700 відбитків пальців у секунду й може використатися для перевірочної ідентифікації (*один–до–одного*) або для встановлення особистості по базі (*один–до–багатьох*) у інтегрованих додатках.

В їхньому числі: системи контролю доступу, робочого часу й присутності на робочих місцях, а також безпеки апаратних засобів. Розроблений на базі застосовуваного 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 й обчислювальною потужністю процесора.

II. VeriFinger 5.0 Standard SDK

Даний алгоритм та ПЗ на його основі (рис. 2.8) 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.

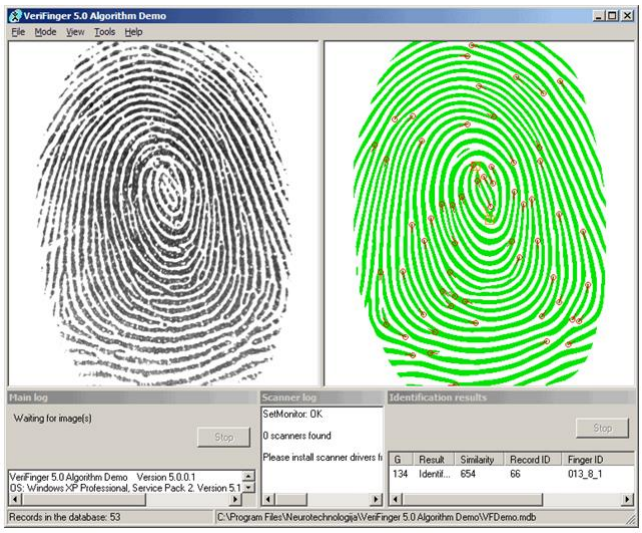


Рисунок 2.8 - VeriFinger 5.0 Standard SDK

Таблиця 2.6. Технічні характеристики VeriFinger 5.0 Standard SDK

Необхідна розп.здатність зображення	> 250 dpi / 500 dpi рекомендовано
Час циклу розпізнання	0.2 – 0.4 секунд
Швидкість пошуку в БД	40,000 відбитків/секунду
Розмір 1 запису в БД	150 байт – 1.8 Кбайт
Максимальний об'єм БД Вірогідність невірного підтвердження	необмежений Менше 0,1%

III. Griaule Fingerprint SDK 2007

Fingerprint SDK (рис 2.9) – інноваційний набір засобів для розробки ПО розпізнавання відбитків пальців (SDK), що дозволяє Вам інтегрувати біометрику в широкому спектрі додатків. Завдяки підтримці безлічі мов програмування, багатства вибірок коду, і його повної документації це стає можливим на протязі кількох годин. Fingerprint SDK виконана у двох різних випусках: для Windows (підтримує багато мов програмування й динамічних бібліотек і технологію ActiveX); Fingerprint SDK для Java дозволяє розробляти крос–платформні програми Java, які будуть працювати в будь–якій операційній системі.

Рисунок 2.9 - Griaule Fingerprint SDK

Таблиця 2.7 - Технічні характеристики Griaule Fingerprint SDK 2007

Необхідна розп.здатність зображення	> 125 –1000 dpi / 500 dpi рекомендовано
Час циклу розпізнання	0.01 секунд
Швидкість пошуку в БД	35,000 відбитків/секунду
Розмір 1 запису в БД	250 байт – 5 Кбайт
Максимальний об'єм БД Вірогідність невірного підтвердження	необмежений Менше 0,01%

IV. IBM ThinkVantage Fingerprint Software

Досить нове програмне забезпечення (рис 2.10), яке отримало акредитацію Ibm kbit минулого року (до того розповсюджувалося як Lenovo Think Vantage). Використовує гібридну математичну модель аналізу та криптографічні системи захисту бази даних. На сьогодні застосовується в різноманітних портативних пристроях компанії Ibm, хоча сам алгоритм дозволяє досить широке використання. З відомих технічних характеристик: швидкість розпізнання одного відбитку – менше 1 секунди. Вірогідність успішного підтвердження особи – 96,67%. Апаратні вимоги не повідомляються.

Рисунок 2.10 - IBM ThinkVantage Fingerprint Software

V. Крім зазначених продуктів є кілька закритих корпоративних пропозицій від окремих виробників. Інформація та технічні данні про них є закритими, тому наведемо лише перелік найвідоміших виробників (програмні продукти мають ідентичну назву): Bioaccez Controls, Biometric Security AG, BQT Solutions Limited, Drax Seguridad Perimetral, EverFocus Electronics (Europe) GmbH, Guardware Systems Limited, MicronID Development Ltd, Precise Biometrics, Texas Instruments.

На основі проведеного аналізу розглянутих існуючих методик, комплексів та алгоритмів було вирішено розробити програмно–апаратний комплекс 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

3 КОНСТРУКТОРСЬКА ЧАСТИНА

3.1 Проектування програмно–апаратного комплексу для зняття відбитків пальців

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

- задання чорно–білого режиму сканування зображення для основного сканеру та 16–ти бітного кольорування для термального сканера;
- задання роздільної здатності для сканування зображення;
- 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 шукаємими об’єктами;
- створення матриці даних тимчасового об’єкта;
- визначення параметрів рівномірності об’єктів по площі;
- остаточне підрахування вірогідності співпадання суб’єкта з існуючими в базі даних;
- визначення автентичності особи відповідно до заданої вірогідності (жорсткості критерій відповідності).

Фактичний математичний алгоритм моделі складається з наступних етапів:

І. 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 (фактично карти розподілу тепла по поверхні пальця).

Передбачається, що сканер буде напряму під’єднаний до комп’ютера – для можливості зміни попередніх параметрів сканування оператором системи. Серед таких параметрів: розподільна здатність першого зображення, глибина кольору другого, допустима вірогідність співпадання (або ж неспівпадання). Всі ці опції доступні завдяки графічному інтерфейсу користувача. Керування сканером відбувається завдяки його драйверу та через систему команд API (Application Programming Interfaces – інтерфейс програмування додатків) операційної системи Microsoft Windows.

II. RAW – формат даних, що не має чіткої специфікації. Файли цього формату містять у собі неопрацьовані (або оброблені в мінімальному ступені) дані, що дозволяє уникнути втрат інформації. У таких файлах, як правило, утримується багато надлишкової інформації, тому файли формату RAW використають набагато більшу кількість дискового простору. Пізніше данні буду конвертовані у формат BMP (Bitmap Image) – цей тип зображення найкраще опрацьовується без застосування ПЗ сторонніх виробників.

III. 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. Однак, найкраще для вирішення математичних та кореляційних задач запропонував себе т.зв. Фільтр Габора, що комбінується в нашому випадку з математичним алгоритмом класування відбитку. Саме цим фільтром буде відбуватися опрацьовування обох зображень, однак з різними настроюваннями.

Головні кроки цього етапу алгоритму наступні:

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, які зберігають глобальні виступи і структури борозен.

3) Обчислити оцінку стандартного відхилення рівня сірого в шкірному секторі, щоб сформувати вектор ознак або код пальця.

Нехай I(x, y) позначають сірий рівень у пікселі (x, y) у M x N зображенні відбитка пальця і нехай (xc, yc) позначають крапку центра (рис 3.1).

Рисунок 3.1 - Відбиток пальця із крапкою центра (x), ядром (o) і відзначеними 48 секторами.

Просторовий склад мозаїки області зображення, що складається зі значимої області, визначено сукупністю секторів Si, де i–сектор Si представлений у вигляді параметрів (r, Θ) у такий спосіб:

$$S_i = \{(x, y) | b(T_i+1) \le r < b(T_i + 2), \theta_i \le \theta < \theta_{i+1}, 1 \le x \le N, 1 \le y \le M\}$$

де $T_i = i \text{ div } k$,

$$\theta_i = (i \bmod k)\left(\frac{2\pi}{k}\right),$$

$$r = \sqrt{(x - x_c)^2 + (y - y_c)^2},$$

$$\theta = \tan^{-1}\left(\frac{y - y_c}{x - x_c}\right),$$

b – ширина кожної смуги, і k – число секторів, які розглядають у кожній

смузі. Використовуються шість концентричних смуг навколо пункту центра. Кожна смуга з 20 пікселями шириною (b = 20), і сегментованим у вісім секторів (k = 8) (рис. 2.8). Сама внутрішня смуга не використається для добування ознак, тому що сектора в області біля центра містять дуже небагато пікселів. Таким чином, у цілому 8 x 6 = 48 секторів (з S0 до S47) визначені.

3.2 Розроблення структури програми

Головні кроки алгоритму класифікації наступні:

1) Визначити місцезнаходження реєстраційних крапок у вхідному зображенні й визначити просторову складову мозаїки області навколо реєстраційної крапки (сектора).

Будь–яка крапка, що може бути послідовно виявлена в зображенні відбитка пальця, може використатися як реєстраційний крапка (або крапка центра (x_c, y_c), тому що вона може бути поміщена в центр зображення). Алгоритм виявлення цієї крапки:

а) Оцінити область орієнтації O, використовуючи алгоритм оцінки орієнтації найменшого квадрата. Область орієнтації O визначена як N x N зображення, де O(i,j) представляє місцеву орієнтацію виступів у пікселі (i,j). Зображення розділене на ряд wxw ненаклавшихся вікон, і єдина місцева орієнтація визначена для кожного вікна.

б) Згладити область орієнтації в місцевому сусідстві. Нехай пригладженої орієнтації області буде представлена як O'.

в) Ініціалізувати A, зображення мітки як правило вказує основну крапку.

г) Для кожного пікселя (i, j) в O', обчислюють індекс Пуанкаре (Poincaré) і призначають відповідні пікселі в A значення одного з індексу Пуанкаре – (1/2). Індекс Пуанкаре в пікселі (i, j) прикладений до пальцевидної кривої, що складається з послідовності пікселів, які на відстані одного пікселя від відповідної кривої, обчислений у такий спосіб:

$$P(i,j) = \frac{1}{2\pi}\sum_{k=0}^{N_{r-1}} \Delta(k),$$

$$\Delta(k) = \begin{cases} \delta(k), & if\ |\delta(k)| < \pi/2 \\ \pi + \delta(k), & if \delta(k) \le -\pi/2 \\ \pi - \delta(k), & інакше\ , \end{cases}$$

$$\delta(k) = O'(\psi_x(k'), \psi_y(k')) - O'(\psi_x(k), \psi_y(k)),$$

$$k' = (k+1) \bmod N_\psi ,$$

де $\psi_x(\cdot)$ і $\psi_y(\cdot)$ – координати x и y закритої пальцевидної кривої з пікселями.

д) Знайти зв'язані компоненти в A. Якщо область зв'язаного компонента більше семи, ядро виявлене в середній крапці зв'язаного компонента. Якщо область зв'язаного компонента більше 20–ти, два ядра виявлені в середній крапці зв'язаного компонента.

е) Якщо виявлено більше, ніж два ядра, повернутися до кроку б).

ж) Якщо два ядра виявлені, то центр призначених координати основної крапки з нижнім значенням y (верхнє ядро). Якщо тільки одне ядро виявлене, центр має координати основного центра.

з) Якщо ніяка основна крапка не виявлена, обчислите матрицю коваріації векторної області в місцевому сусідстві (q x q) кожної крапки в області орієнтації. Визначите зображення ознак I з найбільшим власним значенням матриці коваріації для кожного елемента в зображенні орієнтації. Ядро виявлене в середній крапці найбільшого зв'язаного компонента в граничному зображенні F і центр призначений координатами ядра.

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

2) Розбити вхідне зображення на ряд складових зображень, кожне з яких зберігає певні структури виступів; обчислити стандартне відхилення складових

зображень у кожному секторі, щоб скласти вектор ознак (названий кодом пальця).

Це досягається за допомогою фільтрів Габора. Фільтри Габора – смугові фільтри, які мають властивості й добірної орієнтації, і добірної частоти, і мають оптимальне поєднане рішення й у просторі й області частоти. Застосовуючи фільтри Габора до зображення відбитка пальця, щирі виступи й структури ряду можуть бути добре виділені (рис. 3.3)

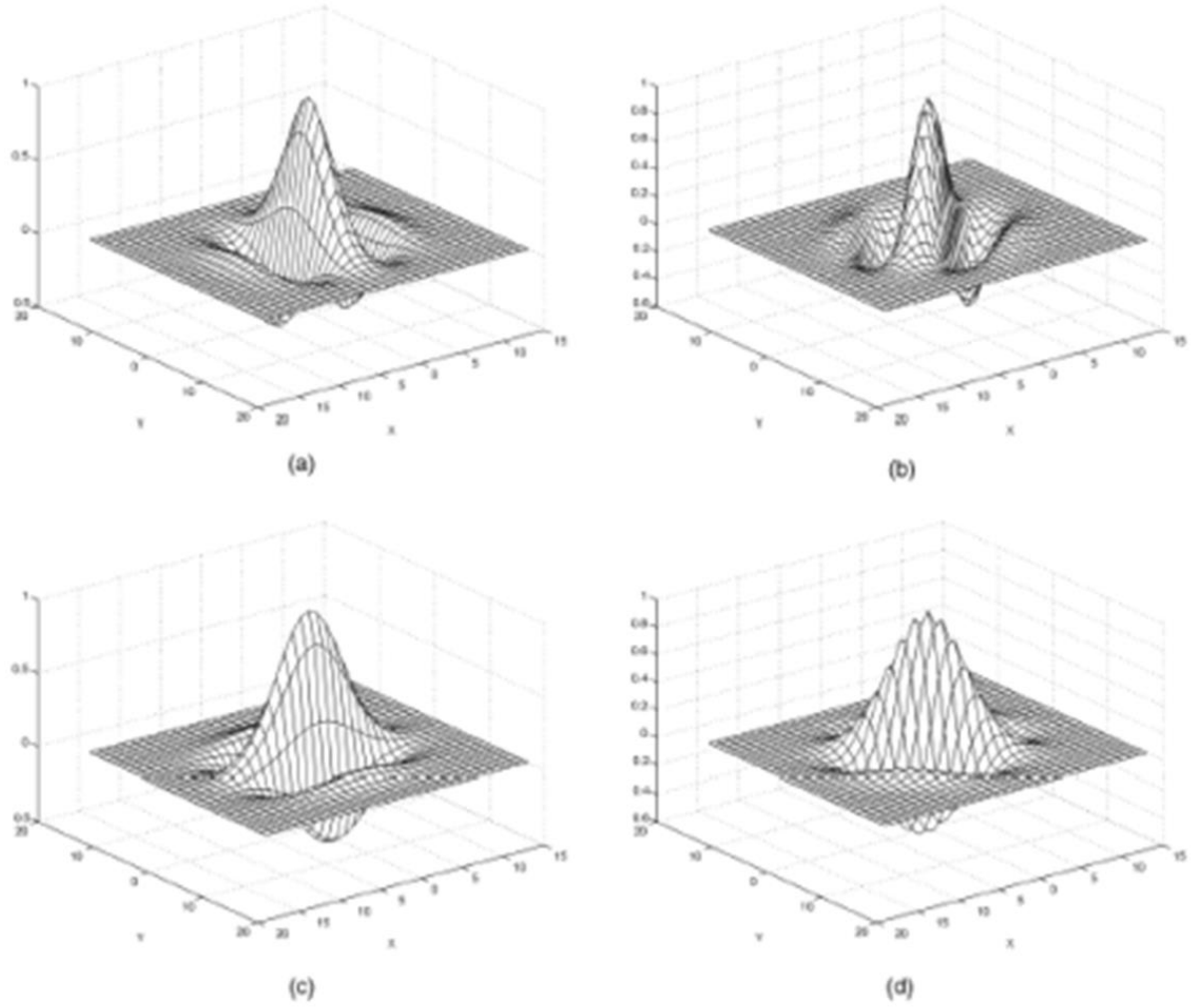


Рисунок 3.3 - Застосування фільтрів Габора. Розмірність 33x33, f=0.1, =4.0, (a) – орієнтація 00. (b) – орієнтація 450. (c) – орієнтація 900. (d) – орієнтація 1350.

Рівний симетричний фільтр Габора має наступну загальну форму в просторовій області:

$$G(x,y;f,\gamma)=\exp\left\{\frac{-1}{2}\left[\frac{x'^2}{\delta_x^2}+\frac{y'^2}{\delta_y^2}\right]\right\}\cdot\cos(2\pi fx'),$$

$$x'=x\cdot\sin\gamma+y\cdot\cos\gamma,$$

$$y'=x\cdot\cos\gamma-y\cdot\sin\gamma,$$

де f – частота синусоїдальної хвилі площини по напрямку від осі X, і й визначають Гауссовську обвідну по осях X и Y, відповідно, які визначають смугу пропущення фільтра Габора.

У нашому алгоритмі, частота фільтра f – це середня частота виступів (1/K), де K – відстань між виступами. Середня відстань між виступами – приблизно 10 пікселів у зображенні відбитка пальця 500 крапок на дюйм (що є мінімальною розподільною здатністю для зображень цього класу).

Зображення відбитка пальця розділено на чотири складові зображення, що відповідають чотирьом різним значенням (00, 450, 900, і 1350) щодо осі X. 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 й різниці. Нормалізація зроблена, щоб видалити ефекти шуму датчика й розходжень тиску пальця. Нехай I (x, y) позначають сіре значення в пікселя (x, y), Mi й Vi, передбачуваному середньому й різниці сектора Si, відповідно, і Ni(x, y), нормалізоване значення сірого рівня в пікселя (x, y). Для всіх пікселів у секторі Si, нормалізоване зображення визначене як:

$$N_i(x,y)=\begin{cases}M_o+\sqrt{\dfrac{(v_o)\times(I(x,y)-M_i)^2}{v_i}}, & if \quad I(x,y)>M_i\\ M_o-\sqrt{\dfrac{(v_o)\times(I(x,y)-M_i)^2}{v_i}}, & інакше\end{cases}$$

де M0 й V0 – необхідне середнє й значення різниці, відповідно.

3.3. Нормалізація зображення

Нормалізація – піксельна операція, що не змінює чіткість структур борозен і виступів. Для наших експериментів, ми встановлюємо обоє значень й M0, і V0 рівними 100. Нормалізовані, фільтровані, і відновлені зображення для відбитка пальця, показані на рисунку 3.4.

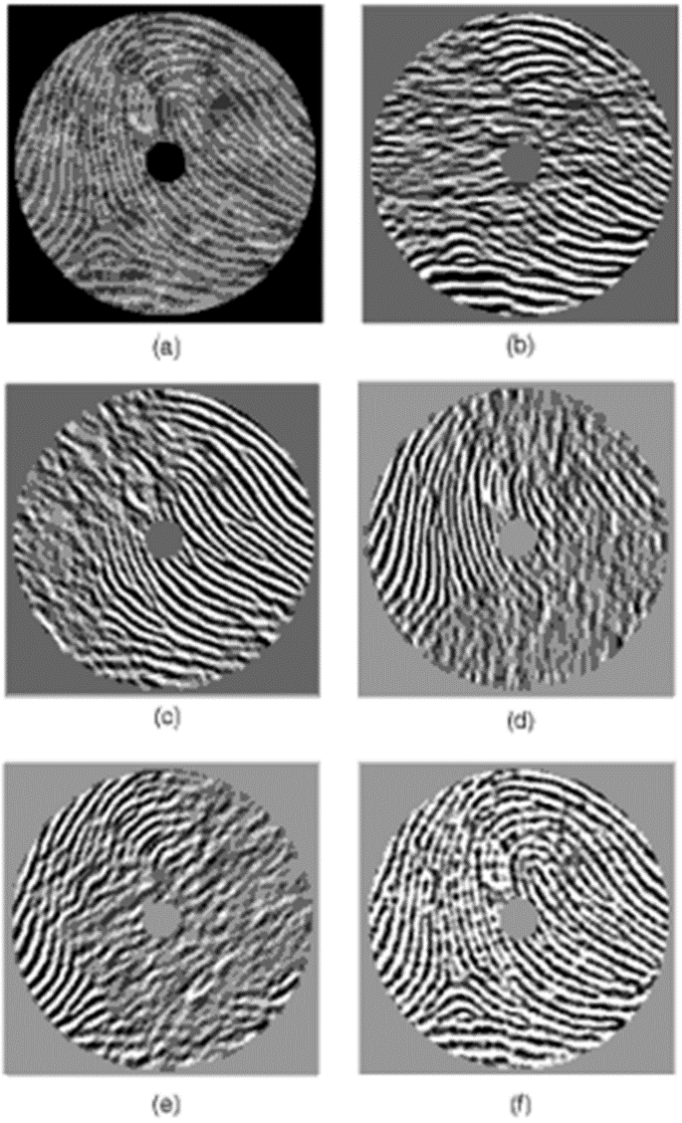


Рисунок 3.4 - Нормалізоване, фільтроване, і відновлене зображення відбитка пальця. (a) – нормалізоване зображення, (b), (c),(d),(e) – фільтроване (00, 450, 900, 1350), (f) – відновлене зображення.

3) Увести вектор ознак у класифікатор.

У цьому алгоритмі, використається двухетапний класифікатор. Цей двухетапний класифікатор використовує класифікатор сусіда K–найближчий на першій стадії й ряд класифікаторів нейронної мережі на другій стадії, щоб класифікувати вектор ознак в один з п'яти класів відбитка пальця. У кожному складовому зображенні, місцеве сусідство з виступами й борознами, які є паралельними відповідному напрямку фільтра, показує більше висока зміна, тоді як місцеве сусідство з виступами й борознами, які не паралельні відповідному фільтру, має тенденцію бути зменшеним фільтром, що приводить до більше низької зміни. У нашому алгоритмі, стандартне відхилення в межах секторів визначає вектор ознак.

Нехай (x, y) буде складовим зображенням, що відповідає для сектора Si. Для i (i = 0,1...47 й Є [00, 450, 900, 1350]), стандартне відхилення , визначено як:

$$F_{i\varphi} = \sqrt{\sum_{K_i} \left(C_{i\varphi}(x,y) - M_{i\varphi} \right)^2}$$

де Ki – число пікселів в Si, i – середні значення пікселя в (x, y). 192–мірні вектори ознак, коди пальців, типових зображень відбитка пальця різних класів показані як зображення сірого рівня із чотирма дисками, кожен диск, що відповідає одному фільтрованому зображенню (рис. 3.5).

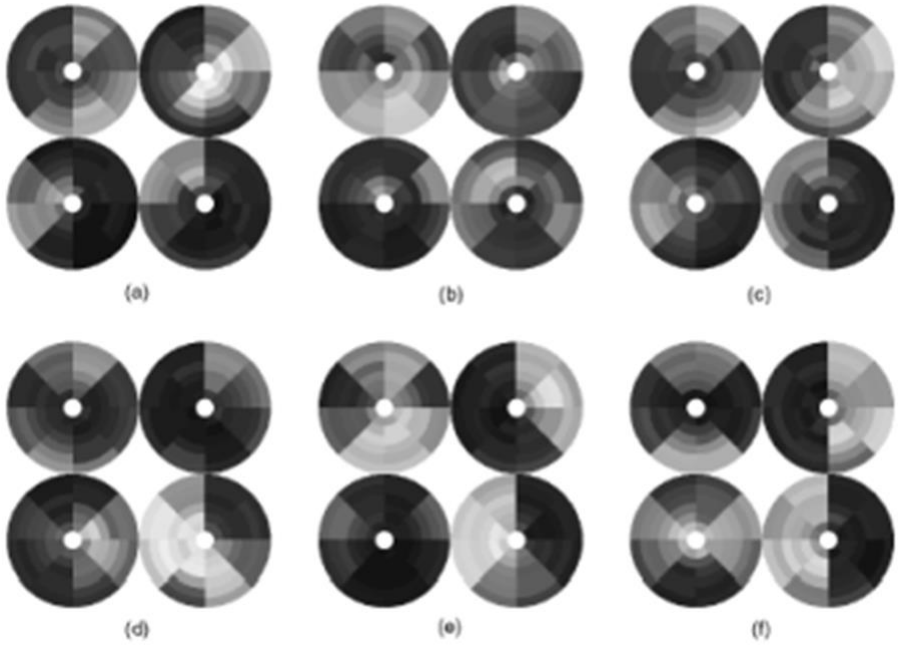


Рисунок 3.5 - 192–мірні вектори ознак (коди пальців).

Сірий рівень у кожному секторі диска представляє значення ознак для цього сектора у фільтрованому зображенні виходу. Можна помітити, що візуально це представлення, здається, дуже добре відрізняє п'ять класів відбитка пальця.

Кожен диск відповідає одному специфічному фільтру з 48 ознаками (показані як сірі значення). Кожен диск (8x6=48 секторів) для в цілому 192 (48 x 4) ознак. (a) Тестова модель, (b) завитушка, (c) права петля, (d) ліва петля, (e) арка, (f) півсфера.

Отже, загальний алгоритм віднесення до класу буде мати такий вигляд (рис.3.6):

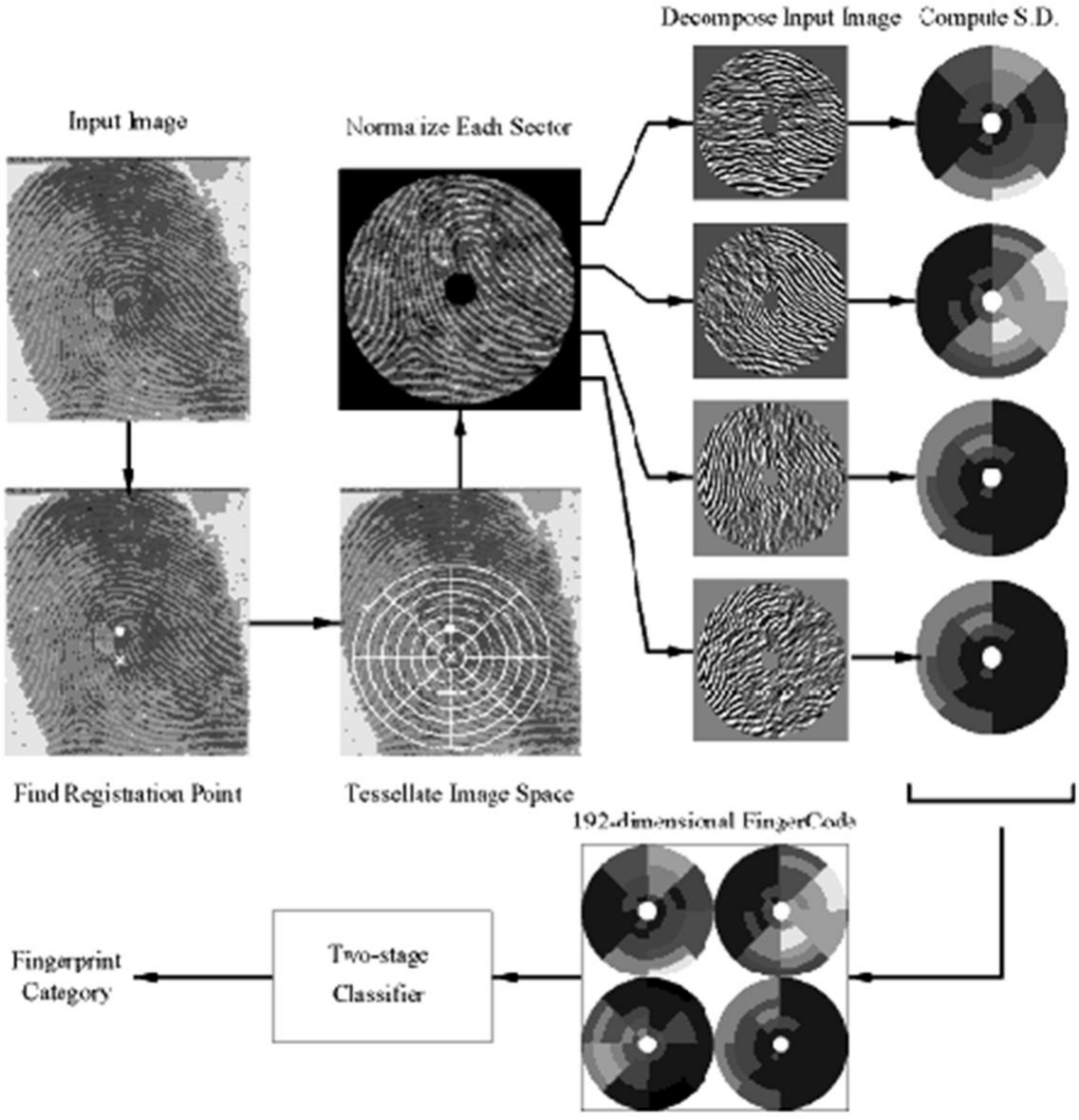


Рисунок 3.6 - Загальна схема алгоритму

Зауважимо, що дана схема застосовується лише для зображення 1.

3.4. Знаходження центра та сегментація оброблюваної області

Щодо термального відбитку, то спільним моментом буде визначення центру відбитку. Наступною дією необхідно визначити розподіл тепла (теплової картини) навколо центру і порівняння з існуючим в базі. Для цього використовується вбудовані у середовище Delphi засоби визначення розподілу спектру (по точках) або автоматизовані фільтри для середовища Adobe (розповсюджуються на вільній основі).

Виділений на первинному зображенні центр відбитка береться за точку відліку. Навколо неї в радіусі 0,5 см виділяється уявна колова область, яка автоматично розбивається на матрицю секторів рівної площі 10 х 10. Після цього функція визначення інтенсивності забарвлення (що фактично є інтенсивністю тепловіддачі) присвоює кожному сектору значення в межах від 0 до 10, яке і відповідає тепловіддачі даної ділянки відбитка.

З отриманих значень створюється числова проста матриця, яке і зберігається в базі даних. Необхідно зазначити, що, при порівнянні термальних відбитків, порівнюються не самі абсолютні значення, а їх відношення між собою. Тобто, якщо в суміжних клітинках матриці є значення 5–3–7, то зовсім не обов’язково, щоб точно такі ж значення були у аналізованого зображення.

Достатньо, щоб співвідношення 5:3:7 (з приблизною точністю до 0,3) відповідало значенню отриманих значень нового відбитку. Схема матриці представлена на рис. 3.7.

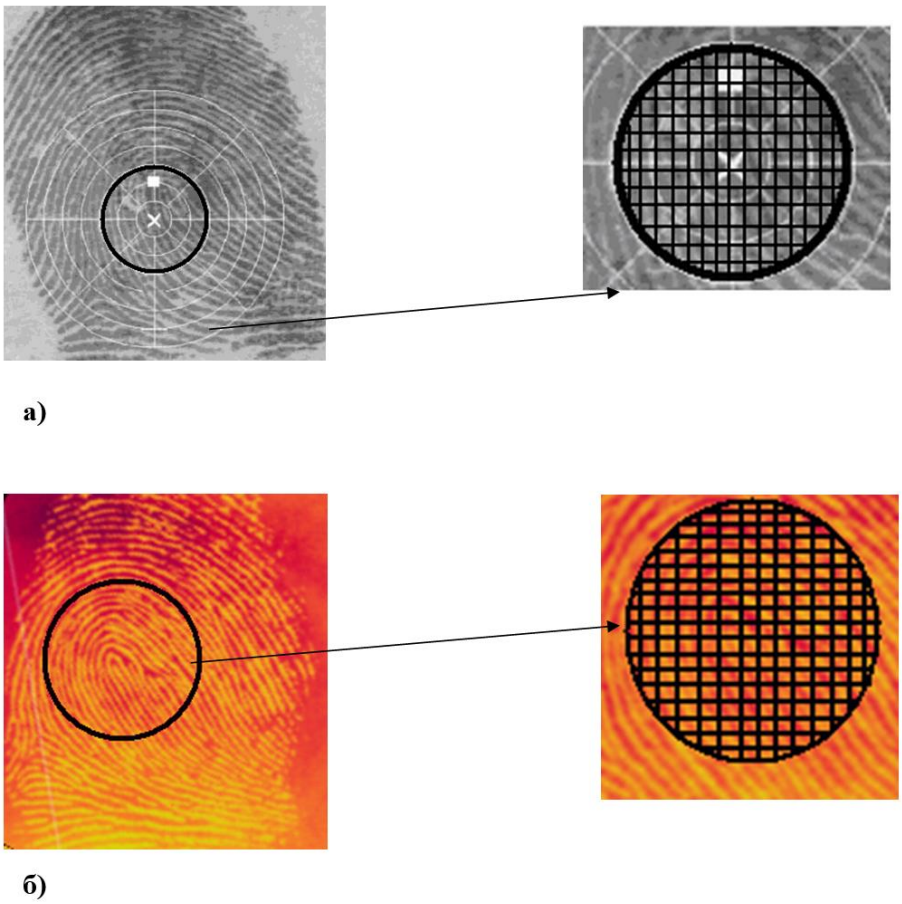


Рисунок 3.7 - Знаходження центра та сегментація оброблюваної області навколо нього на II етапі ідентифікації:

а) для первинного (чорно–білого зображення поверхні) зображення;

б) для вторинного (кольорового зображення тепловіддачі) зображення.

Отримані дані по обох зображеннях у вигляді матриць значень (різної розмірності для кожного з зображень, відповідно до кількості шуканих та отриманих параметрів) порівнюються на співпадання з даними в існуючій Базі Даних. Однак зображення №1 (висококонтрастне чорно–біле зображення) потребує ще однієї дії над собою перед цим порівнянням.

Оскільки порівнювати на відповідність і координати кілька десятків (до сотні) реєстраційних крапок потребувало б значних часових затрат та обчислювальної потужності. Тому, перш ніж порівнювати виконується наступна

дві дія: кожна з отриманих після обробки крапок сполучається умовною лінією з двома найближчими своїми сусідами (так що утворяться трикутники).

Після цього отримані трикутники буду корелюватися з даними в базі на просторове (в двокоординатній системі) розміщення. Це виключає можливість помилки при повороті зображення, адже порівняння йде не по абсолютним координатам, а по розміщенню трикутників один щодо одного. Дослідним шляхом було встановлено, що даний тип розмежування є найбільш оптимальним і по математичній ефективності (мінімальна кількість дій, що потребують значного навантаження обчислювальної потужності) і по часовим затратам, і по величині ймовірності похибки та відхилень значень (не перевищує 5%, в загальному 2–3%).

Кореляційний принцип в своїй основі полягає у визначені середньоквадратичного відхилення у виборках значень. При цьому, M_o середнє значеннння j координати векторів вхідної виборки:

$$M_j = \frac{1}{m}\sum_{i=1}^{m} x_j^i.$$

Величини s_j задають природний масштаб для виміру j–х координат векторів x. Крім того, нам будуть потрібні величина s_f і коефіцієнти кореляції f з j–ми координатами векторів x – r_{fj} :

$$s_f = \sqrt{\frac{1}{m}\sum_{i=1}^{m}(f_i - M_f)^2}, M_f = \frac{1}{m}\sum_{i=1}^{m} f_i, r_{fj} = \frac{\frac{1}{m}\sum_{i=1}^{m}(f_i - M_f)(x_j^i - M_j)}{s_f s_j}$$

Це, зокрема, означає, що всі розглянуті координати вектора x мають ненульову дисперсію, тобто постійні координати виключаються з розгляду – вони не несуть корисної інформації.

Рівняння регресії будемо шукати у формі:

$$\varphi(y) = (\beta, y) + \beta_0$$

Одержимо:

$$\beta_0 = M_f, \beta = s_f R^{-1} R_f,$$

де R_f – вектор коефіцієнтів кореляції f з j–ми координатами векторів x, що має координати r_{fj}, R – матриця коефіцієнтів кореляції між координатами вектора даних (матриця–рядок). Сумарний коефіцієнт буде середнім значення даної матриці.

Отже, кількість співпадань по кожному з зображень у відсотках становить коефіцієнт відповідності К1 і К2. Саме порівняння відбувається за рахунок команд sql. Метод порівняння наступний (приклад):

```
declare @dt datetime
set @dt = getdate()
select case
  when (select count(*) from #T1) <> (select count(*) from #T2) then 'not equal'
  when count(*)-(select count(*) from (select x,z,count(*)C from #T1  group by  x,z)T)=0 then 'equal'
  else 'not equal' end
from
(
select x,z,count(*)C from #T1  group by x,z
union
select x,z,count(*)C from #T2  group by x,z
)TT
go
```

Сумарний коефіцієнт співпадіння порівнюється з попередньо заданим. Якщо відхилення не більше 0,06 (6%), то вважається що відбиток співпав. Результат може виводитись на дисплей або відразу на виконавчий інтерфейс (наприклад, двері).

4. НАУКОВО-ДОСЛІДНА ЧАСТИНА

4.1 Обґрунтування раціональних параметрів і режимів роботи алгоритму

Якість роботи програмно-апаратного комплексу для визначення особи по зображенню відбитків пальців було перевірено на основі аналізу вже попереньо визначених стандартних зображень відбиків, що надаються як тестові для визначення ефективності роботи алгоритмів ідентифікації.

В результаті проведення дослідів з обробкою зображень та наступною їх ідентифікацією в залежності від іх розподільної здатності δ, кольрової насиченості μ ліній відбитку на зображенні і кількості відбитків, що належать одній особі (ймовірнісна характеристика) - τ.

Обробка експериментальних даних, результати яких наведені в додатку 3, проводилася відповідно до методики, що застосовується у лабораторії криміналістики ФБР, а також прийнята як тестова Всесвітньою організацією біометрії:

1) на основі відгуків в п’ятикратному повторі досліду (середніх п’яти різних по якості зображень відбитку однієї людини y_1, y_2, y_3, y_4, y_5) підраховувалося середнє значення відгуків $\bar{y}_{cp}$;

2) визначалася дисперсія, що характеризує розсіювання результатів в кожному досліді за формулою

$$\bar{\bar{S}}_u^2 = \frac{1}{m_0 - 1} \sum_{i_k=1}^{m_0} \left(y_{cpi_k} - \bar{y}_{cp} \right)^2,$$

де m_0 – кількість повторностей;

i_k – номер повторюваності;

y_{cpi_k} – вихідний параметр при i_k-й повторюваності.

3) визначалася дисперсія відтворюваності S_y^2 (помилка досліду) за виразом

$$S_y^2 = \frac{1}{n}\sum_{u=1}^{n} S_u^2 .$$

де n – кількість дослідів;

u – номер досліду.

Як показали розрахунки вона для нашого алгоритму вона рівна 0,0473 (тобто 4,73% помилкових визначень крапок)

4) по критерію Кохрена проводилася перевірка відтворності дослідів, шляхом порівняння розрахункового значення G з табличним $G(0{,}05;27;2)$

$$G \le G(0{,}05;27;2).$$

Розрахункове значення критерію Кохрена визначалося за формулою

$$G = \frac{S_{u\max}^2}{\sum_{u=1}^{n} \overline{\overline{S}}_u^2},$$

де $\overline{\overline{S}}_u^2$ – дисперсія, що характеризує розсіювання (невідповідність) результатів в u-му досліді;

$S_{u\max}^2$ – найбільша з дисперсій.

В результаті розрахунків виявилося, що значення критерію Кохрена для пшениці складає 0,085.

Табличне значення критерію Кохрена при $n = 3$ і $f_u = m_0 - 1 = 2$ рівне 0,128, що значно більше розрахункового. Отже процес відтворюється.

5) коефіцієнти b_0, b_1, b_2, b_3, b_{12}, b_{13} і b_{23} рівняння регресії визначалися за виразами

$$\left.\begin{aligned} b_o &= \frac{1}{n}\sum_{u=1}^{n}\bar{y}_u \\ b_i &= \frac{1}{n}\sum_{u=1}^{n}x_{iu}\bar{y}_u \\ b_{ij} &= \frac{1}{n}\sum_{u=1}^{n}x_{iu}x_{ju}\bar{y}_u \end{aligned}\right\},$$

де n – кількість дослідів;

$\bar{y}_u$ – середнє арифметичне значення вихідного параметра в u-му досліді;

x_{iu} – значення i-го кодованого фактора в рядку матриці в u-му досліді;

x_{ju} – значення j-го кодованого фактора в рядку матриці в u-му досліді (тут i – номер кодованого фактора в лінійних членах рівняння, j – номер другого кодованого фактора в членах рівняння).

Значення коефіцієнтів рівняння моделі зведені в таблицю 4.1.

Таблиця 4.1 - Розрахункові значення коефіцієнтів рівняння моделі

Культура	Значення коефіцієнтів (фактори)							
	b_0	b_1	b_2	b_3	b_4	b_{10}	b_{25}	b_{100}
Відбиток	62,111	0,4333	0,2222	0,34444	0	$-5\cdot10^{-6}$	-0,0444	0

6) визначалося критичне значення коефіцієнтів рівняння моделі з допомогою критерію Стьюдента за формулою

$$|b_a| \geq \Delta b_a = t(0{,}05;\, f_y)\frac{s_y}{\sqrt{n}},$$

де b_a – коефіцієнти b_0, b_i і b_{ij}, значення яких визначаються за формулами;

Δb_a – довірча границя;

$t(0{,}005;\ f_y)$ – критерій Стьюдента при 5%-му рівні значимості та кількості ступенів вільності дисперсії відтворюваності f_y.

Рівень значущості дорівнює $1-\alpha$ (де α – довірча ймовірність).

Для α = 0,95 і f_y = 27 · (3 - 1) = 54 значення критерію Стьюдента t=2,0.

Після обчислень отримаємо, що критичне значення коефіцієнтів для насіння пшениці складає 0,0544.

7) проводилася оцінка значущості коефіцієнтів регресії шляхом порівняння значення коефіцієнтів, які наведені в таблиці 5.1 з їх критичними значеннями. Якщо $|b_a| < \Delta b_a$, то коефіцієнт (взаємодію коефіцієнтів) рахували незначним, а вплив відповідного фактора (взаємодії факторів) – несуттєвим. Як бачимо для нашого алгоритму взаємодії факторів x_1x_3 та x_2x_3 будуть несуттєвими. Таким чином після виключення незначних коефіцієнтів було отримано наступне рівняння регресії

$$y = 62{,}9111 + 0{,}4333 \cdot x_1 + 0{,}2222 \cdot x_2 + 0{,}3444 \cdot x_3 .$$

8) на основі лінійної частини отриманих рівнянь підраховувалися розрахункові значення вихідного параметра y_{∂}, і визначалися дисперсії неадекватності за формулою

$$S_{ad}^2 = \frac{1}{n-k-1}\sum_{u=1}^{n}\left(y - \bar{y}_u\right)^2$$

де y – розрахункове значення відгуку в i-му досліді лінійної частини рівняння.

В результаті отримали, що дисперсія неадекватності для алгоритму ідентифікації складає 0,0265.

9) проводилася перевірка адекватності отриманих математичних моделей за

критерієм Фішера. Гіпотеза про адекватність приймається, якщо розрахункове значення критерію Фішера менше $F(0{,}05;\, f_{ad};\, f_y)$ табличного, тобто

$$F = \frac{S_{ad}^2}{S_y^2} < F(0{,}05;\, f_{ad};\, f_y)$$

де S_{ad}^2 - дисперсія адекватності;

$F(0{,}05;\, f_{ad};\, f_y)$ - критерій Фішера при 5%-му рівні значущості;

f_{ad} - число ступенів вільності дисперсії адекватності;

$f_{ad} = n - k - 1 = 27 - 3 - 1 = 23$ (k - число факторів);

f_y - число ступенів вільності дисперсії відтворюваності;

$f_y = n \cdot (m_0 - 1).$

Розрахункове значення критерію Фішера для насіння пшениці рівне 1,05.

Порівняння критеріїв показує, що табличне значення, яке рівне 1,7, більше розрахункових. Отже, отримані математичні моделі адекватно описують процес обробки розподілу реєстраційних крапок по площі поверхні пальця.

10) перехід від рівняння, в якому x_1, x_2 і x_3 є фактори в кодованому вигляді, до рівняння з факторами X_1, X_2 і X_3 в натуральному вигляді здійснювали, з врахуванням рівності:

$$x_i = \frac{X_i - X_{io}}{\Delta X_i},$$

де x_i, X_i – відповідно кодове та натуральне значення i-го фактора;

X_{io} – натуральне значення i-го фактора при його нульовому рівні;

ΔX_i – інтервал варіювання i-го фактора.

Відповідно до цього після перетворень одержуємо рівняння моделі в остаточному вигляді

$$y = 59{,}6 + 0{,}0433 \cdot \alpha + 0{,}2222 \cdot \omega + 3{,}444 \cdot R.$$

Математична модель в геометричній інтерпретації є певними поверхнями відгуку, вивчення і аналіз яких зручно проводити в просторовій системі координат.

Аналіз поверхонь відгуку показує, що дані фактори X_1, X_2 і X_3 здійснюють суттєвий вплив на коефіцієнт рівномірності знаходження реєстраційних точок. Тому оптимізацію проводили по максимальному значенню коефіцієнта рівномірності розподілу ($\eta \to \max$) графо-аналітичним методом. Результати оптимізації наведені в таблиці 4.2

Таблиця 4.2 - Результати оптимізації параметів алгоритму

Назва парметру	Пікселів, δ	Кількість відбитків однієї особи, τ	Насиченість ліній (відн.), μ	Рекомендована межа ідентифікації (по класам точності), N, точок	Клас точності сканера
Значення	600	3	20	**I – 90** **II – 120** **III – >150**	**A**

За допомогою цієї таблиці можна настроїти коефіцієнти алогритму для коректної роботи з поставленою задачею та відповідний режим роботи. Для цього необхідно залежно необхідної точності ідентифікації, забезпечити відповідні значення розподільної здатності зображень, насиченості кольорування їх ліній та встановити відповідне значення допустимої кількості реєстраційних точок на вхідному зображенні (відповідно до необхідного класу точності).

На рис. 4.1 показана схема поверхні відгуку.

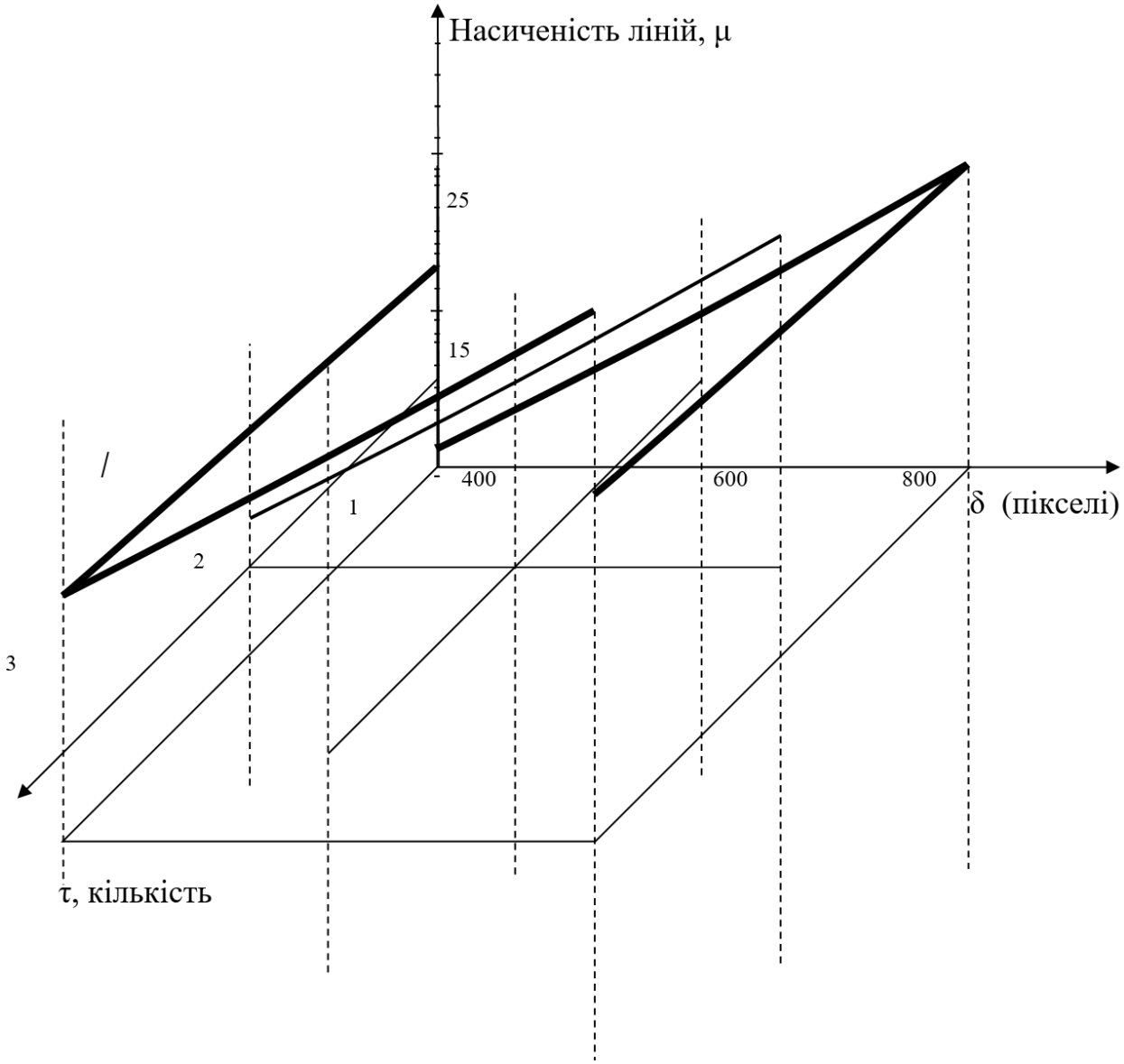


Рисунок. 4.1 - Схема поверхні відгуку

5. СПЕЦІАЛЬНА ЧАСТИНА

5.1 Графічний інтерфейс користувача програми

При запуску виконавчого файлу проекту Fingers.exe користувач бачить на екрані робочу оболонку програми, яка має наступний вигляд (рис. 5.1)

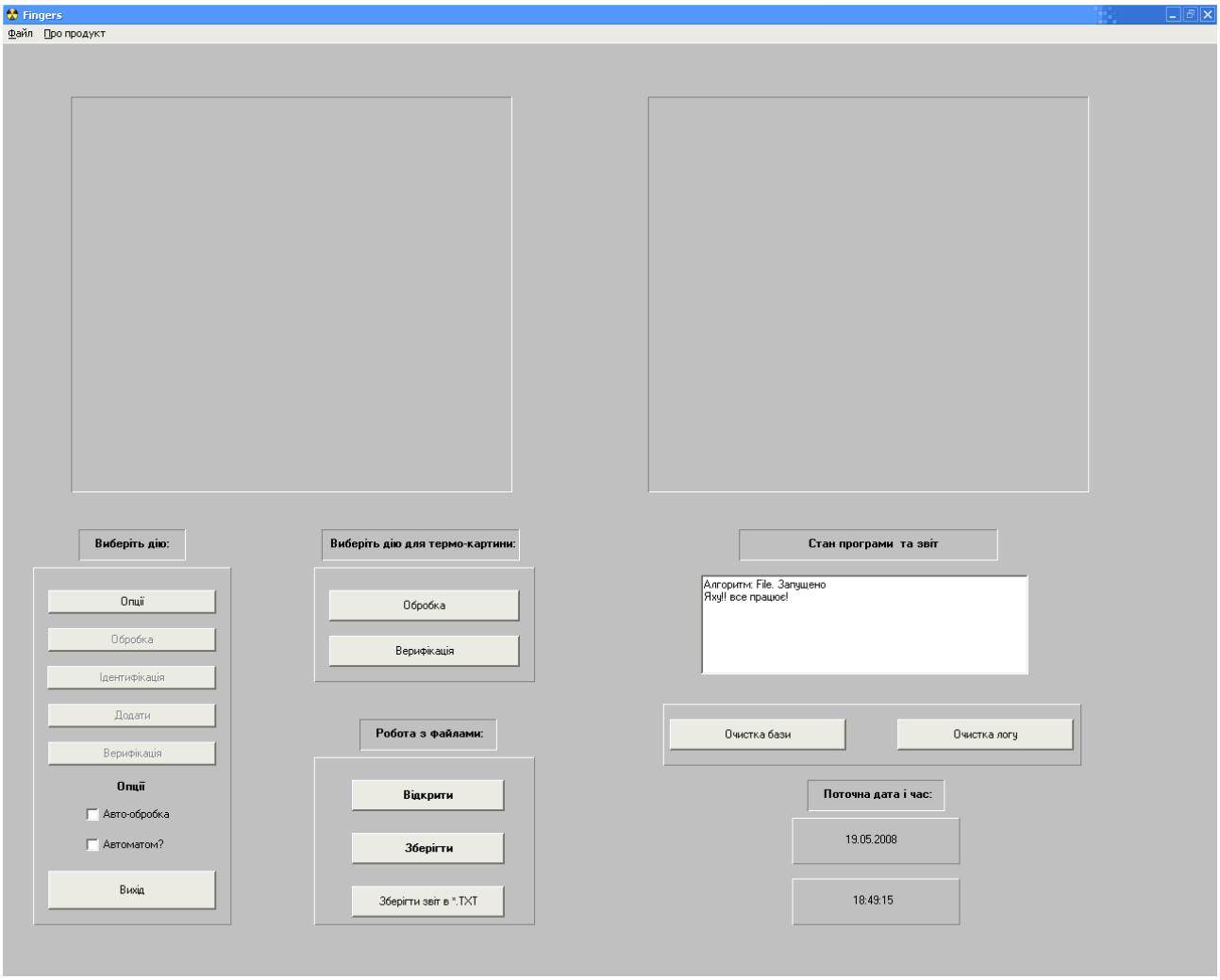


Рисунок 5.1 - Робоча оболонка програми

Як видно з рисинку 5.1, робоча область поділена на 3 сектори відповідно до функціонального призначення. Також присутнє головне меню програми, за допомогою якого здійснюється управління файлами.

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

- «Опції» – кнопка виклику модуля опцій відображення (рис. 5.2);
- «Обробка» – пошук та виділення спеціальних точок на зображенні, їх сполучення у трикутники (рис. 5.3);
- «Ідентифікація» – порівняння отриманих даних із присутніми в базі даних та виявлення співпадань;
- «Додати» – додавання нового відбитку в базу даних (при невизначені попередніми діями);

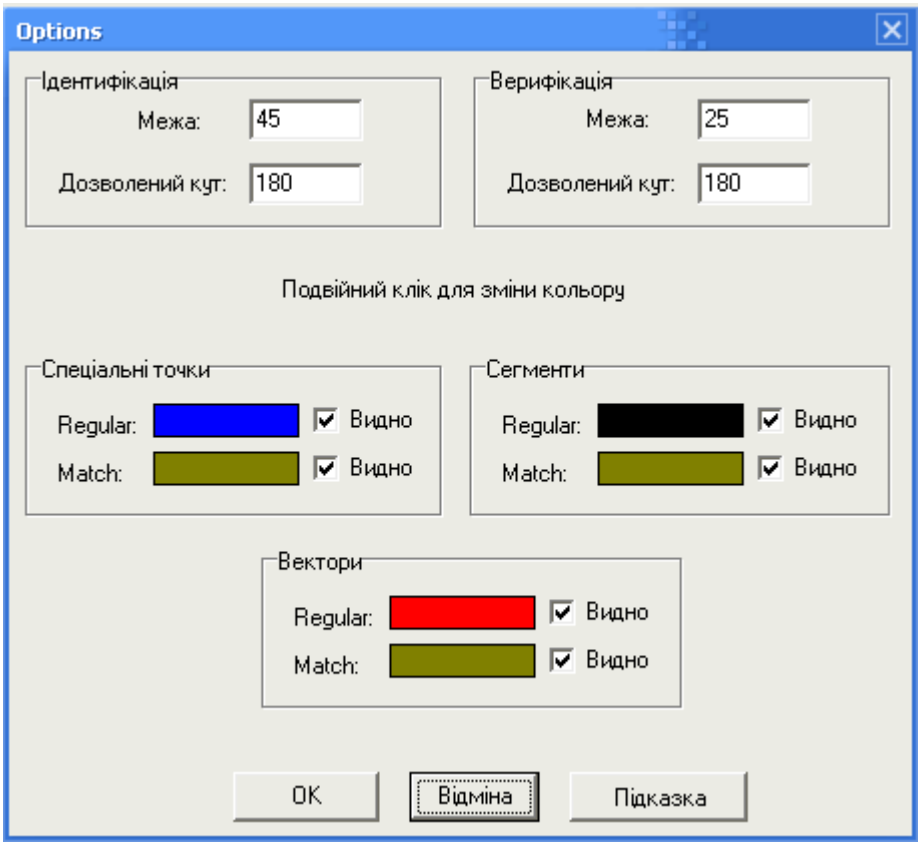


Рисунок 5.2 - Модуль опцій відображення

- «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. 5.4.);

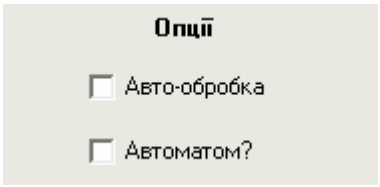


Рисунок 5.3 - Група опцій автоматичної обробки

- «Вихід» – закриття програми та фіналзація 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 являє собою 2 фаски, на яких, при завантаженні, відображається зображення відбитку (область малюнку зліва), а також тимчасове зображення після обробки (область малюнку справа).

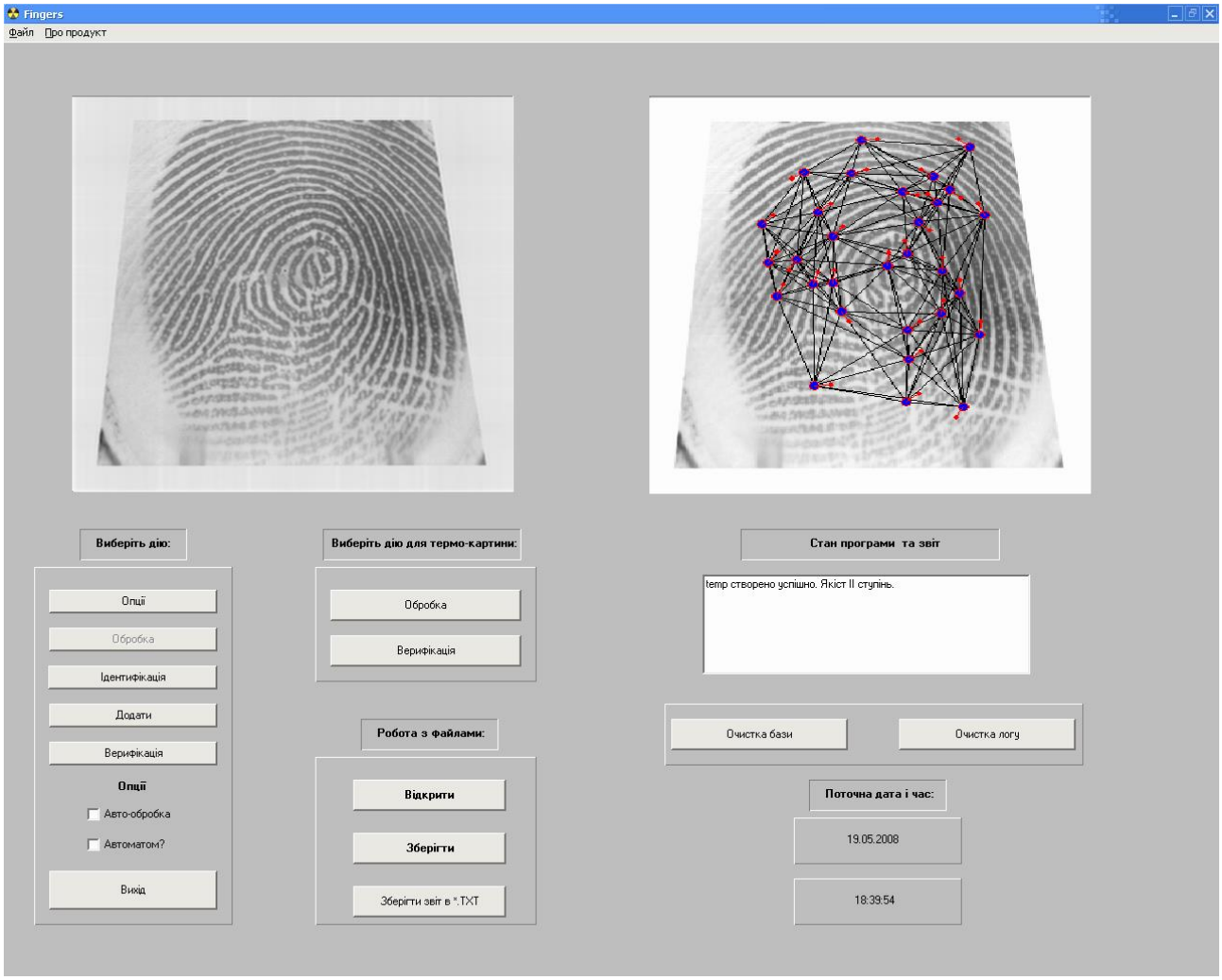


Рисунок 5.4 - Вікно програми після виконання обробки

Сектор III являє собою текстове поле звітування роботи програми (рис. 5.5.).

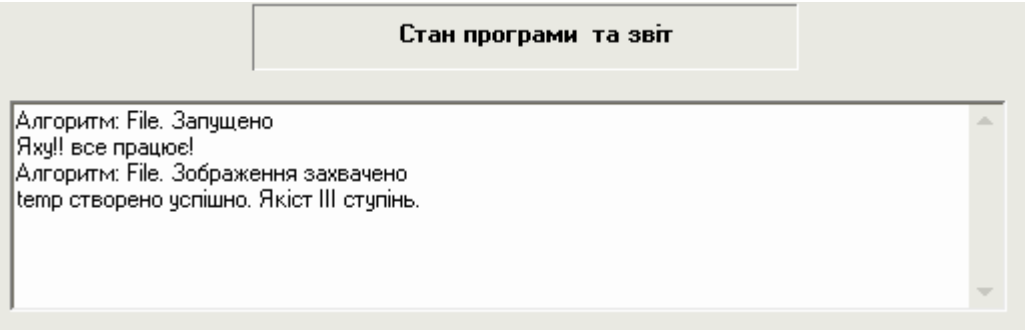


Рисунок 5.5 - Область звітування

- «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 отримає наступне повідомлення (рис. 5.6.):

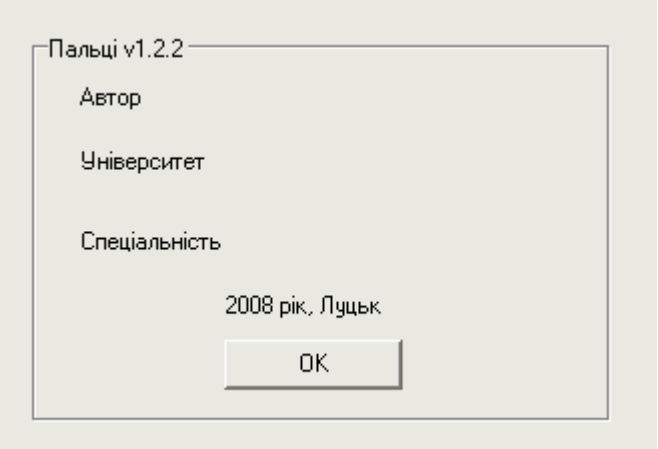


Рисунок 5.6 - Повідомлення «про продукт».

В програмі також реалізовано комбінації клавіш для швидкої та зручної роботи з файлами:

- Ctrl+L (Load) – завантаження зображення;
- Ctrl+S (Save) – збереження зображення;

5.2. Інтерфейс та специфікація програми установки

Програмний продукт є засобом безпеки, отже його встановлення також повинне бути захищене від зловмисників. Крім того, програма працює з динамічними бібліотеками, що вимагає додаткового їх пропису у реєстрі операційної системи Windows. Виходячи з цих вимог, мною був обраний пакет для створення установочних файлів та скриптів Inno Setup Compiler (http://www.innosetup.com/isinfo.php), що розповсюджується на безкоштовній основі та надає надзвичайно широкі можливості по створенню, налагодженню та конфігурації установки.

Робота з Inno Setup Compiler досить проста і не вимагає додаткових знань мови скриптування. Усі можливості детально описані у документації. Головне вікно програми являє собою простий на вигляд редактор скрипту, усі додаткові

функції якого реалізуються через головне меню (рис. 5.7.).

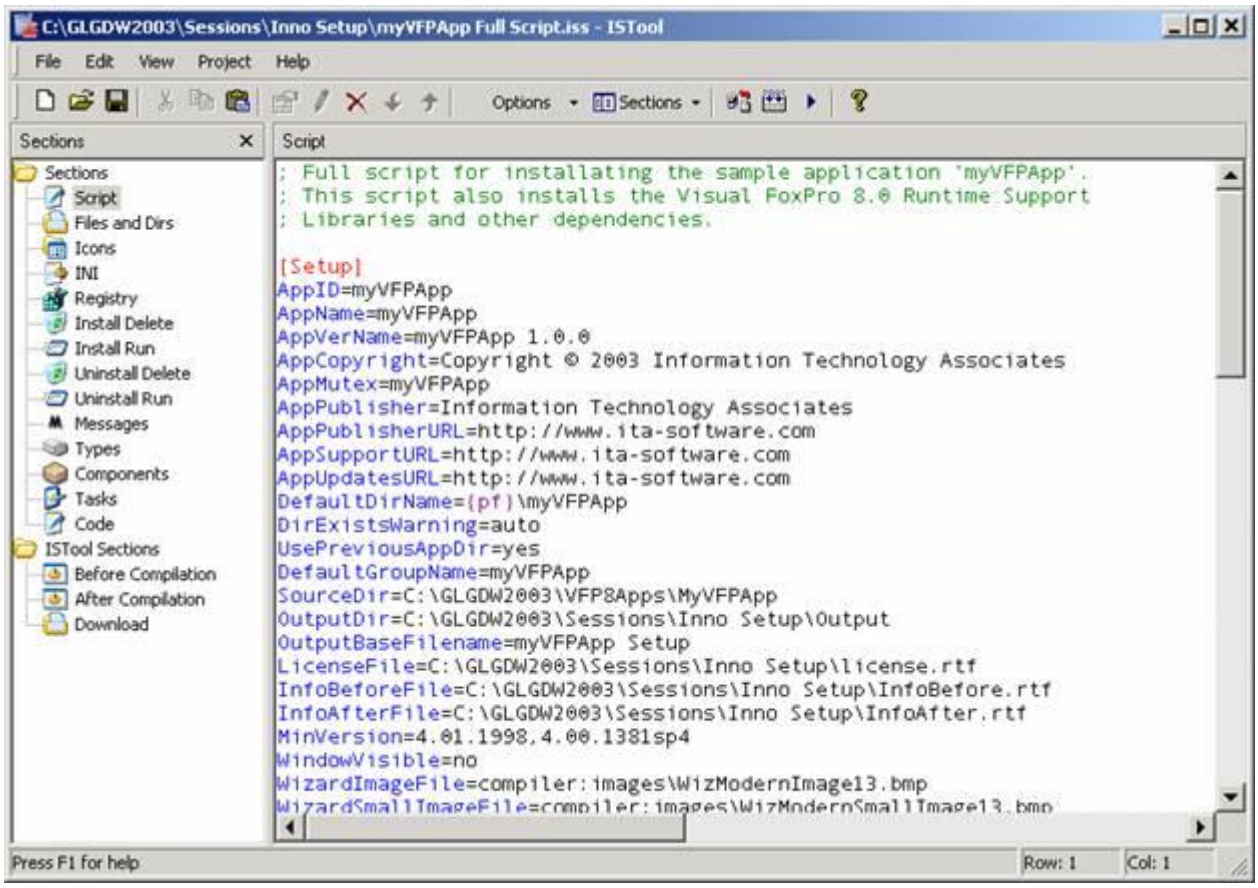


Рисунок 5.7 - Головне вікно пакету Inno Setup Compiler.

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

Оскільки в нашій установці не вимагається додаткових модулів, весь скрипт буде являти собою перелік файлів-джерел та шляхів для їх встановлення (фактично копіювання).

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]
```

- 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 т.д.;
- додаткова перевірки цілісності файлів;
- додаткова перевірка версії файлів;
- додаткові мови установки

Після перевірки та виконання написаного скрипту Inno Setup Compiler компіює виконуючий exe-файл, що і буде здійснювати саму установку. Виконання цього файлу не вимагає ніяких додаткових встановлених програмних продуктів у системі. Сам файл установки компілюється в захищеному режимі, тому змінити його після створення неможливо.

Створена програма установки є надзвичайно зручною та легкою у використані. Фактично, уся установка вимагає від недосвідченого користувача лише 3 натискання кнопки «Next» (тобто «Далі»). Після цього наш програмний продукт буде встановлено у визначеному наперед місці, а його компоненти автоматично зареєстровані.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1 Ергономічне дослідження та організація робочого місця користувача ЕОМ

Прискорене впровадження ЕОМ практично в усі області діяльності веде до появи великої кількості робочих місць із візуальними дисплейними терміналами (ВДТ). Вони широко поширюються як на різні виробництва в різних системах контролю і керування, так і в різних адміністративно-суспільних будинках, де розміщуються обчислювальні центри організацій й інститутів, читальні і довідкові зали бібліотек, комп'ютерні зали шкіл, технікумів, і, зрештою, офісів і приватних квартир.

Сучасна професія користувача ЕОМ являє собою модель розумової праці, що виконується в одноманітній позі в умовах обмеження м'язової активності при рухливості кистей рук, при високій напрузі зорових функцій і нервово-емоційній напрузі в умовах впливу багатьох фізичних факторів. Встановлено, що стан організму користувачів по суб'єктивних і об'єктивних показниках залежить від типу роботи біля екрану й умов її виконання. Усі користувачі поділяються на програмістів (розробників і користувачів програм) і операторів прецизійних робіт, а також вводу і виводу даних. Непрофесіонали – це касири, бібліотекарі, студенти, школярі і т.д.

У період роботи з ВДТ на електронно-променевих трубках на організм користувачів діє цілий ряд фізичних факторів, але усі вони знаходяться в межах, які значно нижчі нормованих величин відповідно до діючих в даний час нормативних документів.

При дослідженні зорових функцій у лабораторних і виробничих умовах були виявлені розлади акомодації, конвергенції, гостроти зору і контрастної

чутливості ока. Причому виявлені зміни носили більш глибокий характер, коли робота супроводжувалася високим нервово-емоційним компонентом, напри-лад, пошук помилок у програмі або її налагодженні в умовах дефіциту часу.

Патологічні зміни зорового аналізатора як наслідок виробничої діяльності в користувачів ЕОМ практично не зустрічаються. Однак фізіологічні дослідження показують, що в більшості програмістів спостерігаються деякі порушення функцій акомодації і контрастної чутливості ока.

У формуванні зорового стомлення користувачів величезну роль грає специфіка зорової роботи з екраном.

Аналізуючи вищенаписане, можна дати наступні рекомендації для збереження працездатності користувачів ЕОМ і усунення можливості виникнення загальних і зорових порушень:

- у дисплейних класах температура повинна складати 19-21^{0}С, відносна вологість повітря 55-56 %, швидкість руху повітря не більше 0.2 м/с;
- рівні звуку не повинні перевищувати 50 дБ. З огляду на те, що основним джерелом шуму в дисплейних класах є вентилятори в системному блоці і, приймаючи до уваги повсюдне використання практично безшумних струменевих принтерів, цієї вимоги досягти не важко;
- необхідні деякі прийоми боротьби зі статичною електрикою. Для цього рекомендується в дисплейних класах підлогу покривати антистатичним лінолеумом;
- з огляду на специфіку роботи оператора ЕОМ, яка пов'язана зі значним зоровим навантаженням, першочерговою задачею є забезпечення прийнятних умов візуальної роботи користувачів за рахунок найкращого розподілу яскравостей у полі зору працюючого і максимально можливого зменшення осліпленості від прямих і відбитих відблисків. Необхідно забезпечити як кількісні, так і якісні параметри освітлення.

З цього випливає, що життєво важливим для підвищення працездатності користувача і збереження його здоров'я, є правильна організація освітленості робочого місця користувача. Параметри висвітлення починати вибирати треба з вибору приміщення. При виборі приміщення необхідно враховувати, що вікна

можуть створювати відблиски на екранах дисплеїв і викликати значну осліпленість у користувачів, які сидять перед ними. Тому рекомендується використання приміщення з однобічним розташуванням світлових прорізів, обов'язково обладнаних сонцезахисними пристроями: шторами, жалюзі і т.д. Необхідно, по можливості, також забезпечити обробку інтер'єра, який має невисокий коефіцієнт відбиття. Тому не рекомендується світла обробка стін приміщення, а також використання світлих меблів. Всі оздоблювальні матеріали повинні бути матовими.

Дуже важливо правильно розташувати робочі місця користувачів. Розташування робочого місця користувача обличчям або спиною до віконного ряду недопустиме. Вибір типу світильника по світлорозподілу і способові розташування в приміщенні залежить від висоти приміщення, кількості робочих місць і деяких інших факторів.

Робочі місця варто розміщувати рядами, які йдуть паралельно віконному рядові таким чином, щоб площина екрана користувача була перпендикулярна до площини віконного ряду. Найбільш оптимальним є варіант використання люмінесцентних світильників денного світла.

Світильники повинні розташовуватися над проходами між рядами робочих місць суцільною лінією або лінією з розривами, в залежності від кількості світильників у лінії, для забезпечення нормованої освітленості робочих місць користувачів.

З метою створення комфортних умов кожному працівникові підбирають висоту і кут нахилу клавіатури, екрану і сидіння. Робоче місце, як правило, розташовують на висоті 74 см від підлоги.

Впровадження вищеописаних рекомендацій при виборі розташування й організації робочого місця користувачів ЕОМ значно знизить скарги користувачів на втому і стомлення, попередить появу і розвиток загальних зорових та інших порушень, а також підвищить працездатність користувачів.

6.2 Заходи пожежної безпеки в приміщеннях з електронною апаратурою

Пожежна безпека повинна забезпечуватися шляхом проведення організаційних, технічних та інших заходів, спрямованих на попередження пожеж, забезпечення безпеки людей, зниження можливих майнових втрат і зменшення негативних екологічних наслідків у разі їх виникнення, створення умов для швидкого виклику пожежних підрозділів та успішного гасіння пожеж.

Небезпека розвитку пожежі у приміщеннях з електронною апаратурою обумовлюється застосуванням розгалужених систем вентиляції і кондиціонування, розвиненою системою електроживлення електронної апаратури, а також особливостями об'ємно-планувальних рішень приміщень.

Небезпека загорання в електронній апаратурі пов'язана із значною кількістю щільно розміщених на монтажних платах і блоках електронних вузлів і схем, електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів і транзисторів. Висока щільність елементів в електронних схемах приводить до значного підвищення температури окремих вузлів (80 … 100 ˚С), що може бути причиною загорання ізоляційних матеріалів. Слабкий опір ізоляційних матеріалів дії температури може викликати порушення схеми і привести до короткого замикання.

Зокрема, 23% пожеж в електронній апаратурі виникають через короткі замикання чи перегрів електричних елементів, 28% пожеж – в апаратурі, пов'язаною з електронними обчислювальними машинами, при цьому причинами пожеж є дефекти люмінесцентних ламп освітлення, несправності систем кондиціонування повітря і автоматичної апаратури друку.

Статистичні дані показують, що самі електронні пристрої рідко спричиняють пожежу, але, опиняючись в пожежнонебезпечному середовищі, сприяють утворенню важких наслідків пожежі. Великий матеріальний збиток наноситься навіть у тих випадках, коли електронне устаткування врятоване від вогню, але в результаті пожежі виявилося забрудненим. Стратегія

протипожежного захисту полягає у виключенні можливості виникнення пожежі, ліквідації загорання на початковій стадії, запобігання загоранню.

Цілком безпечних і нешкідливих виробництв не існує. Однак задача охорони праці – це звести до мінімуму імовірність нещасного випадку або захворювання працюючого з одночасним забезпеченням комфортних умов при максимальній продуктивності праці.

Так як основна частина даної дипломної роботи виконувалася на комп'ютері і реалізація описуваного методу, в основному, також буде виконуватися на комп'ютері, то дуже важливо забезпечити операторові достатню освітленість робочого місця для запобігання втоми очей і погіршення зору. Вище була розрахована схема розташування світильників для створення максимально комфортних умов оператора з метою підвищення його працездатності і попередження появи та розвитку зорових і інших порушень.

6.3. Електромагнітний імпульс ядерного вибуху і захист від нього радіоелектронних засобів

На початку 90-х років у США стала зароджуватися концепція, відповідно до якої збройні сили країни повинні мати не тільки ядерні і звичайні озброєння, але і спеціальні засоби, що забезпечують ефективну участь у локальних конфліктах без нанесення супротивнику зайвих втрат у живій силі і матеріальних цінностях.

До цієї спеціальної зброї американські військові фахівці в першу чергу відносять:

- засоби створення електромагнітного імпульсу (EMI);
- генератори інфразвуку;
- хімічні склади і біологічні рецептури, здатні змінювати структуру базових матеріалів основних елементів бойової техніки;
- речовини, що виводять з ладу змащення і гумові вироби;

- лазери.

Найбільш близькі до прийняття на озброєння різні типи лазерів для осліплення особового складу, хімічні засоби для його знерухомлення, генератори ЕМІ, що негативно впливають на роботу електронної техніки.

Генератори ЕМІ (супер ЕМІ), як показують теоретичні роботи і проведені за кордоном експерименти, можна ефективно використовувати для виводу з ладу електронної й електротехнічної апаратури, для стирання інформації в банках даних і псування ЕОМ.

За допомогою ЗНСД на основі генераторів ЕМІ можливий вивід з ладу ЕОМ, ключових радіо й електротехнічних засобів, систем електронного запалювання й інших автомобільних агрегатів, чи підривши інактивація мінних полів. Вплив цієї зброї досить вибірково і політично цілком прийнятний, однак потрібна точна доставка його в райони ураження.

Незважаючи на визнання військово-політичним керівництвом США і НАТО неможливості перемоги в ядерній війні, різні аспекти вражаючого дії ядерної зброї продовжують широко обговорюватися. Так, в одному з розглянутих іноземними фахівцями сценаріїв початкового періоду ядерної війни особливе місце приділяється потенційної можливості висновку з ладу радіоелектронної техніки в результаті впливу на неї ЕМІ.

Вважається, що підірвавши на висоті близько 400 км тільки одних боєприпасів потужністю більш 10 Мт приведе до такого порушення функціонування радіоелектронних засобів у великому районі, при якому час їхнього відновлення перевищить припустимі терміни для вживання відповідних заходів.

По розрахунках американських експертів, оптимальною точкою підриву ядерних боєприпасів для поразки ЕМІ радіоелектронних засобів майже на всій території США була би точка в космосі з епіцентром у районі географічного центра країни, що знаходиться в штаті Небраска.

Теоретичні дослідження і результати фізичних експериментів показують, що ЕМІ ядерного вибуху може привести не тільки до виходу з ладу напівпровідникових електронних пристроїв, але і до руйнування металевих провідників кабелів наземних споруд. Крім того, можлива поразка апаратури, що знаходяться на низьких орбітах.

Для генерації ЕМІ ядерні боєприпаси можуть підриватися в космічному просторі, що не приводить до виникнення ударної хвилі і випаданню радіоактивних опадів. Тому в закордонній пресі виголошуються наступні думки про "неядерний характер" такого бойового застосування ядерної зброї і про те, що удар з використанням ЕМІ не обов'язково приведе до загальної ядерної війни.

Небезпека цих заяв очевидна, тому що одночасно деякі закордонні фахівці не виключають можливість масової поразки за допомогою ЕМІ і живої сили. У всякому разі цілком очевидно, що наводимі під впливом ЕМІ в металевих елементах техніки струми і напруги будуть смертельно небезпечні для особового складу.

6.3. Шляхи вирішення задачі захисту від ЕМІ

Ідеальним захистом від ЕМІ було б повне закрите приміщення металевим екраном, в якому розміщена радіоелектронна апаратура. Разом з тим ясно, що практично забезпечити такий захист в ряді випадків неможливо, тому що для роботи апаратури часто потрібно забезпечити її електричний зв'язок із зовнішніми пристроями.

Тому, використовуються менш надійні засоби захисту, такі як струмопровідні сітки чи плівкові покриття для вікон, стільникові металеві конструкції для воздухозабірників і вентиляційних отворів та контактні пружинні прокладки, розташовувані по периметру дверей і люків.

Більш складною технічною проблемою вважається захист від проникнення ЕМІ в апаратуру через різні кабельні вводи. Радикальним вирішенням даної проблеми міг би стати перехід від електричних мереж зв'язку до практично не підданих впливу ЕМІ волоконно-оптичних.

Однак заміна напівпровідникових приладів у всьому спектрі виконуваних ними функцій електронно-оптичними пристроями можливо тільки у віддаленому майбутньому. Тому в даний час як засоби захисту кабельних вводів найбільше широко використовуються фільтри, в тому числі волоконні, а також іскрові розрядники, металоокисні варистори і високошвидкісні зенеровські діоди.

Усі ці засоби мають як переваги, так і недоліки. Так, ємнісно-індуктивні фільтри досить ефективні для захисту від ЕМІ малої інтенсивності, а волоконні фільтри захищають у відносно вузькому діапазоні надвисоких частот. Іскрові розрядники володіють значною інерційністю й, в основному, придатні для захисту від перевантажень, що виникають під впливом напруг і струмів, що наводяться в обшиваці літака, кожусі апаратури й екрануванні кабеля.

Металлоокисні варистори являють собою напівпровідникові прилади, що різко підвищують свою провідність при високій напрузі. Однак, при застосуванні цих приладів, як засобу захисту від ЕМІ, варто враховувати їхню недостатньо високу швидкодію і погіршення характеристик при кількаразовому впливі навантажень.

Ці недоліки відсутні у високошвидкісних зенеровських діодах, дія яких базується на різкій лавиноподібній зміні опору від відносно високого значення практично до нуля при перевищенні прикладеної до них напруги визначеної граничної величини. Крім того, на відміну від варисторів, характеристики зенеровських діодів після багаторазових впливів високих напруг і переключень режимів не погіршуються.

Найбільш раціональним підходом до проектування засобів захисту від ЕМІ кабельних вводів є створення таких роз’ємів, в конструкції яких передбачені спеціальні міри, що забезпечують формування елементів фільтрів і установку

вмонтованих зенеровських діодів. Подібне вирішення сприяє одержанню дуже малих значень ємності й індуктивності, що необхідно для забезпечення захисту від імпульсів, що мають незначну тривалість і, отже, потужну високочастотну складову. Використання роз'ємів подібної конструкції дозволить вирішити проблему обмеження масо-габаритних характеристик пристрою захисту.

Складність вирішення задачі захисту від ЕМІ і висока вартість розроблених для цих цілей засобів і методів змушують піти на перших порах по шляху їхнього вибіркового застосування в особливо важливих системах зброї і військової техніки. Першими цілеспрямованими роботами в даному напрямку були програми захисту від ЕМІ стратегічної зброї.

Такий же шлях обраний і для захисту систем, що мають велику довжину керування і зв'язку. Однак, основним методом вирішення даної даної проблеми закордонні фахівці вважають створення так званих розподілених мереж зв'язку (типу "Гвен"), перші елементи яких уже розгорнуті на континентальній частині США.

Сучасний стан проблеми ЕМІ можна оцінити в такий спосіб. Досить добре досліджені теоретично і підтверджені експериментально механізми генерації ЕМІ і параметри його вражаючої дії.

Розроблено стандарти захищеності апаратури і відомі ефективні засоби захисту. Однак, для досягнення достатньої впевненості в надійності захисту систем і засобів від ЕМІ необхідно провести випробовування за допомогою імітатора. Що стосується повномасштабних випробовувань систем зв'язку і керування, то ця задача навряд чи буде вирішена в доступному для огляду майбутньому.

В даний час у деяких західних країнах ведуться роботи з генерації імпульсів електромагнітного випромінювання магнітодинамічними пристроями, а також високовольтними розрядами. Тому питання захищеності від впливу ЕМІ будуть залишатися в центрі уваги фахівців при будь-якому результаті переговорів про ядерне роззброювання.

ВИСНОВКИ

В даній кваліфікаційній роботі була розроблена автоматизована система ідентифікації особи по відбитках пальців. На основі огляду існуючих методик і методів ідентифікації осіб розроблено комбінований програмно-апаратний комплекс, який визначає відповідність існуючим у базі записам суб'єктів доступу.

При огляді програмних та програмно-апаратних комплексів для обробки і ідентифікації зображень відбитків пальців було виявлено такі їх недоліки як: низька швидкість обробки зображень, низька ефективність алгоритму, велике математичне навантаження на систему, відсутність доступної документації на різних мовах.

Розроблений програмно-апаратний комплекс для ідентифікації осіб по зображенням їх відбитків, який реалізується за допомогою комп'ютера, спеціалізованого сканера і програми написаної на мові програмування Delphi, здійснює виконання наступних функцій:

- знаходження реєстраційних крапок на зображенні;
- їх сполучення у трикутники з наступним обрахунком сумарного вектора кожного з них;
- визначення кількості співпадаючих точок;
- виділення центру на термо картині;
- визначення матриці значень тепловіддачі (насиченість кольору) секторів навколо нього.

ПЕРЕЛІК ПОСИЛАНЬ

1. Методичні рекомендації з виконання, оформлення та захисту кваліфікаційних робіт магістрів спеціальності 151 – «Автоматизація та комп’ютерно-інтегровані технології» / ТНТУ ім. І. Пулюя; уклад. А.Г. Микитишин, М.М. Митник. – Тернопіль: ТНТУ, 2020. – 80 с.
2. Тотосько О.В. Введення в комп’ютерну графіку та дизайн : Навчальний посібник для студентів спеціальності 174 «Автоматизація, комп’ютерно-інтегровані технології та робототехніка» / Укладачі : О.В. Тотосько, П.Д. Стухляк, А.Г. Микитишин, В.В. Левицький, Р.З. Золотий – Тернопіль : ФОП Паляниця В.А., 2023 – 304 с. ISBN 978-617-7875-60-3
3. Пилипець М. І. Правила заповнення основних форм технологічних документів : навч.-метод. посіб. / Уклад. Пилипець М. І., Ткаченко І. Г., Левкович М. Г., Васильків В. В., Радик Д. Л. Тернопіль : ТДТУ, 2009. 108с.
4. Микитишин А.Г., Митник, П.Д. Стухляк. Комплексна безпека інформаційних мережевих систем: навчальний посібник – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 256 с.
5. Телекомунікаційні системи та мережі : навчальний посібник для студентів спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» / Укладачі : Микитишин А.Г., Митник М.М., Стухляк П.Д. – Тернопіль : Тернопільський національний технічний університет імені Івана Пулюя, 2017 – 384 с.
6. Шпак Ю.А. Delphi 7 на примерах // Под ред. Ю.С. Ковтанюка – К.: Издательство Юниор, 2003. – 384 с.
7. Путятін Є. П., Гороховатській В.О., Матат О.О. Методи та алгоритми комп’ютерного зору: Навч. посібник. Х: СМІТ, 2006. 236 с.
8. Тимощук П. В. Штучні нейронні мережі. Штучні нейронні мережі. Навчальний посібник. Львів: Видавництво Львівської політехніки, – 2011, – 444 с.

9. Вовк С.М., Гнатушенко В.В., Бондаренко М.В. Методи обробки зображень та компютерний зір : навч. посіб. /С.М. Вовк, В.В. Гнатушенко, М.В. Бондаренко. – Д. : ЛІРА, 2016. – 148 с.
10. А.О. Різуненко Р 49 Теорія та практика цифрової обробки зображень: Монографія. – Полтава: РВВ ПУСКУ, 2009. – 195 с.
11. Р. Гонсалес, Р. Вудс Цифровая обработка изображений в среде MatLab 3. Pattern recognition, fourth edition / Sergios Theodoridis, Konstantinos Koutroumbas. – Elsevier Inc., 2009. – 961 p
12. Методичні вказівки для написання розділу «Безпека життєдіяльності, основи охорони праці» в кваліфікаційних роботах здобувачів освітнього рівня „бакалавр”. Для студентів всіх форм навчання рівень вищої освіти перший (бакалаврський) / укл. : О. Я. Гурик , І. Б. Окіпний. – Тернопіль : ТНТУ імені Івана Пулюя, 2021. - 20 с.
13. Стручок В.С. Навчальний посібник до написання розділу дипломного проекту та дипломної роботи ″Безпека в надзвичайних ситуаціях″ для студентів всіх спец. денної, заочної (дистанційної) та екстернатної форм навчання / В.С. Стручок, О.С. Стручок, Д.В. Мудра. - Тернопіль : ТНТУ, 2016. - 112 с.
14. Вовк Ю. Я. Охорона праці в галузі. Навчальний посібник / Ю. Я. Вовк, І. П. Вовк – Тернопіль: ФОП Паляниця В.А. – 2015. – 172 с.