Міністерство освіти і науки України
Державний університет «Одеська політехніка»

Інститут штучного інтелекту та робототехніки

Кафедра «Комп'ютерні системи»

Букрєєв Артем Валерійович,

студент групи УК-161

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

ДОСЛІДЖЕННЯ МЕТОДІВ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ БІОМЕТРИЧНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ЗА ВЕНОЗНИМ РИСУНКОМ

Спеціальність: 123 – "Комп'ютерна інженерія"

Спеціалізація: Спеціалізовані комп'ютерні системи

Керівник:

Стрельцов Олег Васильович,

кандидат техн. наук, доцент

Одеса — 2021

Міністерство освіти і науки України
Державний університет «Одеська політехніка»

Інститут штучного інтелекту та робототехніки
Кафедра комп'ютерних систем

Рівень вищої освіти другий (магістерський)
Спеціальність 123 Комп'ютерна інженерія
(шифр і назва)
Спеціалізація / освітня програма Спеціалізовані ком'ютерні системи

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____

“____” _____ 2021 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Букрєєву Артему Валерійовичу
(прізвище, ім’я, по батькові)

1. Тема роботи Дослідження методів підвищення ефективності біометричної системи ідентифікації за венозним рисунком

Керівник роботи Стрельцов Олег Васильович, кандидат техн. наук, доцент,
(прізвище, ім’я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ректора ДУОП від “ 01 ” жовтня 2021 року № 346-в
2. Зміст роботи

3. Перелік ілюстративного матеріалу

4. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

5. Дата видачі завдання xx.xx.21

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Затвердження теми кваліфікаційної роботи		
2			
3			
4			
5			
6			
7			
8			
9			
10			
11			

Здобувач вищої освіти _____ Букрєєв А. В.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Стрельцов О. В.
(підпис) (прізвище та ініціали)

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ ТА УМОВНИХ ПОЗНАЧЕНЬ

AFIS	Automated Fingerprint Identification System
BRIEF	Binary Robust Independent Elementary Features
CAGR	Compound Annual Growth Rate
EER	Equal Error Rate
FAR	False Accept Rate
FAST	Features from Accelerated Segment Test
FER	Failure to Enroll Rate
FMR	False Match Rate
FNMR	False Non-Match Rate
FRR	False Reject Rate
FTC	Failure to Capture Rate
FTE	Failure To Enroll
GAR	Genuine Accept Rate
IDE	Integrated Development Environment
ORB	Oriented FAST and Rotated BRIEF
RANSAC	RANdom SAmple Consensus
ROC	Receiver Operating Characteristic
SIFT	Scale-Invariant Feature Transform
SURF	Speeded Up Robust Features
TEE	Trusted Execution Environment
БД	База даних
ІЧ	ІнфраЧервоне [випромінювання]
ОІ	Область Інтересу
ПЗЗ	Прилад із Зарядним Зв'язком
ЦП	Центральний процесор

ВСТУП

На даний момент біометричні технології продовжують активно інтегруватися в різні сфери по всьому світу і безпосередньо в життя людини. Вони стали невід'ємним компонентом світового ринку інформаційних технологій і є зручним інструментом для вирішення широкого кола завдань.

Біометричні технології знайшли своє застосування і широко використовуються в банках, школах, бібліотеках, інститутах, фінансовому секторі, корпоративних та державних установах, а також в побутовій електроніці, такій як смартфони та планшети. Вони також допомагають великому бізнесу автоматизувати процеси управління і контролю доступом, опиняючись незамінними помічниками на додачу до традиційних методів захисту.

Актуальність роботи

Основною перевагою біометричних технологій є можливість швидкої й простої ідентифікації або верифікації особи без спричинення якихось незручностей користувачу. За прогнозами, ринок біометрії до 2026 року досягне майже 40,5 млрд доларів США.

Окремої уваги заслуговує відносно новий вид біометричної ідентифікації – за венозним малюнком руки. Дана технологія грунтується на оптичній візуалізації вен людини за допомогою інфрачервоного випромінювання і подальшому їх розпізнаванні.

На думку фахівців, біометрія малюнка вен людини дуже перспективна. Точність подібного методу ідентифікації надто висока, оскільки форма малюнка вен у людини не змінюється впродовж усього життя. Ще одна перевага в технології – її безконтактність. Тобто, з одного боку, ця система ідентифікації найбільш захищена від можливості підробки, з іншого ж, такий метод ідентифікації гігієнічніший за найпоширеніший нині – за відбитками пальців.

Більша частина досліджень в області біометрії спрямована на збільшення точності й ефективності таких систем.

Мета і задачі дослідження

Метою даної роботи є підвищення ефективності системи біометричної ідентифікації особистості шляхом розробки прототипу власної системи біометричної ідентифікації за венозним рисунком, інтегрованої у смартфон.

Завданнями даного дослідження є:

- аналіз предметної області: розглянути існуючі методи біометричної ідентифікації особистості, їх переваги та недоліки, проаналізувати глобальний ринок біометрії, а також основні принципи і поняття біометрії;
- дослідження вимог, методів і алгоритмів вирішення поставленого завдання;
- розробка програмного забезпечення для проведення експериментального дослідження застосування системи ідентифікації за венозним рисунком;
- проведення експерименту;
- висновки і аналіз отриманих результатів.

Об’єктом дослідження в даній роботі є процес ідентифікації особистості за венозним рисунком.

Предметом дослідження є метод ідентифікації за венозним рисунком за рахунок інноваційного рішення інтеграції до смартфону додаткових програмно-апаратних модулів.

Методи дослідження

У якості методів дослідження був застосований теоретичний підхід до аналізу біометричних методів та систем аутентифікації, статистичні методи та методи комп’ютерного моделювання, а також емпіричний підхід до тестування спроектованої системи.

Інноваційність роботи

На сьогоднішній день не існує на ринку добре відомих комерційних систем, заснованих на біометричному розпізнаванні рисунка вен та інтегрованих в мобільні пристрої. Дана робота – спроба створити подібну систему, яка б вирішувала проблеми і недоліки існуючих методів біометричної ідентифікації, була б швидкою, зручною і була реалізована в найпростішому вигляді.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Біометричні технології і тенденції їх розвитку у світі

Біометрія (Biometrics) — наука, що вивчає способи вимірювання різних параметрів людини з метою встановлення подібності або відмінностей між людьми і виділення однієї конкретної людини з множини інших людей [1]; сукупність автоматизованих методів і засобів ідентифікації людини, заснованих на її фізіологічній або поведінковій характеристиці [2].

В області інформаційних технологій біометричні дані використовуються в якості форми управління ідентифікаторами доступу та контролю доступу.

Біометричні технології засновані на ідентифікації людини за унікальними, властивим тільки їй біологічними ознаками. Залежно від того, чи є ідентифікатор незмінним (протягом тривалого часу) або постійно змінюваним, виділяють два типи систем біометричний даних [2, 3]:

- статичні – грунтуються на фізіологічній (статичній) характеристиці людини, тобто це унікальні ознаки, одержані людиною від моменту народження (наприклад, ДНК, відбитки пальців, геометрія руки, райдужна оболонка ока та інші);
- динамічні – базуються на поведінковій (динамічній) характеристиці людини, тобто побудовані на особливостях, характерних для підсвідомих рухів в процесі відтворення якої-небудь дії. Вони можуть бути придбані з часом, змінюватися з віком або під зовнішнім впливом (динаміка відтворення підпису, хода, набор тексту, голос і інші).

У таблиці 1.1 наведено перелік основних біометричних технологій і методів ідентифікації, а також їх переваги та недоліки [4].

Таблиця 1.1 – Порівняльна характеристика методів біометричної ідентифікації

Метод ідентифікації	**Принцип дії**	**Переваги**	**Недоліки**
Відбитки пальців	Найпоширеніший метод, в основі якого лежить унікальність для кожної людини малюнка папілярних візерунків на пальцях. Зображення відбитка пальця, отримане за допомогою спеціального сканера, перетвориться в цифровий код (згортку) і порівнюється з раніше введеним шаблоном (еталоном) або набором шаблонів (у випадку ідентифікації) [5]	Простота та висока швидкість аутентифікації, низька вартість	Негігієнічність, забруднення поверхні рук, сезонні зміни візерунка, різного роду ушкодження шкірного покрову, низька стійкість до фальсифікації
Геометрія долоні, кисті руки або пальця	За допомогою спеціального пристрою, що дозволяє отримувати тривимірний образ руки, здійснюють вимірювання певних параметрів, наприклад: довжина, товщина і вигини пальців, загальна структура кисті, відстань між суглобами, ширина і товщина долоні	Відсутність дискомфорту у користувача, відсутність впливу температури, забрудненості, вологості	Досить мала надійність

Продовження таблиці 1.1

Рисунок вен на долоні або пальці руки	За допомогою інфрачервоної камери зчитується рисунок вен на тильній стороні долоні або кисті руки, отримана картинка обробляється, і за схемою розташування вен формується цифрова згортка.	Відсутність контакту з приладом, висока точність, фальсифікація неможлива, середня чутливість до впливу зовнішніх факторів	Дорожнеча, вплив деяких джерел освітлення (наприклад, галогенних) може заважати роботі приладу
Сітківка ока	Ідентифікація за малюнком кровоносних судин очного дна	Високий рівень статистичної надійності, фальсифікація неможлива	Висока чутливість до впливу зовнішніх факторів, низька швидкість аутентифікації, висока вартість, низький комфорт користувача
Райдужна оболонка ока	Метод заснований на унікальності малюнка райдужної оболонки ока. Для реалізації методу необхідні спеціальна камера і відповідне програмне забезпечення, що дозволяє	Фальсифікація безуспішна, висока швидкість аутентифікації [6]	Процедура аутентифікації є неприємною і психологічно важкою для людини, висока вартість,

Продовження таблиці 1.1

	виділити з отриманого зображення малюнок райдужної оболонки ока, за яким будується цифровий код		виникнення труднощів у людей, що носять окуляри або контактні лінзи
Форма і геометрія обличчя	Будується дво- або тривимірний образ обличчя людини. За допомогою камери і спеціалізованого програмного забезпечення на зображенні виділяються контури очей, брів, носа, губ і т. д., обчислюються відстані між ними. За цими даними будується образ, що перетворюється в цифрову форму для порівняння	Можливість розпізнавання обличчя на великій відстані, висока швидкість обробки даних, головні убори, зміна зачіски, рослинність на обличчі не впливають на достовірність результату	Не володіє високою унікальністю і внаслідок цього збільшується ймовірність виникнення помилок 1-го і 2-го роду («помилкова відмова» і «помилковий доступ» відповідно), вплив освітлення (надто сонячно або похмуро) і зміни міміки обличчя

Продовження таблиці 1.1

Термографія обличчя, руки	В основі цього методу лежить унікальність розподілу на обличчі артерій, які постачають кров'ю шкіру і виділяють тепло. Обличчя сканується за допомогою інфрачервоного світла і формується термограмма – температурна карта лиця, що є досить унікальною	Сканування можна здійснювати з великої відстані, метод ефективний не зважаючи на температуру тіла і старіння організму	Низька якість одержуваних термограмм, засновані на використанні цих ідентифікаторів технології не набули поширення
Рукописний текст	Використовується підпис людини (іноді написання кодового слова). Цифровий код формується за динамічними характеристиками написання, тобто будується згортка, в яку входить інформація щодо графічних параметрів, часових характеристик нанесення підпису та динаміки натиску на поверхню тощо	Невелика вартість пристрою, використовується у всіх сферах життєдіяльності	Можлива підробка, залежність від емоційного стану людини, збільшується ймовірність «помилкової відмови» системи
Клавіатурний почерк	Основна характеристика, за якою будується згортка — динаміка набору кодового слова (швидкість вводу, час утримання клавіш, інтервали	Зручність користування, можливість здійснення процедури	Залежність від вікових чинників та стану здоров'я користувача,

Продовження таблиці 1.1

	між натисканнями на них та ін.)	аутентифікації без спеціального обладнання, а також можливість прихованої аутентифікації.	проблема адаптації до нового пристрою вводу
Голос	Як правило, код ідентифікації за голосом будується на різних поєднаннях частотних і статистичних характеристик голосу	Фінансова доступність, простота використання і практичність	Залежність від емоційного стану людини, наявність фонових шумів
Рух губ	Розпізнавання характерних рухів губ з урахуванням текстури та міміки, наприклад, під час вимови пароля конкретною людиною	Безконтактне сканування; Швидкий час розпізнавання; Підвищує точність розпізнавання в поєднанні з іншими формами біометрії	Необхідність тривалого сканування різних емоцій для створення точного образу
Хода	Для ідентифікації застосовуються алгоритми обробки відеоряду з кадрами людини, що рухається:	Можливість ідентифікації людини на великій відстані і	Метод не набув поширення

Продовження таблиці 1.1

	аналізуючи ці матеріали, біометрична система формує цифрові шаблони ходи конкретної людини, і потім порівнює їх з шаблонами, отриманими в новому сеансі ідентифікації. Вона фіксує пересування людей, формує тривимірну модель їх повного зображення, і на цій основі здійснює ідентифікацію.	без безпосереднього контакту	

Процес ідентифікації з використанням будь-якого з наведених типів біометричних даних, як правило, складається з етапів, наведених на Рисунку 1.1.

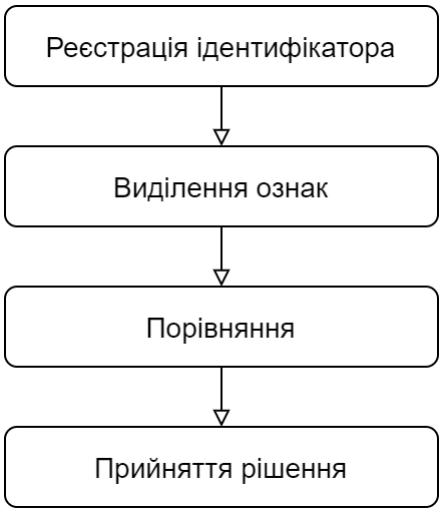


Рисунок 1.1 – Основні етапи роботи біометричних технологій

- **реєстрація ідентифікатора** – відомості про фізіологічну або поведінкову характеристику перетворюються в форму, доступну комп'ютерним технологіям, і вносяться в пам'ять біометричної системи;
- **виділення ознак** – з пред'явленого зразка виділяються унікальні ознаки, що аналізуються системою, потім вони обробляються і перетворюються в математичний код;
- **порівняння** – зіставляються відомості про пред'явлений і раніше зареєстрований зразок;
- **прийняття рішення** – робиться висновок про те, чи співпадають або не співпадають пред'явлений і раніше зареєстрований зразок.

Висновок про збіг / розбіжність ідентифікаторів може потім транслюватися іншим системам (контролю доступу, захисту інформації і т.д.), які далі діють на основі отриманої інформації.

Згідно з оцінками Expert Market Research [7], обсяг світового ринку біометричних систем досяг в 2020 році майже 17,5 млрд доларів США. Очікується, що ринок біометрії буде рости із середньорічним темпом зростання (CAGR) 15% в період з 2021 по 2026 рік і до 2026 року досягне майже 40,5 млрд доларів США (Рис. 1.2).

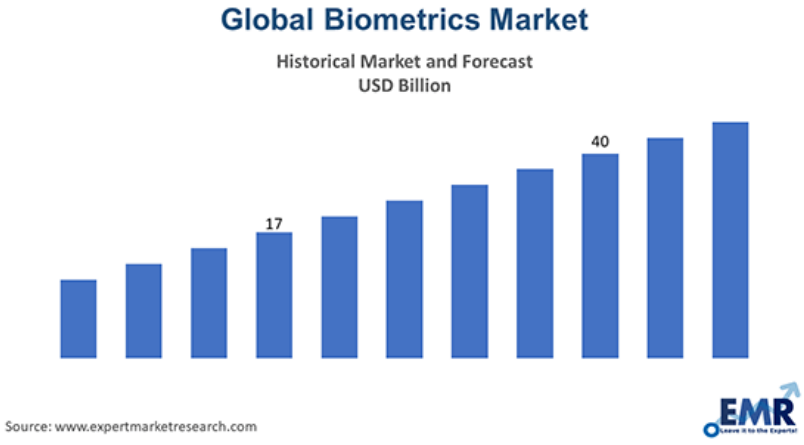


Рисунок 1.2 – Обсяг світового ринку біометричних систем 2016-2026 рр.,

млрд дол. США

На сучасному світовому ринку біометричних систем активно застосовуються технології, засновані на розпізнаванні і використанні наступних біометричних даних (Рис. 1.3) [7]:

- Розпізнавання обличчя
- Геометрія руки
- Розпізнавання голосу
- Розпізнавання підпису
- Розпізнавання райдужної оболонки ока
- Відбиток пальця (AFIS, Non-AFIS)
- Інші

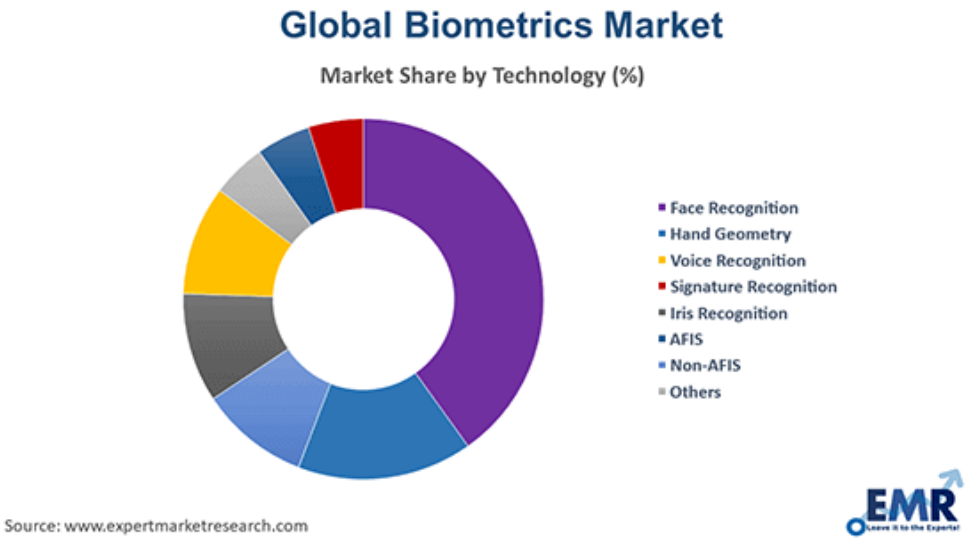


Рисунок 1.3 – Структура ринку біометричних систем у розрізі технологій

1.2 Рейтинг країн за використанням біометрії

Фахівці компанії Comparitech вивчили 96 країн на предмет використання та захисту персональних даних [8]. Зокрема, їх цікавило питання, де збираються біометричні дані, для чого і як вони зберігаються. На підставі цього кожній країні присуджувалася відповідна кількість балів (максимум 31). Чим нище бал – тим ширший і агресивніший ведеться збір біометричних даних в цій країні. Високі ж

бали навпаки свідчать про великі обмеження і контроль у сфері збору біометрії і урядового нагляду.

Найменшу кількість балів (2/31) набрав Китай, далі йде Коста-Ріка (3/31), потім Іран (5/31), США, Саудівська Аравія, Об'єднані Арабські Емірати, Бангладеш, Філіппіни і Уганда (6/31) і замикають п'ятірку Ірак та Малайзія (7/31).

Топ-5 країн-«відмінниць», де збір біометричних даних ведеться не так жорстко і краще контролюється, виглядає наступним чином: Туркменістан (25/31), Ефіопія (22/31), Азербайджан і Бахрейн (20/31), Португалія та Ірландія (19/31) Гватемала, Люксембург, Парагвай, Польща, Румунія, Туніс і Великобританія (17/31). Що стосується України, то їй присудили 14 балів з 31 можливих.

Слід зазначити вплив триваючої пандемії COVID-19 на рейтинг, оскільки збір деяких біометричних даних був введений як захід надзвичайного контролю. Однак не можна сказати, що рейтинг зазнав великих змін, оскільки країни, в яких встановлено найгірше використання біометричних даних, як правило, впровадили (чи планують впровадити) найбільш суворі біометричні заходи контролю за пандемією.

У кожній вивченої дослідниками країні біометрія використовується в банкінгу (наприклад, відбитки пальців для авторизації в банківських додатках або ідентифікації клієнтів в самих банках). У багатьох країнах також ведеться збір біометричних даних іноземців (через візи і перевірки в аеропортах). Хоча біометричні дані визнані надзвичайно чутливою інформацією, у багатьох країнах допускається їх повсюдне використання. Більш того, в більшості країн використовуються або тестуються камери відеоспостереження з функцією розпізнавання облич.

Як показало дослідження, в цілому по Європі справи із захистом біометричних даних йдуть краще, ніж за її межами. За словами фахівців, це пов'язано з дією в Євросоюзі «Загального регламенту щодо захисту даних» (GDPR).

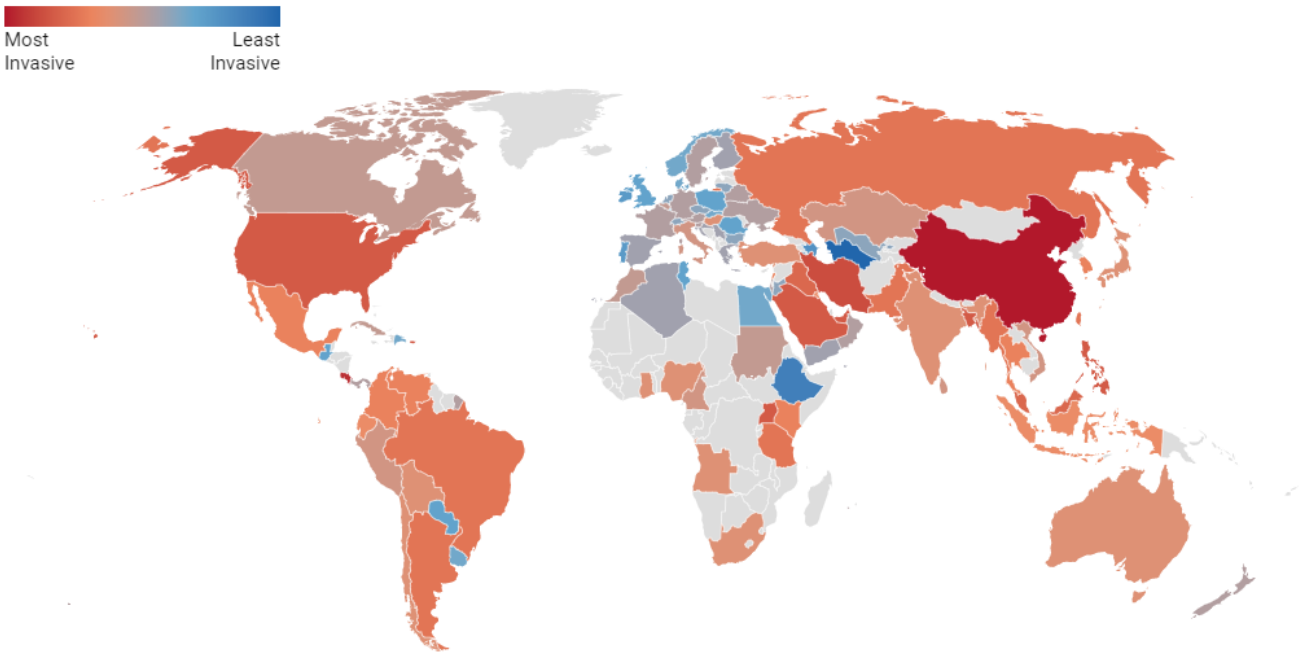


Рисунок 1.4 – Збір та зберігання біометрії за країнами станом на 2021 рік (червоним кольором – більш агресивна політика за збором біометричних даних, синім – менш агресивна)

1.3 Оцінка ефективності біометричної ідентифікації

Для визначення ефективності та продуктивності біометричних систем використовують наступні показники [2, 6]:

FAR – коефіцієнт помилкового пропуску;

FMR – ймовірність, що система невірно порівнює вхідний зразок з невідповідним шаблоном в базі даних;

FRR – коефіцієнт помилкової відмови;

FNMR – ймовірність того, що система помилиться у визначенні збігів між вхідним зразком і відповідним шаблоном з бази даних;

Графік ROC – візуалізація компромісу між характеристиками FAR і FRR;

Коефіцієнт відмови в реєстрації (**FTE** або **FER**) – коефіцієнт безуспішних спроб створити шаблон з вхідних даних (при низькій якості останніх);

Коефіцієнт помилкового утримання (FTC) – ймовірність того, що автоматизована система не здатна визначити біометричні вхідні дані, коли вони представлені коректно;

Ємність шаблону – максимальна кількість наборів даних, які можуть зберігатися в системі.

При цьому головними для оцінки будь-якої біометричної системи є саме параметри **FAR** (відсоток виникнення ситуацій, коли система дозволяє доступ користувачу, незареєстрованому в системі, тобто помилка другого роду) і **FRR** (відмова в доступі справжньому користувачеві системи, тобто помилка першого роду). Їх обчислення проводиться за формулами 1.1 та 1.2 [9]:

$$FRR = \frac{\text{загальне число помилкових відмов у доступі}}{\text{загальне число тестованих об′єктів}} \quad (1.1)$$

$$FAR = \frac{\text{загальне число помилкових доступів}}{\text{загальне число тестованих об′єктів}} \quad (1.2)$$

Обидві характеристики отримують розрахунковим шляхом на основі методів математичної статистики. Чим нижче ці показники, тим точніше розпізнавання об'єкта.

Показник істинного прийняття **GAR** – це ймовірність істинного прийняття користувача, що має право доступу:

$$GAR = 1 - FRR \quad (1.3)$$

Ідеальна система біометричної аутентифікації мала б FAR = 0 і FRR = 0, Проте, такі значення в реальності недосяжні. Значення будь-якої з двох помилок можливо зменшити. Недолік цього у тому, що друге значення зросте. Зазвичай системні параметри налаштовують так, щоб домогтися необхідного коефіцієнта помилкових підтверджень, що визначає відповідний коефіцієнт помилкових відмов [9].

У таблиці 1.2 наведено порівняльний аналіз основних методів біометричної ідентифікації за середніми значеннями FAR і FRR [6].

Таблиця 1.2 – Середні значення FAR і FRR для популярних методів біометричної ідентифікації

Метод ідентифікації	**FAR**	**FRR**
Відбиток пальця	0,001%	0,6%
Розпізнавання обличчя 2D	0,1%	2,5%
Розпізнавання обличчя 3D	0,0005%	0,1%
Райдужна оболонка ока	0,00001%	0,016%
Сітківка ока	0,0001%	0,4%
Рисунок вен	0,0008%	0,01%

Якщо систему необхідно охарактеризувати одним критерієм, то використовується коефіцієнт еквівалентної ймовірності помилок 1-го і 2-го роду **EER**, який графічно є точкою збігу ймовірностей FRR і FAR. Якісна і надійна система також повинна мати низький рівень EER [9].

На Рис. 1.5 показані графіки помилок першого і другого роду, а також коефіцієнт EER для методу ідентифікації за рукописним підписом [10].

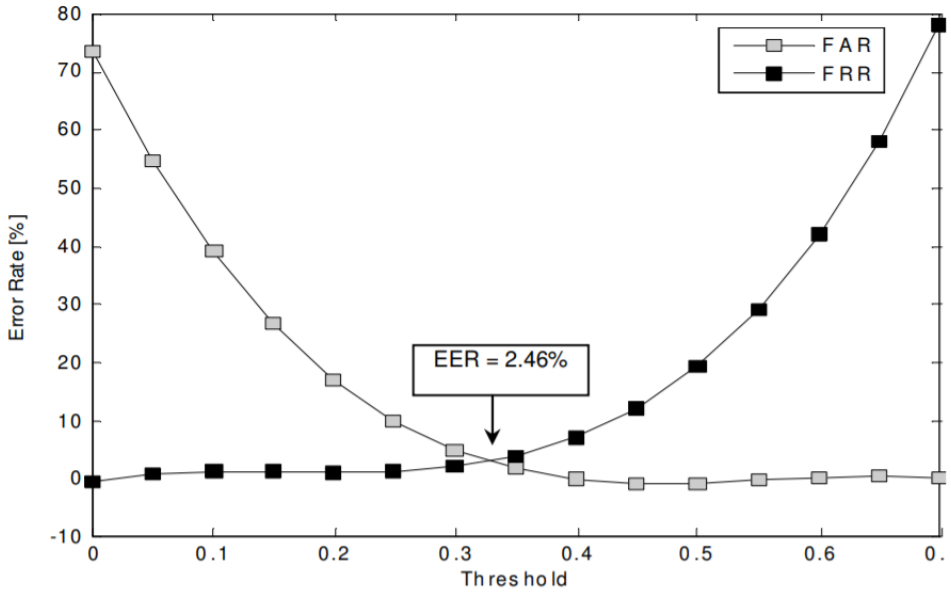


Рисунок 1.5 – Графіки FAR і FRR для методу біометричної ідентифікації за рукописним підписом

Для побудови ефективної системи контролю доступу недостатньо відмінних показників FAR і FRR. Важливим є також час ідентифікації, вплив людського фактора, вартість системи.

Таким чином, для якісного аналізу біометричної системи необхідно використовувати і інші дані, наприклад, отримані дослідним шляхом. До них відносяться: можливість підробки біометричних даних для ідентифікації в системі і способи підвищення рівня безпеки, стабільність біометричних факторів (незмінність з часом і незалежність від умов навколишнього середовища), швидкість аутентифікації, можливість швидкого безконтактного зняття біометричних даних, вартість реалізації на основі розглянутого методу аутентифікації і доступність складових [6].

1.4 Технологія біометричної аутентифікації за венозним рисунком

Технологія біометричної аутентифікації за венозним рисунком ґрунтується на оптичній візуалізації вен людини і їх подальшому розпізнаванні. На відміну від таких біометричних ознак, як відбиток пальця, геометрія руки або обличчя, вени знаходяться всередині тканин людського тіла і підробити їх дуже складно.

Ідея даної технології базується на припущенні про унікальність венозного малюнка кожної людини. Вважається, що не існує двох людей з однаковим малюнком вен [11]. При цьому венозний малюнок формується у дитини ще в утробі матері і не змінюється протягом усього життя.

Малюнок вен формується завдяки тому факту, що гемоглобін крові поглинає інфрачервоне випромінювання. Гемоглобін — складний залізовмісний білок еритроцитів тварин і людини, здатний оборотно зв'язуватися з киснем, забезпечуючи його перенесення до тканин [12]. Кров транспортує кисень за допомогою гемоглобіну, що міститься в ній; гемоглобін насичується киснем, коли кисень приєднується до нього в легенях, і стає бідним на кисень (дезоксигенованим), коли кисень втрачається в периферійних судинах організму. Тобто артерії містять кисневий гемоглобін, а вени містять дезоксигенований гемоглобін. Два типи гемоглобіну мають різні спектри поглинання [13].

На Рис. 1.6 зображено графік поглинання ІЧ-випромінювання насиченої киснем крові і крові без кисню.

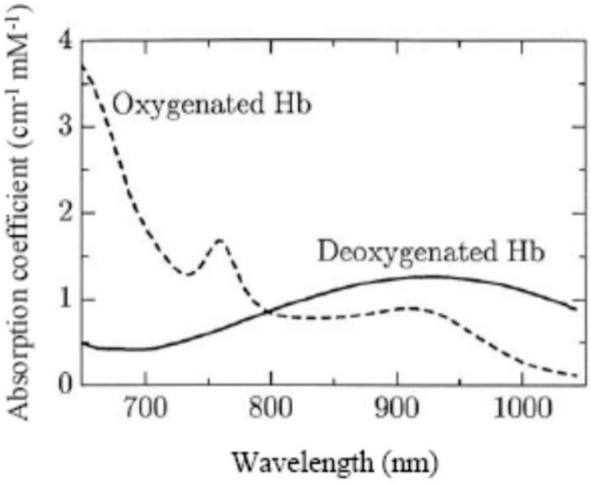


Рисунок 1.6 – Спектри поглинання гемоглобіну

Зокрема, дезоксигенований гемоглобін поглинає світло, що має довжину хвилі близько 760 нм у межах ближньої інфрачервоної області (Рис. 1). При скануванні за допомогою ближнього інфрачервоного випромінювання судини будуть виглядати темнішими за інші частини (у вигляді чорних ліній), оскільки тільки судини поглинають промені (Рис. 1.7) [13].

Рисунок 1.7 – Зображення долоні в інфрачервоному діапазоні

На практиці фактично співіснують дві конкуруючі технології: ідентифікація за малюнком вен на долоні та ідентифікація за малюнком вен пальця.

Принцип роботи

Існує два методи отримання зображення малюнка вен:

1**. Метод пропускання** ІЧ-світла (transmission method) полягає в установці ІЧ-підсвічування на одній стороні пальця (або долоні), а сама камера з фільтром встановлюється на іншій стороні пальця і приймає ІЧ-випромінювання, що проходить крізь весь палець (Рис. 1.8, а). Оскільки вени поглинають світло ближнього ІЧ діапазону, через них буде проходити менше світла, і вони будуть виглядати як темний візерунок. За допомогою методу пропускання одержувані зображення більш деталізовані [14].

2. У **методі відображення** (reflection method) джерело освітлення та датчик розташовані на одній стороні, за рахунок чого зменшується розмір пристрою. Світло проникає в палець і розсіюється в тканинах. Частина цього розсіяного світла відбивається назад до поверхні пальця, а потім фіксується датчиком (Рис. 1.8, б). Зображення створюється за рахунок відмінності в інтенсивності відбитого світла. Вени поглинають світло ближнього ІЧ діапазону, від них відбивається менше світла, і вони також будуть виглядати як темний візерунок, тоді як для решти пальця зображення буде яскравішим. Даний метод знижує психологічний бар'єр (не потрібно нікуди засовувати руку або палець) [14].

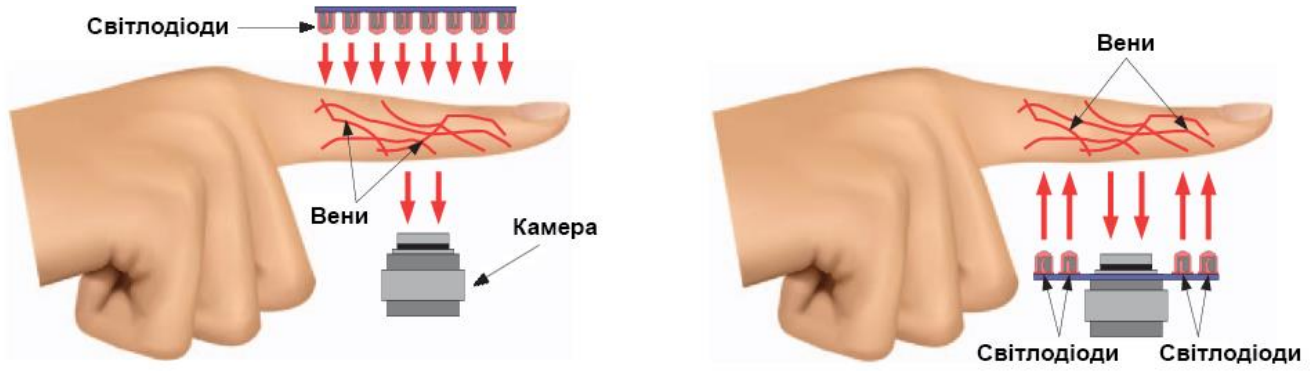


Рисунок 1.8 – Розпізнавання вен пальців: а) за допомогою пропускаючого світла; б) за допомогою відбиваючого світла.

Потім спеціальна програма на основі отриманих даних створює цифрову згортку зображення малюнка вен, яке в подальшому порівнюється з еталонним шаблоном з бази даних (Рис. 1.9).

Рисунок 1.9 – Процес отримання цифрової моделі зображення малюнка вен

Беззаперечною перевагою даної технології є те, що під час проведення ідентифікації не має необхідності у фізичному контакті людини зі скануючим пристроєм. Через що цей метод найбільш прийнятний у медичній та фармацевтичній сферах, де питання гігієни має найважливіше значення. Варто також відзначити, що цей метод абсолютно нешкідливий для шкіри та кровоносних судин. Даний вид ідентифікації є досить безпечним методом і може застосовуватися в системах санкціонованого доступу особливої важливості.

1.5 Аналіз ринку та огляд існуючих систем

В ході дослідження та перед розробкою власної системи, було проаналізовано ринок існуючих аналогів і сервісів, які вирішували б поставлене або подібне завдання.

Технологія Fujitsu PalmSecure

Компанія «Fujitsu» запровадила в дію власну систему аутентифікації, створену за принципом розпізнавання унікального малюнка кровоносних судин долоні, як спосіб боротьби проти фінансових махінацій в Японії [15].

Технологія під назвою Fujitsu PalmSecure дозволяє підтвердити особу користувача за допомогою ряду біометричних даних, включаючи перевірку унікального для кожної людини малюнка кровоносних судин.

PalmSecure використовує випромінювання ближнього інфрачервоного діапазону для сканування малюнка вен долоні людини. Спеціальний алгоритм використовує отримане в результаті сканування зображення для створення унікального біометричного образу. Ця ідентифікаційна інформація підтверджується шляхом порівняння зразків з базою даних попередньо зареєстрованих користувачів. Аутентифікація виконується менш ніж за одну секунду, що набагато швидше і простіше в порівнянні з введенням паролів.

Варто врахувати, що сканер може розпізнати малюнок тільки тоді, коли по

венах біжить кров, що практично виключає вірогідність фальсифікації.

Будучи безконтактною, технологія знаходить широку підтримку серед користувачів, оскільки запобігає поширенню бактерій. На роботу технології PalmSecure не чинять вплив зовнішні фактори, зокрема тип шкіри, температура долоні і порізи або подряпини на шкірі [16].

Технологія компанії Fujitsu має впровадження у різних сегментах бізнесу. Так, «Bank of Tokyo Mitsubishi UFJ» і «Suruga Bank» в Японії, а також бразильський «Banco Bradesco» застосували її для організації доступу до банківських касових терміналів і банкоматів, а також для обслуговування VIP-клієнтів. У японському «National Institute of Radiological Sciences» нову технологію використовують під час роботи з репозиторієм клінічних даних, для дотримання необхідних доз опромінювання електронами і важкими іонами хворих, для управління доступом до системи радіологічної інформації. У «Todholm Primary School» (Шотландія) рішення на базі «PalmSecure» використовуються для безготівкового розрахунку за сніданки у шкільному буфеті [17].

Ще одним прикладом впровадження технології є біометричний термінал **PalmSecure ID Access** (Рис. 1.10), який компанія представила в 2016 році. За його допомогою великі корпорації і компанії малого та середнього бізнесу можуть модернізувати свої системи контролю доступу.

Рисунок 1.10 – Біометричний термінал PalmSecure ID Access

Пристрій являє собою компактний термінал з датчиком PalmSecure і сенсорним екраном, призначений для аутентифікації особистості за допомогою технології безконтактного сканування малюнка вен долоні.

Технологія біометричної аутентифікації забезпечує високий рівень точності в порівнянні з системами безпеки на базі пін-кодів, паролів, ключів або карт доступу. Вона відрізняється винятковою зручністю використання і гігієнічністю.

PalmSecure ID Access можна легко інтегрувати в існуючі системи контролю доступу [16].

Система «Finger Vein»

Із 2007 року компанія «Hitachi» почала продаж системи, яка отримала назву «Finger Vein». Принцип дії сканера-зчитувача на основі технології «Finger Vein» заснований на формуванні зображення венозного малюнку пальця за допомогою камери з ПЗЗ-матрицею і джерела інфрачервоного випромінювання ближнього діапазону. Такий спосіб ідентифікації гарантує стовідсоткову точність, а експерти з безпеки називають його повністю захищеним від шахрайства [18].

Як об’єкти, що підлягають захисту, фахівці «Hitachi» називають автомобілі та персональні комп’ютери. Цей засіб ідентифікації вбудовується у різні системи контролю фізичного доступу, зокрема до банкоматів, і використовується для персональної ідентифікації [17].

Рисунок 1.11 – Сканер-зчитувач Finger Vein інтегрований в банкомат

Наприклад, японські інженери спільно з компанією Itcard S.A, яка надає сервісне обслуговування банків в Польщі, приступили до реалізації проекту Planet Cash, в рамках якого 1730 польських банкоматів було оснащено сканером-зчитувачем Finger Vein (Рис. 1.11) [18].

Таким чином, власнику банківської карти досить буде прикласти палець до пристрою замість того, щоб вставляти карту і вводити пін-код. Подібними сканерами вже оснащені деякі банкомати в Туреччині та Японії.

Смартфон LG G8 ThinQ та функція «Hand ID»

У 2019 році компанія LG представила перший у світі смартфон LG G8 ThinQ з підтримкою розпізнавання вен, офіційно відомої як «Hand ID» [19]. Принцип дії заснований на тому, що користувач підносить руку до верхньої частини екрану, і смартфон за допомогою камери та інфрачервоного датчика сканує та ідентифікує його за унікальним малюнком руки з урахуванням розташування сітки кровоносних судин (Рис. 1.12). На аутентифікацію йде менше секунди.

Рисунок 1.12 – Технологія розпізнавання вен «Hand ID»
у смартфоні LG G8 ThinQ

Основний недолік даної технології розблокування полягає в тому, що користувачеві необхідно здійснювати деякі неприродні рухи і маніпуляції, а саме наводити долоню на селфі-камеру і повільно підняти її. Крім того, даний спосіб

трохи незручний у використанні, наприклад, розблокувати смартфон можна тільки другою рукою, тримаючи телефон в першій, або однією рукою, але тільки якщо він лежить на столі.

Face ID з можливістю зчитування малюнка вен на обличчі

У 2020 році Apple запатентувала [20] оновлення інфрачервоного датчика Face ID. Цей крок полягає в тому, щоб усунути всі недоліки системи і можливі помилки з ідентифікацією, які пов'язані з зовнішньою схожістю людей. Домогтися цього компанія планує, навчивши свою систему Face ID зчитувати малюнок вен на обличчі людини.

Біометричні системи, такі як Face ID або Touch ID, є відмінним інструментом для швидкого доступу до смартфону. Однак їхня головна проблема в тому, що такі системи не завжди правильно можуть ідентифікувати людину через схожість обличчя. Такі випадки вже мали місце, тому Apple і планує вдосконалити механізм ідентифікації.

Новий метод полягає в використанні інфрачервоного датчика для сканування вен на обличчі власника iPhone. Датчик Face ID зможе створити об'ємну карту лиця з розташуванням і розмірами судин верхніх шарів шкіри (Рис. 1.13). Справа в тому, що венозний малюнок на обличчі не співпадає ні в однієї людини. Це дозволить розрізняти обличчя навіть у однояйцевих близнюків – незважаючи на ідентичну зовнішність у них різний венозний малюнок [21].

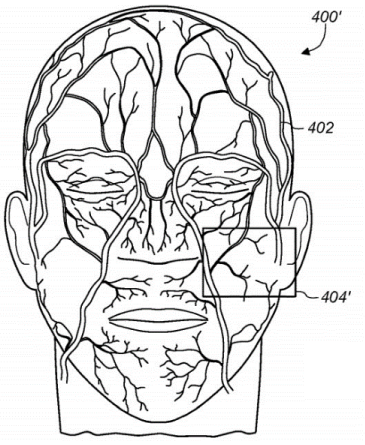


Рисунок 1.13 – Приклад структури вен під шкірою обличчя людини

1.6 Висновки

В даному розділі були описані такі поняття, як біометрія, ідентифікація та аутентифікація, а також загальні принципи роботи біометричної системи, основні її характеристики та оцінка її ефективності. Проаналізовано глобальний ринок біометрії і тенденції її розвитку в світі. Також розглянуто найбільш популярні методи біометричної аутентифікації – статичні та динамічні.

Метод біометричної ідентифікації за венозним рисунком руки – відносно новий і в той же час перспективний вид біометрії. Дана технологія поєднує в собі як високу точність ідентифікації, так і безконтактність. Безпека, комфорт і, звичайно ж, гігієна – три головні причини, що стоять за постійним і вражаючим зростанням використання безконтактних біометричних систем.

Смартфони відіграють важливе значення в повсякденному житті людини і являють собою системи з великою кількістю біометричних датчиків, одночасно вбудованих в одному пристрої. Аналіз показав, що на сьогоднішній день не існує на ринку добре відомих комерційних систем, заснованих на біометричному розпізнаванні рисунка вен і інтегрованих в смартфони.

З огляду на все вищесказане, можна зробити висновок про актуальність розробки системи біометричної ідентифікації за венозним рисунком для мобільних пристроїв.

РОЗДІЛ 2
КОМП'ЮТЕРНИЙ ЗІР ТА МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ БІОМЕТРИЧНОЇ СИСТЕМИ ІДЕНТИФІКАЦІЇ ЗА ВЕНОЗНИМ РИСУНКОМ

2.1 Комп'ютерний зір

Комп'ютерний зір (Computer vision) — теорія та технологія створення машин, які можуть проводити виявлення, стеження та визначення об'єктів. Як наукова дисципліна, комп'ютерний зір належить до теорії та технології створення штучних систем, які отримують інформацію у вигляді зображень. Причому зображення може бути як окремою фотографією, так і послідовністю кадрів відео, отриманої з відеофайлу або відеокамери (наприклад, з камери зовнішнього спостереження, з веб-камери або зі стереокамери) в режимі реального часу [22, 23].

Щоб комп'ютер знаходив на зображеннях певні об'єкти, його потрібно навчити. Для цього складається величезна навчальна вибірка, наприклад, з фотографій, частина з яких містять об'єкт, що шукається, а інша частина — навпаки, не містить. Далі у справу вступає машинне навчання. Комп'ютер аналізує зображення з вибірки, визначає, які ознаки та його комбінації свідчить про наявність шуканих об'єктів, і прораховує їх значимість [25].

Після закінчення навчання комп'ютерний зір можна використовувати у справі. Для комп'ютера зображення — це набір пікселів, кожен з яких має значення яскравості або кольору. Наприклад, на Рис. 2.1 зображено фотографію автомобіля. Комп'ютер «бачить» лише матрицю чисел. До будь-якого числа доданий досить сильний шум, тому саме собою воно дає мало інформації, проте ця матриця – це все, що «бачить» комп'ютер. Завдання комп'ютерного зору – перетворити цю зашумлену числову матрицю на образ конкретного об'єкта, в даному випадку – «бічного дзеркала» [24].

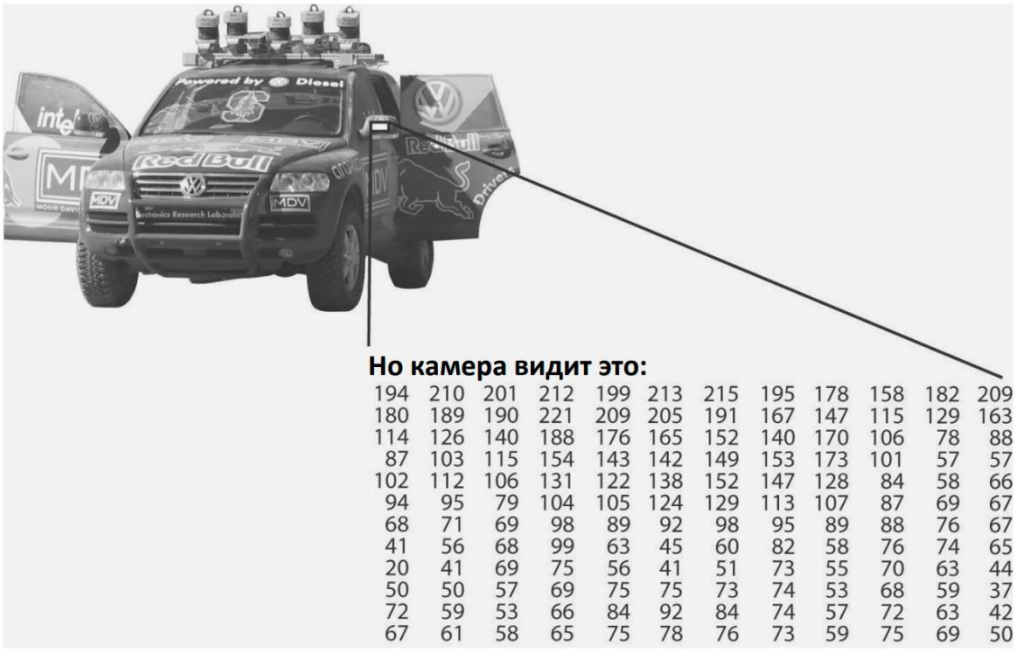


Рисунок 2.1 – Для комп'ютера зображення бічного дзеркала автомобіля є просто матрицею чисел

На Рис. 2.2 перелічені типові завдання комп'ютерного зору.

Рисунок 2.2 – Типові завдання комп'ютерного зору

Щоб комп'ютер зміг одержати уявлення про вміст картинки, її обробляють за допомогою спеціальних алгоритмів. Спочатку виявляють потенційно значимі місця. Це можна робити кількома способами. Наприклад, вихідне зображення

кілька разів піддають розмиттям за Гауссом, використовуючи різний радіус розмиття. Потім результати порівнюють один з одним. Це дозволяє виявити найбільш контрастні фрагменти - яскраві плями та злами ліній.

Після того, як значущі місця знайдені, комп'ютер описує їх у числах. Запис фрагмента картинки у числовому вигляді називається дескриптором (Рис. 2.3). За допомогою дескрипторів можна точно порівнювати фрагменти зображення без використання самих фрагментів. Для прискорення обчислень комп'ютер проводить кластеризацію або розподіл дескрипторів по групах. У той самий кластер потрапляють схожі дескриптори з різних зображень. Після кластеризації важливим стає лише номер кластера з дескрипторами, найбільш схожими на цей. Перехід від дескриптора до номера кластера називається квантуванням, а номер кластера — квантованим дескриптором. Квантування значно скорочує обсяг даних, які потрібно обробити комп'ютеру [25].

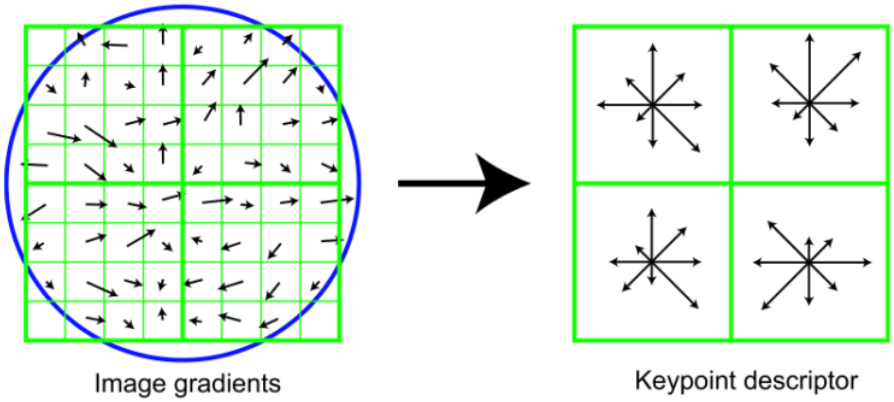


Рисунок 2.3 – Дескриптор ключових точок

Спираючись на квантовані дескриптори, комп'ютер може порівнювати зображення та розпізнавати на них об'єкти. Він зіставляє набори квантованих дескрипторів з різних зображень і робить висновок про те, наскільки вони чи їх окремі фрагменти схожі. Таке порівняння у тому числі використовується пошуковими системами для пошуку за завантаженою картинкою [25].

У таблиці 2.1 наведено функції комп'ютерного зору [22].

Таблиця 2.1 – Функції комп'ютерного зору та їх опис

Функція	**Опис**
Отримання зображень	Цифрові зображення отримуються від одного чи декількох датчиків зображення. Залежно від типу датчика, отримані дані можуть бути звичайним 2D зображенням, 3D зображенням чи послідовністю зображень. Значення пікселів зазвичай відповідають інтенсивності світла в одній чи декількох спектральних смугах (кольорові чи зображення у відтінках сірого), але можуть бути пов'язані з різноманітними фізичними вимірюваннями.
Попередня обробка	Перед тим, як методи комп'ютерного зору можуть бути застосовані до відеоданих з метою вилучення певної частини інформації, необхідно обробити відеодані, щоб вони задовольняли деяким вимогам залежно від метода, що використовується (наприклад: повторна вибірка, видалення шумів, покращення контрастності, масштабування).
Виокремлення деталей	Деталі зображення різного рівня складності виділяються з відеоданих. Типовими прикладами таких деталей є лінії та межі; локалізовані точки інтересу, такі як кути, краплі чи точки: складніші деталі можуть належати до структури, форми чи руху.
Детектування/ Сегментація	На певному етапі обробки приймається рішення про те, які точки чи ділянки зображення є важливими для подальшої обробки. Прикладами є: • виділення визначеного набору точок, що цікавлять; • сегментація одного або кількох ділянок зображення, які містять характерний об'єкт.

Продовження таблиці 2.1

Високорівнева обробка	На цьому кроці вхідні дані зазвичай представляють невеликий набір даних, наприклад, набір точок чи ділянка зображення, в якій за припущенням знаходиться певний об'єкт. Прикладами є: • перевірка того, що дані задовольняють умовам, що залежать від методу і застосування; • оцінка характерних параметрів (положення або розмір об'єкта); класифікація знайденого об'єкта за різними категоріями.

З комп'ютерним зором тісно пов'язана ще одна технологія – обробка зображень. Перед тим, як шукати об'єкти на зображенні, необхідно виконати попередню обробку. Зокрема, в більшості випадків йдеться про зміну розмірів зображення та вирівнювання гістограми. Крім того, потрібно згладити зображення, щоб позбавитися цифрового шуму, який виникає при використанні дешевих камер, а також при різних специфічних режимах зйомки (наприклад, при високих значеннях ISO або тривалих витримках). Багато алгоритмів дуже чутливі до шумів, і їх наявність може призвести, наприклад, до неправильно знайдених меж об'єкта або хибних особливих точок. [25].

2.2 Виявлення та вилучення ознак

Для того, щоб знайти на зображенні який-небудь об'єкт, потрібно попередньо виділити на ньому характерні ознаки. Такими ознаками є особливі точки – наприклад, кути, центри кіл і т.д. Після знаходження особливих точок потрібно обчислити дескриптори – вектори, що характеризують околиці особливих точок. Порівнюючи дескриптори двох точок, можна знайти відповідність особливої точки на одному зображенні з особливою точкою на іншому [23].

Рисунок 2.4 містить зображення будівлі та 6 невеликих фрагментів цього зображення зверху. Фрагменти A і B – однотипні плоскі поверхні, що розкидані на досить великій площі. Точне місцезнаходження цих ділянок визначити дуже складно.

Знайти приблизне розташування фрагментів C і D вже набагато простіше – це краї будівлі. Можна визначити вертикальну або горизонтальну орієнтацію фрагмента, проте усе ще залишаються варіанти відносно його розташування вздовж цих вертикальних чи горизонтальних площин. Таким чином, край (грань) – краща характеристика в порівнянні з плоскою областю, але все ще не ідеальна.

Нарешті, E та F – це деякі кути будівлі. Очевидно, що впізнати їх дуже легко. Тому що по кутах, куди б ми не перемістили цей фрагмент, він виглядатиме інакше. Тож їх можна вважати характерною особливістю.

Рисунок 2.4 – Зображення будівлі, а також деяких його фрагментів з різним ступенем розпізнавання їхнього розташування

Після того, як особливості на зображенні були знайдені, необхідно виконати цей процес щодо інших зображень. Комп'ютер повинен описати область навколо об'єкта, щоб знайти його на інших зображеннях. Це називається описом особливостей. Наявність особливостей та їх описів дозволяє знайти однакові ознаки на усіх зображеннях.

Особливі точки повинні відповідати вимогам, переліченим у таблиці 2.2 [27].

Таблиця 2.2 – Властивості особливих точок

Властивість	**Характеристика**
Відмінність (distinctness)	Особлива точка повинна явно виділятися на фоні і бути відмінною (унікальною) у своїй околиці.
Інваріантність (invariance)	Визначення особливої точки має бути незалежним до афінних перетворень.
Стабільність (stability)	Визначення особливої точки повинно бути стійким до шумів та помилок.
Унікальність (uniqueness)	Крім локальної відмінності, особлива точка повинна мати глобальну унікальність для поліпшення помітності повторюваних патернів.
Інтерпретованість (interpretability)	Особливі точки повинні визначатися так, щоб їх можна було використовувати для аналізу відповідностей та виявлення інтерпретованої інформації із зображення.

Таким чином у методології комп’ютерного зору елементи, яким можна дати характеристику, називаються **характерні ознаки** (features). Процес опису цих елементів – це **опис ознаки** (Feature Description), а їх ідентифікація за певним алгоритмом – **виявлення ознак** (Feature Detection).

Визначення кутів методом Харріса (детектор Харріса)

Наприкінці 80-х років минулого століття Кріс Харріс розробив метод, покладений в основу сучасних алгоритмів у галузі Комп'ютерного зору, мета яких – ідентифікація кутів на зображеннях. Кути, як було зазначено раніше – це області зображення з великим розкидом інтенсивності в усіх напрямках.

Метод Харріса полягав у тому, що весь малюнок розділявся на окремі частини. Далі, у процесі руху вздовж кожної частини, алгоритм порівнював їх з сусідніми частинами – по горизонталі і вертикалі. Далі усе залежало від того, чи змінюються характеристики зображеного об’єкта при русі. Метод оперував трьома основними визначеннями:

- **плоский об'єкт** – якщо характеристики на сусідніх частинах не відрізняються ні по вертикалі, ні по горизонталі;
- **межа** – характеристики змінюються тільки по одному з напрямків;
- **кут** – спостерігаємо зміну характеристик як у вертикальній, так і у горизонтальній площині.

Для даного зображення *I* (Рис. 2.5) розглянемо вікно *W* (зазвичай розмір вікна дорівнює 5x5 пікселів, але може залежати від розміру зображення) у центрі *(x, y)*, а також його зсув на *(u, v)*.

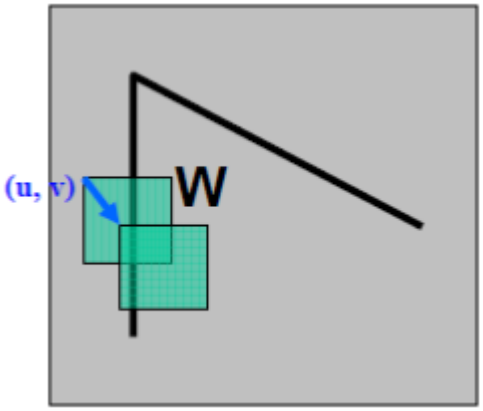


Рисунок 2.5 – Вікно W з центром в (x, y) та його зсув на (u, v)

Тоді зважена сума квадрата різниць між зрушеним і вихідним вікном (тобто зміна околиці точки (x, y) при зсуві на (u, v)) дорівнює:

$$E(u,v) = \sum_{x,y} \underbrace{w(x,y)}_{\text{вагова функція}} \left[\underbrace{I(x+u,y+v)}_{\text{зміщена інтенсивність}} - \underbrace{I(x,y)}_{\text{інтенсивність}} \right]^2 \quad (2.1)$$

Ми повинні максимізувати цю функцію *E(u,v)* для виявлення кутів. Застосовуючи розширення Тейлора до рівняння (2.1) та використовуючи деякі математичні кроки, ми отримаємо остаточне рівняння як:

$$E(u,v) = \sum_{x,y} w(x,y) \left[I_x(x,y)u + I_y(x,y)v \right]^2 \approx (x\ y)\ M \begin{pmatrix} x \\ y \end{pmatrix}, \quad (2.2)$$

де *w(x, y)* – вагова функція (зазвичай використовується функція Гауса чи бінарне вікно).

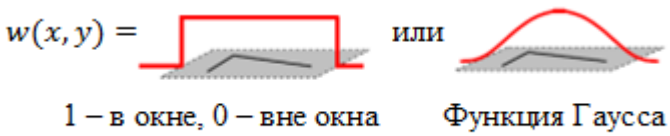


Рисунок 2.6 – вагова функція *w(x, y)*

M – автокореляційна матриця:

$$M = \sum_{x,y} w(x,y) \begin{bmatrix} I_x I_x & I_x I_y \\ I_x I_y & I_y I_y \end{bmatrix}$$

Тут I_x та I_y є похідними зображення в напрямках x і y відповідно.

Кут характеризується великими змінами функції *E(x,y)* за всіма можливими напрямами (x,y), що еквівалентно великим за модулем власним значенням матриці M. Розташування власних значень наведено на Рисунку 2.7.

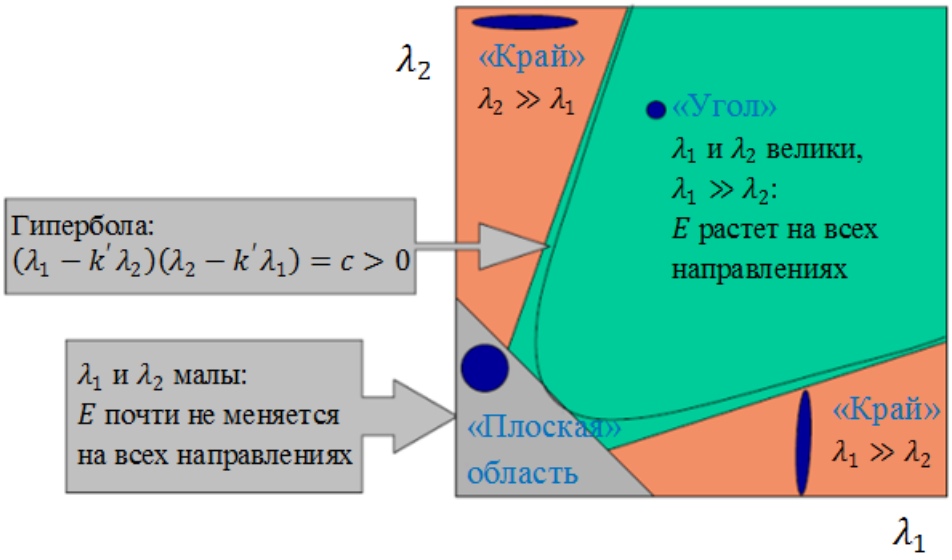


Рисунок 2.7 – Розташування власних значень

Оскільки безпосередньо рахувати власні значення є трудомістким завданням, було запропоновано міру відгуку. Наступне рівняння, по суті, визначає, чи може вікно містити кут чи ні [26]:

$$R = \det(M) - k\left(trace(M)\right)^2 > k, \tag{2.3}$$

де: k – емпірична константа, $k \in [0{,}04;\ 0{,}06]$;

$det(M) = \lambda_1 \lambda_2$

$trace(M) = \lambda_1 + \lambda_2$

λ_1 та λ_2 є власними значеннями M

Отже, значення цих власних значень вирішують, чи є область кутовою, ребровою чи плоскою:

- коли **|R|** є малим, що відбувається, коли λ_1 і λ_2 також малі, область є **плоскою**.
- коли **R < 0**, що відбувається, коли $\lambda_1 >> \lambda_2$ або навпаки, область є **ребровою**.
- коли **R** є великим, у випадку, якщо λ_1 і λ_2 великі та $\lambda_1 \sim \lambda_2$, область є **кутом**.

Таким чином, значення **R** є позитивним для кутових особливих точок. Потім проводиться відсікання точок за знайденим порогом R (тобто ті точки, у яких значення R менше деякого порога, виключаються з розгляду). Далі знаходяться локальні максимуми функції відгуку (non-maximal suppression) по околиці заданого радіусу і вибираються як кутові особливі точки.

Детектор Харріса інваріантний до поворотів, частково інваріантний до афінних змін інтенсивності. До недоліків варто віднести чутливість до шуму та залежність детектора від масштабу зображення (для усунення цього недоліку використовують багатомасштабний детектор Харріса (multi-scale Harris detector)) [27].

2.3 Алгоритми виявлення особливих точок та їх дескрипторів

У попередньому пункті було розглянуто кутовий детектор Харріса. Він (а також інші подібні детектори) інваріантні до обертання, що означає, що навіть якщо зображення повернуто, ми все одно зможемо знайти ті самі кути. У той же час, якщо зображення масштабуватиметься, кут може втратити свою форму. Таким чином, детектор Харріса не інваріантний масштабно.

Алгоритм SIFT

У 2004 році Девід Лоу з Університету Британської Колумбії представив новий алгоритм **Масштабно-інваріантної трансформації ознак** (Scale-Invariant Feature Transform, **SIFT**), який вилучає ключові точки та обчислює їх дескриптори [28].

В основному алгоритм SIFT складається з наступних етапів [29]:

1) побудова піраміди гауссіанів (Gaussian) та їх різниць. На цьому етапі забезпечується інваріантність до масштабування;

2) визначення екстремумів;

3) уточнення особливих точок;

4) побудова дескрипторів (забезпечується інваріантність до освітлення, шуму, зміни положення камери).

Гауссіаном є зображення [30]:

$$L(x, y, \sigma) = G(x, y, \sigma) * I(x, y), \tag{2.4}$$

де: L – значення гауссіана в точці з вимірюванням (x, y);

σ – радіус розмиття;

G – гауссове ядро;

I – значення вихідного зображення;

* – операція згортки.

На першому етапі алгоритму SIFT будується масштабоване простір зображень – набір зображень, згладжених фільтром Гауса:

$$G(x, y, \sigma) = \frac{1}{2\pi\sigma^2} e^{\frac{x^2+y^2}{2\sigma^2}}, \tag{2.5}$$

де: (x, y) – координати точки;

σ – радіус розмиття.

За ними будується **різниця гауссіан D(x, y, σ)**. Різницею за Гауссом називають зображення, отримане шляхом віднімання одного гауссіана вихідного зображення з гауссіана іншого радіусу розмиття, тобто попіксельне віднімання зображень в одній октаві з різним коефіцієнтом розмиття:

$$D(x, y, \sigma) = (G(x, y, k\sigma) - G(x, y, \sigma)) * I(x, y) = L(x, y, k\sigma) - L(x, y, \sigma) \tag{2.6}$$

Октава – зображення в одному масштабі, розмите фільтром Гауса (4 зображення в одній октаві).

На Рис. 2.8 зліва зображена піраміда гауссіанів, а праворуч - їх різниці. Схематично показано, що кожна різниця виходить із двох сусідніх гауссіанів, кількість різниць на одиницю менша за кількість гауссіанів. При переході до наступної октави розмір зображень зменшується вдвічі.

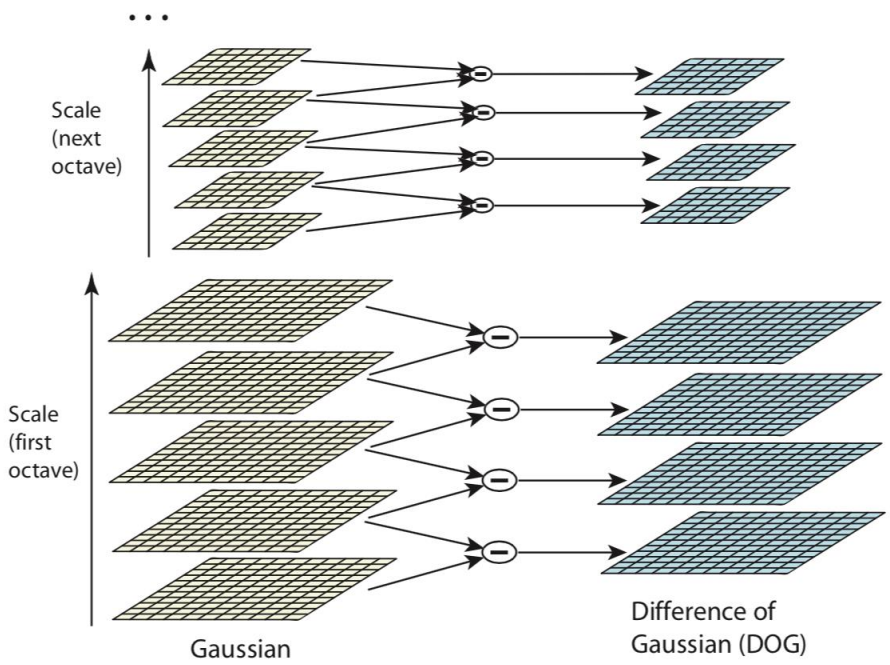


Рисунок 2.8 – Різниця Гаусо-розмитих зображень

Потім визначаються екстремуми, що заносяться до списку потенційних особливих точок. Після побудови пірамід точка вважається особливою, якщо вона є локальним екстремумом різниці гауссіанів. Для пошуку екстремумів використовується метод, схематично зображений на Рис. 2.9.

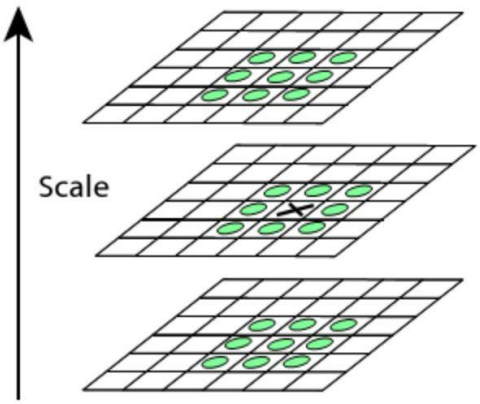


Рисунок 2.9 – Метод пошуку екстремумів різниці гауссіанів

Якщо значення різниці гауссіанів у точці, позначеній хрестиком, більше (менше) всіх значень у точках, помічених колами, то ця точка вважається точкою екстремуму.

Далі відбувається уточнення особливих точок, що складається з двох складових:

1) виключаються точки з малою контрастністю за допомогою обчислення екстремуму різниці гауссіанів. Різниця гауссіанів розкладається багаточленом Тейлора другого порядку, взятого в точці розрахованого екстремуму;

2) виключаються граничні точки (точки, що мають великий локальний вигин уздовж кордону та малий у перпендикулярному напрямку).

На заключному етапі для околиці особливої точки обчислюються зміни яскравостей точок, за якими будується дескриптор. Дескриптор – це вектор із 64 чисел, що дозволяє отримати інваріантність щодо положення камери. Потім дескриптор нормалізується, рахунок чого досягається інваріантність щодо зміни освітлення [29, 30].

Алгоритм SURF

Іншим відомим алгоритмом є **Метод прискорених надійних характеристик** (Speeded Up Robust Features, **SURF**), представлений у 2006 році. Метод позиціонується як покращений варіант SIFT зі збільшеною швидкістю детектування і побудови дескриптора.

Визначення особливих точок на зображенні виконується на основі матриці Гессе (FAST-Hessian detector). Скажімо, що вихідне зображення задається матрицею інтенсивностей I, поточний піксель, що розглядається, позначається як $X = (x, y)$, а σ - масштаб фільтра. Тоді матриця Гессе має вигляд:

$$H(x, y, \sigma) = \begin{bmatrix} L_{xx}(x, y, \sigma) & L_{xy}(x, y, \sigma) \\ L_{yx}(x, y, \sigma) & L_{yy}(x, y, \sigma) \end{bmatrix}, \quad (2.7)$$

де:

$$L_{xx}(x, y, \sigma) = I(x, y) * \frac{d^2 g_\sigma}{dx^2},$$

$$L_{yy}(x, y, \sigma) = I(x, y) * \frac{d^2 g_\sigma}{dy^2},$$

$$L_{xy}(x, y, \sigma) = I(x, y) * \frac{d^2 g_\sigma}{dxdy}.$$

Тут I(x,y) – вихідне зображення,

$g_\sigma(x, y)$ – функція Гауса,

«∗» – оператор згортки.

Використання Гессіана не забезпечує інваріантності щодо зміни масштабу. Тому SURF застосовує фільтри різного масштабу для обчислення Гессіана.

Детермінант матриці Гессе досягає екстремуму в точках максимальної зміни градієнта яскравості. Тому SURF пробігається фільтром з гаусовим ядром по всьому зображенню і знаходить точки, в яких досягається максимальне значення детермінанта матриці Гессе. Зазначимо, що такий прохід виділяє як темні плями на білому фоні, так і світлі плями на темному фоні [29].

На Рис. 2.10 видно, що особливі точки (окреслені кольоровими колами) є локальними екстремумами яскравості зображення. Дрібні точки не розпізнані як особливі, через порогове відсікання за величиною гесіана [31].

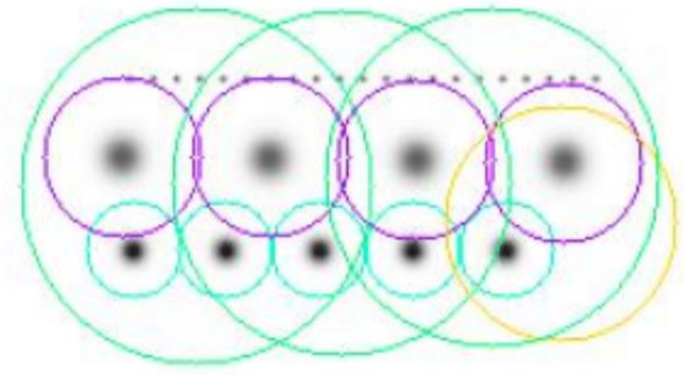


Рисунок 2.10 – Особливі точки детектора SURF

Далі для кожної знайденої особливої точки за допомогою фільтра Хаара обчислюється її орієнтація – переважний напрямок різниці яскравості. Поняття орієнтації близьке до поняття напрямку градієнта, але для визначення орієнтації особливої точки застосовується фільтр Хаара. Приклад фільтрів Хаара показано на Рис. 2.11.

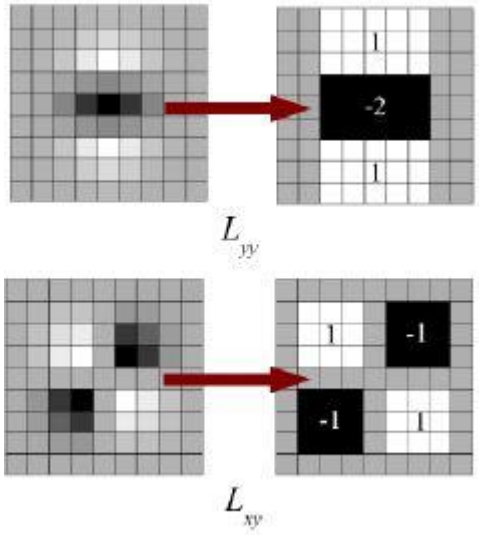


Рисунок 2.11 – Фільтри Хаара (чорні області мають значення "-1", білі "+1")

Дескриптор є масивом з 64 (у розширеній версії 128) чисел, які дозволяють ідентифікувати ключову точку. Дескриптори повинні приблизно збігатися в одній і тій же точці на першому і другому зображенні. Метод обчислення дескриптора не залежить від масштабу та обертання.

Для обчислення дескриптора навколо особливої точки утворюється прямокутна область розміром 20s де s – масштаб, в якому знайдена особлива точка. Для першої октави область має розмір 40×40 пікселів. Квадрат орієнтований уздовж пріоритетного напряму, обчисленого для особливої точки. Дескриптор розглядається як опис градієнта для 16 квадрантів навколо особливої точки.

Потім квадрат ділиться на 16 менших квадрантів, як показано на Рис. 2.12. У кожному квадранті береться регулярна сітка 5×5 та підбирається точки сітки з використанням фільтра Хаара. Розмір фільтра Хаара приймається рівним 2s, і для першої октави – 4×4.

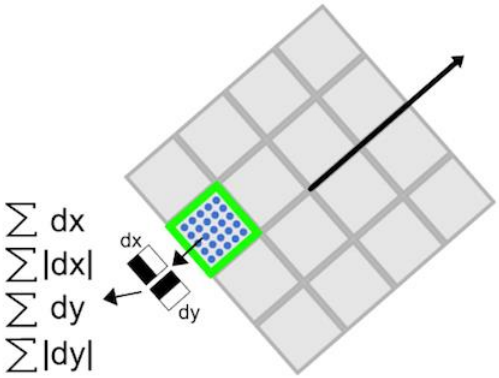


Рисунок 2.12 – Обчислення дескриптора особливої точки

Слід зазначити, що при обчисленні фільтра Хаара зображення не обертається, фільтр розглядається у звичайних координатах зображення. Отримані градієнтні координати (dX, dY) повертаються на кут, що відповідає орієнтації квадрата. Загалом, для обчислення дескриптора особливої точки потрібно обчислити 25 фільтрів Хаара, в кожному з 16 квадрантів. Усього 400 фільтрів Хаара. Враховуючи, що фільтру потрібно 6 операцій, виявиться, що дескриптор вимагатиме виконання не менше 2400 операцій.

Після знаходження 25 градієнтів точки квадранту обчислюються чотири значення, які фактично є компонентами дескриптора:

$$\sum dX, \sum |dX|, \sum dY, \sum |dY|.$$

Дві з них – це повний градієнт по квадранту, а дві інших – сума модулів точкових градієнтів. На Рис. 2.13. показані значення розрахункових величин для різних зображень.

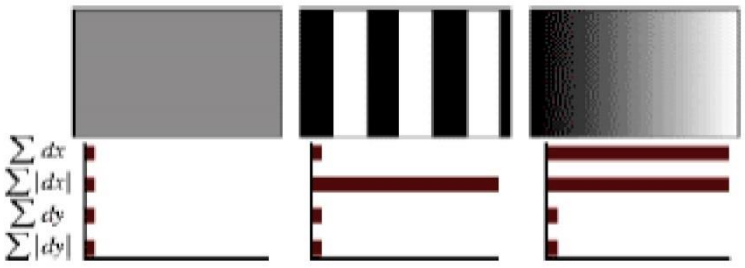


Рисунок 2.13 – Поведінка дескриптора для різних зображень

Для однорідних областей всі значення близькі до нуля. Для вертикальних смужок, що повторюються, всі величини, крім другої близькі до нуля. Зі збільшенням яскравості в напрямку осі *X* перші дві компоненти мають високі значення. Чотири компоненти на кожен квадрант і 16 квадрантів дають 64 компоненти дескриптора для області особливої точки. При введенні в масив значення дескрипторів множаться на гауссіану, з центром в особливій точці і з σ =3.3s. Це необхідно для більшої стійкості дескриптора до шуму в областях, віддалених від особливої точки. На додаток до дескриптора для опису точки використовується знак сліду матриці Гессе, тобто величина *sign(Dxx+Dyy)*. Для світлих точок на темному фоні слід від'ємний, для темних точок на світлому фоні – позитивний. Подібним чином, SURF розрізняє темні та світлі плями [32].

Коротше кажучи, SURF додає багато функцій для покращення швидкості на кожному кроці. Аналіз показує, що він в 3 рази швидший, ніж SIFT, а продуктивність порівнянна з SIFT. SURF добре обробляє зображення з розмиттям і обертанням, але погано справляється зі зміною точки огляду та освітленням [33].

Алгоритм FAST

Алгоритм **Функцій прискореного та сегментного тесту** (Features from Accelerated Segment Test, **FAST**) було запропоновано Е. Ростеном та Т. Драммондом у 2006 р.

Виявлення ознак за допомогою FAST відбувається наступним чином [34].

Розглянемо коло з 16 пікселів навколо пікселя, що аналізується (див. Рис. 2.14). Вибирається піксель ***p*** на зображенні, який потрібно ідентифікувати як точку інтересу. Нехай його інтенсивність (яскравість) буде I_p. Обирається відповідне порогове значення ***t***. Яскравість пікселів, що лежать на колі, порівнюється з яскравістю центральної точки, і на підставі низки перевірок приймається рішення, чи є центральна точка особливою.

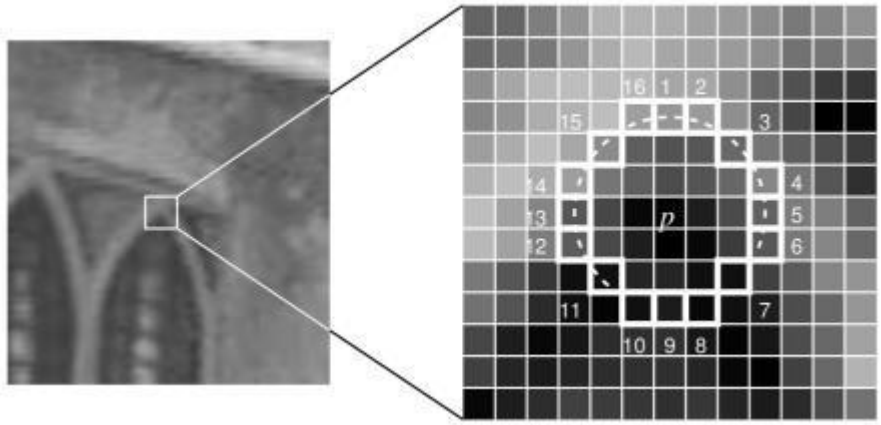


Рисунок 2.14 – Область точки p FAST детектора

Якщо в колі існує набір з ***N*** суміжних пікселів (з 16 пікселів), та усі ***N*** яскравіше $\boldsymbol{I_p + t}$ або темніше $\boldsymbol{I_p - t}$ (показано білими штриховими лініями на зображенні нижче), то точка ***p*** помічається як можливо особлива. ***N*** було обрано 12 (в даному випадку). Якщо є помічена точка, тоді проводиться дослідження яскравості в області цієї точки – номера пікселів **1, 5, 9, 13**. Точок тільки чотири, бо це дозволяє швидко відсіяти точки, що не підходять. Точка ***p*** вважається характерною, якщо не менше трьох пікселів виконують умову [35]:

$$I_i < I_p - t \text{ АБО } I_i > I_p + t; \qquad i = 1 \dots 4$$

Послідовність перевірок та їх загальна кількість підбираються та оптимізуються заздалегідь на основі великої навчальної вибірки зображень. В

результаті, перевірки виконуються дуже швидко. Для ухвалення рішення, чи є точка кутом чи ні, потрібно лише кілька десятків операцій порівняння.

Алгоритм FAST добре зарекомендував себе у програмах, які здійснюють стеження за об'єктами у реальному часі. Він в кілька разів швидше, ніж інші існуючі кутові детектори, але не стійкий до високих рівнів шуму [34].

Алгоритм BRIEF

Метод **Бінарних надійних незалежних елементарних ознак** (Binary Robust Independent Elementary Features, **BRIEF**) визначає перетворення (2.8), яке полягає у попарному порівнянні пікселів (заздалегідь згладженої, наприклад, фільтром Гауса) області *l* розміру *s*×*s* [36]:

$$\tau(p, x, y) = \begin{cases} 1, p(x) < p(y), \\ 0, p(x) \geq p(y), \end{cases} \quad (2.8)$$

де: *p(x)* – інтенсивність пікселя у точці з координатами *x = (u, v)* області *l*.

Набір таких пар пікселів *(x, y)* розміру n_d називається множиною "бінарних тестів". Таким чином, дескриптор особливої точки визначається як n_d-мірний бітовий рядок, який визначається за формулою:

$$f_{n_d}(p) = \sum_{1 \leq i \leq n_d} 2^{i-1} \tau(p, x_i y_i). \quad (2.9)$$

Величина n_d вибирається рівною 128, 256, 512. Важливим є вибір пікселів в області для бінарного тесту, в [37] автори розглядають п'ять методів визначення векторів *x* і *y*:

1. *x* та *y* вибираються випадковим чином рівномірно розподіленими;
2. *x* та *y* вибираються випадково, згідно з розподілом Гауса;
3. *x* та *y* вибираються випадково у два етапи. Спочатку згідно з розподілом Гауса вибирається *x* щодо центру координат, потім *y* – щодо *x*;

4. *x* та *y* вибираються випадково на дискретній радіальній сітці;
5. для кожної пари *x* вибирається у центрі координат, а *y* – на дискретній радіальній сітці.

За результатами порівняння в [37] точність розпізнавання в п'яти перерахованих випадках приблизно однакова. Для порівняння дескрипторів використовується міра Хеммінга.

Мета створення дескриптора BRIEF полягала у забезпеченні розпізнавання однакових частин зображення, отриманих із різних кутів огляду. Завдання полягало в тому, щоб скоротити кількість виконаних обчислень. Основними проблемами методу BRIEF є неоптимальний вибір точок для розрахунку дескриптора та неможливість враховувати орієнтацію точки при розпізнаванні.

Алгоритм ORB було запропоновано як ефективну альтернативу SIFT або SURF у 2011 році.

Дескриптор **ORB** (Oriented FAST and Rotated BRIEF) є комбінацією детектора ключових точок **FAST** і бінарних дескрипторів **BRIEF** [38].

У методі ORB для розрахунку орієнтації кута використовуються координати центру ваги *C*, що обчислюються через моменти зображення m_{pq}:

$$m_{pq} = \sum_{x,y} x^p y^q I(x,y) \quad C = \left(\frac{m_{10}}{m_{00}}, \frac{m_{01}}{m_{00}}\right), \tag{2.10}$$

тоді орієнтація кута задаватиметься вектором, початок якого буде у центральній точці, а кінець – у центрі тяжіння, а кут дорівнюватиме:

$$\theta = arctg\left(\frac{m_{01}}{m_{10}}\right).$$

Ці ідеї втілюються методом «steered» BRIEF. Для множини бінарних тестів розміру *n*, з координатами (x_i, y_i) будується матриця *S* розмірності $2xn$:

$$S = \begin{pmatrix} x_1 & \dots & x_n \\ y_1 & \dots & y_n \end{pmatrix}.$$

Використовуючи розрахований кут θ, будується матриця обертання R_θ і тоді можна отримати матрицю S_θ з урахуванням повороту рівну $S_\theta = R_\theta S$. Далі виконується дискретизація кута зі збільшенням 2π/30, тобто по 12°, і виконується пошук та узгодження дескриптора з S_θ.

Тепер дескриптор, на відміну від (2.9), матиме вигляд:

$$g_n(p, \theta) = f_{n_d}(p) \Big|_{(x, y) \in S_\theta} \tag{2.11}$$

Метод BRIEF має важливу властивість – кожен дескриптор має велику дисперсію та середнє значення близько 0,5. Але як тільки дескриптор стає орієнтованим у напрямку ключової точки, він втрачає цю властивість. Також важливо, що бінарні тести були некорельованими, тобто краще розпізнавались. Щоб вирішити ці проблеми, метод ORB використовує пошук серед усіх можливих бінарних тестів, щоб знайти ті, які мають як високу дисперсію, так і середні значення, близькі до 0,5, а також некорельовані між собою. Результат називається **rBRIEF**. Для зіставлення дескриптора використовується LSH (Locality-sensitive hashing) – спосіб зниження розмірності багатовимірних даних [36, 38].

Короткий огляд найбільш популярних з існуючих методів дозволяє зробити висновок, що всі дескриптори мають свої переваги, виявляючи слабку інваріантність до різних змін зміни масштабу, зсуву, повороту. У зв'язку з патентними обмеженнями алгоритмів SIFT і SURF у цій роботі передбачається використання одного з алгоритмів, що вільно розповсюджуються – ORB в рамках бібліотеки OpenCV.

2.4 Зіставлення особливих точок

Після здійснення пошуку та опису особливих точок необхідно вибрати алгоритм для їхнього зіставлення. Зіставлення може проводитися на основі різних метрик (наприклад, метод k-середніх, Евклідова відстань, Відстань Хеммінга, Чебишева та Манхеттена).

Евклідова відстань

Порівнюючи кожен набір дескрипторів із першого зображення з кожним таким набором із другого зображення, знаходимо найкращу відповідність між особливими точками. Зіставлення розраховується на основі евклідової відстані:

$$d(x, y) = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}, \tag{2.12}$$

де: d – відстань між об'єктами x та y;

x_i – значення i-властивості об'єкта x;

y_i – значення i-властивості об'єкта y;

i – (1, 2, ... n).

Відстань Хеммінга

Визначення 1. Міра відмінності об'єктів, що задаються дихотомічними ознаками. Визначається за допомогою формули:

$$d_H(X_i X_j) = \sum_{s=1}^{p} \left| x_i^{(s)} - x_j^{(s)} \right| \tag{2.13}$$

І, отже, дорівнює числу невідповідностей між значеннями відповідних ознак у аналізованих i-му та j-му об'єктах.

Визначення 2. Відстанню Хеммінга називається кількість біт, що відрізняються, у двох бінарних векторах.

Відстань Хеммінга вже досить широко використовується для різних завдань, таких як пошук близьких дублікатів, розпізнавання образів, класифікація документів, виправлення помилок, виявлення вірусів тощо. У більш загальному випадку відстань Хеммінга застосовується до рядків однакової довжини будь-яких *k*-вих алфавітів і служить метрикою різниці (функцією, що визначає відстань у метричному просторі) об'єктів тієї ж розмірності. Таку метрику можна подати у вигляді формули (2.14).

$$hamming(x, y) = \sum_{x_i \neq y_i} 1 \qquad i = 1, \dots, n \tag{2.14}$$

де: *x* та *y* – дескриптори (бінарні вектори).

2.5 Поєднання зображень

У комп'ютерному зорі будь-які два зображення одного й того самого плоского об'єкта у просторі пов'язані перетворенням гомографії [29]. Для врахування проективних спотворень можна використовувати перетворення матричної форми в однорідних координатах.

$$\begin{pmatrix} \tilde{u}w \\ \tilde{v}w \\ w \end{pmatrix} = H \begin{pmatrix} u \\ v \\ 1 \end{pmatrix}, \tag{2.15}$$

де: $H=(h_{ij})_{3\times 3}$ – матриця гомографії.

Матриця гомографії має такий вигляд:

$$\begin{bmatrix} h_{11} & h_{12} & h_{13} \\ h_{21} & h_{22} & h_{23} \\ h_{31} & h_{32} & 1 \end{bmatrix}.$$

Вона містить 8 невідомих параметрів, для їх знаходження як мінімум 4 пари ключових точок на зображеннях, що зіставляються. Метою є знаходження матриці за знайденими парами особливих точок. Для цього було обрано алгоритм **RANSAC**, що складається з наступних етапів:

– знайти матрицю гомографії по всій множині пар ключових точок і виконувати суміщення зображень;

– оцінити якість поєднання зображень.

Якщо суміщення незадовільне, то знаходити пару (пари) ключових точок, відстань між образами яких виявилася найбільшою, і видаляти їх з множини пар ключових точок;

– знову знайти матрицю гомографії по скороченій множині пар ключових точок, виконувати суміщення зображень, оцінити якість суміщення і, можливо, видалити деякі пари ключових точок і т.д., поки не буде отримано задовільне суміщення зображень.

2.6 Методи підвищення ефективності біометричної системи

Метод біометричної ідентифікації за венозним рисунком забезпечує практично 100% точність і достовірність ідентифікації, але, як і будь-яка технологія, не позбавлена "слабких місць". До них можна віднести: підміну «живої» долоні високоякісним муляжем (з рисунком вен); складність застосування при зовнішніх засвітках (сонце, галогенні лампи тощо); деякі захворювання (наприклад, у людей похилого віку – артрит та інші).

Актуальним постає питання у **збільшенні точності** й **ефективності** біометричної системи. Існує низка підходів, спрямованих на досягнення бажаного результату у цій галузі.

Найчастіше для підвищення якості прийняття рішення застосовуються **мультимодальні** біометричні системи, тобто такі, які використовують більше однієї біометричної характеристики для розрахунку оцінки схожості. Такі системи

дозволяють використовувати більшу кількість факторів для прийняття рішення. При даному підході використовують нечітку логіку, так як даний підхід забезпечує меншу втрату інформації при роботі системи [].

Інший підхід полягає у виключенні можливості підробки долоні руки, шляхом введення проміжних етапів (між основними загальновикористовуваними) детектування життєздатності долоні руки і контрольній перевірці прийнятого рішення на наявність помилок 1 і 2 роду.

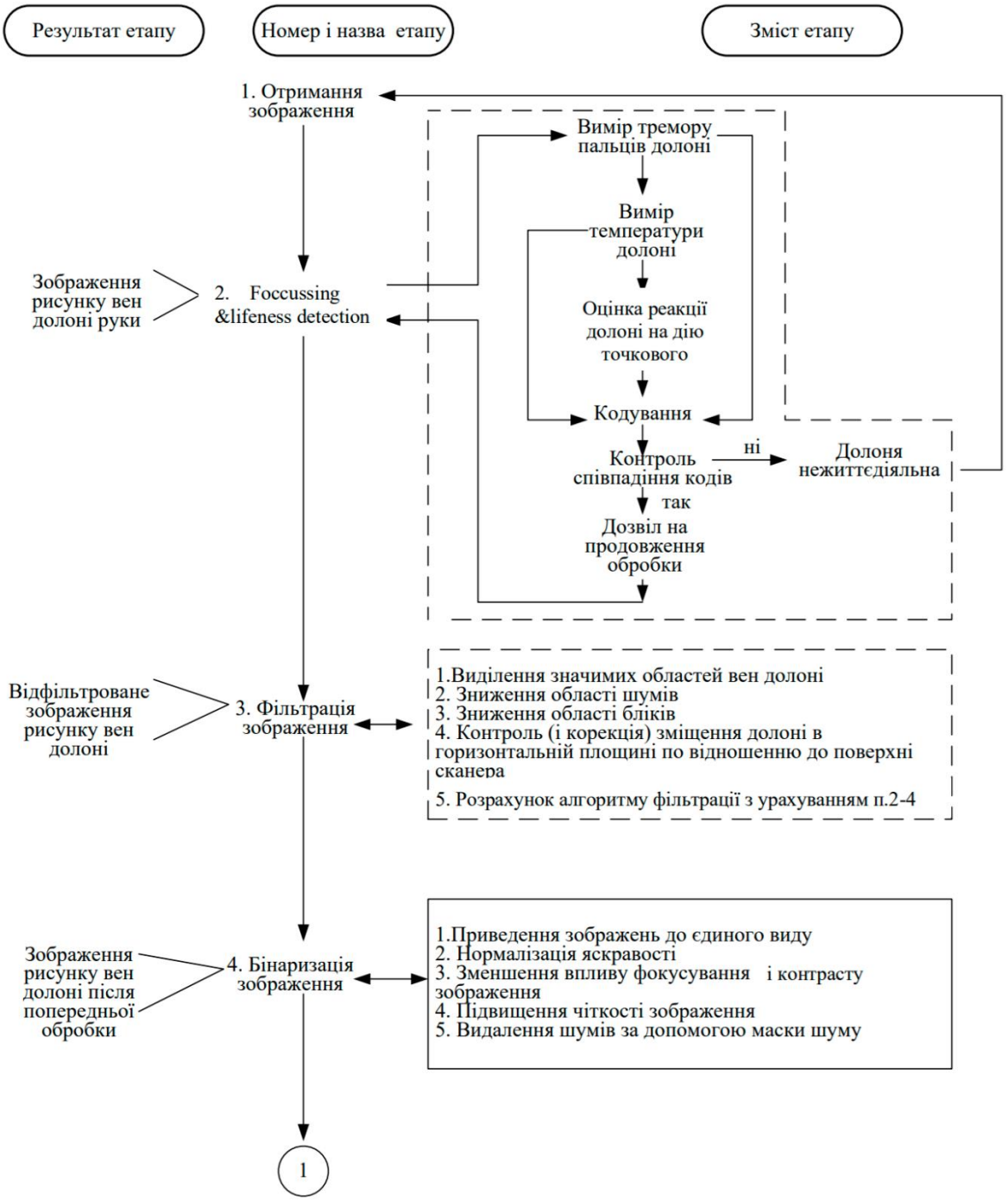
Крім того, останні дослідження та розробки у галузі біометрії відкривають нові можливості у підвищенні безпеки біометричної аутентифікації. Наприклад, розробка гнучкого комбінованого датчика вимірювання пульсової хвилі людини, який пропонується використовувати чи не вперше для визначення особистості.

Метод введення етапів «Детектування життєдіяльності долоні та контрольної перевірки прийнятого рішення»

В роботі [39] автором був запропонований та описаний удосконалений метод біометричної ідентифікації за венозним рисунком долоні рук, новизна якого полягає у введенні до його структури нових етапів: **Focussing & lifeness detection** (детектування життєдіяльності долоні) і **«контрольна перевірка прийнятого рішення на наявність помилок 1 і 2 роду».**

Нова структура передбачає включення трьох етапів (Рис. 2.15).

Етап детектування, за своєю сутністю, є тестовим етапом, побудованим таким чином, щоб повністю виключити можливість підміни руки живого пацієнта будь-яким, навіть і високоякісним, муляжем. Це досягається контрольною тестовою перевіркою долоні, що прикладається до сканера. Температурний тест, який передбачає наявність температури долоні руки живої людини, виконується за допомогою вбудованого в сканер термометра.


Результат етапу
Номер і назва етапу
Зміст етапу
1. Отримання зображення
Вимір тремору пальців долоні
Вимір температури долоні
Оцінка реакції долоні на дію точкового
Кодування
Контроль співпадіння кодів
ні
Долоня нежиттєдіяльна
так
Дозвіл на продовження обробки
Зображення рисунку вен долоні руки
2. Foccussing &lifeness detection
1.Виділення значимих областей вен долоні
2. Зниження області шумів
3. Зниження області бліків
4. Контроль (і корекція) зміщення долоні в горизонтальній площині по відношенню до поверхні сканера
5. Розрахунок алгоритму фільтрації з урахуванням п.2-4
Відфільтроване зображення рисунку вен долоні
3. Фільтрація зображення
Зображення рисунку вен долоні після попередньої обробки
4. Бінаризація зображення
1.Приведення зображень до єдиного виду
2. Нормалізація яскравості
3. Зменшення впливу фокусування і контрасту зображення
4. Підвищення чіткості зображення
5. Видалення шумів за допомогою маски шуму
1

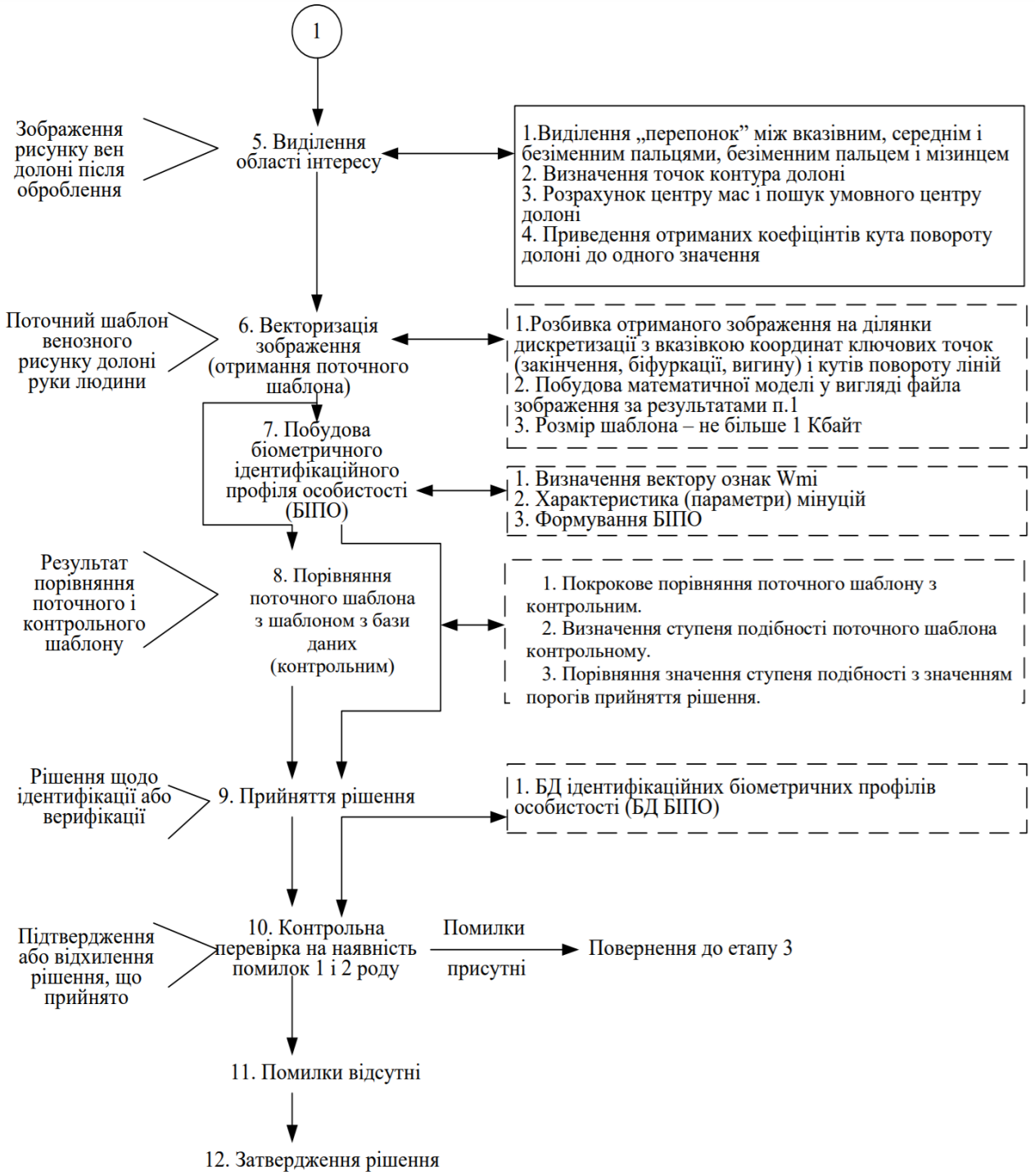


Рисунок 2.15 – Алгоритм роботи удосконаленого методу біометричної ідентифікації за венозним рисунком долоні рук [39]

Для перевірки «речовини» долоні автором запропоновано **тепловий тест**, який передбачає запрограмований нагрів поверхні долоні за допомогою точкового

нагрівача. Дія сфокусованого теплового променя на муляж долоні, виконаний із воску, призведе до того, що віск почне плавитись і викриє, таким чином, підробку.

І нарешті, третій рівень захисту (контролю), реалізовано за допомогою **фізіологічного тесту**, який передбачає контроль наявності фізіологічного тремору пальців долоні за допомогою безконтактного спеціалізованого засобу, який, як і термометр, вбудовано в сканер долоні. Сенс застосування такого тесту полягає в тому, що кожна людина має свій рівень тремору, який, зрозуміло, буде свідчити про те, що ми маємо справу з живою людиною, а не муляжем [39].

Таким чином, метод передбачає введення трьох додаткових критеріїв правдоподібності, кожен з яких, належить до різних фізіологічних систем організму людини, що збільшує точність і достовірність результатів ідентифікації.

Метод вимірювання пульсової хвилі

Для підвищення безпеки біометричної аутентифікації, японська компанія **Japan Display** спільно з вченими з Токійського університету розробила [40] гнучкий комбінований датчик зображення, що поєднує сканер відбитка пальців, сканер малюнка вен та датчик вимірювання пульсової хвилі (Рис. 2.16).

Рисунок 2.16 – Датчик зображення, що може вимірювати відбитки пальців, вени та пульсові хвилі

На думку розробників, якщо існуючі методи біометричної аутентифікації підкріпити датчиком вимірювання пульсової хвилі, це збільшить надійність захисту від несанкціонованого доступу.

Пульсова хвиля – це хвиля підвищеного тиску, що поширюється артеріями до капілярів. Її значення прямо залежить від еластичності артерій та судин і, строго кажучи, індивідуально. Принаймні, разом із рештою біометричною інформацією дані про значення пульсової хвилі дозволяють точно визначити особистість.

Представлений датчик має роздільну здатність 508 пікселів на дюйм і працює зі швидкістю 41 кадр на секунду. Датчик гнучкий завтовшки 15 мкм. Сенсор зображень виконаний з низькотемпературного полікристалічного кремнію, що передбачає високу мобільність електронів у тонкоплівкових транзисторах і, відповідно, можливість з високою точністю визначати такий параметр, як значення пульсової хвилі [41].

2.7 Висновки

Даний розділ був присвячений розгляду теорії Комп'ютерного зору, його типовим завданням та функціям, а також принципам виявлення та вилучення унікальних ознак на зображеннях.

Розглянуто популярні алгоритми виявлення особливих точок та їх дескрипторів: SIFT, SURF, FAST, BRIEF та ORB. Алгоритми SIFT та SURF мають велику точність обчислення особливих точок та їх дескрипторів, проте мають патентні обмеження. Метод ORB (що представляє собою комбінацію з модифікованих алгоритмів FAST і BRIEF) має кращу швидкість у обчисленні особливих точок та розрахунку їх дескрипторів, що дозволяє використовувати його в завданнях, де потрібна обробка зображень у реальному часі.

Метод біометричної ідентифікації за венозним рисунком не позбавлений недоліків, проте існуючі методи підвищення ефективності таких систем дозволяють довести точність та достовірність ідентифікації практично до 100%.

Були розглянуті 2 методи – метод введення етапів «Детектування життєдіяльності долоні та контрольної перевірки прийнятого рішення», основна ідея якого полягає у введенні додаткових критеріїв оцінки правдоподібності та метод вимірювання пульсової хвилі, який базується на впровадженні додаткового датчика вимірювання пульсової хвилі, що має збільшити надійність захисту від несанкціонованого доступу.

РОЗДІЛ 3
ПРОГРАМНА РЕАЛІЗАЦІЯ ТА РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

3.1 Вибір засобів розробки

Для проведення експерименту розроблено додаток "**Biometric Vein Recognition**" для мобільних пристроїв під ОС "Android" з використанням мови Java. Розглянуті у Розділі 2 алгоритми пошуку ключових точок, обчислення дескрипторів та їх зіставлення на зображеннях, а також фільтрація реалізовані за допомогою бібліотеки OpenCV версії 3.1.0 [42].

OpenCV (Open Source Computer Vision Library) — бібліотека алгоритмів комп'ютерного зору, обробки зображень і чисельних алгоритмів спільного назначення з відкритим кодом. Реалізована на C/C++, також є підтримка Python, Java, Ruby, Matlab, Lua, Matlab та інших мов. Може вільно використовуватися в академічних і комерційних цілях – розповсюджується в умовах ліцензії BSD (Berkeley Software Distribution). Бібліотека складається з різних модулів (модуль **core** є основним і називається ядром бібліотеки), кожний з котрих, реалізує визначений клас функціональності.

Бібліотека має приблизно майже 3000 алгоритмів, спрямованих на вирішення таких завдань: ідентифікація об'єктів та тексту, усунення спотворень, розкриття подібності і форми сутностей, стеження за переміщенням об'єкта, розпізнавання рухів, жестів та багато іншого, що працює в реальному часі. Деякі алгоритми реалізовані у вигляді окремих класів, а більшість – у вигляді статичних методів якого-небудь класу. Класи в OpenCV версії 3 в Java розділені на наступні пакети [23]:

- org.opencv.imgcodecs — включає клас Imgcodecs, за допомогою якого можна завантажити зображення з файлу або буфера, а також зберегти зображення у файл або буфер в різних форматах (наприклад, в JPEG);

- org.opencv.core — містить основні класи бібліотеки, що реалізують базові структури (вектори, матриці тощо). Крім того, пакет включає допоміжні класи (наприклад, класи Point, Rect та ін.). Клас Core із цього пакета містить статичні методи, за допомогою яких можна виконати різні операції з матрицями;
- org.opencv.imgproc — включає класи, призначені для обробки та аналізу зображень;
- org.opencv.features2d — містить класи, за допомогою яких можна знаходити та порівнювати особливі точки;
- org.opencv.photo — включає класи, призначені для створення HDR-зображень;
- org.opencv.video — містить класи, призначені для роботи з відеоданими (аналіз руху та відстеження об'єктів);
- org.opencv.videoio — за допомогою класу VideoCapture з цього пакета можна завантажувати кадри з відеофайлу або послідовності кадрів, а також захоплювати кадри в режимі реального часу з камер зовнішнього відеоспостереження, веб-камер та ін.;
- org.opencv.calib3d — містить класи, за допомогою яких можна виконати калібрування камери, працювати зі стереокамерами та обробляти тривимірні дані;
- org.opencv.objdetect — включає класи пошуку об'єктів на зображенні. За допомогою навчених класифікаторів можна шукати людей, обличчя, очі, ніс, дізнатися, усміхається людина чи ні, і т. д. При великому бажанні можна навчити власний класифікатор з довільним призначенням або завантажити вже навчений з Інтернету;
- org.opencv.ml — містить класи, призначені для машинного навчання;
- org.opencv.dnn — включає класи для роботи з нейронними мережами. Можна завантажувати моделі, навчені у популярних бібліотеках Caffe, TensorFlow та Torch;
- org.opencv.utils — містить допоміжний клас Converters, який переважно

використовується для внутрішніх потреб бібліотеки;

- org.opencv.android — включає класи для роботи з ОС Android. Пакет доступний лише у складі дистрибутива під Android.

Для розробки використовувалося інтегроване середовище **Android Studio Arctic Fox (2020.3.1)** [43], засноване на програмному забезпеченні IntelliJ IDEA від компанії JetBrains. Необхідна мінімальна версія ОС на смартфоні для встановлення додатку – Android 5.0 Lollipop (API level 21).

Android Studio — офіційне інтегроване середовище розробки (IDE) для платформи Android (Рис. 3.1). Воно адаптоване для виконання типових завдань, що вирішуються в процесі розробки додатків для платформи Android. На додаток до потужного редактора коду і інструментів розробника, Android Studio пропонує ще більше функцій, які підвищують продуктивність під час створення додатків, наприклад: гнучку систему збірки та розгортання застосунків на основі Gradle, швидкий і багатофункціональний емулятор, підтримку C++ і NDK. У тому числі у середовище включені засоби для спрощення тестування програм на сумісність з різними версіями платформи та інструменти для проектування застосунків, що працюють на пристроях з екранами різної роздільності (планшети, смартфони, ноутбуки, годинники, окуляри тощо).

Для прискорення розробки додатків представлена колекція типових елементів інтерфейсу і візуальний редактор для їхнього компонування, що надає зручний попередній перегляд різних станів інтерфейсу застосунку (наприклад, можна подивитися як інтерфейс буде виглядати для різних версій Android і для різних розмірів екрану). Для створення нестандартних інтерфейсів присутній майстер створення власних елементів оформлення, що підтримує використання шаблонів [44].

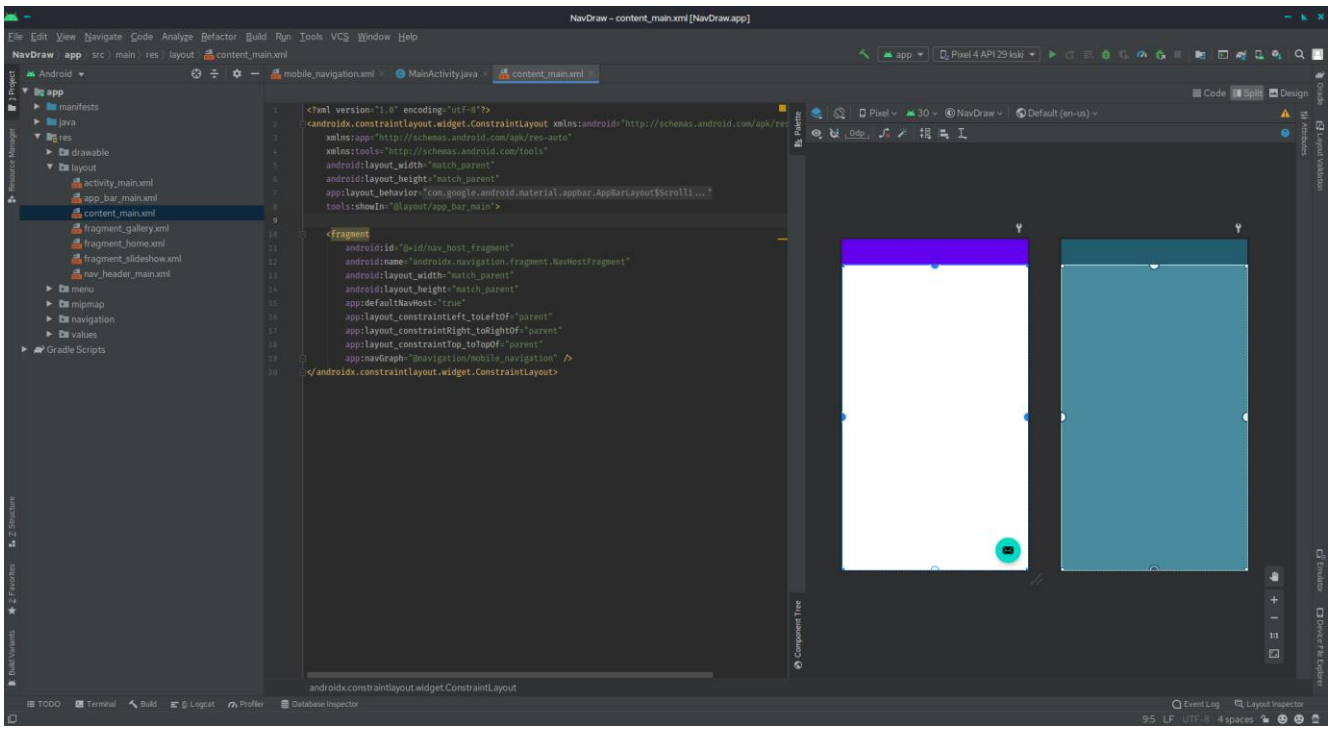


Рисунок 3.1 – Інтерфейс Android Studio IDE

Тестування роботи додатку проводилося на смартфоні Samsung Galaxy A7 2018, основні технічні характеристики якого наведено у таблиці 3.1.

Таблиця 3.1 – Технічні характеристики Samsung Galaxy A7 2018

	Властивість	**Характеристика**
Апаратне забезпечення	Оперативна пам'ять, ГБ	4
	Вбудована пам'ять, ГБ	64
	Процесор	Exynos 7885 + GPU Mali-G71
	Кількість ядер	8
	Частота, ГГц:	2x2,2 + 6x1,6
	Діагональ, дюйми	6
	Роздільна здатність	2220x1080

Продовження таблиці 3.1

	Основна камера, Мп	24 (f / 1.7) + 5 (f / 2.2) + 8 (f / 2.4)
	Фронтальна камера, Мп	24 (f / 2.0)
Програмне забезпечення	Операційна система	Android™ 10 Q
	Версія One UI	2.0

3.2 Створення системи верифікації для смартфона

Як зазначалося у Розділі 1, роль смартфона у житті сучасної людини важко переоцінити. Ці гаджети є системами з великою кількістю біометричних датчиків і підсистем, одночасно вбудованих в одному корпусі: сканер відбитка пальця (наприклад, смартфони Apple починаючи с iPhone 5s), розпізнавання обличчя (наприклад, iPhone X, Huawei Mate 20 Pro, Honor 9X), сканер райдужної оболонки ока (наприклад, Samsung Galaxy S21 Ultra) та голосові помічники (наприклад, Google Assistant, Siri).

Існуючі методи біометричної аутентифікації можуть бути “обдурені” різними способами, тому всі подальші дослідження та розробки спрямовані на збільшення надійності захисту від несанкціонованого доступу шляхом впровадження нових біометричних систем у мобільні пристрої (або їх комбінування).

Однією з перспективних можна вважати біометричну систему розпізнавання за рисунком вен руки. Для цього в якості обладнання для захоплення, обробки та зберігання використовується смартфон з інтегрованою інфрачервоною камерою. Слід зазначити, що на сьогоднішній день є кілька моделей мобільних телефонів на ринку з вже вбудованою інфрачервоною камерою, що використовується для їхнього розблокування за допомогою розпізнавання обличчя. Наприклад, Xiaomi Pocophone F1, Google Pixel 4 та інші.

Зазвичай, на будь-якому сучасному смартфоні датчики та фронтальна камера розташовані над екраном у верхній частині – так званий "чубчик", або у верхній частині окантовки дисплея (Рис. 3.2).

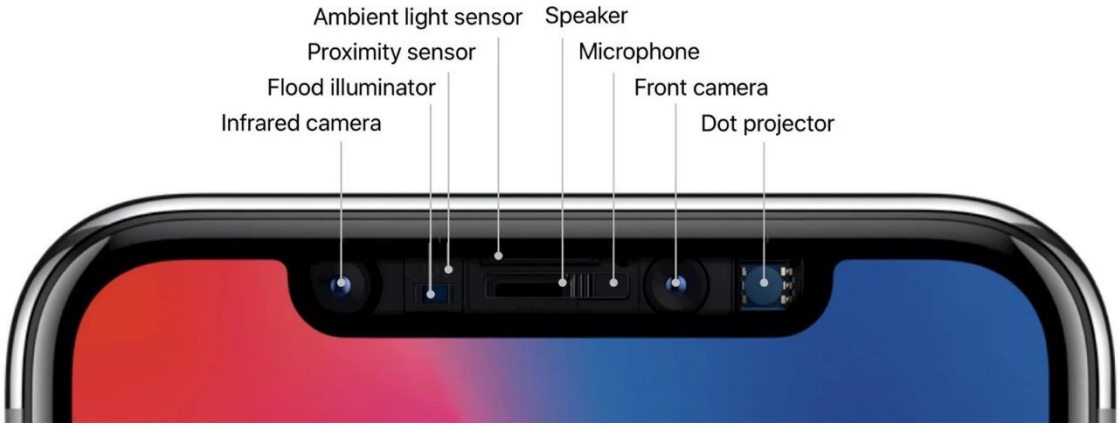


Рисунок 3.2 – Розміщення камери та датчиків у верхній частині сучасного смарфтону

Оскільки процес верифікації та розблокування повинен проходити максимально швидко та комфортно для користувача, пропонується **два підходи** у вирішенні цього питання:

1. Розташування інфрачервоної камери та датчика в нижній частині екрана (актуально при розпізнаванні вен пальця – немає необхідності тягтися до верхньої частини екрана, коли користувач бере в руки пристрій) (Рис. 3.3, а).
2. Розташування інфрачервоної камери і датчика зі зворотного боку телефону, там де розташовані модулі основної камери (зручно сканувати вени долоні чи зап'ястя, тримаючи телефон в іншій руці) (Рис. 3.3, б).

Вже зараз виробники телефонів навчилися вбудовувати камери безпосередньо під дисплей смартфона. Це дозволить візуально приховати датчики пропонованої біометричної системи (див. Рис 3.3, а), а також не заважати апаратним або сенсорним кнопкам, які також розташовані в нижній частині екрана.

Ймовірно, у майбутньому решта датчиків також буде поміщено виробниками під екран, що дозволить відмовитися від широких рамок.

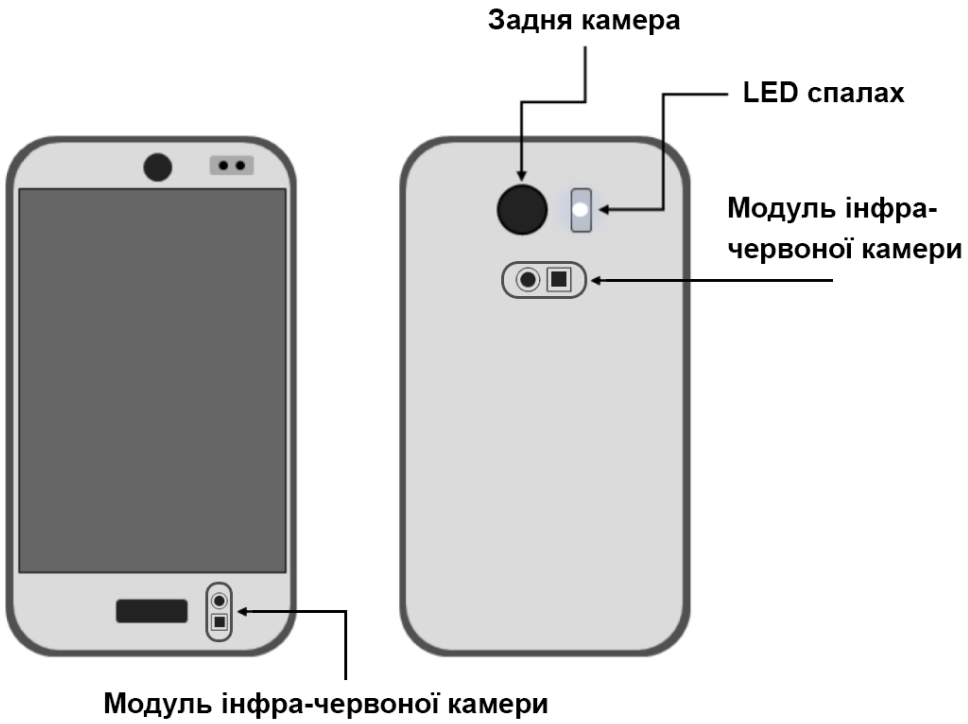


Рисунок 3.3 – Пропоноване розташування функціональних компонентів біометричної системи сканування вен: а) вид спереду, б) вид ззаду

Система була спроектована згідно зі схемами на Рис. 3.4 та Рис. 3.5. Як видно з рисунків, система складається з кількох підсистем.

Процес розпізнавання починається із отримання зразка зап'ястя або пальця користувача через біометричний датчик смартфона – камеру ближнього інфрачервоного спектру. За це відповідає **підсистема захоплення та отримання даних.** Потім отримане зображення обробляється у два етапи (**підсистема обробки даних**): зображення попередньо обробляється та виділяються ключові точки. Вилучені унікальні ознаки зберігаються у базі даних або пам'яті телефону (**підсистема зберігання даних**) і порівнюються для подальшої верифікації користувача (**підсистеми порівняння** та **прийняття рішень**).

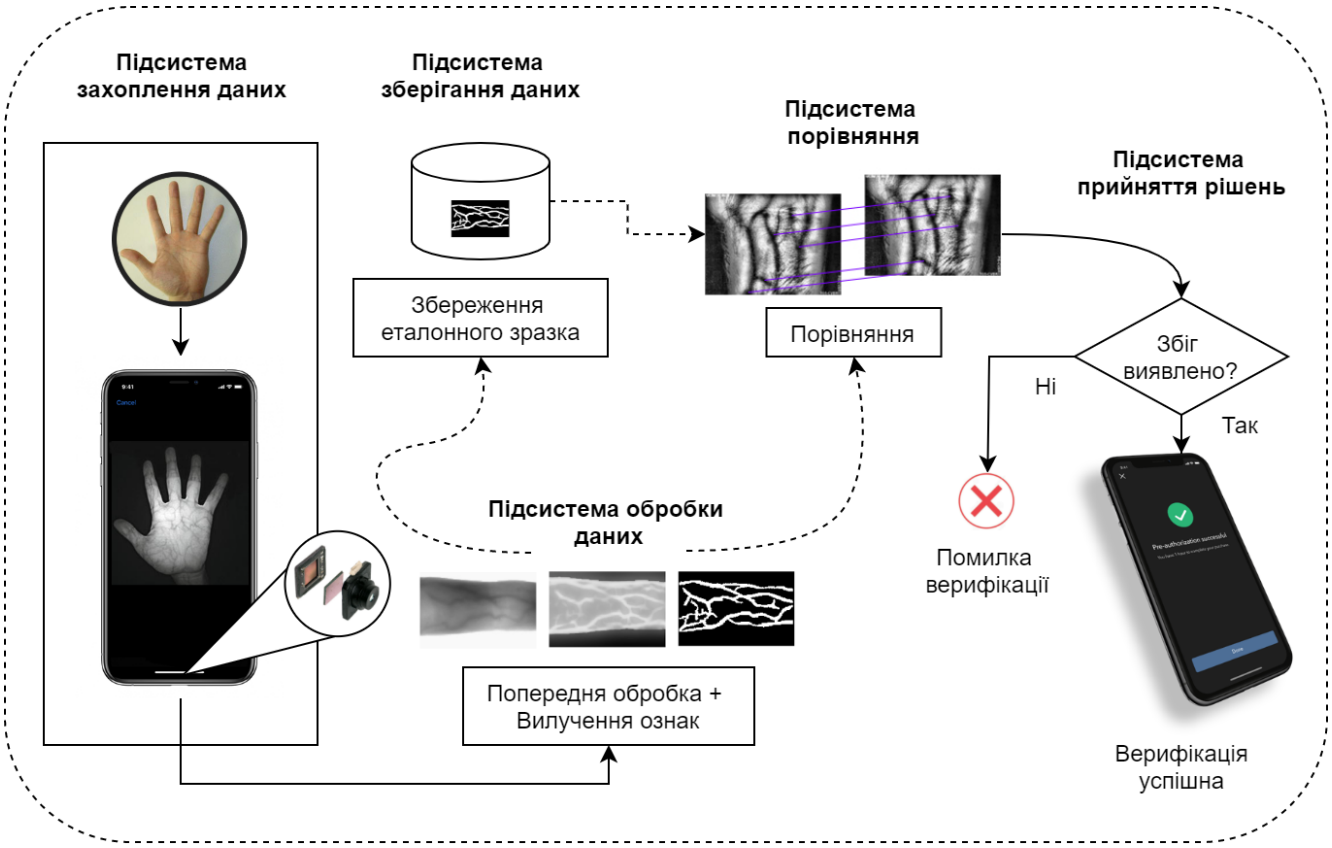


Рисунок 3.4 – Функціональна схема розробленої біометричної системи розпізнавання за рисунком вен для смартфона

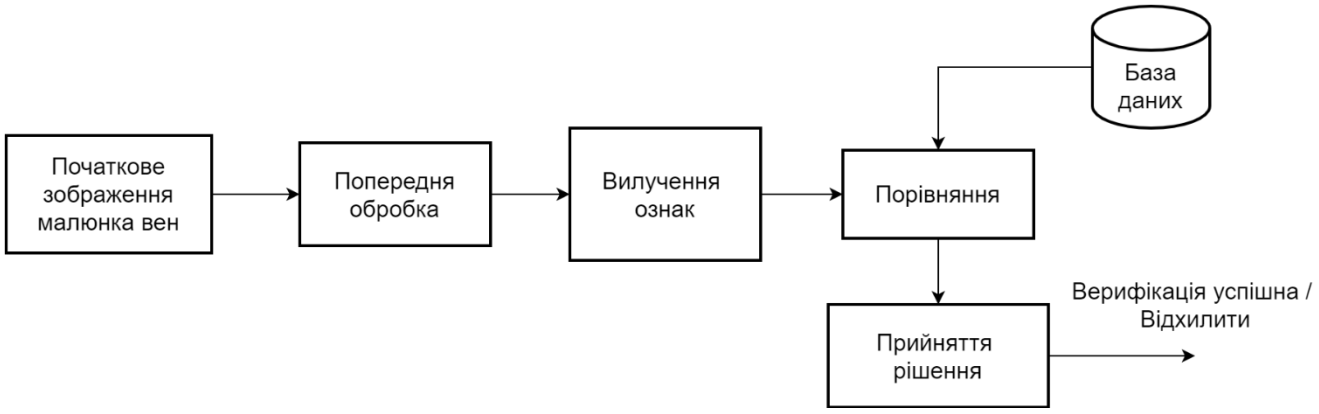


Рисунок 3.5 – Структурная схема розробленої біометричної системи розпізнавання за рисунком вен

3.2.1 Підсистема захоплення та отримання зображення

Камера ближнього інфрачервоного діапазону та світлодіодний індикатор ближнього інфрачервоного діапазону (Light Emitting Diode), необхідні для біометричної системи розпізнавання, показані на Рис. 3.6. ІЧ-камера здатна працювати при будь-якому видимому людині освітленні. Видиме світло не може засліпити таку камеру, а відсутність світла їй не завада за наявності власного невидимого людському оку джерела світла. Простими словами, ІЧ-камери можуть бачити у повній темряві. IR-проектор у смартфонах випромінює інфрачервоне світло певної довжини хвилі. Щоб він не був помітний людському оку, використовують довжини хвиль 850 нм та 940 нм.

Рисунок 3.6 – Приклад модуля ІЧ-камери у розібраному вигляді

3.2.2 Підсистема обробки даних

Першим етапом у створенні біометричного шаблону (Рис. 3.7) є фільтрація вихідного графічного зображення та виділення області інтересу (OI). Фільтрація дозволяє виділити значні області вен та знизити області шумів та відблисків. Для таких завдань загальноприйнятим є використання алгоритму дискретного перетворення Фур'є.

Наступним етапом проводиться бінаризація, яка потрібна для приведення всіх зображень до єдиного вигляду та зменшення впливу різного фокусування та

контрастності зображення. При бінаризації областей відсікається частина шумів з використанням так званої маски шуму.

Для збільшення контрастності вен, а також зменшення високочастотного шуму, були застосовані кілька програмних фільтрів. Нижче наведено реалізацію метода ***filtering()***, в якому використовуються деякі функції бібліотеки OpenCV, що призначені для фільтрації та попередньої обробки зображень.

```
private void filtering() {
        Mat enhanced, floatGray, blur, num, den;

        enhanced = new Mat();
        floatGray = new Mat();
        blur = new Mat();
        num = new Mat();
        den = new Mat();

        img1.convertTo(floatGray, CvType.CV_32F, 1.0 / 255.0);
        Imgproc.GaussianBlur(floatGray, blur, new Size(0, 0), 10);
        Core.subtract(floatGray, blur, num);

        Imgproc.GaussianBlur(num.mul(num), blur, new Size(0, 0), 20);
        Core.pow(blur, 0.5, den);
        Core.divide(num, den, enhanced);
        Core.normalize(enhanced, enhanced, 0.0, 255.0, Core.NORM_MINMAX, -
1);
        enhanced.convertTo(enhanced, CvType.CV_8UC1);

        // Low-pass filter
        Mat gaussian = new Mat();
        Imgproc.GaussianBlur(enhanced, gaussian, new Size(0, 0), 3);

        // High-pass filter on computed low-pass image
        Mat laplace = new Mat();
        Imgproc.Laplacian(gaussian, laplace, CvType.CV_32F, 19, 0, 0);

        double lapMin, lapMax;
        Core.MinMaxLocResult r = Core.minMaxLoc(laplace);
```

```
        lapMin = r.minVal;
        lapMax = r.maxVal;
        double scale = 0;
        if (android.os.Build.VERSION.SDK_INT >=
android.os.Build.VERSION_CODES.N) {
            scale = 127 / Double.max(-lapMin, lapMax);
        }
        laplace.convertTo(laplace, CvType.CV_8U, scale, 128);

        // Thresholding using empirical value of 150 to create a vein mask
        Mat mask = new Mat();
        Imgproc.threshold(laplace, mask, THRESHOLD, 255,
Imgproc.THRESH_BINARY);

        // Clean-up the mask using open morphological operation
        Imgproc.morphologyEx(mask, mask, Imgproc.MORPH_OPEN,
                Imgproc.getStructuringElement(Imgproc.MORPH_ELLIPSE, new
Size(5, 5)));

        // Connect the neighboring areas using close morphological
operation
        Mat connected = new Mat();
        Imgproc.morphologyEx(mask, mask, Imgproc.MORPH_CLOSE,
                Imgproc.getStructuringElement(Imgproc.MORPH_ELLIPSE, new
Size(11, 11)));

        // Blurry the mask for a smoother enhancement
        Imgproc.GaussianBlur(mask, mask, new Size(15, 15), 0);

        // Blurry a little bit the image as well to remove noise
        Imgproc.GaussianBlur(enhanced, enhanced, new Size(3, 3), 0);

        // The mask is used to amplify the veins
        img1 = enhanced;
        double[] newPixel;
        double coeff;
        for (int i = 0; i < mask.rows(); i++) {
            for (int j = 0; j < mask.cols(); j++) {
                newPixel = mask.get(i, j);
```

```
                coeff = (1.0 - (mask.get(i, j)[0] / 255.0)) * BRIGHT + (1 -
DARK);
                newPixel[0] = coeff * enhanced.get(i, j)[0];
                img1.put(i, j, (newPixel[0] > 255) ? 255 : newPixel[0]);
            }
        }
    }
```

Жодних подальших кроків для попередньої обробки не вживалося. Важливо відзначити, що виділення області інтересу (OI) не вимагалося через відмінну ізоляцію від фону, отриманої за допомогою камери та короткої дистанції. Однак це, ймовірно, покращить продуктивність системи і є моментом, який слід враховувати в майбутньому.

Отримане оброблене зображення розбивається на ділянки дискретизації із зазначенням координат контрольних точок, кутів поворотів ліній, та записується у зашифрованому вигляді у файл, який і є математичною моделлю. Вочевидь, що відновити вихідне графічне зображення рисунка вен долоні неможливо.

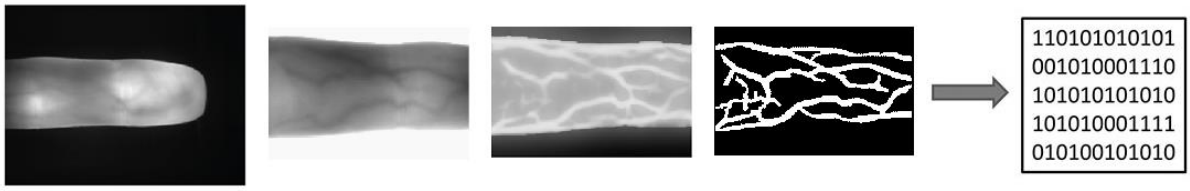


Рисунок 3.7 – Створення біометричного шаблону

3.2.3 Підсистема зберігання даних

Еталонні шаблони рисунка вен повинні зберігатися в ізольованому сховищі даних, у випадку пристроїв, що працюють на ОС Android, йдеться про так зване безпечне середовище виконання (Trusted Execution Environment, **TEE**). Наприклад, усі дані відбитків пальців також зберігаються у середовищі TEE.

TEE – це окрема ізольована область апаратного забезпечення телефону. Вона може використовувати власний процесор та пам'ять, або віртуалізований екземпляр

на основному ЦП. Для того, щоб її підтримувати, Google використовує Trusty TEE – маленьку та ефективну ОС, яка, відповідно, називається **Trusty OS** та використовує апаратні можливості TEE та драйвери ядра, що дозволяють їй взаємодіяти із системою в цілому. Trusty та Android працюють паралельно один одному. Ізоляція Trusty захищає її від шкідливих додатків, встановлених користувачем, та потенційних вразливостей, які можуть бути виявлені в Android [45-46].

Для спрощення експерименту (не для реальних систем біометричної верифікації) еталонний зразок являє собою зображення формату ".jpg", попередньо збережене у внутрішній у пам'яті Android-пристрою для швидкого доступу.

3.2.4 Підсистеми порівняння та прийняття рішень

Для процесу аутентифікації / верифікації (порівняння користувачів 1:1) унікальні ознаки, вилучені з раніше визначеного зразка рисунка вен користувача, порівнюються із зображенням, що отримується в реальному часі, тобто ключові точки рисунка вен (Рис. 3.8, ліворуч) порівнюються з ключовими точками, отриманими з відеозахоплення (Рис. 3.8, праворуч). Цей процес відображається на екрані пристрою для візуалізації.

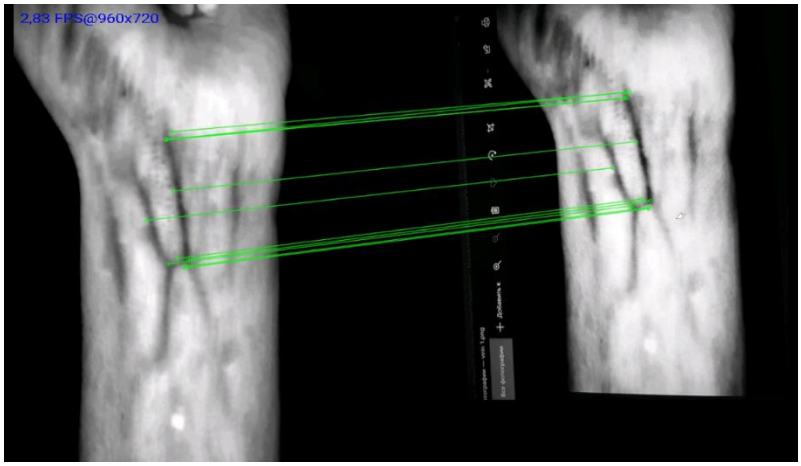


Рисунок 3.8 – Процес порівняння захопленого зображення з еталонним зразком

З метою прийняття рішення, чи була верифікація успішною, після порівняння характеристик був реалізований поріг оцінки кількості знайдених особливих точок:

$$\text{Верифікація успішна} = \begin{cases} \text{Ні}, & \text{якщо } p < \delta \\ \text{Так}, & \text{якщо } p \geq \delta \end{cases}, \tag{3.1}$$

де: p – кількість знайдених особливих точок;

δ – вибрана гранична кількість унікальних особливих точок.

У методі ***recognizeFeatures()***, наведеному нижче, реалізований функціонал вилучення особливих точок, обчислення дескрипторів та їх порівняння.

```
// Метод для распознавания и сравнения
    private Mat recognizeFeatures(Mat aInputFrame) {
        // Преобразование изображения в оттенки серого
        Imgproc.cvtColor(aInputFrame, aInputFrame, Imgproc.COLOR_RGB2GRAY);

        // Находим ключевые точки и вычисляем дескрипторы
        descriptors2 = new Mat();
        keyPoints2 = new MatOfKeyPoint();
        detector.detect(aInputFrame, keyPoints2);
        descriptorExtractor.compute(aInputFrame, keyPoints2, descriptors2);

        // Сравниваем дескрипторы
        MatOfDMatch matches = new MatOfDMatch();
        if (img1.type() == aInputFrame.type()) {
            matcher.match(descriptors1, descriptors2, matches);
        } else {
            return aInputFrame;
        }

        // Вычисляем минимальное и максимальное значения
        List<DMatch> matchesList = matches.toList();
        double maxDist = 0.0;
        double minDist = MIN_DISTANCE;
```

```
        for (int i = 0; i < matchesList.size(); i++) {
            double dist = matchesList.get(i).distance;
            if (dist == 0) continue;
            if (dist < minDist)
                minDist = dist;
            if (dist > maxDist)
                maxDist = dist;
        }

        // Находим лучшие совпадения
        LinkedList<DMatch> goodMatchesList = new LinkedList<>();
        for (int i = 0; i < matchesList.size(); i++) {
            if (matchesList.get(i).distance <= (1.5 * minDist))
                goodMatchesList.addLast(matchesList.get(i));
        }

        MatOfDMatch goodMatches = new MatOfDMatch();
        goodMatches.fromList(goodMatchesList);

        // Отрисовываем результат
        Mat outputImg = new Mat();
        MatOfByte drawnMatches = new MatOfByte();
        if (aInputFrame.empty() || aInputFrame.cols() < 1 ||
aInputFrame.rows() < 1) {
            return aInputFrame;
        }
        Features2d.drawMatches(img1, keyPoints1, aInputFrame, keyPoints2,
goodMatches,
                outputImg, GREEN, RED, drawnMatches,
Features2d.NOT_DRAW_SINGLE_POINTS);
        Imgproc.resize(outputImg, outputImg, aInputFrame.size());

        Log.d("LOG!", "Number of good key points= " +
goodMatchesList.size());

        // Верификация успешна
        if (goodMatchesList.size() >= MIN_MATCHES) {
            endTime = System.currentTimeMillis();
```

```
            Intent intent = new Intent(MainActivity.this,
SuccessActivity.class);
            String info = getString(R.string.toast_algorithm_used) + " " +
descriptorType
                    + "\n" + getString(R.string.toast_hamming_distance) + "
" + MIN_DISTANCE
                    + "\n" + getString(R.string.toast_minimum_good_matches)
+ " " + MIN_MATCHES
                    + "\n" + getString(R.string.toast_matches_found) + " "
+ goodMatchesList.size()
                    + "\n" + getString(R.string.toast_time_elapsed) + " "
                    + (endTime - startTime) / 1000 + " c";
            intent.putExtra("info", info);
            startActivity(intent);
        }
        return outputImg;
    }
```

Основна логіка додатку, включаючи описані раніше методи, міститься в класі **MainActivity.java**, повний лістинг якого наведено в Додатку А. Лістинг класу **SettingsActivity.java**, що відповідає за налаштування та параметри порівняння, наведено в Додатку Б.

3.3 Інтерфейс користувача

Після запуску додатка, перше, що побачить користувач – це головний екран (Рис. 3.9). На ньому відображені базові підказки та поточні параметри (алгоритм, що використовується для обчислення дескрипторів, відстань Хеммінга, мінімальна кількість особливих точок для розпізнавання). Нижче розташована область для завантаження еталонного зразка рисунка вен користувача (зображення вибирається з галереї пристрою) та вікно попереднього перегляду камери, яке стає активним відразу після завантаження еталонного зразка та отримання необхідних дозволів доступу до камери від користувача.

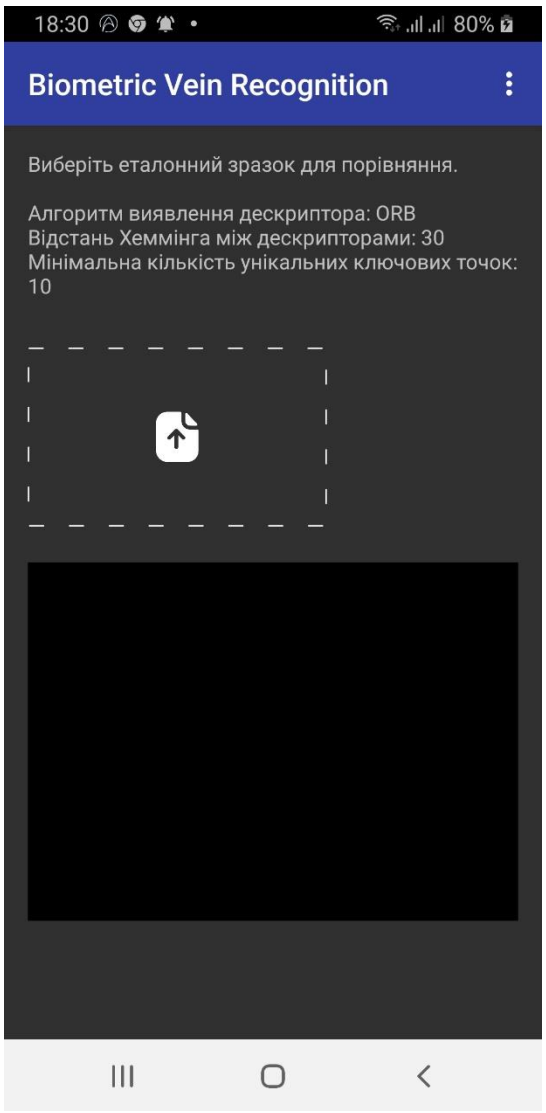


Рисунок 3.9 – Головне вікно додатку

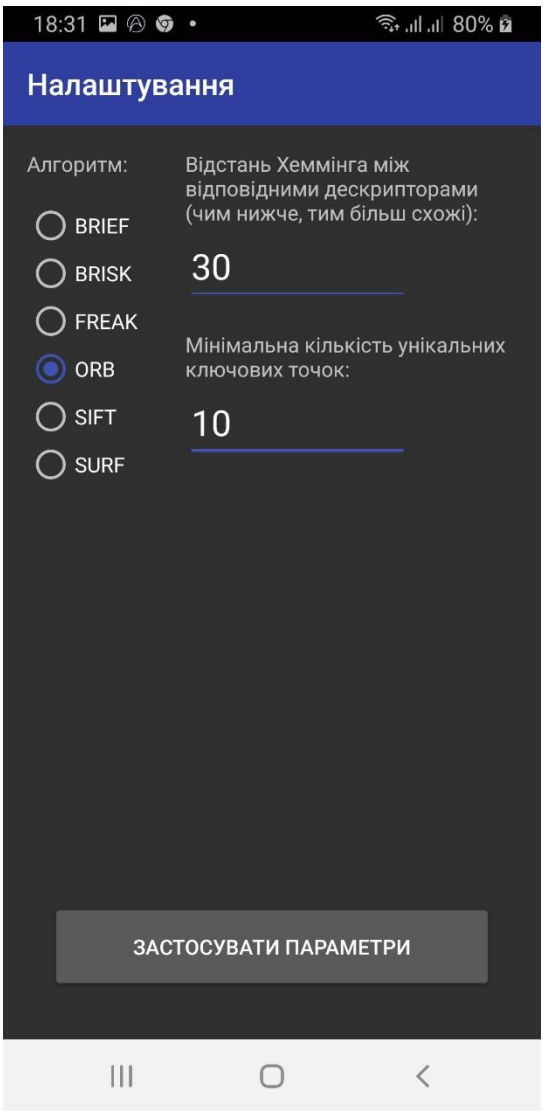


Рисунок 3.10 – Вікно налаштувань

Користувач може перейти на екран налаштувань (Рис. 3.10), відкривши меню в правому верхньому куті. Тут є можливість обрати необхідний алгоритм, параметри та зберегти вибрані установки. Відразу після завантаження еталонного зразка користувачем починається процес аутентифікації шляхом порівняння двох зображень. Візуалізація результатів порівняння представлена у вигляді двох розташованих поруч зображень (ліворуч – еталонний зразок, праворуч – що порівнюється), та з відображеними (зеленим кольором) лініями, що пов'язують знайдені відповідні особливі точки (Рис. 3.11).

У разі успішної верифікації користувач буде повідомлений шляхом появи відповідного екрана (Рис. 3.12). У спливаючому Toast-повідомленні вказується

використаний алгоритм, відстань Хеммінга, кількість мінімальних особливих точок, витрачений час, кількість знайдених зв'язків у процесі верифікації.

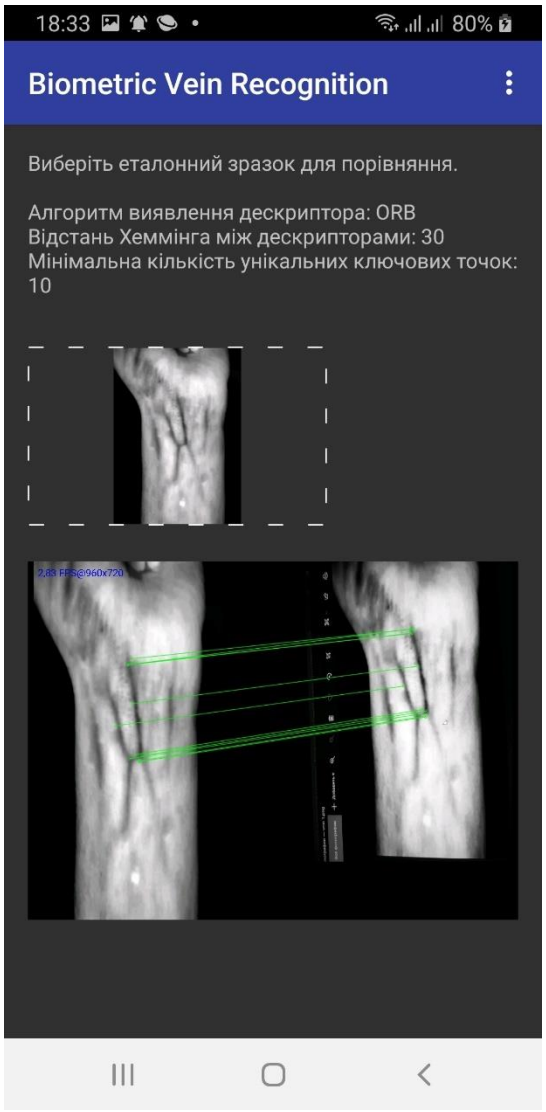


Рисунок 3.11 – Процес порівняння еталонного зразка з одержуваним з камери

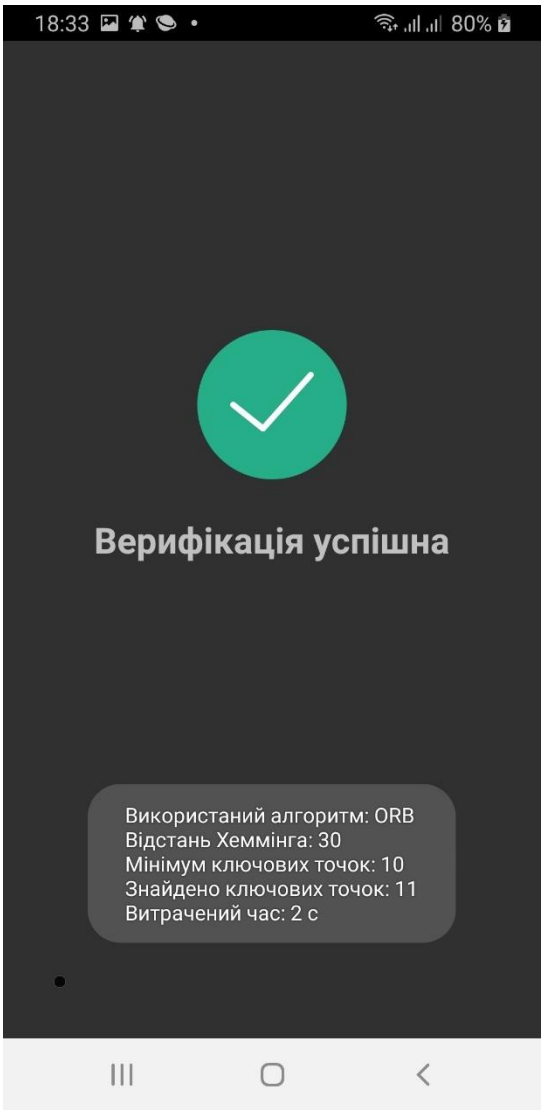


Рисунок 3.12 – Екран додатку, що сигналізує про те, що верифікація була успішною

3.4 Результати експерименту

В рамках експерименту був протестований процес аутентифікації одного користувача 100 разів. У тестуванні використовувався алгоритм **ORB**.

Оскільки запропонована біометрична система розпізнавання за венозном рисунком передбачає наявність вмонтованої в корпус пристрою камери ближнього інфрачервоного діапазону і LED індикатора, через відсутність останніх було вирішено використовувати основну (задню) камеру пристрою, тим самим імітуючи роботу ІЧ-камери. Загальний принцип функціонування системи при цьому залишається незмінним.

В якості еталонного зразка було взято зображення вен зап'ястя руки користувача роздільною здатністю 756 × 1008 у відтінках сірого, попередньо знятого на відстані 10-15 см на задню камеру пристрою. Вибір області зап'ястя для розпізнавання пояснюється наявністю складнішої структури вен (порівняно з венами пальця), отже більшою ефективністю (може бути знайдена більша кількість особливих точок). Зображення було збережено у внутрішній пам'яті пристрою у форматі ".jpg".

Дослідним шляхом були визначені та використані у ході експерименту наступні значення:

відстань Хеммінга між відповідними дескрипторами (чим значення нижче, тим більш схожі) – 30;

мінімальна кількість особливих точок для успішної верифікації – 11.

Витрачений час, кількість знайдених збігів і кількість помилкових збігів можуть варіюватися в залежності від заданих вище значень та методу (алгоритму) пошуку спеціальних точок та їх дескрипторів. У реальних системах кількість особливих точок (так само як і поріг спрацьовування), очевидно, мають бути значно більшими.

За результатами тестів цей підхід дає досить правильний результат з високою точністю (у тому числі при обертанні, зміні масштабу зображення та перспективних спотвореннях).

Середній час процесу верифікації становив **2-3 с** (бували значні відхилення).

На Рис. 3.13 показані графіки FAR та FRR, а також коефіцієнт еквівалентної ймовірності помилок **EER**, що становить приблизно 12%.

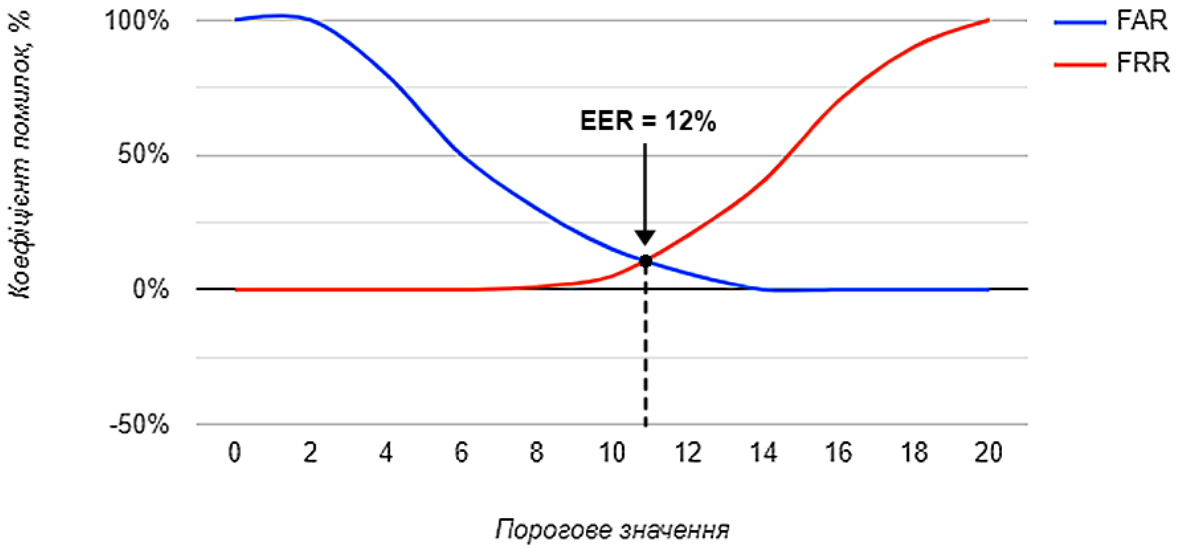


Рисунок 3.13 – Криві FAR, FRR та EER розробленої біометричної системи верифікації за венозним рисунком для смартфону

3.5 Висновки

У цьому розділі обґрунтовано вибір програмних засобів та бібліотек для розробки запропонованої системи біометричної верифікації користувача за венозним рисунком для смартфону. Центральним місцем під час розробки стала бібліотека алгоритмів комп’ютерного зору та обробки зображень OpenCV. Описано загальну структуру, основні підсистеми та функціональність розробленого програмного забезпечення. В результаті розробло додаток "Biometric Vein Recognition" для мобільних пристроїв під ОС "Android" та проведено його тестування.

ВИСНОВКИ

У дипломній роботі було досліджено технологію біометричної ідентифікації особистості за венозним рисунком руки – найбільш перспективний та багатообіцяючий вид біометрії.

Запропоновані у роботі наукові підходи та програмно-апаратні рішення дозволили спроектувати та реалізувати біометричну систему верифікації за допомогою бібліотеки OpenCV для мобільних пристроїв під управлінням ОС Android. Розроблений додаток здатний за лічені секунди в режимі реального часу порівнювати відсканований рисунок вен зап'ястя руки з еталонним шаблоном, імітуючи процес авторизації користувача.

В рамках дослідження також було проаналізовано існуючі методи біометричної ідентифікації, проведено їх порівняльний аналіз. Було розглянуто 2 методи підвищення точності та ефективності біометричної системи ідентифікації за венозним рисунком.

Тим не менш, не дивлячись на те, що показник еквівалентної ймовірності помилок EER та швидкість процесу верифікації є далекими від прийнятних, запропонована система може бути покращена, а точність розпізнавання підвищено за рахунок подальших розробок. Крім того, вона може бути інтегрована з іншими біометричними системами, що існують, в смартфонах.

Подібна система, вбудована в смартфон і працююча в реальному часі, може використовуватися, наприклад, для здійснення онлайн-платежів, підтвердження важливих дій і, перш за все, розблокування екрану пристрою безконтактним шляхом.

СПИСОК ЛІТЕРАТУРИ І ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Тумоян Е. П. Разработка и исследование метода создания и использования хранилищ ключевой информации на основе распознавания биометрических образов. – Таганрог, 2003. – 158 с.
2. Біометрія [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Біометрія
3. Биометрия - как это работает? [Електронний ресурс]. – Режим доступу: http://fingramota.by/ru/guide/practical/biometria
4. Общая характеристика биометрических технологий [Електронний ресурс]. – Режим доступу: https://www.biolink.ru/technology/biometric.php
5. В. Моржаков, А. Мальцев. Современные биометрические методы идентификации [Електронний ресурс]. – Режим доступу: http://masters.donntu.org/2013/fknt/fomenko/library/article4.htm
6. Биометрическая идентификация [Електронний ресурс]. – Режим доступу: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html
7. Global Biometrics Market Report and Forecast 2021-2026 [Електронний ресурс]. – Режим доступу: https://www.expertmarketresearch.com/reports/biometrics-market
8. Biometric data: 96 countries ranked by how they’re collecting it and what they’re doing with it [Електронний ресурс]. – Режим доступу: https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/
9. Методи біометричної автентифікації для використання в паспортній системі / І.Д. Горбенко, І.В. Олешко // Прикладна радіоелектроніка: наук.-техн. журнал. – 2011. Том 10. № 2. – С. 233–239. [Електронний ресурс]. – Режим доступу: https://openarchive.nure.ua/bitstream/document/4269/1/233-239.pdf

10. Sayeed S., Kamel N. S., Besar R. A Sensor-Based Approach for Dynamic Signature Verification using Data Glove, 2009. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/41845983_A_Sensor-Based_Approach_for_Dynamic_Signature_Verification_using_Data_Glove

11. С.О. Баранов, Д.Б. Абрамов. Технология биометрической аутентификации пользователя по венозному рисунку кистей рук, 2017. [Електронний ресурс]. – Режим доступу: https://www.researchgate.net/publication/319382974_PALM_VEIN_PATTERN_BIOMETRIC_AUTHENTICATION_TECHNOLOGY

12. Гемоглобін [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Гемоглобін

13. Watanabe, M. Palm vein authentication. [Електронний ресурс]. – Режим доступу: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.135.8983&rep=rep1&type=pdf

14. Alexandre Sierro, Pierre Ferrez, Pierre Roduit. Contact-less Palm/Finger Vein Biometrics. [Електронний ресурс]. – Режим доступу: https://subs.emis.de/LNI/Proceedings/Proceedings245/145.pdf

15. Fujitsu PalmSecure [Електронний ресурс]. – Режим доступу: https://www.fujitsu.com/ru/solutions/business-technology/security/product/palmsecure/

16. Fujitsu представляет новый биометрический терминал PalmSecure ID Access [Електронний ресурс]. – Режим доступу: https://fujitsu-online-shop.ru/news/fujitsu-introduces-new-biometric-palmsecure-id-terminal-access/

17. Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. – 2-ге вид., доп. / В. П. Захаров, В. І. Рудешко. – Львів: ЛьвДУВС, 2015. – 492 с [Електронний ресурс]. – Режим доступу: http://dspace.lvduvs.edu.ua/bitstream/1234567890/6/1/%D0%97%D0%B0%D1%85%D0%B0%D1%80%D0%BE%D0%B2%20%D0%B1%D1%96%D0%BE

%D0%BC%D0%B5%D1%82%D1%80%D0%B8%D1%87%D0%BD%D1%96%20%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97.pdf

18. Авторизация по венозному рисунку пальца как замена банковских карт [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/223585/

19. Выпущен LG G8 ThinQ: поддержка распознавания вен, известная как Palm ID [Електронний ресурс]. – Режим доступу: https://ru.chinacoupon.info/lg-g8-thinq-released-supports-vein-recognition-known-as-palm-id.html

20. Future Face ID could map a user's veins to foil 'evil twin' attack [Електронний ресурс]. – Режим доступу: https://appleinsider.com/articles/20/07/21/future-face-id-could-map-a-users-veins-to-foil-evil-twin-attack

21. Face ID в iPhone сможет сканировать венозный рисунок на лице [Електронний ресурс]. – Режим доступу: https://mobidevices.mediasole.ru/face_id_v_iphone_smozhet_skanirovat_venoznyy_risunok_na_lice

22. Комп'ютерний зір [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Комп%27ютерний_зір

23. Прохоренок Н. А. OpenCV и Java. Обработка изображений и компьютерное зрение. — СПб.: БХВ-Петербург, 2018. — 320 с.: ил.

24. Кэлер А., Брэдски Г. Изучаем OpenCV 3 / пер. с анг. А. А. Слинкина. – М.: ДМК Пресс, 2017. – 826 с.: ил.

25. Как это работает? | Компьютерное зрение [Електронний ресурс]. – Режим доступу: https://hi-news.ru/eto-interesno/kak-eto-rabotaet-kompyuternoe-zrenie.html

26. Harris Corner Detection [Електронний ресурс]. – Режим доступу: https://opencv24-python-tutorials.readthedocs.io/en/latest/py_tutorials/py_feature2d/py_features_harris/py_features_harris.html#harris-corners

27. Детекторы углов [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/244541/

28. Introduction to SIFT (Scale-Invariant Feature Transform) [Електронний ресурс]. – Режим доступу: https://opencv24-python-tutorials.readthedocs.io/en/latest/py_tutorials/py_feature2d/py_sift_intro/py_sift_intro.html

29. Толеген М. О. Разработка алгоритма построения панорам [Стаття]. – Режим доступу: https://core.ac.uk/download/pdf/80134977.pdf

30. Построение SIFT дескрипторов и задача сопоставления изображений [Електронний ресурс]. – Режим доступу: https://habr.com/ru/post/106302/

31. Обнаружение особых точек в SURF основано на вычислении детерминанта матрицы Гессе (гессиана) [Стаття]. – Режим доступу: http://www.rusnauka.com/17_ENXXI_2016/Informatica/1_213256.doc.htm

32. Обнаружение устойчивых признаков изображения: метод SURF [Електронний ресурс]. – Режим доступу: https://studentopedia.ru/informatika/obnaruzhenie-ustojchivih-priznakov-izobrazheniya-metod-surf---razrabotka-sistemi-avtomaticheskogo.html

33. Introduction to SURF (Speeded-Up Robust Features) [Електронний ресурс]. – Режим доступу: https://opencv24-python-tutorials.readthedocs.io/en/latest/py_tutorials/py_feature2d/py_surf_intro/py_surf_intro.html

34. FAST Algorithm for Corner Detection [Електронний ресурс]. – Режим доступу: https://opencv24-python-tutorials.readthedocs.io/en/latest/py_tutorials/py_feature2d/py_fast/py_fast.html

35. Т. А. ПАРОМОВА, И. Я. ЗЕЛЕНЕВА, Н. В. ЛУЦЕНКО, Е. А. БИЛЫК. Сравнительный анализ методов определения ключевых точек при поиске изображений по фрагментам [Стаття]. – Режим доступу: http://nbuv.gov.ua/j-pdf/Npdntu_inf_2018_1_11.pdf

36. Сравнение бинарных дескрипторов особых точек изображений в условиях искажений [Стаття]. – Режим доступу: http://oaji.net/articles/2019/2401-1563524429.pdf

37. Calonder, M. BRIEF: binary robust independent elementary features / M. Calonder, V. Lepetit, C. Strecha, P. Fua // European Conference on Computer Vision, – 2010.– Vol. 6314. – P. 778-792. – DOI: 10.1007/978-3-642-15561-1_56.

38. ORB (Oriented FAST and Rotated BRIEF) [Електронний ресурс]. – Режим доступу: https://opencv24-python-tutorials.readthedocs.io/en/latest/py_tutorials/py_feature2d/py_orb/py_orb.html

39. Г. М. НОВІЦЬКИЙ. Розвиток методу ідентифікації особистості за венозним рисунком долоні руки [Стаття]. – Режим доступу: http://ir.lib.vntu.edu.ua/bitstream/handle/123456789/31598/%D0%9D%D0%BE%D0%B2%D1%96%D1%86%D1%8C%D0%BA%D0%B8%D0%B9.pdf?sequence=1&isAllowed=y

40. Joint R&D With University of Tokyo Leads to World's First Thin Image Sensor that Can Measure Fingerprints, Veins, and Pulse Waves [Електронний ресурс]. – Режим доступу: https://www.j-display.com/english/news/2020/20200121.html

41. Обмануть биометрию станет сложнее: датчики начнут измерять пульсовую волну [Електронний ресурс]. – Режим доступу: https://3dnews.ru/1001897

42. Open Source Computer Vision Library [Електронний ресурс]. – Режим доступу: https://opencv.org/

43. Android Studio – the official integrated development environment (IDE) for Android [Електронний ресурс]. – Режим доступу: https://developer.android.com/studio

44. Android Studio User guide [Електронний ресурс]. – Режим доступу: https://developer.android.com/studio/intro

45. Отпечатки пальцев в Android: как они хранятся и насколько это безопасно [Електронний ресурс]. – Режим доступу: http://android.mobile-review.com/articles/51661/

46. Trusty TEE [Електронний ресурс]. – Режим доступу: https://source.android.com/security/trusty