МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет
Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки

СОКОЛІК Максим Анатолійович

Алгоритми ідентифікації користувачів із використанням біометричних даних / User Identification Algorithms Using Biometric Data

спеціальність: 125 – Кібербезпека та захист інформації
освітньо–професійна програма – Кібербезпека

Кваліфікаційна робота

Виконав студент групи КБм –21
М. А. Соколік

Науковий керівник
д. філософії, С. В. Кулина

Кваліфікаційну роботу допущено
до захисту:

«____» _____ ___2025 р.

Завідувач кафедри
_____ В. В. Яцків

ТЕРНОПІЛЬ – 2025

Факультет комп'ютерних інформаційних технологій
Кафедра кібербезпеки
Освітній ступінь «магістр»
спеціальність: 125 – Кібербезпека та захист інформації
освітньо–професійна програма – Кібербезпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ В. В. Яцків
«____» _____ 2024 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ
СОКОЛІК Максим Анатолійович
(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи:
Алгоритми ідентифікації користувачів із використанням біометричних даних / User Identification Algorithms Using Biometric Data
керівник роботи д. філософії С. В. Кулина
затверджені наказом по університету від 20 грудня 2024 року № 938

2. Строк подання студентом закінченої кваліфікаційної роботи 5 грудня 2025 р.

3. Вихідні дані до кваліфікаційної роботи: завдання на випускну кваліфікаційну роботу студента, наукові статті, технічна література.
4. Основні питання, які потрібно розробити:
– провести аналіз методів аутентифікації, зокрема багатофакторної аутентифікації;
– обґрунтувати використання двохфакторної аутентифікації, одним із методів якої є біометрична аутентифікація;
– проаналізувати показники ефективності біометричних систем аутентифікації для оцінки систем біометричної аутентифікації;
– дослідити сучасні алгоритми виділення ознак та визначити ключові властивості, що впливають на їх вибір;
– розробити алгоритм ідентифікації користувача із використанням біометричних даних;
– спроектувати систему ідентифікації користувачів із використанням біометричних даних та провести моделювання її роботи.
5. Перелік графічного матеріалу у роботі:
– реалізація методу локальних бінарних шаблонів;
– алгоритм роботи функції втрати на парах;
– алгоритм роботи функції втрати на трійках;
– алгоритм ідентифікації користувачів із використанням біометричних модальностей;
– структурна схема системи ідентифікації;
– генерація імені файлу з ембедінгом;
– порівняння двох файлів з ембедінгами.

6. Консультанти розділів кваліфікаційної роботи

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

7. Дата видачі завдання 20 грудня 2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строки виконання етапів кваліфікаційної роботи	Примітка
1	Аналіз та теоретичні основи біометричної ідентифікації	12.2024 р. – 03.2025 р.	
2	Дослідження архітектур глибокого навчання та алгоритми реалізації	03.2025 р. – 06.2025 р.	
3	Система ідентифікації користувача за біологічними модальностями	06.2025 р. – 11.2025 р.	

Студент _____ Соколік М. А.
підпис

Керівник роботи _____ д. філософії, КУЛИНА С. В.
підпис

АНОТАЦІЯ

Соколік М. А. Алгоритми ідентифікації користувачів із використанням біометричних даних. – Рукопис.

Дослідження на здобуття освітнього ступеня «магістр» за спеціальністю 125 «Кібербезпека та захист інформації», освітньо-професійна програма «Кібербезпека». – Західноукраїнський національний університет, Тернопіль, 2025.

У роботі досліджено методи аутентифікації та розроблено алгоритм двохфакторної аутентифікації користувачів, що поєднує біометричну верифікації користувача із використанням паролю, та забезпечує достатній рівень достовірності та захисту.

Ключові слова: АУТЕНТИФІКАЦІЯ, ВЕРИФІКАЦІЯ, ВИДІЛЕННЯ ОЗНАК, ЕМБЕДІНГИ, БІОМЕТРИЧНІ МОДАЛЬНОСТІ, ЗАХИСТ БІОМЕТРИЧНИХ ДАНИХ.

ABSTRACT

Sokolic M. A. User Identification Algorithms Using Biometric Data. – Manuscript.

Doctoral studies for the education level «Master» with the title 125 «Cybersecurity and Information Protection». – West Ukrainian National University, Ternopil, 2025.

The thesis investigates authentication methods and develops a two-factor user authentication algorithm that combines biometric verification with password usage, ensuring a sufficient level of trustworthiness and protection.

Keywords: AUTHENTICATION, VERIFICATION, FEATURE EXTRACTION, EMBEDDINGS, BIOMETRIC MODALITIES, BIOMETRIC DATA PROTECTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

MFA – Multi–Factor Authentication, багатофакторної автентифікації.

TOTP – Time–based One–Time Password, одноразові коди.

AFIS – Automated Fingerprint Identification System, автоматичні ідентифікаційні системи.

FAR – False Acceptance Rate.

FMR – False Match Rate.

FRR – False Rejection Rate.

FNMR – False Non–Match Rate.

DET – Detection Error Trade–off.

EER – Equal Error Rate.

LBP – Local Binary Patterns, локальні бінарні шаблони.

LBPH – Local Binary Patterns Histograms.

HOG – Histogram of Oriented Gradients, гістограми орієнтованих градієнтів.

CNN – згорткові нейронні мережі.

ВСТУП

Зі зростанням кількості користувачів глобальної мережі та спеціалізованих систем зокрема, значно зріс попит на системи ідентифікації та аутентифікації, що забезпечать доступ до конфіденційних даних тільки тим особам, кому він необхідний. В такій ситуації на перше місце виходять багатофакторні системи ідентифікації та аутентифікації, які складно зламати або пройти в них використовуючи вкрадені дані для доступу.

Однією із категорій таких систем є системи на основі біометричної ідентифікації. Завдяки своїм властивостям вони використовують для входу дані які складно або неможливо підробити і водночас такі, які є простими у використанні. Аутентифікація на основі біометричних властивостей людини таких як риси обличчя, відпечатки пальців, сітківка ока або ДНК є унікальними для кожного користувача, що унеможливлює підміну.

Розробка алгоритмів роботи та систем із біометричною автентифікацією на їх основі ї є актуальним завданням, що потребує дослідження та удосеконалення.

Мета і завдання дослідження. Метою кваліфікаційної роботи є дослідження методів та алгоритмів багатофакторної аутентифікації.

Досягнення визначеної мети передбачає вирішення таких завдань:

– провести аналіз методів аутентифікації, зокрема багатофакторної аутентифікації;

– обґрунтувати використання двохфакторної аутентифікації, одним із методів якої є біометрична аутентифікація;

– проаналізувати показники ефективності біометричних систем аутентифікації для оцінки систем біометричної аутентифікації;

– провести аналіз сучасних алгоритмів виділення ознак та визначити ключові властивості, що впливають на їх вибір;

– розробити алгоритм ідентифікації користувача із використанням біометричних даних;

– спроектувати систему ідентифікації користувачів із використанням біометричних даних та провести моделювання її роботи.

Об’єкт дослідження – процеси ідентифікації та аутентифікації користувачів у сучасних системах аутентифікації.

Предмет дослідження – алгоритми, методи та механізми побудови захищених систем аутентифікації на основі біометричних даних.

Методи досліджень. Для розв’язання поставлених задач у даній кваліфікаційній роботі використано: теоретичний аналіз, алгоритмічний синтез, методи комп’ютерного зору та машинного навчання, експериментальні методи.

Наукова новизна одержаних результатів. Наукова новизна одержаних результатів полягає у розробці алгоритму двохфакторної аутентифікації користувачів, що поєднує біометричну верифікації користувача із використанням паролю, та забезпечує достатній рівень достовірності та захисту.

Практичне значення отриманих результатів. Розроблена система двохфакторної аутентифікації користувача на основі запропонованого у роботі алгоритму та проведено її практичну оцінку.

Публікації та апробація до магістерської роботи.

1. Соколік, М., Гарматюк, В., Кулина С. Методи ідентифікації користувачів із використанням біометричних даних. Інноваційні підходи до розвитку технологій та економіки (IADTE 2025). – Свалява: ЗУНУ, 2025. – С. 215–216.

2. Соколік, М., Кулина С. Аналіз сучасних алгоритмів виділення ознак в біометрії. Захист інформації: Збірник матеріалів науково–практичного симпозіуму, 28.11.2025. – Тернопіль, 2025. – С. 94–96.

1. АНАЛІЗ ТА ТЕОРЕТИЧНІ ОСНОВИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

1.1. Виклики сучасної кібербезпеки та необхідність захисту даних

У сучасному інформаційному суспільстві обсяги та важливість обробки цифрових даних стрімко зростають. Організації та окремі учасники оперують різноманітними даними, що потребують захисту – персональними даними, бізнес–інформацією, державними або науковими таємницями. У той же час зростає кількість кіберзагроз – фішинг, злом облікових записів, атаки «людина посередині», злочини із використанням витоків паролів, соціальна інженерія та інші [1, 3].

У такому контексті ключовим завданням стає забезпечення належного рівня захисту даних та гарантованого контролю доступу до них. Основою такого захисту є підтвердження автентичності користувача – тобто перевірка, що особа, яка входить в систему, справді має право це робити. Не забезпечивши таку перевірку жодна, навіть сама найкраща система шифрування або контроль доступу втрачає сенс, якщо зловмисник зможе видати себе за легітимного користувача.

Одним із методів забезпечення необхідного рівня доступу є застосування багатофакторної автентифікації (Multi–Factor Authentication – MFA). Її основою є те, що користувач має надати два або більше незалежних факторів підтвердження особи перед тим, як отримати доступ до ресурсу або системи [2, 4].

Ідея MFA полягає у тому, що злом одного фактора (наприклад, пароля) сам по собі недостатній для доступу до даних, оскільки зловмиснику доведеться подолати інші, незалежні від першого засоби захисту (рис. 1.1).

Згідно з інформацією Агентства з кібербезпеки США (CISA), застосування MFA зменшує ймовірність успішного злому приблизно на 99 % [5].

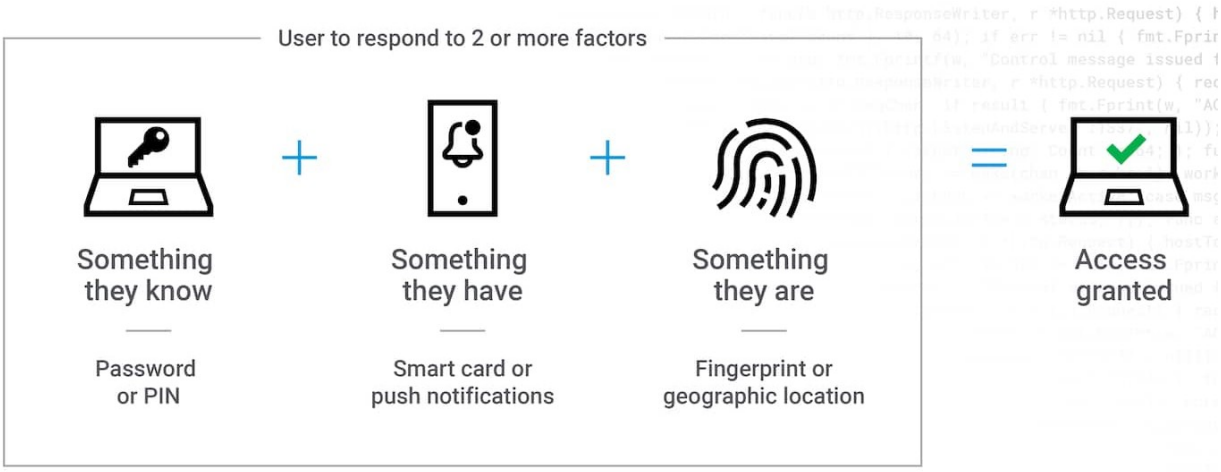

Рисунок 1.1 – Поєднання двох і більше методів автентифікації

Традиційно виділяють декілька ключових категорій факторів автентифікації їх порівняння представлено в таблиці 1.1.

Таблиця 1.1

Порівняння категорій факторів автентифікації

Категорія	**Що це означає**	**Приклади**
Що ви знаєте	Інформація, відома тільки користувачу	Пароль, PIN–код, секретне питання
Що ви маєте	Фізичний або цифровий об’єкт, що належить користувачу	Смартфон, апаратний токен/ключ, смарт–карта
Що ви є	Біометрична характеристика користувача	Відбиток пальця, розпізнавання обличчя, скан сітківки ока
Додаткові фактори		
Де ви є	Місцеперебування	Геолокація
Що ви робите	Різноманітні поведінкові чинники притаманні саме користувачу	Аналіз манери введення, поведінкові біометрії

Кожна категорія з таблиці 1.1 забезпечує одну властивість, яку складно або неможливо відтворити за допомогою іншої. Використання лише однієї категорії недостатньо і саме тут, для ефективного захисту, починають застосовувати комбінацію факторів з різних категорій.

1.2. Методи реалізації MFA

До категорії «**Що ви знаєте**» (англ. “Something you know”) належать фактори автентифікації, що базуються на знанні користувачем певної інформації, яку він має запам’ятати та ввести під час входу в систему [6]. Це може бути будь–який секрет, відомий лише законному користувачу, наприклад пароль або PIN–код, зазвичай ця категорія є обов’язковою складовою багатофакторної авторизації і поєднується з іншими.

До категорії «**Що ви маєте**» (англ. “Something you have”) належать фактори автентифікації, що підтверджують наявність у користувача певного фізичного пристрою або об’єкта, який використовується для доведення його особи [6].

Одним із представників такої категорії є застосування одноразових кодів (Time–based One–Time Password TOTP) [7]. Зазвичай це локально згенеровані короткочасні коди (зазвичай 6 цифр), які змінюються кожні 30 секунд. Завдяки тому, що цей код генерується локально (без інтернет–з'єднання) на пристрої користувача, наприклад через додаток–автентикатор (Google Authenticator, Authy, FreeOTP), забезпечується додаткова надійність, та висока стійкість до перехоплення. Одноразові коди підтримуються багатьма сервісами, проте мають і недоліки. Ключовим з яких є те, що якщо пристрій втрачено або зламано відновити доступ стає надзвичайно складно. Вони працюють наступним чином: коли користувач реєструє MFA в сервісі, він сканує QR–код, що містить початковий секрет. Після цього при кожному вході він вводить пароль + код із своєї програми [8].

Іншим представником категорії «Що ви маєте» є SMS або Email–коди. При їх використанні користувач під час спроби входу отримує одноразовий код або посилання через SMS або лист на електронну пошту. Клік по посиланню або введення коду підтверджує особу. Перевагами такого методу є його простота для користувачів та те, що він не потребує встановлення додаткових програм (якщо користувач уже має телефон/пошту). Але є і недоліки, ключеві з яких уразливість до атаки *SIM–swapping* (захоплення номеру телефону) або

перехоплення SMS [9]. Ну і звичайно, якщо поштовий акаунт зламано, то код може отримати зловмисник. Такий метод використовують банківські сервіси коли надсилають SMS із кодом для підтвердження операції переказу коштів або при вході з нового пристрою.

Схожим є метод використання Push–сповіщенн (Push–based MFA) [6]. Коли користувач намагається увійти кудись, сервер надсилає push–повідомлення до мобільного застосунку (наприклад, Microsoft Authenticator, Duo, Okta Verify). Користувач отримує запит «Підтвердити вхід» чи «Скасувати», і одне натискання підтверджує або відхиляє вхід. Перевагами даного методу є те, що він навіть не потребує введення додаткових кодів, вхід відбувається миттєво. Проте він потребує стабільного інтернет–зв'язку для своєї роботи і якщо користувач випадково натисне «Підтвердити» – може дозволити вхід зловмиснику (наприклад, через соціальну інженерію). Також недоліком є залежність від пристрою. Якщо смартфон вимкнено чи розряджено метод не буде працювати і користувач не зможе отримати доступ [10].

Всі вище згадані способи є дуже зручними для користувачів, не потребують додаткових фінансових витрат, та можуть бути швидко реалізовані, проте вони є менш безпечними порівняно з апаратними чи біометричними факторами.

В свою чергу апаратні токени або як їх ще називають ключі безпеки (Hardware Tokens / Security Keys) це фізичні пристрої (наприклад, USB–ключі або смарт–карти), що зберігають криптографічні ключі або генерують спеціальні коди [11]. Для входу користувач підключає цей апаратний токен або натискає на нього (рис. 1.2).

Рисунок 1.2 – Приклад апаратного ключа безпеки (токена)

Їх використання забезпечує дуже високий рівень безпеки, оскільки для доступу зловмисник має фізично заволодіти апаратним токеном, а сам метод робить неможливим перехоплення ключа чи коду через мережу. Недоліком даного методу є те, що кожен користувач повинен придбати апаратний ключ (його вартість становить від 2 000 грн), а у випадку його втрати необхідно додатковий механізм, щоб підтвердити особу користувача. Існуючий стандарт *FIDO2* дозволяє використовувати USB–ключі або Bluetooth / NFC–токени як один із факторів автентифікації [12].

З перелічених методів найбільш захищеним є застосування апаратних токенів, оскільки кожен такий прилад має свій ключ, тобто можна сказати, що він є одиничним екземпляром, який гарантує захист. Проте його необхідно носити із собою і захищати від спроб фізичної крадіжки. На відміну від апаратних ключів є те, що людина завжди носить із собою, а саме свої біологічні дані.

Саме на методі використання фізичних ознак людини, таких як відбиток пальця, розпізнавання обличчя, райдужка ока, голос та інші базується біометрична автентифікація. Вона забезпечує високу унікальність та зручна у використанні, проте потребує додаткової апаратної підтримки – сканери, камери тощо. При використанні біометричних методів автентифікації ключовим є питання приватності, зберігання та безпеки біометричних шаблонів і якщо біометричні дані скомпрометовано, то їх не можна змінити.

Використання категорій «Де ви є» і «Що ви робите» використовується додатково до вище згаданих методів для підтвердження автентичності. При віддаленій роботі перевірка місця входу, а також поведінкових характеристик користувача зменшує ймовірність витоку даних. в основі поведінкової автентифікація лежить активний моніторинг поведінкових характеристик користувача швидкість набору тексту, рухи миші, шаблони навігації, взаємодія зі сторінками, не лише при початковому вході а і під час сеансу. Якщо виявляється “аномальна” поведінка, система може запросити повторну верифікацію або обмежити доступ. Перевагами такого методу є додатковий рівень безпеки протягом всієї сесії та можливість виявляти атаки після

початкового входу. До його недоліків відносять складність реалізації, необхідність аналізу великих обсягів даних, можливість хибних спрацьовувань, потреба балансування між безпекою і зручністю [13].

1.3. Передумови та обґрунтування біометричних систем

1.3.1. Класифікація та режими функціонування біометричних модальностей

Після обґрунтування необхідності біометрії як ключового фактору автентифікації "Що ви є", наступним кроком є проведення систематизації та класифікації біометричних систем. Такий аналіз становить теоретичне підґрунтя для розуміння їхніх можливостей, обмежень та методів оцінки зокрема.

Біометричні ідентифікатори, або як їх ще називають модальності, класифікуються на основі характеристик, які вимірюються. Вони поділяються на дві основні категорії [14]:

1. Фізіологічні модальності. Ця категорія охоплює статичні, вроджені риси, пов'язані з формою та структурою тіла людини.

До них належать:

- відбиток пальця – аналіз унікальних патернів гребенів та западин на кінчиках пальців;
- розпізнавання обличчя – вимірювання та аналіз просторової геометрії рис обличчя;
- розпізнавання райдужної оболонки – аналіз високодеталізованої, унікальної текстури райдужної оболонки ока;
- сканування сітківки – Ідентифікація за унікальним патерном кровоносних судин на задній стінці ока;
- геометрія долоні – вимірювання форми та розмірів долоні та пальців;
- ДНК – аналіз унікальної генетичної послідовності індивіда.

2. Фізіологічні риси, які демонструють високі показники унікальності та постійності протягом життя, так звані поведінкові модальності. Вони

стосується патернів, що випливають із поведінки індивіда. Оскільки ці риси вивчаються з часом, вони часто використовуються для безперервної або пасивної автентифікації. До них належать:

- динаміка натискання клавіш – аналіз ритму та швидкості набору тексту;
- аналіз ходи – ідентифікація за унікальними патернами ходьби;
- розпізнавання голосу – аналіз акустичних властивостей голосу, що поєднує фізіологічні та поведінкові аспекти;
- динаміка підпису – аналіз швидкості, тиску та напрямку рухів під час написання підпису.

Поведінкові модальності можуть бути менш постійними, оскільки на них можуть впливати такі фактори, як втома, стрес або хвороба.

У таблиці 1.2 представлено порівняльний аналіз біометричних модальностей, ключевим для яких є висока універсальність кожного із згаданих методів.

Таблиця 1.2

Порівняльний аналіз біометричних модальностей

Модальність	**Унікальність**	**Постійність**	**Збираність**	**Прийнятність**	**Захист**
Відбиток пальця	Висока	Висока	Висока	Середня	Середня
Обличчя	Середня	Середня	Висока	Висока	Низька
Райдужна оболонка	Дуже висока	Дуже висока	Середня	Низька	Висока
Голос	Середня	Середня	Висока	Висока	Середня
Геометрія долоні	Середня	Висока	Висока	Висока	Середня
Хода	Низька	Середня	Висока	Висока	Середня
ДНК	Дуже висока	Дуже висока	Низька	Низька	Дуже висока

Отже, як бачимо з таблиці 1.2, кожну із модальностей можна характеризувати по одному із параметрів:

- унікальність – це оцінка того, наскільки кожна із розглянутих модальностей унікальна для користувача;

– постійність – це оцінка того, наскільки модальність користувача змінюється протягом життя;
– збираність – це оцінка того, наскільки складно зібрати зразок модальності з користувача;
– прийнятність – це оцінка того, наскільки система (або її функція) є задовільною, доречною та бажаною для використання у конкретному контексті;
– захист – це оцінка того, наскільки складно підробити саму модальність, а отже яким чином можливо її підробити.

Аналіз таких критеріїв виявляє що не існує "ідеальної" біометричної модальності, яка б мала найвищі бали за всіма показниками. Наприклад, ДНК має найвищу *унікальність* та *постійність*, але водночас "бідну" ***збираність*** (вимагає інвазивного збору зразків) та *прийнятність* (викликає значні занепокоєння щодо приватності). З іншого боку, розпізнавання обличчя має "високу" *прийнятність* та *збираність* (камери є всюди), але нижчу *унікальність* (проблеми з ідентичними близнюками) та *постійність* (вплив старіння, макіяжу, масок). Навіть райдужна оболонка, що має "високу" *унікальність* та *постійність*, часто оцінюється як така, що має "бідну" *прийнятність*, оскільки користувачі можуть сприймати процес сканування ока як інвазивний. Така відсутність єдиного, простого, миттєвого чи чудодійного рішення для складної проблеми є основною рушійною силою для двох основних напрямків досліджень в біометрії, а саме:

1) розробки ***мультимодальних*** систем, які комбінують сильні сторони різних модальностей (наприклад, обличчя та голос);

2) постійного вдосконалення алгоритмів виділення ознак та зіставлення з метою максимізації ***ефективності*** та ***унікальності*** легкодоступних модальностей.

Окрім цього будь–яка біометрична система, незалежно від модальності, функціонує в одному з двох фундаментальних режимів: верифікація або ідентифікація.

Вибір режиму визначає основне питання, на яке відповідає система, та має кардинальні наслідки для архітектури, обчислювальної складності та вимог до точності.

Верифікація (1:1 або One–to–One). При обиранні такого режиму процес підтвердження заявленої особистості проводиться шляхом порівняння живого біометричного зразка з *одним* із збережених шаблонів, що належить заявленій особі [15]. Грубо кажучи система для себе має відповісти на питання: "Чи є ця особа тим, ким вона себе називає?" В процесі підтвердження користувач спочатку заявляє свою особу (наприклад, вводить ім'я користувача, PIN–код, або просто володіє пристроєм, як–от смартфон), а система отримує цей ідентифікатор та знаходить відповідний шаблон у базі даних де і проводить порівняння "один до одного". Наприклад, розблокування смартфона за допомогою відбитка пальця, коли система порівнює палець користувача лише з тими шаблонами, які зареєстровані на цьому пристрої (рис. 1.3).

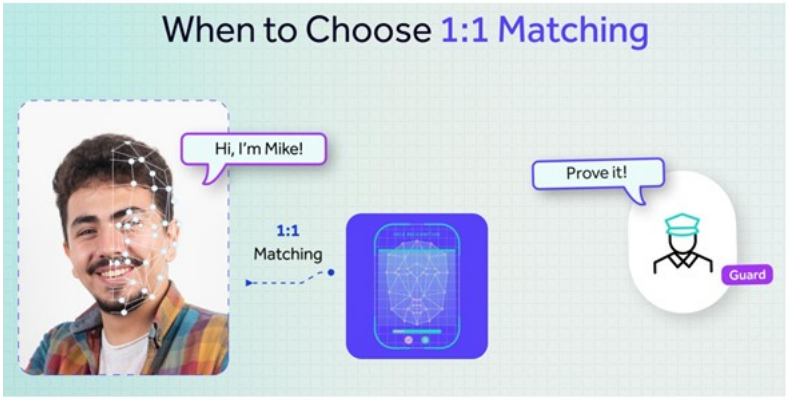

Рисунок 1.3 – Принцип верифікації 1:1

Ідентифікація (1:N або One–to–Many). При обиранні такого режиму процес пошуку здійснюється в ***усій*** базі даних біометричних шаблонів (розміром *N*) з метою визначити, чи збігається живий зразок з *будь–яким* із *N* шаблонів [15]. У цьому випадку система має для себе відповісти на питання: "Хто ця особа?" або "Чи відома ця особа системі?". В процесі підтвердження користувач не робить попередньої заяви про свою особу. Система проводить *N* порівнянь, зіставляючи живий зразок з кожним шаблоном у базі даних, щоб

знайти потенційний збіг. Наприклад, Криміналістичні системи AFIS (Automated Fingerprint Identification System), система дедуплікації при реєстрації виборців (запобігання створенню дублікатів записів), або ідентифікація несвідомого пацієнта в лікарні (рис. 1.4).

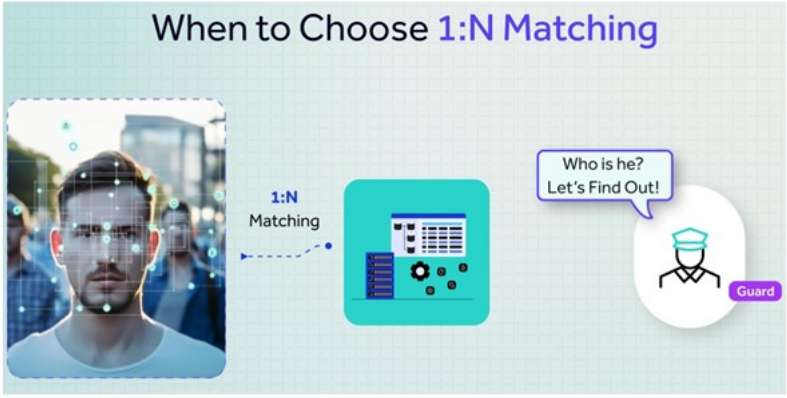

Рисунок 1.4 – Принцип верифікації 1: N

Ключова відмінність між такими резимами підтвердження полягає в обчислювальній складності та вимогах до точності. Режим ідентифікації (1:N) є не просто в *N* разів обчислювально складнішим, він експоненційно збільшує ймовірність помилкового спрацювання (False Acceptance) і вимагає значно вищої базової точності.

Ця проблема описується наступним співвідношенням:

$$P(N) = 1 - (1 - Pi)^N,$$

де

P(N) – це загальна ймовірність помилкової *ідентифікації* (ймовірність знайти хоча б один помилковий збіг у всій базі даних);

Pi – це ймовірність помилкової *верифікації* (тобто, базовий показник FAR для одного порівняння 1:1);

N – це кількість шаблонів у базі даних.

Розглянемо приклад такої системи.

Припустимо, що біометрична система має *Pi* (FAR) = 0.01% (або 10^{-4}). Такий показник є надзвичайно надійним при задачі верифікації (1:1), проте,

якщо таку ж систему застосовувати для ідентифікації (1:N) у базі даних середнього розміру, наприклад, при $N = 1{,}000{,}000$:

Ймовірність не знайти помилковий збіг в одному порівнянні дорівнює $(1 - 10^{-4})$, а імовірність не знайти помилковий збіг у мільйоні незалежних порівнянь дорівнює $(1 - 10^{-4})^{1{,}000{,}000}$. Використовуючи апроксимацію $(1 - x/N)^N \approx e^{-x}$

при $N \to \omega$, отримуємо:

$$(1 - 10^{-4})^{1{,}000{,}000} \approx e^{-1{,}000{,}000*1 - 10-4} = e^{-100}$$

Значення e^{-100} є числом, надзвичайно близьким до нуля., таким чином, загальна ймовірність помилкової ідентифікації *PN* становить:

$$PN \approx 1 - 0 \approx 1$$

З наведеного прикладу можна зробити висновок що система з 99 % точністю (FAR=0.01%) у режимі верифікації (1:1) матиме ймовірність видати хоча б один помилковий збіг під час пошуку у базі даних що містить 1 мільйон осіб. Такий приклад означає, що для великомасштабних 1:N систем базовий FAR (*Pi*) має бути на порядки кращим, ніж для 1:1 систем. Це фундаментально обґрунтовує необхідність передових алгоритмів та спеціалізованих функцій втрат, здатних забезпечити такий екстремальний рівень розрізнювальної здатності.

1.3.2. Ключові показники ефективності

Для кількісної оцінки, порівняння та налаштування біометричних систем використовуються стандартизовані метрики помилок. До який відносяться FAR (False Acceptance Rate), FMR (False Match Rate), FRR (False Rejection Rate) та FNMR (False Non–Match Rate).

- FAR / FMR – це показники помилкового допуску [16]. Ймовірність того, що система помилково прийме неавторизованого користувача (самозванця) як авторизованого. FAR є основним показником безпеки системи. Його значення обчислюється за наступною формулою:

$$FAR = \frac{FP}{FP + TN}$$

де

FP – кількість помилкових прийнятть;

FP + TN – загальна кількість спроб самозванців.

- FRR / FNMR – це показники помилкового відхилення [17]. Ймовірність того, що система помилково відхилить легітимного, авторизованого користувача. FRR є основним показником зручності та доступності системи. Його значення обчислюється за наступною формулою:

$$FRR = \frac{FN}{FN + TP}$$

де

FN – кількість помилкових відхилень;

FN + TP – загальна кількість спроб авторизованих користувачів.

FAR та FRR знаходяться в оберненій залежності, яка контролюється *порогом чутливості* системи. У залежності від якого системі або потрібен "дуже хороший" збіг – високий поріг (висока безпека), що знижує FAR (самозванцям важко пройти), але підвищує FRR (авторизованим користувачам також важче пройти) або системі достатньо "посереднього" збігу – низький поріг (висока зручність), що знижує FRR (легко потрапити в систему), проте підвищує FAR (самозванцям також легше).

Такий компроміс візуалізується за допомогою кривої DET (Detection Error Trade–off). Для порівняння загальної точності двох різних систем часто використовують єдиний числовий показник Equal Error Rate (EER) – показник рівних помилок. Це точка на кривій DET, в якій FAR дорівнює FRR [18].

EER надає єдине значення, що репрезентує збалансовану продуктивність системи, незалежно від конкретного налаштування порогу. Відповідно чим нижчий EER, тим точнішою буде система.

Як було показано, у задачах ідентифікації (1:N) набір даних є вкрай незбалансованим (*1* правильний збіг проти *N–1* неправильних). У такому сценарії проста "точність" є неефективною метрикою, оскільки система, що завжди каже "немає збігу", матиме 99.9999% точності, але буде марною. Тому застосовують додаткові метрики із галузі інформаційного пошуку, наприклад

F–measure (F1–Score), яка є гармонійним середнім між точністю та повнотою. У даному випадку під точністю розуміють, який відсоток з усіх ідентифікацій, що система *визнала* позитивними були *справді* правильним? (це мінімізує помилкові збіги). Під повнотою розуміють, який відсоток з усіх позитивних збігів, які *існували* в базі система *змогла* знайти? (це мінімізує пропуски).

Відповідно значення *F1* обчислюється за наступною формулою:

$$F1 = \frac{Pr * Rc}{Pr + Rc}$$

де

Pr – точність, а Rc – повнота.

Значення *F1* буде високим, лише якщо *обидва* показники, Pr та Rc, є високими. Це робить метрику *F1* надійною та збалансованою, яка може застосовуватися для оцінки ефективності 1:N систем.

Хоча FAR, FRR та EER є галузевими стандартами, вони мають суттєві обмеження. Вони є "наївними" (простими) метриками, оскільки представляють лише середнє значення помилок у всій тестовій вибірці та не фіксують розподіл таких помилок.

Для прикладу розглянемо дві гіпотетичні системи, А і Б, обидві з мають однаковий показник – EER = 5%, проте система А має 5 % помилок, що рівномірно розподілені серед усіх демографічних груп (вік, стать, етнічна приналежність). На відміну від А, система Б має 0 % помилок для 95 % населення, але 100 % помилок для 5 % населення, наприклад, система не може розпізнати людей з темнішим відтінком шкіри або жінок.

За традиційною метрикою EER, системи А і Б рахуються *еквівалентними*, проте у реальному світі система Б буде недієздатною та дискримінаційною. Така проблема, відома як *алгоритмічна упередженість*, є однією з найактуальніших у сучасній біометрії. Вона підкреслює, що для повноцінного аналізу недостатньо просто повідомити EER; необхідно аналізувати ROC–криві та розподіл балів подібності для різних підгруп населення, щоб виявити потенційну упередженість.

1.4. Аналіз сучасних алгоритмів виділення ознак

Процес біометричної ідентифікації складається з двох основних етапів:

1) виділення ознак;

2) зіставлення ознак.

Виділення ознак – це процес перетворення вхідних необроблених даних (наприклад, зображення обличчя або відбитка пальця) у компактний числовий вектор (відомий як *вектор ознак* або *шаблон*). Цей вектор має бути достатньо інформативним, щоб бути унікальним для кожної особи, але водночас достатньо стабільним, щоб залишатися незмінним при незначних варіаціях (наприклад, різне освітлення або кут огляду). Історично, цей процес еволюціонував від "рукотворних" алгоритмів до підходів, що базуються на глибокому навчанні.

Традиційні алгоритми виділення ознак покладаються на знання експертів у предметній галузі для розробки алгоритмів, які виділятимуть специфічні, заздалегідь визначені патерни (текстури, краї, ключові точки). До таких алгоритмів відносять: виділення Мінуцій (Minutiae) з відбитків пальців, локальні бінарні шаблони та гістограми орієнтованих градієнтів.

Виділення Мінуцій (Minutiae) з відбитків пальців – це класичний і найбільш поширений підхід до розпізнавання відбитків пальців [19]. Замість того, щоб порівнювати цілі зображення (що є обчислювально дорогим і чутливим до зсувів), цей метод фокусується на локальних особливостях гребенів. Його концепція полягає в тому, що Мінуції (minutiae) – це точки, де гребені на відбитку пальця закінчуються або розгалужуються (рис. 1.5).

В процесі роботи алгоритм зазвичай включає бінаризацію зображення (перетворення на чорно–біле) та скелетизацію (стоншення гребенів до товщини в один піксель).

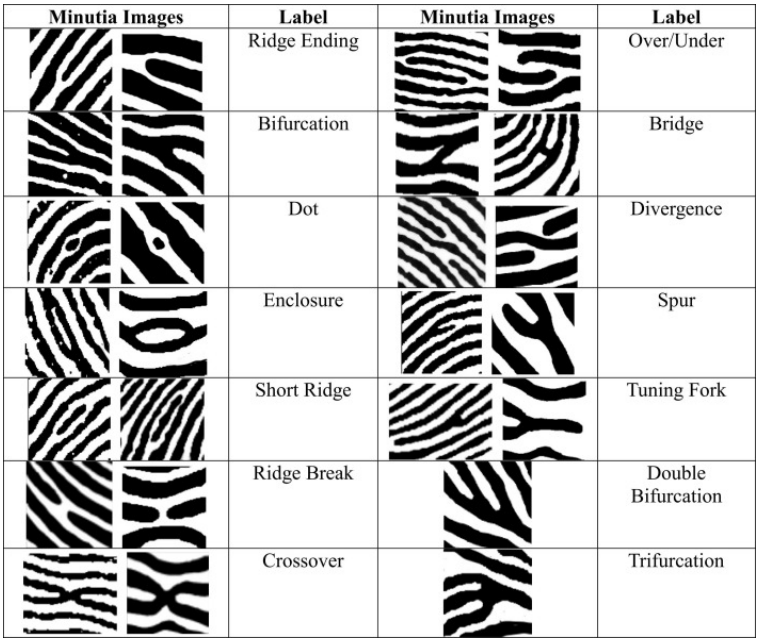

Рисунок 1.5 – Типи гребенів Мінуцій

Потім система сканує скелетонізоване зображення для виявлення мінуцій і записує їхні характеристики, зазвичай у вигляді трійки:

$$m = (x, y, \theta)$$

де

(x, y) – координати

θ – кут напрямку гребеня в цій точці.

В такому випадку задача розпізнавання зводиться до "зіставлення точкових патернів". Такий метод має наступні переваги:

1. Ефективність зберігання – шаблон на основі мінуцій є дуже компактним.

2. Приватність – нереально відновити оригінальне зображення відбитка пальця, маючи лише дані про мінуції., що допомагає у вирішенні проблем конфіденційності.

3. Надійність – мінуції є більш стабільними до невеликих змін тиску та орієнтації порівняно з методами, що базуються на кореляції зображень.

Проте, не існує методів без недоліків. Основною проблемою даного методу є те, що на можливість впізнання дуже сильно впливає якість вхідного зображення. Бруд, шрами, надмірна сухість або вологість шкіри створюють помилкові мінуції або призводять до пропуску справжніх. Це вимагає складних

етапів попередньої обробки та покращення зображення.

Локальні бінарні шаблони (Local Binary Patterns, LBP) – це потужний дескриптор текстури, який широко використовується для розпізнавання обличчя та аналізу райдужної оболонки. Його концепція полягає в тому, що LBP описує локальну текстуру шляхом порівняння кожного пікселя з його сусідами [20].

В процесі роботи виконується наступний алгоритм:

1. Для кожного пікселя (центра) розглядається його оточення 3 х 3.
2. Інтенсивність кожного з 8 сусідніх пікселів порівнюється з інтенсивністю центрального пікселя.
3. Сусіду присвоюється '1', якщо його інтенсивність більша або дорівнює центральній, і '0', якщо вона менша.
4. Результатом є 8–бітний бінарний рядок (наприклад, '10110010'), який перетворюється на десяткове число (від 0 до 255).
5. Цей процес повторюється для всього зображення, створюючи LBP–карту.
6. Для отримання фінального вектора ознак будується *гістограма* цих LBP–значень.

Цей підхід ще також відомий як **LBPH** (Local Binary Patterns Histograms) [20]. Перевагами LBP є те, що він обчислювально простий і, що найважливіше, *високо стійким до монотонних змін освітлення* (наприклад, затемнення або освітлення всього обличчя), оскільки він базується на *відносних* різницях інтенсивності, а не на абсолютних значеннях (рис .1.6).

Третім поширеним алгоритмом виділення ознак є **гістограми орієнтованих градієнтів** (Histogram of Oriented Gradients, HOG) [21]. На відміну від LBP (який фіксує текстуру), HOG є потужним дескриптором форми та країв. Його ідея полягає в тому, що локальну форму об'єкта можна ефективно описати розподілом напрямків градієнтів (тобто напрямків країв) у цьому регіоні.

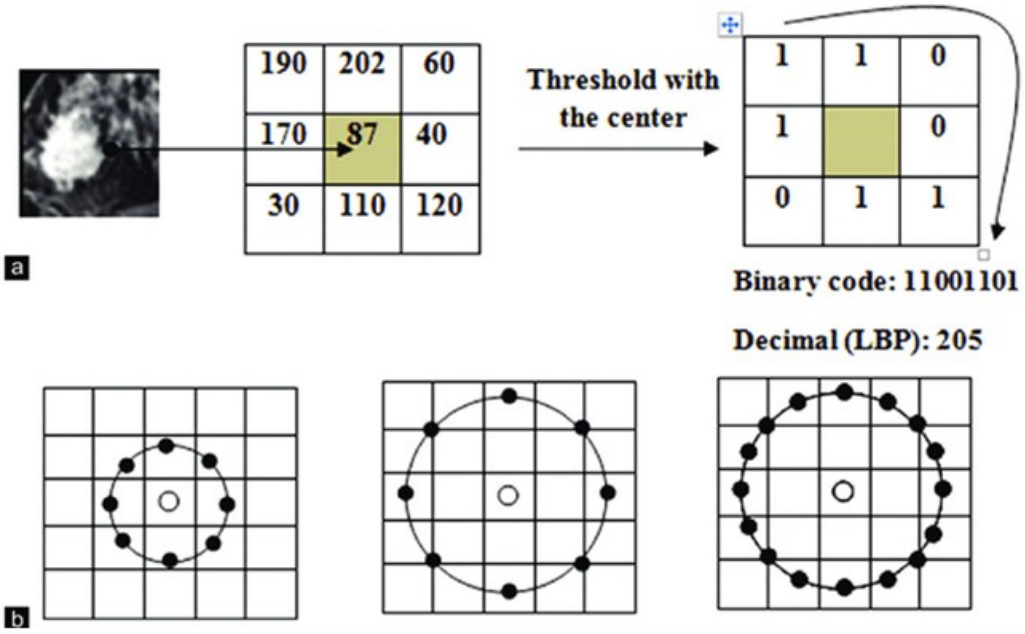

Рисунок 1.6 – Реалізація методу локальних бінарних шаблонів

Процес алгоритму містить наступні кроки:

1. Зображення ділиться на малі зв'язані регіони, які називаються "клітинками".

2. У кожній клітинці обчислюється градієнт (величина та напрямок) для кожного пікселя.

3. Будується *гістограма напрямків градієнтів* (наприклад, 9 бінів / напрямків) для кожної клітинки.

4. Клітинки об'єднуються в більші, частково перекриті "блоки". Гістограми в межах одного блоку нормалізуються (це забезпечує стійкість до змін освітлення та контрасту).

5. Усі нормалізовані гістограми з усіх блоків об'єднуються (конкатенуються) в єдиний, великий вектор ознак.

Перевагами такої реалізації ж те, що HOG є дуже надійним для виявлення об'єктів (спочатку він був розроблений для виявлення людей) і добре працює в біометрії, де форма є ключовою, наприклад, у розпізнаванні патернів вен долоні або аналізі медичних зображень.

Традиційні методи (HOG, LBP, мінуції) базуються на інженерії ознак – процесі, де експерт вручну розробляє алгоритм, базуючись на припущеннях про

те, які ознаки є важливими (наприклад, "градієнти важливі" або "текстура важлива"). На відміну від них, **згорткові нейронні мережі** (CNN) представляють фундаментальний зсув до навчання ознакам [22]. Замість того, щоб програмувати екстрактор ознак вручну, CNN автоматично вивчає оптимальну ієрархію ознак безпосередньо з необроблених пікселів під час процесу навчання. Згорткові нейронні мережі виділяють три рівні або шари:

- Нижні шари CNN зазвичай вчаться розпізнавати прості ознаки, такі як краї та градієнти (подібно до HOG).
- Середні шари комбінують їх у складніші патерни, такі як текстури (подібно до LBP) або прості форми.
- Верхні шари вчаться розпізнавати семантичні частини об'єктів (наприклад, "око", "ніс", "рот" у розпізнаванні обличчя).

У контексті біометрії, CNN зазвичай використовується як *екстрактор ознак* – зображення подається на вхід мережі, а вихід *передостаннього* шару (перед фінальним класифікатором) використовується як той самий *вектор ознак*.

Основна перевага CNN полягає в їхній здатності досягати "істотно кращої продуктивності" порівняно з традиційними методами, особливо на великих і складних наборах даних. Мережа вчиться ігнорувати нерелевантні варіації (наприклад, освітлення) і фокусуватися на найбільш дискримінативних (розрізнювальних) ознаках. Однак, традиційні методи не є повністю застарілими і часто використовуються в гібридних підходах. Дослідження [23] демонструє такий підхід для *перікулярної ідентифікації*.

В таблиці 1.3 представлено порівняння ключових характеристик для традиційних метрик та згорткових нейронних мереж.

Як видно із таблиці 1.3 і традиційні метрики, і згорткові нейронні мережі мають свої переваги та недоліки в залежності від сфери застосування.

Таблиця 1.3

Порівняння парадигм виділення ознак

Метрика	Традиційні (LBP / HOG / Мінуції)	CNN
Принцип реалізації	Інженерія ознак	Навчання ознакам
Необхідність експертних знань	Висока (потрібно визначити, *що* шукати)	Низька (мережа вчиться *що* шукати)
Потреба в даних для навчання	Низька / Середня	Дуже висока
Обчислювальна складність	Низька	Висока (залежить від архітектури)
Енергоефективність	Висока	Низька (за винятком спецмереж)
Потенційна точність (на великих даних)	Середня / Висока	Дуже висока
Стійкість до перенавчання	Висока	Низька

Вибір між традиційними методами та CNN не є вибором між старою технологією та новою, це більше компроміс, що базується на трьох факторах:

1. Точність CNN полягає в тому, що зазвичай цей метод забезпечує вищу точність при складних завданнях [24].

2. Обчислювальна вартість. Традиційні методи, такі як HOG, є *значно* ефективнішими з точки зору енергоспоживання. Дослідження [25] вказує на "значну різницю у споживанні енергії" між CNN та HOG. Енергоспоживання та енергозаощадження є *критично* важливим для вбудованих та мобільних пристроїв, де час роботи від батареї є пріоритетом [25].

3. CNN потребують *великих* наборів даних для ефективного навчання. У дослідженні [26] зазначено, що CNN "вигідні переважно для великих баз даних". На *малих* наборах даних добре налаштований алгоритм LBP або HOG може показати кращі результати через значно менший ризик перенавчання.

Отже, потужні CNN, такі як ResNet, є кращим вибором для *серверних* 1:N систем з великими об’ємами даними, де точність системи є пріоритетом. Натомість традиційні методи або спеціалізовані легкі CNN є необхідними для *клієнтських* 1:1 систем на пристроях з обмеженими ресурсами.

2. ДОСЛІДЖЕННЯ АРХІТЕКТУР ГЛИБОКОГО НАВЧАННЯ ДЛЯ БІОМЕТРІЇ

У попередньому розділі було встановлено фундаментальний зсув парадигми від "інженерії ознак" до "навчання ознакам" завдяки впровадженню згорткових нейронних мереж (CNN). Було продемонстровано, що CNN здатні автоматично вивчати ієрархію ознак і, як правило, демонструють вищу точність порівняно з традиційними методами на великих наборах даних.

Проте, термін "CNN" охоплює широкий спектр архітектур, кожна з яких має унікальні характеристики, що визначають компроміс між точністю, обчислювальною вартістю та енергоефективністю. Як було зазначено в п. 1.4, вибір між "важкою" серверною моделлю (1:N) та "легкою" клієнтською (1:1) є ключовим інженерним рішенням.

Цей розділ присвячений детальному дослідженню конкретних архітектур та математичних підходів, які є основою сучасних біометричних систем, побудованих на глибокому навчанні, а також побудові алгоритму ідентифікації користувачів із використанням біометричних даних.

2.1. Проблема глибини мережі та шляхи її вирішення

Вибір базової архітектури визначає здатність моделі виділяти розрізнювальні ознаки та її придатність для розгортання на цільових платформах.

Архітектури, розроблені Visual Geometry Group (VGG), такі як VGG–16 та VGG–19, були піонерськими у демонстрації того, що значна глибина мережі є ключовим фактором для досягнення високої продуктивності [27]. Завдяки їм було досягнуто ключової інновація – використання виключно малих згорткових фільтрів (3x3), але у великій кількості послідовних шарів (16–19).

На рисунку 2.1 представлено принцип роботи архітектури VGG. Проте таке застосування має свої обмеження, хоча VGG встановила нові стандарти точності, вона зіткнулася з проблемою "деградації".

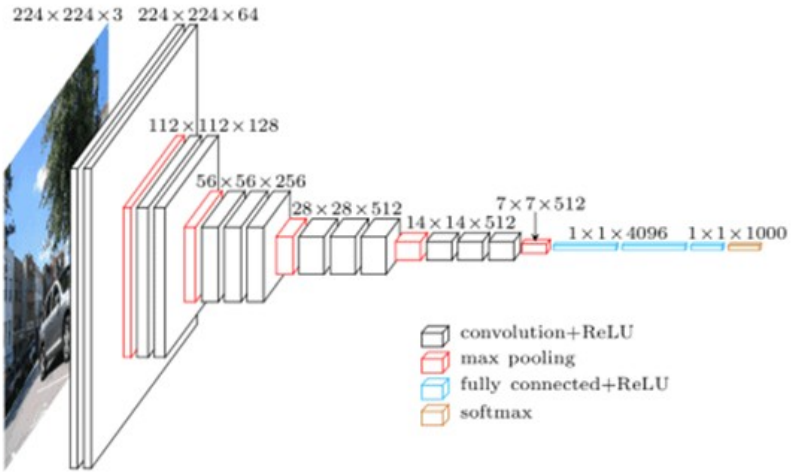

Рисунок 2.1 – Архітектура VGG

Було виявлено, що дуже глибокі "прості" мережі починали показувати гірші результати, ніж їхні менш глибокі аналоги, значною мірою через проблему "згасаючого градієнта"[28]. Крім того, такі мережі є обчислювально "важкими" і мають велику кількість параметрів.

Для вирішення проблеми деградації була розроблена спеціальну архітектуру ResNet (Residual Networks), що дозволило успішно тренувати надзвичайно глибокі мережі (50, 101, 152 шарів і більше). Її ключовою інновацією було впровадження "Залишкового Блоку" (Residual Block). Механізм роботи ResNet полягає в тому, що замість того, щоб змушувати стек шарів вивчати бажане перетворення $H(x)$, ResNet вводить "коротке з'єднання", яке передає вхід x в обхід блоку і додає його до виходу $F(x)$. Таким чином, мережа вивчає лише залишкову функцію $F(x) = H(x) – x$ [29].

На рисунку 2.2 представлено архітектуру моделі Resnet–50. Перевагою такого підходу є те, що він радикально спрощує оптимізацію. У найгіршому випадку, якщо певний блок не є корисним тобто, оптимальним є тотожне перетворення $H(x) = x$, мережі набагато легше навчитися обнуляти ваги $F(x)$ досягти $F(x) = 0$, ніж змусити стек нелінійних шарів ідеально імітувати тотожну функцію $H(x) = x$.

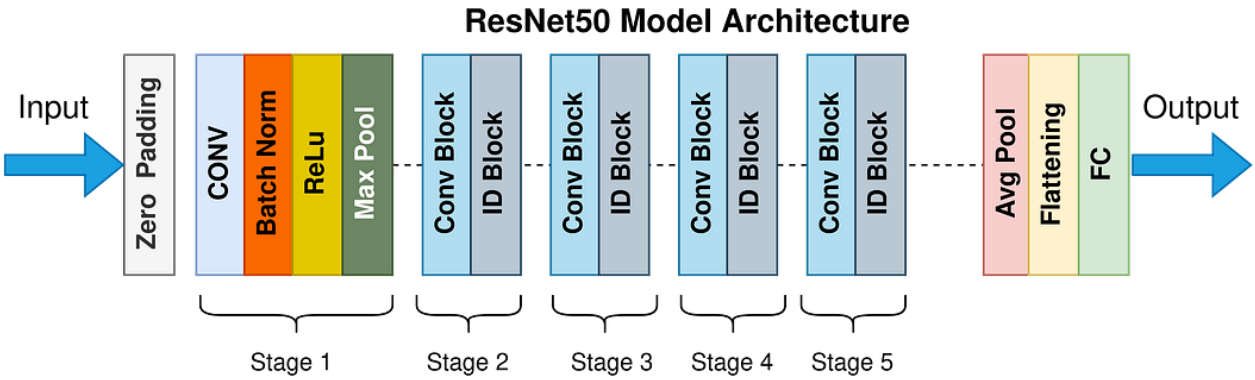

Рисунок 2.2 – Архітектура Resnet–50

В біометрії даний метод застосовується завдяки своїй здатності вивчати надзвичайно складні ознаки без деградації, ResNet, зокрема його версія ResNet–50, став золотим стандартом для біометричних завдань, що вимагають максимальної точності. Це де–факто основна архітектура для серверних 1:N систем ідентифікації наприклад, великомасштабного розпізнавання обличчя або зіставлення райдужної оболонки, де доступні значні обчислювальні ресурси і точність є пріоритетом.

У той час як ResNet вирішує проблему точності, він залишається обчислювально дорогим для пристроїв з обмеженими ресурсами, таких як смартфони, планшети або камери IoT [30]. На противагу йому була розроблена з нуля архітектура MobileNet, яку застосовують для досягнення максимальної обчислювальної ефективності [31]. Ключовою інновацією даної архітектури є "Глибинно–роздільні згортки", які замінюють стандартний згортковий шар, розділяючи його на два окремі, значно "легші" етапи [32].

На рисунку 2.3 представлено архітектуру моделі MobileNet V1.

На першому рівні, який називають глибинна згортка, застосовується один просторовий фільтр (наприклад, 3x3) до кожного вхідного каналу окремо. Цей етап фільтрує просторову інформацію, але не комбінує інформацію між каналами.

На другому рівні, який називають Точкова згортка застосовується обчислювально "дешеву" 1x1 згортку для лінійної комбінації виходів глибинної згортки, створюючи нові ознаки.

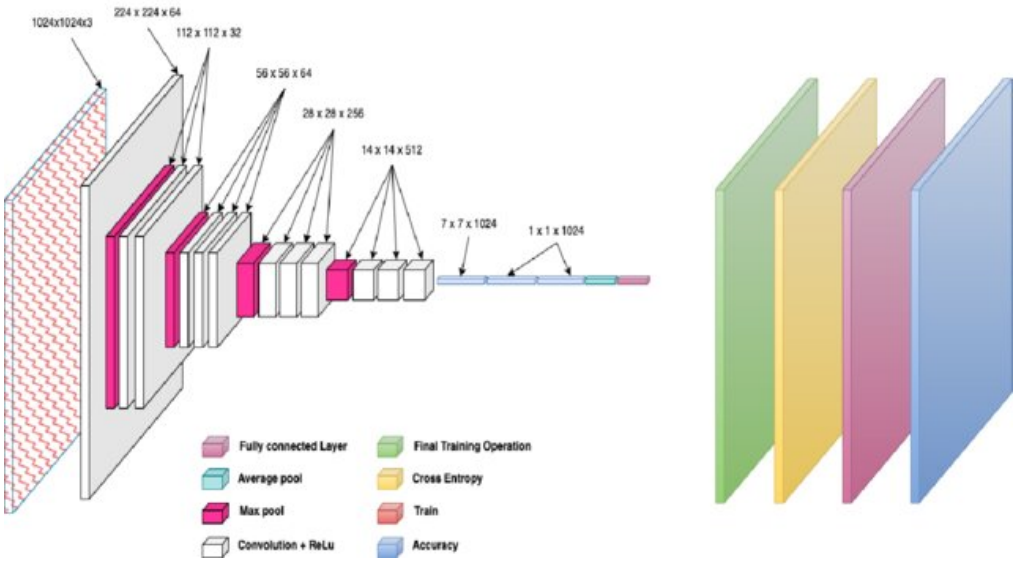

Рисунок 2.3 – Архітектура MobileNet V1

Перевагами даного методу є факторизація стандартної згортки на ці два етапи, що радикально (на порядок) зменшує загальну кількість параметрів та обчислювальних операцій.

В біометрії MobileNet є ідеальною архітектурою для вбудованої біометрії, як–от розпізнавання обличчя [33], райдужної оболонки [34] або відбитків пальців [35] безпосередньо на мобільному пристрої. Це забезпечує швидку 1:1 верифікацію, зберігає час роботи батареї та підвищує приватність, оскільки біометричний шаблон не покидає пристрій.

В таблиці 2.1 представлено порівняння ключових архітектур CNN у сфері біометрії.

Отже, як видно з таблиці 2.1 VGG–16 та VGG–19 застаріли і не можуть застосовуватися в розробці будь яких технічних рішень. ResNet є найкращим рішенням для серверних рішень, де потрібен баланс між точністю та ресурсами. У випадку розробки для слабких телефонів та мобільних рішень загалом застосовують MobileNet, яка спеціально створена для телефонів та вбудованих систем.

Для розуміння принципів роботи та навчання VGG–16 та VGG–19 можна застосовувати у вигляді практичних завдань.

Таблиця 2.1

Порівняння ключових архітектур CNN для біометрії

Характеристика	VGG–16	VGG–19	ResNet–50	MobileNet V2
Рік випуску	2014	2014	2015	2018
Кількість шарів	16	19	50 (є версії 18, 34, 101, 152)	53 (глибина)
Кількість параметрів	~138 млн	~143 млн	~25.6 млн	~3.5 млн
Розмір моделі (ваги)	~528 МБ	~549 МБ	~98 МБ	~14 МБ
Ключова ідея	Глибоке накладання згорткових шарів 3x3	Ще більше шарів, ніж у VGG–16	Залишкові зв'язки (skip connections)	Роздільна згортка (depthwise separable convolutions)
Точність	~71.3%	~71.3% (схожа на VGG–16)	~76.0%	~72.0%
Швидкість	Дуже повільна	Дуже повільна	Середня / Швидка	Дуже швидка
Вимоги до пам'яті	Дуже високі	Екстремально високі	Середні	Мінімальні
Основне призначення	Вилучення ознак, навчання	Дослідження, трансферне навчання	Серверні рішення, високоточні завдання	Мобільні пристрої, IoT, Edge AI

2.2. Аналіз спеціалізованих функцій втрат

Як було обґрунтовано в пункті 1.3, для великомасштабних систем ідентифікації (1:N) потрібен екстремальний рівень розрізнювальної здатності, щоб мінімізувати ймовірність помилкового збігу. Стандартні функції втрат для класифікації оптимізують роздільність між класами у тренувальному наборі, але не обов'язково компактність або відстань між ними.

Для біометрії потрібен інший підхід – навчання метриці. Мета такого навчання полягає в тому, щоб навчити модель генерувати такі вектори ознак, щоб у цьому векторному просторі відстань між зразками однієї особи (внутрішньокласова відстань) була мінімальною, а відстань між зразками різних осіб (міжкласова відстань) – максимальною.

В біометрії вводять поняття функції втрат на основі відстані – це ключовий інструмент, який вчить моделі (наприклад, нейронні мережі) розуміти наскільки "схожими" є два біометричні зразки [36].

Замість того, щоб просто казати "це людина А" (класифікація), такі функції вчать модель створювати цифровий "відбиток" для кожного зразка.

У галузі біометричного захисту зокрема у розпізнаванні облич, ходи та голосу домінують функції втрати на парах та втрати на трійках.

Функція **втрати на парах** (Contrastive Loss) навчається на парах зображень: позитивних, наприклад два зображення однієї особи та негативних – зображення різних осіб [36]. Її мета – притягнути позитивні пари (зробити відстань $d(a, p)$ між ними якомога меншою) і відштовхнути негативні пари (зробити відстань $d(a, n)$ більшою за певний відступ m). Алгоритм порівняння двох щасливих людей представлено на рисунку 2.4.

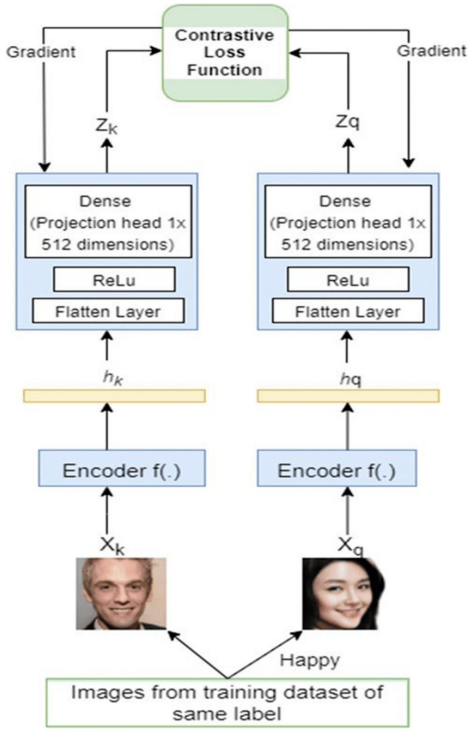

Рисунок 2.4 – Алгоритм роботи функції втрати на парах

На відміну від звичайної класифікації (де ми кажемо "це кіт"), Contrastive Loss вчить нейромережу розуміти **відстань**: "ці два зображення схожі (відстань

0)" або "ці два зображення різні (відстань > 0)". Проте такий метод має певні обмеження, ключовий з яких називають "жадібність".

Функція втрати на парах намагається "згорнути" всі позитивні зразки в одну точку, що є надто жорстким обмеженням і не враховує природну внутрішньокласову варіативність (наприклад, одна й та сама людина з різними виразами обличчя) [37].

Інша функція – **втрати на трійках** (Triplet Loss) використовується в роботі FaceNet і навчається на наступних трійках зразків:

– Anchor (*a*) – якірний зразок (основа).

– Positive (*p*) – позитивний зразок (та сама особа, що й *a*).

– Negative (*n*) – негативний зразок (інша особа).

Мета такого навчання полягає в тому, щоб не просто мінімізувати *d(a, p)*, а забезпечити, щоб "якір" був ближче до "позитива", ніж до "негатива", з певним відступом *m*.

Функція втрат на трійках мінімізує самі втрати:

$$L = max(d(a, p) – d(a, n) + m, 0).$$

Алгоритм роботи Функції втрата на трійках представлено на рисунку 2.5, де одночасно надається три типи зразків.

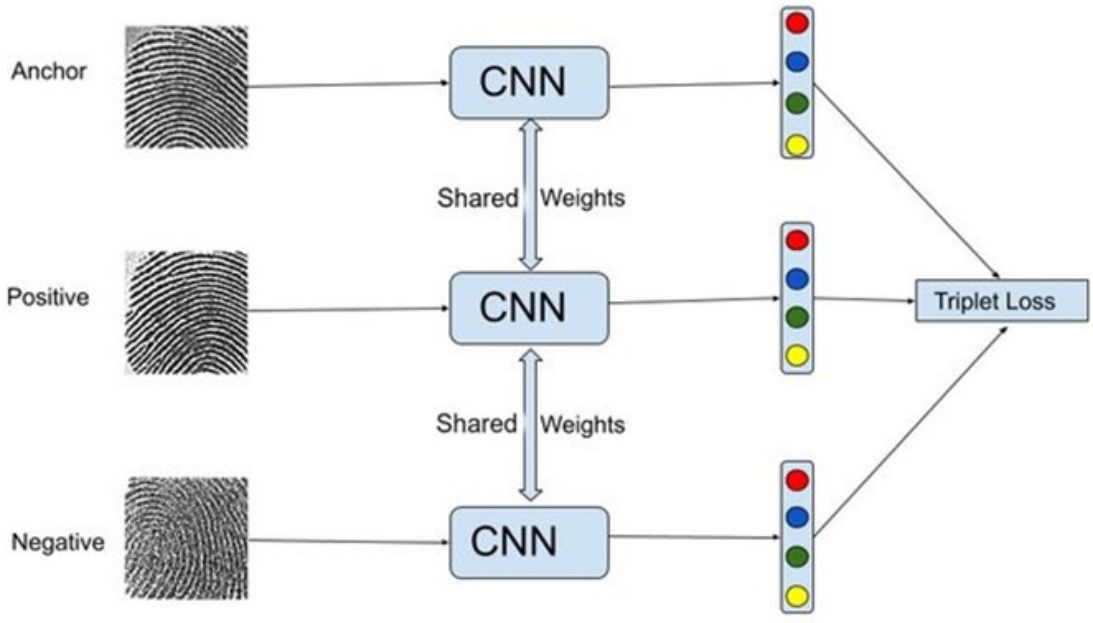

Рисунок 2.5 – Алгоритм роботи функції втрати на трійках

Відповідно, функція втрат на трійках є більш гнучкою, дозволяє існування внутрішньокласової варіативності (кластер однієї особи може бути "розтягнутим"), доки зберігається чіткий відступ m між класами.

Проте, такий метод звичайно має і свої обмеження – відбір трійок. Кількість можливих трійок у наборі даних є величезною $O(N^3)$. Для ефективного навчання необхідно знаходити "важкі" трійки, тобто такі, де $d(a, p)$ велике, а $d(a, n)$ відповідно мале. Такий процес відбору є обчислювально дорогим та може призвести до проблем зі збіжністю, тобто отримання в результаті рішення, що не є найкращим або найдоцільнішим в застосуванні.

Іншою відомою групою функцій втрат, що є сучасною еволюцією та вирішує проблеми функція втрат на трійках є група **функцій втрат на основі кутового відступу** (Angular Margin–based) (рис. 2.6). Вони поєднують високу ефективність навчання класифікаційних функцій (як–от Softmax) з дискримінаційною силою метричного навчання. Замість оптимізації евклідової відстані, ці методи нормалізують вектори ознак та вектори ваг, проєктуючи їх на поверхню гіперсфери. Таким чином, відстань між двома векторами визначається лише кутом між ними. Для здійснення таких розрахунків використовуються функції CosFace та ArcFace [38].

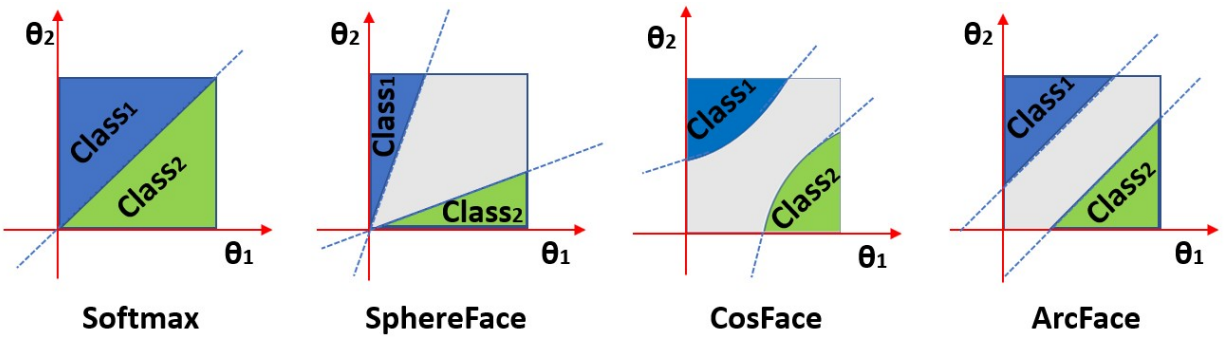

Рисунок 2.5 – Межі прийняття рішень для різних функцій втрат на основі кутового відступу

На рисунку 2.6 представлено межі прийняття рішень для різних функцій втрат на основі кутового відступу у випадку бінарної класифікації. Пунктирна

лінія позначає межу прийняття рішень, а сірі області – це межі прийняття рішень.

Функція **CosFace** (Large Margin Cosine Loss) вводить адитивний відступ m безпосередньо до косинуса кута θ_y, де θ_y – кут між вектором ознак x та вектором ваг правильного класу y. Функція втрат оптимізує $cos\ \theta_y - m$ [39].

Функція **ArcFace** (Additive Angular Margin Loss) вважається більш геометрично інтуїтивною, оскільки вводить адитивний відступ m безпосередньо до самого кута θ_y, а не до його косинуса, а функція втрат оптимізує $cos\ (\theta_y - m)$.

Перевагою ArcFace є те, що вона має чітку геометричну інтерпретацію – створюється кутовий простір, що відповідає геодезичній відстані на гіперсфері, між класами. Це змушує мережу вивчати ознаки, які є надзвичайно компактними всередині одного класу та максимально віддаленими між різними класами. Саме ці функції втрат дозволяють досягти екстремально низьких показників FAR, необхідних для надійних великомасштабних 1:N систем ідентифікації.

2.3. Алгоритми ідентифікації користувачів із використанням біометричних даних

2.3.1. Класифікація та види біометричних характеристик для ідентифікації користувачів

Процес збору інформації при біометричній ідентифікації є ключовим етапом у функціонуванні біометричних систем. Він передбачає перетворення унікальних фізичних або поведінкових характеристик людини на цифровий формат, який потім може бути використаний для ідентифікації або верифікації.

Першим кроком є вибір біометричної характеристики:

- Фізіологічні (статичні) характеристики:
  - відбитки пальців (дактилоскопія);
  - малюнок райдужної оболонки ока;
  - геометрія обличчя;
  - малюнок вен долоні або пальця;

- ДНК;
- термограма обличчя.

– Поведінкові (динамічні) характеристики:
  - голос;
  - клавіатурний почерк (динаміка набору тексту).
  - підпис (динаміка та графічні параметри).
  - хода.

У додатку А детально описано переваги та недоліки поширених біометричних характеристик. У зв’язку з поширенням коронавіруса та інших хвороб, що передаються через дотик, особливу увагу необхідно звернути на безконтактні методи ідентифікації користувачів. Найпростішим з них є ідентифікація за допомогою визначення геометрії обличчя та переведення її у відповідні ембедінги.

Другим кроком – захоплення даних (сканування). Тут використовуються спеціальні пристрої (сканери, камери, мікрофони) для збору "сирих" біометричних даних.

Третій крок – Обробка даних (виділення ознак)."Сирі" біометричні дані є занадто великими і містять зайву інформацію. На цьому етапі відбувається їхнє перетворення у компактний та унікальний цифровий формат, який називається шаблоном, вектором ознак або ембедінгом. Це включає: фільтрацію шуму; виділення ключових ознак та нормалізацію.

Четвертий крок – створення біометричного шаблону, тобто виділені ознаки перетворюються на математичний або цифровий шаблон. Цей шаблон не є прямим зображенням або записом, а є унікальним цифровим представленням біометричної характеристики. Важливо, що більшість систем не зберігають саме зображення відбитка пальця чи обличчя, а лише його цифровий шаблон. Це підвищує безпеку.

П’ятий крок – зберігання шаблону, коли створений біометричний шаблон зберігається у базі даних (наприклад, у захищеному сховищі, на смарт–карті або в електронному чіпі біометричного паспорта). Це еталонний шаблон, з яким

будуть порівнюватися наступні біометричні дані для ідентифікації або верифікації. Графічно кроки збору інформації представлено на рисунку 2.6.

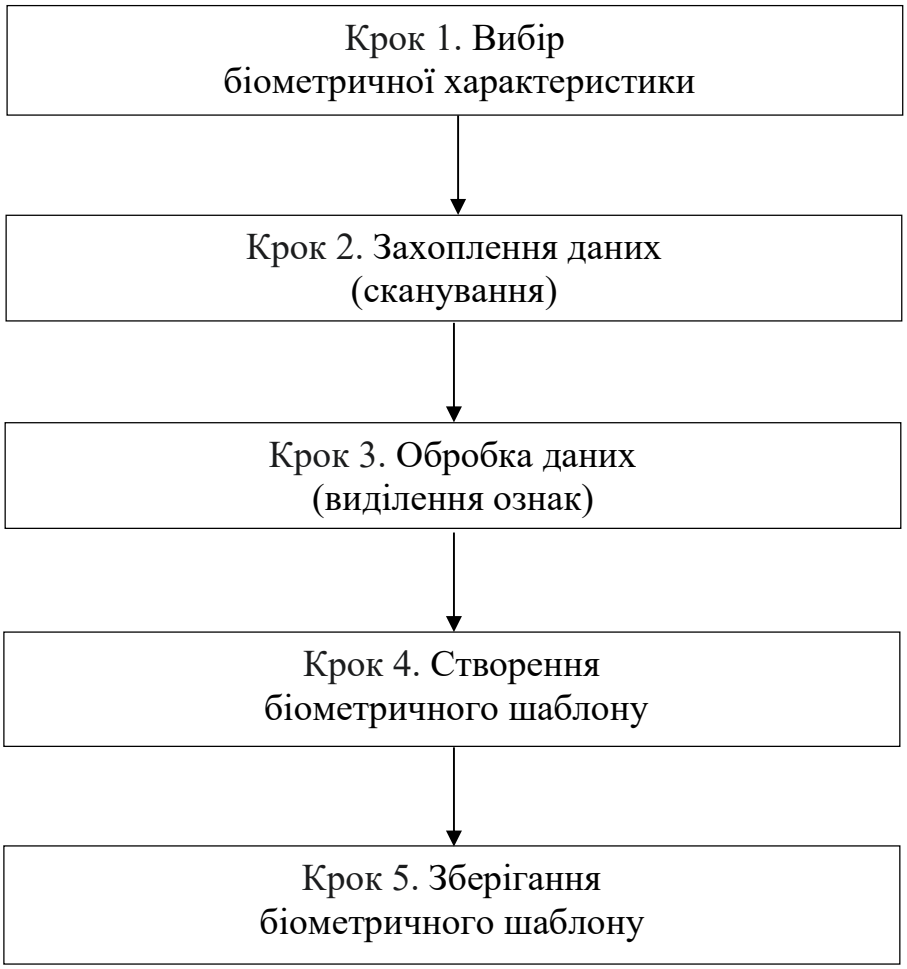

Рисунок 2.6 – Кроки збору інформації

Після збору інформації відбувається процес ідентифікації або верифікації. Сам процес збору інформації є фундаментальним для функціонування біометричних систем, забезпечуючи перетворення унікальних людських характеристик у формат, придатний для машинного порівняння та розпізнавання.

2.3.2. Структура алгоритму ідентифікації користувачів

На основі проведених у попередньому пункті досліджень можна запропонувати наступний алгоритм ідентифікації користувачів із використанням біометричних модальностей:

Крок 1. Доступ до зовнішніх джерел. На цьому кроці алгоритму необхідно здійснити підключення та налаштування відповідного пристрою для зчитування біологічних модальностей.

Крок 2. Процес збору інформації. Цей крок полягає в одержанні набору біологічних модальностей для подальшої роботи з ним.

Крок 3. Попередня обробка даних. На даному кроці необхідно підготувати початкове зображення обличчя до виділення ознак, мінімізуючи вплив зовнішніх факторів.

Крок 4. Виділення ключових ознак. Для подальшого порівняння отриманого набору даних із записаними раніше необхідно провести перетворення обробленого зображення обличчя у компактний числовий вектор (ембеддінг), що містить унікальні дискримінантні ознаки.

Крок 5. Запис числових характеристик шаблонів. Безпечне та ефективне зберігання біометричних шаблонів (ембеддінгів обличчя) зареєстрованих користувачів дасть змогу в подальшому швидко провести порівняння нових значень із існуючими.

Крок 6. Ідентифікація / автентифікація користувача. На даному кроці проводиться порівняння вхідного біометричного ембеддінгу з базою зареєстрованих шаблонів та прийняття рішення про ідентифікацію / автентифікацію користувача.

Запропонований алгоритм представлений на рисунку 2.7, та включає всі кроки необхідні для проведення ідентифікації / автентифікації користувача на основі біологічних модальностей, зокрема фотографії зображення.

Розберемо кожен крок алгоритму більш детально.

На першому кроці здійснюється підключення та налаштування пристрою для зчитування біологічних модальностей. Як зазначалося раніше до зовнішніх джерел отримання біологічних модальностей відносять будь які засоби, що можуть їх зібрати, такі як датчики для зчитування відпечатків пальців, сканери сітківки, камери для захоплення кадрів із обличчям користувача та інші. Це перший крок, де є загроза зловмисних дій, оскільки саме в процесі одержання біологічних модальностей є висока ймовірність їх підміни.

Рисунок 2.7 – Алгоритм ідентифікації користувачів із використанням біометричних модальностей

Згідно із представленим у додатку А порівнянням біометричних модальностей для ідентифікації користувача однією із найдоступніших та ефективніших біологічних модальностей є аналіз обличчя людини. Відповідно на другому кроці від налаштованих на попередньому кроці пристроїв отримують необхідне зображення обличчя, що буде досліджуваним зразком.

Третій крок відповідає за підготовку "сирих" зображень обличчя до виділення ознак, мінімізуючи вплив зовнішніх факторів. Він полягає в детекції та вирівнюванні досліджуваного обличчя, тобто його виявленні та геометричній трансформація для стандартизації його відображення, а саме ротація, масштабування, зсув. На зображенні може бути декілька облич, тому детекція також полягає в визначенні їх кількості та пріоритетності для перевірки.

На четвертому кроці відбувається перетворення обробленого на попередньому кроці зображення у ембеддінг. Ембеддінги є внутрішнім представленнями сучасних глибоких нейронних мереж (DNNs), що

функціонують як автоматизована форма традиційної інженерії ознак [40]. Вони дозволяють даним, які часто мають форму тексту чи зображень, бути представленими у великому векторному просторі для чисельного аналізу. Цей процес є ключовим у глибинному навчанні, де моделі вчаться вилучати значущі ознаки або патерни з необроблених даних, стискаючи їх у компактний, низьковимірний формат.

П’ятий крок полягає у безпечному зберіганні ембеддінгів обличчя зареєстрованих користувачів у базах даних (MySQL, SQLite, PostgreSQL). Ключовим є зашифровування ембеддінгів перед збереженням у БД.

Цей крок включає в себе:

- вибір алгоритму шифрування (наприклад, AES 256);
- надійне управління ключами шифрування;
- розшифрування ембеддінгів перед їх використанням для порівняння;
- CRUD–операції (англ. create read update delete) – реєстрація, отримання шаблонів, оновлення, видалення профілів користувачів та їхніх біометричних шаблонів.

На шостому кроці проводиться порівняння вхідного ембеддінгу з кожним ембеддінгом у базі даних, використовуючи метрику відстані. Для ідентифікації / автентифікації користувача застосовується заздалегідь визначений поріг схожості для прийняття відповідного рішення. Якщо максимальна схожість перевищує поріг, ідентифікація успішна, якщо ні, то досліджуване обличчя вважається невідомим або неідентифікованим.

Важливо розуміти, що ідентифікація часто є першим кроком, який передує аутентифікації. У біометричних системах може спочатку відбуватися 1:N ідентифікація для визначення особи, а потім 1:1 автентифікація для підтвердження цієї особи за допомогою додаткових факторів (наприклад, додатковий пароль). У більшості систем безпеки наприклад, при вході у комп'ютер, смартфон або веб–сайт, застосовується автентифікація 1:1, оскільки користувач спочатку заявляє про свою ідентичність.

Відповідно використання біологічних модальностей для ідентифікації та відповідне їх використання в даних процесах багато в чому залежить від

трансформації графічного зображення у відповідний ембеддінг. Основний принцип, що лежить в основі ембеддінгів, полягає в тому, що схожі об'єкти отримують векторні представлення, які є близькими один до одного у просторі внутрішнього добутку або метричному просторі.

Ця властивість є критично важливою, оскільки вона дозволяє системі кількісно оцінювати подібність між різними зразками даних. Ембеддінги відіграють вирішальну роль у сучасній літературі з глибокого навчання, оскільки вони забезпечують ефективне представлення високорозмірних даних у компактному, щільному форматі. Така компресія не тільки зменшує вимоги до зберігання, але й дозволяє здійснювати офлайн–обчислення, які потім можуть бути легко використані в реальних застосуваннях, таких як системи пошуку та рекомендацій, зі швидкими онлайн–операціями, наприклад, порівнянням подібності векторів.

Таким чином, ембеддінги зберігають важливу семантичну та синтаксичну інформацію, уможливлюючи виконання складних операцій, таких як порівняння подібності або кластеризація, зі значно меншими обчислювальними витратами. Здатність ембеддінгів розкривати інтерпретовані, високорівневі концепції та виявляти притаманну неоднорідність у даних, а також людсько–зрозумілі пояснення для неї, підкреслює, що вони є не просто стисненими представленнями, а й носіями глибокого змісту. Це означає, що ембеддінги захоплюють сутність біометричних даних, роблячи їх надзвичайно дискримінаційними.

2.4. Порівняльний аналіз методів генерації ембеддінгів

Розуміння відмінностей між методами генерації ембеддінгів є ключовим для вибору найбільш підходящого підходу для конкретного завдання NLP.

Основна відмінність між статичними та контекстуалізованими ембеддінгами полягає в їхній здатності адаптуватися до контексту:

Залежність від контексту:

- Статичні моделі (Word2Vec, GloVe, FastText) є контекстно–незалежними.

Вони призначають один фіксований вектор кожному слову, незалежно від його оточення в реченні.

- Контекстуалізовані моделі (ELMo, BERT, GPT) є контекстно–залежними. Вони динамічно змінюють вектори слів на основі навколишнього тексту, дозволяючи розуміти значення слова в конкретному контексті.

Обробка полісемії (Багатозначності):

- Статичні моделі мають труднощі з обробкою полісемії, оскільки одне слово має лише одне представлення, незалежно від його різних значень.[2]
- Контекстуалізовані моделі явно вирішують проблему полісемії, надаючи різні вектори для одного слова залежно від його значення в контексті (наприклад, "банк" як фінансова установа чи берег річки).

Обробка OOV (Out–of–Vocabulary) слів:

- Word2Vec/GloVe не можуть генерувати ембеддінги для слів, яких не було в навчальних даних.
- FastText обробляє OOV слова за допомогою підслів (символьних n–грам), дозволяючи виводити їхнє значення.
- ELMo (на основі символів) та BERT (токенізація підслів) також ефективно обробляють OOV слова завдяки своїм архітектурам.

Вибір моделі ембеддінгів часто передбачає компроміс між продуктивністю та обчислювальними витратами (табл. 2.2).

Таблиця 2.2

Порівняльний аналіз методів генерації ембеддінгів

Модель	Контекстуальна	Обчислювальна вартість
FastText	Ні	Низька
Word2Vec	Ні	Низька
GloVe	Ні	Низька
Cohere Embeddings	Так	Середня–Висока
OpenAI Embeddings	Так	Висока
SentenceTransformers	Так	Середня–Висока
BERT	Так	Висока
ELMo	Так	Середня–Висока

Як видно з таблиці 2.2, статичні ембеддінги мають низьку обчислювальну вартість, що робить їх привабливими для ресурсів, що мають обмеження, але є простими та ефективними. Однак їхня семантична точність, як правило, нижча порівняно з моделями на основі трансформерів.

Контекстуалізовані моделі, такі як BERT, ELMo, GPT та SentenceTransformers, пропонують значно вищу семантичну точність та контекстуальне розуміння. Це досягається за рахунок вищих обчислювальних витрат, особливо для великомасштабної генерації ембеддінгів. Контекстуальні ембеддінги, як правило, більші за розміром (наприклад, 1024 виміри проти 300 для статичних) і призводять до більших та важчих моделей.

Дослідження показують, що контекстуальні ембеддінги, як правило, перевершують статичні в більшості завдань NLP. Наприклад, BERT значно перевершив ELMo в завданнях розпізнавання кореференції. ELMo також показав найкращі результати в цілому в завданнях розпізнавання кореференції. Однак, спостерігається зменшення віддачі від продуктивності зі збільшенням розміру ембеддінгів. Модель, що використовує лише символьні ембеддінги, може досягти 86% продуктивності найбільшої моделі (ELMo, GloVe, символьні) при 1.2% її розміру. Це свідчить про компроміс між продуктивністю (прогностичною та часом виконання) та розмірністю.

Незважаючи на те, що більші моделі можуть сходитися швидше (за кількістю епох та загальним часом навчання), вони все ще повільніші під час тестування. FastText показав кращі результати, ніж Word2Vec та Polyglot, у завданнях узгодження онтологій та краще обробляє OOV слова. GloVe перевершив FastText та Word2Vec у завданні класифікації твітів, особливо при навчанні на специфічних корпусах.

Тому вибір моделі для обробки ембедінгів повністю залежить від поставленого інженерного завдання та може бути реалізовано як на основі статичних, так і на основі контекстуалізованих моделей.

3. СИСТЕМА ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА ЗА БІОЛОГІЧНИМИ МОДАЛЬНОСТЯМИ

3.1. Розробка системи ідентифікації користувача

На основі запропонованого у пункті 2.3.2 алгоритму спроектована система ідентифікації користувача за обличчям. Вона представлена у вигляді набору взаємозв'язаних модулів, кожен із яких відповідає за свою функціональність, а модульний підхід до реалізації системи дозволяє тестувати та вдосконалювати компоненти незалежно один від одного.

Згідно із алгоритмом можна запропонувати розробку наступних ключових модулів:

1. Модуль збору даних;
2. Модуль попередньої обробки зображень;
3. Модуль виділення ознак;
4. Модуль збереження шаблонів;
5. Модуль ідентифікації / аутентифікації;
6. Модуль оцінки ефективності;
7. Інтерфейс користувача.

А сама структурна схема системи ідентифікації користувача представлена на рисунку 3.1.

1. Модуль збору даних. Відповідає за отримання вхідних зображень обличчя, отримує відеопотік з веб–камери або статичні зображення з файлової системи. Результатом його роботи є послідовність сирих зображень/кадрів. У процесі роботи здійснює корекцію якості зображення шляхом фільтрація шумів, корекція освітлення, підвищення контрасту. Проводить попереднє виявлення на зображеннях біометричних ознак та його позиціонування (наприклад, поворот обличчя до фронтальної позиції).

2. Модуль попередньої обробки зображень відповідає за підготовку "сирих" зображень обличчя до виділення ознак, мінімізуючи вплив зовнішніх факторів.

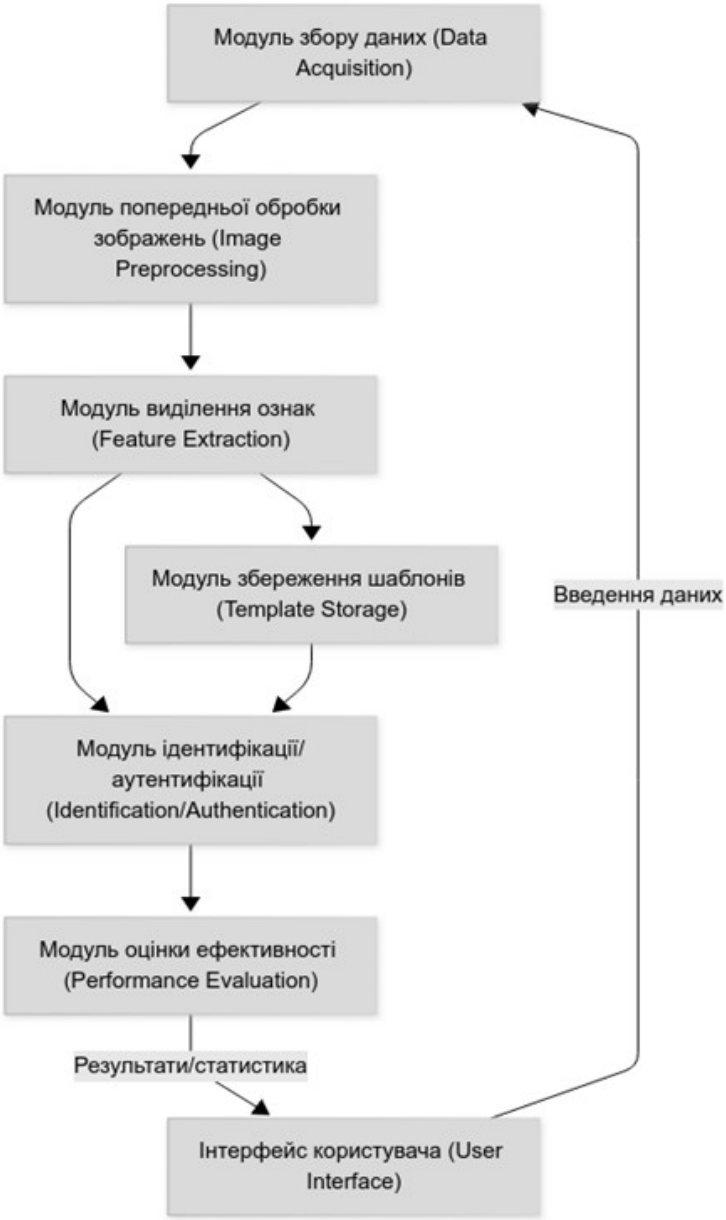

Рисунок 3.1 – Структурна схема системи ідентифікації

Отримуючи з модуля збору даних сире зображення (кадр) проводить виявлення місця розташування обличчя на зображенні застосовуючи існуючі алгоритми пошуку (Haar Cascades, dlib HOG+SVM, або CNN–based (MTCNN, RetinaFace). Якщо знайдено кілька облич, може бути реалізована логіка вибору (наприклад, найбільше обличчя, або всі обличчя в залежності від запиту користувача). Масштабування та обрізка до фіксованого розміру (наприклад, 160x160 пікселів), що є стандартним для багатьох моделей глибокого навчання.

3. Модуль виділення ознак забезпечує перетворення обробленого зображення обличчя на компактний числовий вектор (ембеддінг), який містить

унікальні дискримінантні ознаки. Отримуючи на вході одне стандартизоване зображення обличчя. Перетворює його у ембеддінг фіксованої розмірності (наприклад, 128 або 512 чисел з плаваючою комою). Завдання модулю є завантаження попередньо навченої моделі глибокого навчання передача їй обробленого зображення обличчя та отримання вихідного ембеддінгу. Цей модуль відповідає лише за генерацію ембеддінгу, а не за порівняння.

4. Модуль збереження шаблонів забезпечує безпечне та ефективне зберігання біометричних шаблонів (ембеддінгів обличчя) зареєстрованих користувачів. На початку своєї роботи модуль отримує ім'я користувача та його біометричний ембеддінг, а результатом є при першому запуску запис в базу даних інформації про нового користвача, а при другому і наступних запусках запис нового користувача в базу даних або пошук інформації про існуючого. В концепції захисту системи цей крок є одним із ключових кроків. Даний модуль забезпечує необхідний рівень захисту інформації про користувача та його рису шляхом шифрування інформації, що в ньому обробляється. На даному кроці ми можемо використовувати простий алгоритм AES 128, який завдяки модульній реалізації системи у будь який момент зможемо поміняти на інший, більш сучасний алгоритм.

5. Модуль ідентифікації / аутентифікації призначений для виконання порівняння вхідного біометричного ембеддінгу з базою зареєстрованих шаблонів та прийняття рішення про ідентифікацію / аутентифікацію користувача. На вхід даного модуля поступає опрацьований ембеддінг обличчя, що потрібно ідентифікувати. Для виконання поставленого завдання цьому модулю необхідний доступ до бази даних. у результаті спроби ідентифікації ми отримаємо або повідомлення що користувач знайдений, або що він невідомий. В процесі роботи модуль проводить розрахунок схожості/відстані, тобто порівняння вхідного ембеддінгу з кожним ембеддінгом у базі даних, використовуючи метрику відстані. Для здійснення даної операції необхідно заздалегідь визначити поріг схожості для прийняття рішення. Якщо максимальна схожість (або мінімальна відстань) перевищує поріг, ідентифікація успішна, якщо ні, обличчя вважається невідомим або

неідентифікованим. На даному етапі необхідно виконувати пошук в базі даних згідно з однієї із раніше розглянутих логік: 1:N ідентифікації або 1:1 аутентифікації.

6. Модуль оцінки ефективності призначений для об'єктивної оцінки точності проведеної ідентифікації та відповідно для оцінки надійності системи в цілому. Для початкового налаштування даного модуля необхідно провести тестування алгоритму шляхом внесення в нього тестового датасету зображень обличчь з відомими ідентифікаторами та результати їх ідентифікації. В резьтаті тестування модуль надасть числові метрики ефективності методу розпізнавання. Він здійснює розрахунок представлених в 2 розділі параметрів, таких як відсоток неправильних ідентифікацій (неавторизований користувач прийнятий) та відсоток правильних користувачів, які були відхилені. Для візуалізації результатів виконаного завдання може бути побудована ROC–крива.

7. Інтерфейс користувача це останній елемент стукрутри системи біометричної ідентифікації, який призначений для забезпечення взаємодії користувача із системою. Він забезпечує адекватну реакцію на дії користувача та вивід графічних та текстових даних отриманих у результаті роботи.

Така архітектура системи дозволяє чітко розділити відповідальності та забезпечити гнучкість у виборі конкретних алгоритмів та технологій для кожного модуля, дозволяючи змінити алгоритм детекції обличчя або модель для виділення ознак, не змінюючи інші частини системи.

3.2.Програмна реалізація семи модульної системи біометричної ідентифікації

Як зазначено в пункті 3.1 реалізація розробленого алгоритму запропонована шляхом побудови системи, що містить сім компонент:

1. Модуль збору даних;
2. Модуль попередньої обробки зображень;
3. Модуль виділення ознак;

4. Модуль збереження шаблонів;
5. Модуль ідентифікації / аутентифікації;
6. Модуль оцінки ефективності;
7. Інтерфейс користувача.

Система реалізована шляхом виконання кожного із модулів на мові програмування Python із залученням модуля *tkinter* для забезпечення останнього пункту – зрозумілого та доступного **інтерфейсу користувача**.

Перший модуль – **модуль збору даних** забезпечує фотографування особи, що потребує ідентифікації чи авторизації із виділенням на ньому обличчя. Код програмної реалізації цього модуля представлено в додатку Б. Модуль Tkinter у реалізації створює графічний інтерфейс що виводить відеопотік із веб–камери ноутбука на екран у реальному часі. Завдяки використанню комп'ютерного зору (бібліотека OpenCV) проводиться автоматичний пошук обличчя на відео – скрипт аналізує кожен кадр, знаходить людське обличчя та малює навколо нього зелений прямокутник (рис. 3.2).

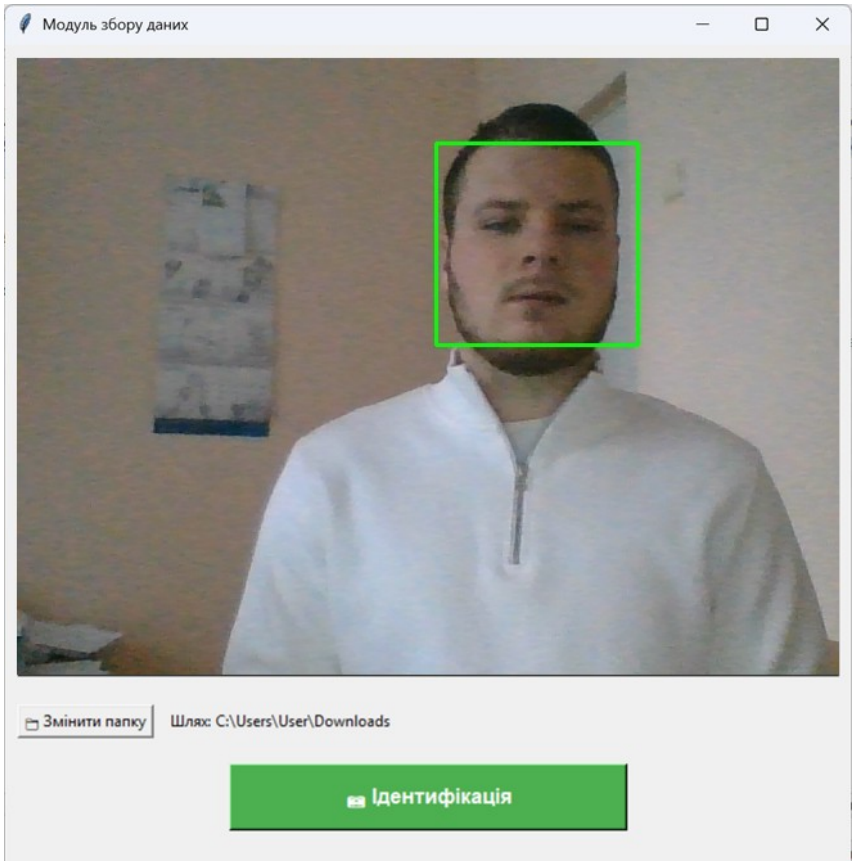

Рисунок 3.2 – Захоплення обличчя модулем збору даних

Використання комп'ютерного зору дозволяє відразу бачити чи у ракурсі камери присутні об’єкти для розпізнавання чи ні та відповідно виділяти їх.

Представлена програмна реалізація дозволяє вибрати папку для зберігання фотографій, причому спеціально реалізований алгоритм дозволяє коректно записувати файли навіть у папки з українськими назвами, що вирішує проблему кодування Windows. При натисканні на кнопку "Ідентифікація" поточний кадр із камери (разом із зеленою рамкою навколо обличчя) миттєво зберігається у вибрану директорію під унікальним ім'ям, що складається з поточної дати та часу.

У запропонованій системі фотографування буде проводитися не при натисканні спеціальної кнопки, а при введенні коду користувача. Це забезпечить базову багатофакторну автентифікацію користувача – через підтвердження пін–кодом або паролем та біометричними даними, такими як обличчя користувача.

Наступним кроком є нормалізація зображень користувачів. Цим займається **модуль попередньої обробки зображень.** Необхідно перевести фотографію у шаблон, який ми в подальшому будемо порівнювати з наступними. Для цього необхідно виділити на фотографії обличчя та стандартизувати його. Під час таких дій можуть виникнути певні неприємні ситуації, наприклад якщо ми просто знайдемо квадрат обличчя і змінимо його розмір наприклад на 600 × 600, обличчя може розтягнутися, якщо вихідний прямокутник не був ідеальним квадратом, що приведе до неможливості аутентифікувати користувача у майбутньому. Для того щоб уникнути такої ситуації необхідно виконати наступні кроки:

1. Знайти обличчя.
2. Трохи розширити зону виділення (додати "повітря" навколо голови, щоб захопити волосся та підборіддя).
3. Обрізати це зображення.
4. Якщо вирізане зображення не квадратне, необхідно додати чорні смуги (поля) з боків або зверху/знизу, щоб зробити його ідеальним квадратом. Такий процес називається "letterboxing".

5. І тільки після цього можна змінити розмір цього квадрата.

В додатку Б представлено код для виконання даної послідовності дій. У результаті його виконання ми отримуємо стандартизований кадр заздалегідь вказаного розміру для подальшого використання.

Модуль виділення ознак здійснює перетворення створеного на попередньому кроці зображення в цифровий ембедінг. У результаті виконання коду представленого на рисунку 3.3 отримуємо цифрове значення збережене у звичному для Python представлені – у вигляді файлу із розширенням **.npy*.

File Edit Format Run Options Window Help

```
import face_recognition
import numpy as np
import os

def create_embedding(image_path, output_path):
    if not os.path.exists(image_path):
        print(f"Помилка: Файл {image_path} не знайдено.")
        return
    print(f"Обробка файлу: {image_path}...")
    image = face_recognition.load_image_file(image_path)
    encodings = face_recognition.face_encodings(image)
    final_encoding = None

    if len(encodings) > 0:
        final_encoding = encodings[0]
        print("Обличчя розпізнано автоматично.")
    else:
        print("Автопошук не дав результату (можливо, через обрізку).")
        print("Генерую ембедінг примусово з усього кадру...")
        height, width, _ = image.shape
        full_image_box = [(0, width, height, 0)]
        encodings = face_recognition.face_encodings(image, known_face_locations=

        if len(encodings) > 0:
            final_encoding = encodings[0]

    if final_encoding is not None:
        np.save(output_path, final_encoding)
        print(f"☑ Ембедінг успішно збережено у файл: {output_path}")
        print(f"Розмірність вектора: {final_encoding.shape}")
    else:
        print("❌ Не вдалося згенерувати ембедінг навіть примусово.")
if __name__ == "__main__":
    input_file = "processed_face_600x600.jpg"
    output_file = "face_embedding.npy"
    create_embedding(input_file, output_file)
```

Ln: 25 Col: 13

Рисунок 3.3 – Код реалізації перетворення зображення у математичний ембедінг

Код представлений на рисунку 3.3 створює бінарний файл у якому збережено масив із ембедінгом (рис. 3.4).

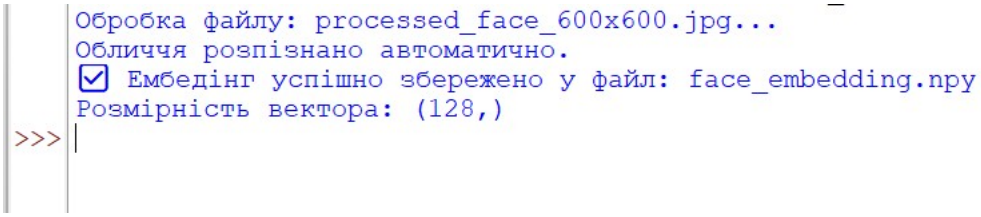

Рисунок 3.4 –Успішна генерація ембедінгу на основі фото

Для захисту від помилок при аналізі стандартизованого зображення введено додаткові команди для примусового аналізу фото. При потребі користувач може вказати шлях де знайти початковий кадр та куди зберігати кінцевий файл, по замовчуванню виконується зберігання у папку де знаходиться файл з кодом.

Наступний елемент системи – модуль збереження шаблонів. Мало сформувати файл з ембедінгом, необхідно інформацію про нього та про користувача якому він відповідає зберегти в базу даних та захистити цей запис. На даному кроці система запитує логін та пароль користувача для сформування специфічної назви файлу (рис. 3.5).

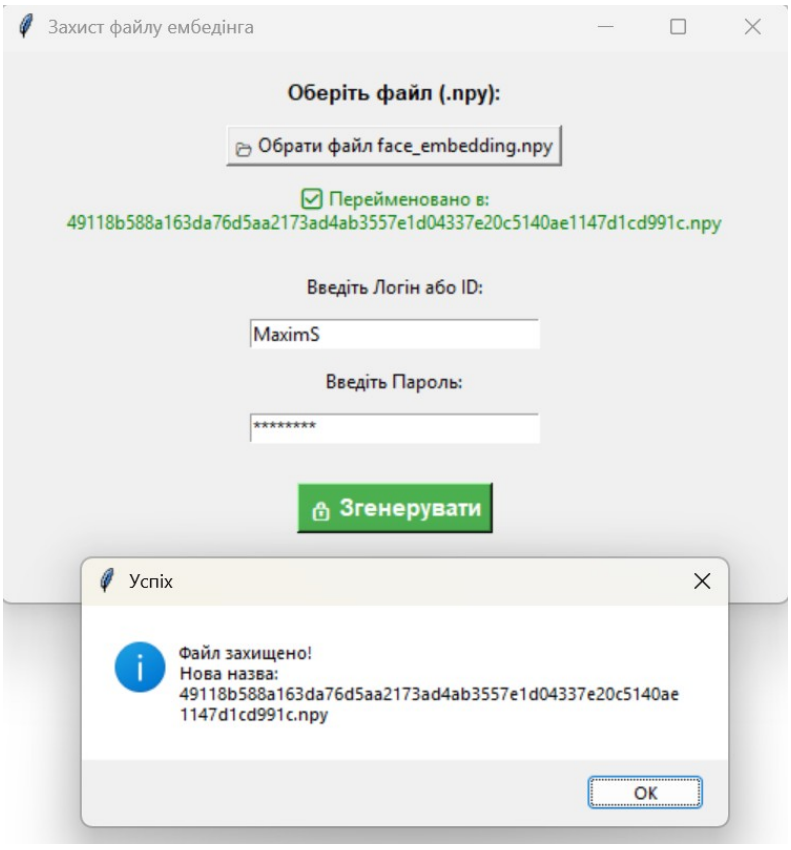

Рисунок 3.5 – Генерація імені файлу з ембедінгом

Програма бере вміст двох полів Логін та Пароль об’єднує їх в одну змінну та використовує алгоритм SHA–256, який перетворює цю змінну на унікальний набір символів що і записується в назву файлу. Таким чином для кожного файлу буде згенеровано унікальну назву.

Наступний елемент системи – **модуль ідентифікації / аутентифікації**. Отримавши доступ до файлу із згенерованою на попередньому кроці назвою, наприклад *49118b588a163da76d5aa2173ad4ab3557e1d04337e20c5140ae1147d1cd991c.npy*, необхідно здійснити одну з двох дій – **ідентифікацію або аутентифікацію** користувача. Логічно, що ідентифікація користувача це крок, що передує автентифікації, але програмно вони виконуються в протилежній послідовності.

Отже, спочатку система перевіряє чи може аутентифікувати такого користувача. для цього у базі даних відбувається пошук по імені файлу. Якщо такий файл в неї добавлений, то це означає, що в системі є користувач із таким ім’ям та паролем. Наступним кроком відбувається порівняння вмісту двох файлів та обчислюється Євклідова відстань і в залежності від неї приймається рішення чи це та сама людина чи ні.

Загально прийнято, що якщо "дистанція":

- **0.00**, то фотографії **ідентичні** (один і той самий файл);
- **0.10 – 0.45**, то обличчя **дуже схожі** (одна й та сама людина, трохи різний ракурс чи світло);
- **0.55 – 0.60**, то це зазвичай **граничний випадок**, може бути які одна людина зі зміненою зовнішністю (окуляри, борода) так і дуже схожий родич.
- **> 0.60**, такі люди **різні**.
- **> 0.90**, такі люди **абсолютно різні** (наприклад, різна стать чи раса).

Провівши порівняння двох файлів із різними ракурсами ми отримуємо результати порівняння (рис. 3.6).

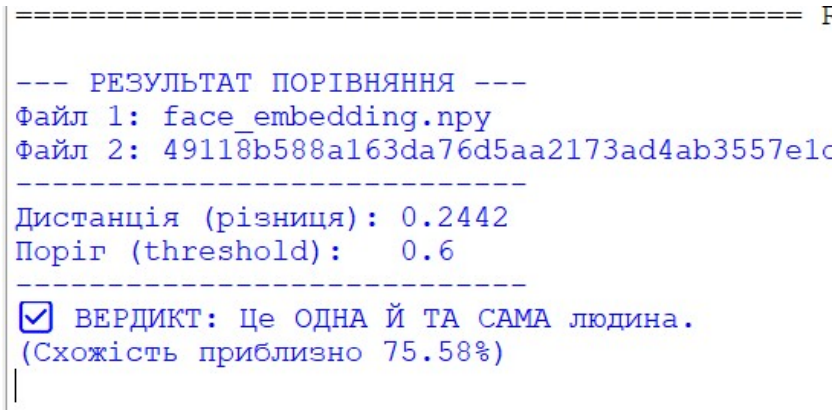

Рисунок 3.6 – Порівняння двох файлів з ембедінгами

Отже, завдяки порівнянню двох файлів ембедінгів приймається рішення по допуску або відхиленню користувача для доступу до інформації або системи. Це є результатом проведення аутентифікації користувача.

Ідентифікація користувача містить всі ті самі початкові кроки що і аутентифікація. Проте, після негативного результату пошуку назви файлу в базі даних відбувається додавання файлу в відповідну папку да створення відповідного запису у базі даних.

Модуль оцінки ефективності призначений для оцінки того, чи правильно система виконує поставлену перед нею задачу та чи здатна відрізнити користувачів один від одного.

3.3. Оцінка ефективності розробленої системи

Оцінка ефективності не може бути при ведена лише для одного користувача та повинна враховувати різні умови здійснення фотографування та оточуючого середовища, тому мінімальною необхідною умову для тестування є виконати наступний практичний дослідний сценарій що містить три кроки:

1. Етап реєстрації
2. Етап тестування точності.
3. Етап дослідження вразливості.

Етап реєстрації полягає у створенні одного основного та кількох додаткових користувачів (табл. 3.1).

Таблиця 3.1

Умови етапу реєстрації

Користувач	Роль	Кількість зразків	Умови зйомки
User A (MaximS)	Основний користувач (об'єкт тестування)	10	Нормальне світло, нейтральні вирази обличчя.
User B	Сторонній користувач (тестування FAR)	10	Нормальне світло, нейтральні вирази обличчя.
User C	Сторонній користувач (тестування FAR)	10	Нормальне світло, нейтральні вирази обличчя.

Як бачимо з таблиця 3.1, пропонується створити три користувачі один із них основний та два додаткових. Для кожного користувача системі необхідно провести зйомку 10 різних кадрів. Користувач **MaximS** в процесі фотографування повинен трохи змінювати ракурс або вираз обличчя між знімками, щоб підвищити надійність еталону.

Для кожного кадру система проведе обчислення ембедінгу та порівняє його із рештою зі списку кадрів цього ж користувача.

На другому етапі **тестування точності** проводиться визначення порогу схожості та обчислення рівня помилок. етап тестування також містить три кроки, а саме: помилкове відхилення, помилковий допуск та аналіз межі.

Помилкове відхилення, тобто FRR визначається в залежності від того, як успішно справжній користувач, в нашому випадку **MaximS** проходить аутентифікацію.

Для тестування помилкових відхилень можуть використовуватися зображення користувача з різних ракурсів, при різному освітленні та при закритті частини обличчя предметом одягу або рукою. Частину таких тестувань можна уникнути заздалегідь завдяки згадуваному раніше модулю комп’ютерного зору. На рисунку 3.7 представлена фотографія користувача MaximS, що відхиляється від обробки у зв’язку із зміщенням ракурсу погляду.

Рисунок 3.7 – Зміна ракурсу погляду

Як бачимо на рисунку 3.7 обличчя користувача **MaximS** не розпізнано на фотографії взагалі. При закритті частини обличчя предметами одягу або рукою (рис. 3.8), обличчя розпізнається, проте при обчисленні ембедінгів воно буде відрізнятися від оригіналу.

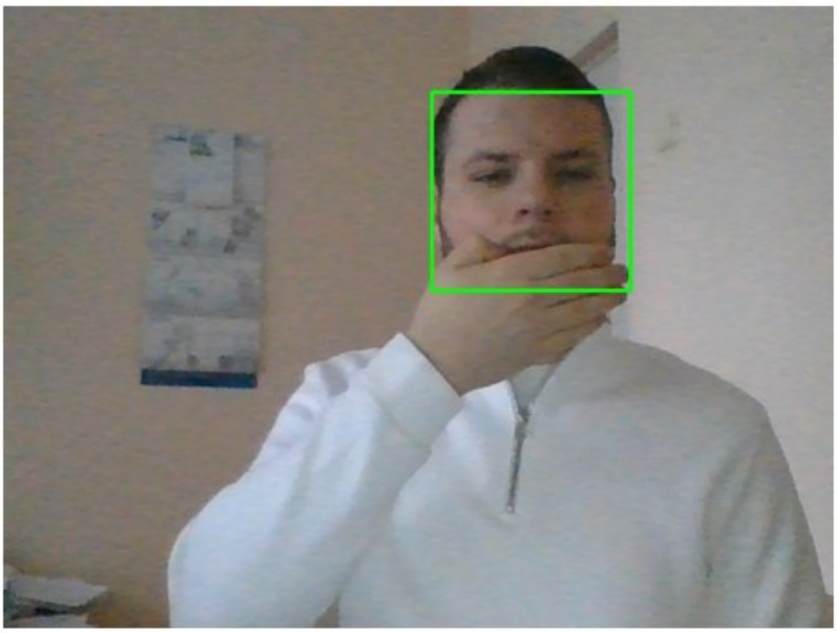

Рисунок 3.8 – Закриття частини обличчя

В таблиці 3.2 представлено статистику кількості проб спроби аутентифікації користувача MaximS та їх наслідки.

Таблиця 3.2

Аутентифікація користувача MaximS

Умови спроби	Кількість	Позитивний результат	Негативний результат	Причина
Ідеальні (Нормальне світло, без аксесуарів)	10	10	0	–
Середні (Часткове затемнення, невеликий ракурс)	10	9	1	Провал через затемнення частини обличчя.
Складні (В окулярах, з шарфом / маскою до носа)	10	7	3	Провал через приховування ключових точок.
Всього	30	26	4	–

Як бачимо з таблиці 3.2, користувач **MaximS** намагався аутентифікуватися 30 раз змінюючи умови спроби. Після 10 базових кадрів на етапі реєстрації у нього не виникло жодних проблем з аутентифікацією при нормальних умовах освітлення та відкритому обличчі. Після зміни освітлення з 10 спроб одна була не успішною, а при закриванні частини обличчя з 10 спроб не успішними були вже три.

Помилковий доступ, тобто FAR, виникає тоді, коли сторонні користувачі, у нашому випадку це користувачі User B та User C намагаються автентифікуватися як користувач MaximS (табл. 3.3).

Таблиця 3.3

Аутентифікація, інші користувачі як користувач MaximS

Користувач	Кількість	Негативний результат	Позитивний результат
User B	15	15	0
User C	15	14	1
Всього	30	29	1

Як бачимо в таблиці 3.3, користувачі User B та User C намагаються автентифікуватися як користувач MaximS, для чого кожен з них здійснює 15 спроб. Якщо користувачі по замовчуванню не є схожими або родичами, то кількість позитивних результатів, тобто результатів входу в систему повинен бути рівний нулю. В ході тестування одна спроба з 30 було успішною, можливо сторонні користувачі повторили вираз обличчя об'єкта тестування.

Аналіз межі або границі допустимої схожості полягає в оцінці коефіцієнта, що використовується при порівнянні двох фотографій. Для цього змінюється поріг, а самі тестування повторюються (табл. 3.4).

Таблиця 3.4

Повторення тестування з різними значеннями межі

Межа	Кількість спроб	FRR	FAR
0,55 (Сувора)	30	18 %	0 %
0,60 (Базова)	30	13,3 %	3,3 %
0,65 (М'яка)	30	3,3 %	10 %

Як бачимо з таблиці 3.4, для проведення даного досліду повторюються досліди відображені в таблицях 3.2 і 3.3. Різниця в тому, що міняється гранична межа допуску користувачів до системи. Відповідно використання більш сурових обмежень, межа = 0,55, приводить то збільшення кількості помилкових відхилень аутентифікації основного користувача, що ускладнює йому доступ але в одночас забезпечує вищий рівень захисту від помилкового доступу.

При використанні м'яких обмежень, межа = 0,65, основний користувач навіть змінюючи освітлення та закриваючи частину обличчя проходить майже всі перевірки (1 відхилення з 30 спроб). Проте, такі м'які обмеження приводять до того, що збільшується кількість позитивних спроб помилкового доступу, коли зловмисники отримують доступ до системи, що працює виключно на основі біометричного захисту (3 успішних доступи з 30 спроб).

Третій етап **дослідження вразливості** полягає в оцінці того, наскільки легко можна обманути систему із використанням простих атак підробки. Для

тестування атак підробки застосовують зовнішні обєкти такі як фото та відео при звичайній межі допустимої схожості (табл. 3.5).

Таблиця 3.5

Спроба автентифікації User A за допомогою зовнішніх об'єктів

Тип атаки	**Джерело**	**Кількість спроб**	**Позитивний результат**
Фото	Роздруковане кольорове фото обличчя User A	10	8
Відео	Відео обличчя User A на екрані смартфона	10	9

Як бачимо з результатів тестування представлених у таблиці 3.5, система виключно із застосуванням біометричного методу аутентифікації є критично вразливою до атак підміни. Використання роздрукованого кольорового обличчя користувача приводить до помилкового доступу у 8 випадках із 10, а використання відео – у 9 із 10.

Тому для додаткового захисту при біометричній аутентифікації використовують модулі визначення живої присутності, які перевіряють рух очей або міміку, а не лише статичний знімок.

У запропонованій системі необхідний рівень захисту забезпечується шляхом багатофакторної аутентифікації, при якій зловмисник повинен не тільки обійти біометричну перевірку, а й отримати доступ до паролю чи пін–коду.

3.4. Переваги розробленого та реалізовано алгоритму

У процесі роботи було розроблено та реалізовано алгоритм роботи системи ідентифікації користувача. Зважаючи на те, що вона побудована на модульному підході, то це дозволяє досягти низки цілей для забезпечення захищеності та ефективності системи, а саме:

1. **Забезпечення послідовності та цілісності даних**. Розроблений алгоритм чітко визначає послідовність обробки біометричних даних від моменту їхнього захоплення до кінцевого рішення про ідентифікацію/автентифікацію. Завдяки послідовному проходженню через модулі попередньої обробки та виділення ознак, алгоритм гарантує, що лише стандартизовані та якісні дані перетворяться на шаблони. Кожен модуль має чітко визначені вхідні та вихідні дані, що мінімізує помилки інтеграції та забезпечує цілісність інформації під час передачі між компонентами.

2. Спрощення розробки та обслуговування. Головна перевага запропонованого алгоритму – модульність, що забезпечує незалежність компонентів та легкість вдосконалення. Якщо необхідно оновити алгоритм, достатньо замінити лише один із модулів, не торкаючись інших частин системи. У разі збою чи помилки можна швидко діагностувати проблему в конкретному модулі та виправити її.

3. Забезпечення безпеки та відповідності стандартам. Запропонована схема дозволяє вбудувати механізми безпеки в найкритичніші точки, а саме:

- Захист шаблонів. Оскільки біометричні дані зберігаються лише у вигляді векторів ознак, а не оригінальних зображень, це підвищує безпеку та забезпечує незворотність, що є критичним для захисту даних.
- Контроль доступу. Система дозволяє розмежовувати доступ до різних компонент та застосовувати жорсткі політики доступу лише наприклад, до Модулів збереження шаблонів та ідентифікації/автентифікації.

4. Настроювання та Оптимізація. Структурна схема робить систему гнучкою для налаштування.

В цілому застосування такого алгоритму із модульною реалізацією забезпечує необхідний рівень захисту та ефективності в цілому.

ВИСНОВКИ

У магістерській роботі вирішено актуальне завдання розробки алгоритмів ідентифікації користувачів із використанням біометричних даних.

У результаті проведеного дослідження отримано такі основні результати:

1. Проведено аналіз методів аутентифікації, зокрема методів багатофакторної аутентифікації. Обґрунтовано використання двохфакторної аутентифікації, одним із методів якої є біометрична аутентифікація.

2. Проведено аналіз ключових показників ефективності біометричних систем аутентифікації для оцінки системи біометричної аутентифікації на основі розроблювального алгоритму.

3. Проведено аналіз сучасних алгоритмів виділення ознак, визначень ключові властивості, що впливають на вибір такого алгоритму в залежності від поставленої задачі.

4. Проведено порівняння ключових архітектур CNN для біометричних систем, що дають змогу зменшити показники FAR, необхідних для надійних великомасштабних 1:N систем ідентифікації.

5. На основі проведеного порівняльного аналізу методів генерації ембеддінгів та принципів їх застосування запропоновано алгоритм ідентифікації користувача із використанням біометричних даних.

6. Спроектовано та проведено моделювання роботи семимодульної системи ідентифікації користувача за обличчям та використанням паролю, що підтверджує ефективність запропонованого алгоритму.

7. Проведено практичну оцінку ефективності змодельованої системи та представлено ключові переваги модульної реалізації системи на основі запропонованого алгоритму багатофакторної аутентифікації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Соколік, М., Гарматюк, В., Кулина С. Методи ідентифікації користувачів із використанням біометричних даних. Інноваційні підходи до розвитку технологій та економіки. – Свалява: ЗУНУ, 2025. – С. 215–216.
2. Соколік, М., Кулина С. Аналіз сучасних алгоритмів виділення ознак в біометрії. Захист інформації: Збірник матеріалів науково–практичного симпозіуму, 28.11.2025. – Тернопіль, 2025. – С. 94–96.
3. Яіцький, А. О. (2022). Ефективні методи та засоби захисту фішингових атак. *Варшава: Problems of science and practice, tasks and ways to solve them*, 417–419.
4. Suleski T, Ahmed M, Yang W, Wang E. A review of multi–factor authentication in the Internet of Healthcare Things. *Digital Health*. 2023;9.
5. Cybersecurity and Infrastructure Security Agency. (n.d.). *Multifactor authentication*. https://www.cisa.gov/topics/cybersecurity–best–practices/multifactor–authentication
6. Kizza, J. M. (2024). Authentication. In *Guide to Computer Network Security* (pp. 215–238). Cham: Springer International Publishing.
7. Cao, X., Yang, Z., Ning, J., Jin, C., Lu, R., Liu, Z., & Zhou, J. (2024). Dynamic group time–based one–time passwords. *IEEE Transactions on Information Forensics and Security*, *19*, 4897–4913.
8. Trevino, A. (2023, June 27). *Types of multi–factor authentication (MFA)*. Keeper Security. https://www.keepersecurity.com/blog/2023/06/27/types–of–multi–factor–authentication–mfa/
9. Kim, M., & Kwon, H. (2022). A study of the emerging trends in SIM swapping crime and effective countermeasures. In *2022 IEEE/ACIS 7th International Conference on Big Data, Cloud Computing, and Data Science* pp. 240–245.
10. Microsoft. (2025, March 4). *Authentication methods and features – Microsoft Entra ID*. Microsoft Learn. https://learn.microsoft.com/en–us/entra/identity/authentication/concept–authentication–methods
11. Li, S., Xu, C., Zhang, Y., & Zhou, J. (2022). A secure two–factor authentication scheme from password–protected hardware tokens. *IEEE Transactions on Information Forensics and Security*, *17*, 3525–3538.
12. Descope. (2023, December 15). *What is FIDO2 & how does FIDO authentication work?* https://www.descope.com/learn/post/fido2
13. Verma, A., Moghaddam, V., & Anwar, A. (2021). *Data–driven behavioural biometrics for continuous and adaptive user verification using Smartphone and Smartwatch*. arXiv. https://doi.org/10.48550/arXiv.2110.03149
14. Єжова, Є. (2025). Методи Захисту Від Атак На Біометричні Системи Аутентифікації. *Міжнародна науково–практична конференція Інформаційні технології та комп'ютерне моделювання*, 161–163.

15. Ayub Khan, A., Laghari, A. A., Shaikh, A. A., Bourouis, S., Mamlouk, A. M., & Alshazly, H. (2021). Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission. *Applied Sciences*, *11*(22), 10917.
16. De Freitas Pereira, T., & Marcel, S. (2021). Fairness in biometrics: a figure of merit to assess biometric verification systems. *IEEE Transactions on Biometrics, Behavior, and Identity Science*, *4*(1), 19–29.
17. Meananeatra, P., Charoendouysil, B., Wisuttikul, T., Kasisopha, N., & Saechiam, S. (2025, May). Comparative performance of face biometric verification system with multi selfie devices. In *2025 8th International Conference on Artificial Intelligence and Big Data* (pp. 605–611). IEEE.
18. Jain, A. K., Deb, D., & Engelsma, J. J. (2021). Biometrics: Trust, but verify. *Transactions on Biometrics, Behavior, and Identity Science*, *4*(3), 303–323.
19. Wijewardena, K. P., Grosz, S. A., Cao, K., & Jain, A. K. (2022). Fingerprint template invertibility: Minutiae vs. deep templates. *IEEE Transactions on Information Forensics and Security*, *18*, 744–757.
20. El–Tarhouni, W., Abdo, A., & ELmegreisi, A. (2021, May). Feature fusion using the local binary pattern histogram fourier and the pyramid histogram of feature fusion using the local binary pattern oriented gradient in iris recognition. In *2021 IEEE 1st International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering MI–STA* pp. 853–857.
21. Kharat, A., Garje, P., & Wantmure, R. (2023). Local approaches in face recognition: a case study using histogram of oriented gradients (HOG) technique. *NCRD's Technical Review: e–Journal*, *8*(1), 1–12.
22. Zhang, H., & Yang, Z. (2023). Biometric Authentication and Correlation Analysis Based on CNN-SRU Hybrid Neural Network Model. *Computational Intelligence and Neuroscience*, *2023*(1), 8389193.
23. Wazirali, R., Ahmed, R. (2022). Hybrid Feature Extractions and CNN for Enhanced Periocular Identification During Covid–19. *Computer Systems Science and Engineering*, *41(1)*, 305–320. https://doi.org/10.32604/csse.2022.020504
24. Soban, K. (2023). *What is biometric spoofing and how to prevent it?* Facia. https://facia.ai/blog/what–is–biometric–spoofing–and–how–to–prevent–it/
25. Office of the Victorian Information Commissioner. (n.d.). *Biometrics and privacy – Issues and challenges*. https://ovic.vic.gov.au/privacy/resources–for–organisations/biometrics–and–privacy–issues–and–challenges/
26. RecFaces. (n.d.). *The false rejection rate: What do FRR & FAR mean?* https://recfaces.com/articles/false–rejection–rate

27. Deo, M. M., Didier, B. M. N. J., Blaise, M. L., & Boaz, N. N. (2024). Multimodal Biometric Revolution: VGG–16 and VGG–19 for Masked Face, Fingerprint and Iris Recognition in Difficult Conditions. *Revue Internationale de la Recherche Scientifique (Revue–IRS)*, *2*(3), 1065–1079.
28. Qawasmeh, B., Oh, J.–S., & Kwigizile, V. (2025). Comparative Analysis of AlexNet, ResNet–50, and VGG–19 Performance for Automated Feature Recognition in Pedestrian Crash Diagrams. *Applied Sciences*, *15*(6), 2928. https://doi.org/10.3390/app15062928
29. Yadav, H. (2022, July 11). *Residual blocks in deep learning*. Towards Data Science. https://towardsdatascience.com/residual–learning–11d95ca12b00/
30. A. (2024, June 6). *What are the differences between VGG, ResNet, DenseNet, MobileNet, EffecientNet, and YOLO autoencoder, Siamese neural networks, capsule networks?* Medium. https://medium.com/what–are–the–differences
31. O'Mahony, N., Campbell, S., Carvalho, A., Harapanahalli, S., Velasco–Hernandez, G., & Walsh, J. (2019). *Deep learning vs. traditional computer vision*. arXiv. https://doi.org/10.48550/arXiv.1910.13796
32. Klingler, N. (2024, May 6). *MobileNet – Efficient deep learning for mobile vision*. viso.ai. https://viso.ai/deep–learning/mobilenet–efficient–deep–learning–for–mobile–vision/
33. National Cyber Security Centre. (2021, June 29). *Device security guidance: Using biometrics*. https://www.ncsc.gov.uk/collection/device–security–guidance/policies–and–settings/using–biometrics
34. Ebrahimpour, N. (2023, March). *Iris recognition using MobileNet for biometric authentication*. 9th International Zeugma Conference on Scientific Research, Gaziantep, Türkiye. https://www.researchgate.net/publication/369033711_iris_recognition_using_mobilenet_for_biometric_authentication
35. Google. (2025). *Biometrics*. Android Open Source Project. https://source.android.com/docs/security/features/biometric
36. Coria, J. M., Bredin, H., Ghannay, S., & Rosset, S. (2020). *A comparison of metric learning loss functions for end–to–end speaker verification*. arXiv. https://doi.org/10.48550/arXiv.2003.14021
37. Sarıgöz, Y. (2022). *Triplet loss – advanced intro*. Towards Data Science. https://towardsdatascience.com/triplet–loss–advanced–intro–49a07b7d8905/
38. Shinde, S. (2021, March 16). *ArcFace explained*. Shubham Shinde. https://shubham–shinde.github.io/blogs/arcface/
39. Musgrave, K. (n.d.). *Losses*. PyTorch Metric Learning. https://kevinmusgrave.github.io/pytorch–metric–learning/losses/
40. Vargas, M., Cannon, R., Engel, A., Sarwate, A. D., & Chiang, T. (2024). *Understanding generative AI content with embedding models*. arXiv. https://doi.org/10.48550/arXiv.2408.10437

Додаток А

Порівняння біометричних модальностей для ідентифікації користувача

Характеристика	Тип	Переваги	Недоліки	Точність	Застосування	Поширення
1	2	3	4	5	6	7
Відбиток пальця	Фізіологічна	Висока унікальність, стійкість до змін, широке поширення, зручність використання, відносно низька вартість сканерів.	Можливість пошкодження пальця, забруднення, проблеми з ідентифікацією у деяких груп людей (старі, будівельники), можливість використання "фальшивих" відбитків.	Висока	Розблокування смартфонів, контроль доступу, банкомати, прикордонний контроль.	Найбільш поширена біометрична технологія.
Малюнок райдужної оболонки ока	Фізіологічна	Надзвичайно висока унікальність, стабільність протягом життя, складно підробити, безконтактність.	Висока вартість обладнання, чутливість до умов освітлення, проблеми з ідентифікацією у людей з катарактою/пошкодженнями ока, необхідність наближення до сканера.	Дуже висока	Контроль доступу до високозахищених об'єктів (банки, лабораторії), аеропорти.	Вважається однією з найточніших біометричних систем.
Геометрія обличчя	Фізіологічна	Природність, безконтактність, можливість ідентифікації на відстані, широке поширення камер.	Чутливість до змін освітлення, виразу обличчя, наявності окулярів/головних уборів, можливість підробки фотографією/відео.	Середня-Висока	Розблокування смартфонів, відеоспостереження, прикордонний контроль, контроль доступу.	Динамічно розвивається, особливо з використанням 3D-технологій та штучного інтелекту.
Малюнок вен долоні/пальця	Фізіологічна	Дуже висока унікальність, висока стійкість до підробки (вени "живої" людини), безконтактність.	Висока вартість обладнання, менша поширеність, вимагає певної пози долоні.	Дуже висока	Банківські термінали, медичні установи, контроль доступу до критичної інфраструктури.	Складність підробки робить цю технологію дуже безпечною.

1	2	3	4	5	6	7
Голос	Поведінкова	Зручність, безконтактність, можливість ідентифікації по телефону.	Чутливість до шуму навколишнього середовища, простуди, зміни емоційного стану, можливість імітації/запису голосу.	Низька-Середня	Телефонні банківські послуги, кол-центри, голосові помічники.	Часто використовується в комбінації з іншими методами для підвищення надійності.
Клавіатурний почерк (динаміка)	Поведінкова	Непомітність, безконтактність, постійний моніторинг, відсутність потреби в додатковому обладнанні.	Низька унікальність, чутливість до зміни клавіатури, емоційного стану, втоми, великий обсяг даних для навчання.	Низька-Середня	Безперервна автентифікація користувача в системах, виявлення шахрайства.	Більш підходить для безперервної верифікації, ніж для первинної ідентифікації.
Підпис (динаміка)	Поведінкова	Природність, загальноприйнятий метод підтвердження, зручність.	Низька унікальність (особливо для статичного підпису), можливість підробки, чутливість до зміни ручки/поверхні.	Середня	Банківські операції (планшети для підпису), поштовий зв'язок, кур'єрські служби.	Важлива динаміка (швидкість, сила натиску), а не лише візуальне зображення.
ДНК	Фізіологічна	Абсолютна унікальність, незмінність.	Дуже висока вартість аналізу, складність та тривалість отримання зразка, етичні та юридичні питання, інвазивність.	Дуже висока	Судова медицина, криміналістика, батьківство.	Не застосовується для щоденної ідентифікації через практичні обмеження.
Хода	Поведінкова	Безконтактність, можливість ідентифікації на відстані без усвідомленої участі.	Низька унікальність, чутливість до взуття, втоми, травм, освітлення, ракурсу.	Низька-Середня	Відеоспостереження для ідентифікації в натовпі (на стадії розробки).	Наразі знаходиться на стадії досліджень та ранніх розробок для масового застосування.

Програмні коди реалізації модулів системи біометричної автентифікації

```
import tkinter as tk
from tkinter import messagebox
import cv2
import face_recognition
import numpy as np
import hashlib
import os
from PIL import Image, ImageTk
# --- НАЛАШТУВАННЯ ---
THRESHOLD = 0.6  # Поріг схожості (менше = суворіше)
TARGET_SIZE = (600, 600)
class BiometricAuthApp:
    def __init__(self, root):
        self.root = root
        self.root.title("Secure Biometric Login")
        self.root.geometry("400x350")

        # Завантаження каскаду для візуалізації
        cascade_path = os.path.join(cv2.data.haarcascades, 'haarcascade_frontalface_default.xml')
        self.face_cascade = cv2.CascadeClassifier(cascade_path)

        self.target_embedding = None # Тут буде еталонний вектор з файлу
        self.create_login_ui()
    def create_login_ui(self):
        """Створює інтерфейс введення логіна/пароля"""
        # Очистка вікна (якщо ми повертаємось сюди)
        for widget in self.root.winfo_children():
            widget.destroy()
        tk.Label(self.root, text="СИСТЕМА КОНТРОЛЮ ДОСТУПУ", font=("Arial", 14,
"bold")).pack(pady=20)

        tk.Label(self.root, text="Логін:").pack()
        self.entry_login = tk.Entry(self.root, width=30)
        self.entry_login.pack(pady=5)
        tk.Label(self.root, text="Пароль:").pack()
        self.entry_pass = tk.Entry(self.root, width=30, show="*")
        self.entry_pass.pack(pady=5)
        tk.Button(self.root, text="УВІЙТИ", bg="#2196F3", fg="white", width=20, height=2,
                  command=self.verify_credentials).pack(pady=30)

        self.status_label = tk.Label(self.root, text="", fg="red")
        self.status_label.pack()
    def verify_credentials(self):
        """Хешує дані і шукає файл"""
        login = self.entry_login.get().strip()
        password = self.entry_pass.get().strip()
```

```
    if not login or not password:
        self.status_label.config(text="Введіть логін та пароль!")
        return
    # 1. Генерація хешу (Логін + Пароль)
    combined = login + password
    file_hash = hashlib.sha256(combined.encode()).hexdigest()
    filename = f"{file_hash}.npy"
    # 2. Перевірка наявності файлу
    if os.path.exists(filename):
        try:
            self.target_embedding = np.load(filename)
            print(f"Профіль знайдено: {filename}")
            self.open_camera_ui()
        except Exception as e:
            messagebox.showerror("Помилка файлу", f"Файл пошкоджено: {e}")
    else:
        self.status_label.config(text="❌ Користувача не знайдено або хибний пароль")
def open_camera_ui(self):
    """Відкриває інтерфейс камери"""
    # Очищаємо вікно логіну
    for widget in self.root.winfo_children():
        widget.destroy()

    # Налаштування камери
    self.cap = cv2.VideoCapture(0)
    if not self.cap.isOpened():
        messagebox.showerror("Помилка", "Не вдалося відкрити камеру")
        self.create_login_ui()
        return
    # Елементи камери
    tk.Label(self.root, text="БІОМЕТРИЧНА ПЕРЕВІРКА", font=("Arial", 12, "bold")).pack(pady=5)

    self.canvas = tk.Canvas(self.root, width=640, height=480, bg="#333")
    self.canvas.pack()

    btn_scan = tk.Button(self.root, text="👁 СКАНУВАТИ ОБЛИЧЧЯ", bg="#4CAF50", fg="white",
                         font=("Arial", 12, "bold"), command=self.process_biometrics)
    btn_scan.pack(pady=10, fill=tk.X, padx=20)

    btn_back = tk.Button(self.root, text="Назад", command=self.close_camera_and_return)
    btn_back.pack(pady=5)
    # Розширюємо вікно під відео
    self.root.geometry("660x650")

    # Запуск циклу відео
    self.update_video()
def update_video(self):
    """Показує відеопотік у реальному часі"""
    if hasattr(self, 'cap') and self.cap.isOpened():
        ret, frame = self.cap.read()
```

```
        if ret:
            self.current_frame = frame.copy() # Зберігаємо "чистий" кадр для обробки

            # Малюємо квадрат для краси (візуалізація)
            gray = cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)
            faces = self.face_cascade.detectMultiScale(gray, 1.1, 5)
            for (x, y, w, h) in faces:
                cv2.rectangle(frame, (x, y), (x+w, y+h), (0, 255, 0), 2)
            # Конвертація для Tkinter
            rgb_frame = cv2.cvtColor(frame, cv2.COLOR_BGR2RGB)
            img = ImageTk.PhotoImage(image=Image.fromarray(rgb_frame))
            self.canvas.create_image(0, 0, image=img, anchor=tk.NW)
            self.canvas.image = img # Збереження посилання, щоб не видалив збирач сміття

    self.root.after(30, self.update_video)
def process_biometrics(self):
    """Основна логіка: Обрізка -> Ембедінг -> Порівняння"""
    if not hasattr(self, 'current_frame'):
        return
    print("Початок обробки...")

    # 1. Спеціальна обрізка та масштабування (наша функція)
    processed_face = self.crop_and_resize(self.current_frame)

    if processed_face is None:
        messagebox.showwarning("Увага", "Обличчя не знайдено або погана якість.")
        return
    # 2. Генерація вектора
    # Оскільки ми вже обрізали фото, кажемо face_recognition, що все фото = обличчя
    h, w, _ = processed_face.shape
    face_locations = [(0, w, h, 0)] # top, right, bottom, left

    encodings = face_recognition.face_encodings(processed_face, known_face_locations=face_locations)

    if len(encodings) == 0:
        messagebox.showerror("Помилка", "Не вдалося згенерувати біометричний код.")
        return

    current_embedding = encodings[0]
    # 3. Порівняння з еталоном (self.target_embedding)
    distance = face_recognition.face_distance([self.target_embedding], current_embedding)[0]

    print(f"Дистанція: {distance:.4f}")
    if distance < THRESHOLD:
        accuracy = (1 - distance) * 100
        self.grant_access(accuracy)
    else:
        self.deny_access(distance)
def grant_access(self, accuracy):
    """Дії при успішному вході"""
```

```
        messagebox.showinfo("УСПІХ", f"✅ ВХІД ДОЗВОЛЕНО!\nСхожість: {accuracy:.1f}%")
        # Тут можна відкрити нове вікно або закрити програму
        self.close_camera_and_return()
    def deny_access(self, dist):
        """Дії при невдачі"""
        messagebox.showerror("ВІДМОВА", f"❌ ВХІД ЗАБОРОНЕНО.\nОбличчя не
розпізнано.\nРізниця: {dist:.3f}")
    def close_camera_and_return(self):
        if hasattr(self, 'cap') and self.cap.isOpened():
            self.cap.release()
        self.root.geometry("400x350")
        self.create_login_ui()
    def crop_and_resize(self, img):
        """
        Логіка з попереднього запиту:
        Знаходить обличчя, додає відступи, робить квадратним, масштабує до 600x600.
        Повертає зображення (numpy array).
        """
        gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
        faces = self.face_cascade.detectMultiScale(gray, 1.1, 5, minSize=(50, 50))
        if len(faces) == 0:
            return None
        # Беремо найбільше обличчя
        largest_face = max(faces, key=lambda rect: rect[2] * rect[3])
        x, y, w, h = largest_face
        # Відступи (20%)
        margin_x = int(w * 0.2)
        margin_y = int(h * 0.2)
        x1 = max(0, x - margin_x)
        y1 = max(0, y - margin_y)
        x2 = min(img.shape[1], x + w + margin_x)
        y2 = min(img.shape[0], y + h + margin_y)
        face_crop = img[y1:y2, x1:x2]
        crop_h, crop_w = face_crop.shape[:2]
        # Letterboxing (квадратизація)
        max_dim = max(crop_h, crop_w)
        square_img = np.zeros((max_dim, max_dim, 3), dtype=np.uint8)

        start_x = (max_dim - crop_w) // 2
        start_y = (max_dim - crop_h) // 2
        square_img[start_y:start_y+crop_h, start_x:start_x+crop_w] = face_crop
        # Масштабування
        final_img = cv2.resize(square_img, TARGET_SIZE, interpolation=cv2.INTER_AREA)
        return final_img
# --- ЗАПУСК ---
if __name__ == "__main__":
    root = tk.Tk()
    app = BiometricAuthApp(root)
    root.mainloop()
```

Додаток В

Копії публікацій

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ

ІІ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ “ІННОВАЦІЙНІ ПІДХОДИ ДО РОЗВИТКУ ТЕХНОЛОГІЙ ТА ЕКОНОМІКИ”

ЗАХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Innovation and science

ЗАКАРПАТСЬКИЙ НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗУНУ

Свалява - 2025

ПОЧЕСНІ ГОЛОВИ КОНФЕРЕНЦІЇ

Микола ДИВАК, д. т. н., професор, проректор з наукової роботи ЗУНУ

СПІВГОЛОВИ КОНФЕРЕНЦІЇ

Едіта ГРАБАР, кандидат педагогічних наук, доцент, директор Закарпатського навчально-наукового центру ЗУНУ
Леся ДУБЧАК, кандидат технічних наук, доцент, завідувач кафедри комп'ютерної інженерії ЗУНУ

ПРОГРАМНИЙ КОМІТЕТ

Мар'ян ТРІПАК, доктор економічних наук, професор кафедри інституту, ректор НРЗВО "Кам'янець-Подільський державний інститут"
Оксана ГОМОТЮК, доктор історичних наук, професор, декан соціально-гуманітарного факультету ЗУНУ
Андрій КОЦУР, к.е.н., доцент, декан факультету економіки та управління
Ігор ЯКИМЕНКО, к.т.н., доцент, декан факультету комп'ютерних інформаційних технологій
Андрій КІЗИМА, к.е.н., доцент, декан факультету фінансів та обліку
Святослав ПИТЕЛЬ, к.е.н., доцент, директор навчально-наукового інституту новітніх освітніх технологій
Василь БРИЧ, д.е.н., професор, директор навчально-наукового інституту інноватики, природокористування та інфраструктури
Віктор РУСІН, к.е.н., доцент, директор Навчально-наукового інституту публічного управління

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ

Олег ПІЦУН - к.т.н., доцент, доцент кафедри комп'ютерної інженерії ЗУНУ
Віктор АНТОНЮК - к.н. з держ.упр., заступник директора з наукової роботи Закарпатського навчально-науково центру
Михайло ШКІЛЬНЯК - д. е. н., професор, завідувач кафедри менеджменту, публічного управління та персоналу
Андрій КРИСОВАТИЙ, доктор економічних наук, професор, завідувач кафедри фінансів ім. С. І. Юрія
Павло ПОПОВИЧ - д.т.н., професор, завідувач кафедри транспорту і логістики
Оксана ТУЛАЙ - д.е.н., професор, завідувач кафедри міжнародних відносин та дипломатії
Оксана МАРУХЛЕНКО - д.н. з держ.упр., завідувач кафедри управління факультету економіки та управління Київського столичного університету імені Бориса Грінченка
Олександр МОЛНАР - к.е.н., доцент, завідувач кафедри економіки, підприємництва та торгівлі економічного факультету ДВНЗ «УжНУ»
Андрій ГІРНЯК - д.пс.н., професор, завідувач кафедри психології та соціальної роботи
Тетяна ПОСПІЄЛОВА - д.н. з держ.упр., доцент, професор кафедри управління факультету економіки та управління Київського столичного університету імені Бориса Грінченка
Аліна ПОМАЗА-ПОНОМАРЕНКО - д.н. з держ. управління, завідувач науково-дослідної лабораторії з дослідження проблем управління у сфері цивільного захисту Національного університету цивільного захисту України (м. Харків)
Вікторія ШВЕДУН - д.н. з держ. управління, професор, професор кафедри економіки та публічного управління Національного аерокосмічного університету «Харківський авіаційний інститут» (м. Харків
Михайло ГАЗУДА - д.е.н., професор, кафедра економіки, підприємництва та торгівлі економічного факультету ДВНЗ «УжНУ»
Вікторія ГОТРА - д.е.н., професор, кафедра економіки, підприємництва та торгівлі економічного факультету ДВНЗ «УжНУ»
Андрій ДЕРЛИЦЯ - к.е.н., в.о. проректора з наукової та міжнародної діяльності НРЗВО "Кам'янець-Подільський державний інститут"
Ірина СИДОР - к.е.н., доцент, доцент кафедри фінансів ім.С.І.Юрія
Руслан РОЗУМ - к.т.н., доцент, доцент кафедри транспорту і логістики
Андрій ВІТРОВИЙ - к.т.н., доцент, доцент кафедри економічної експертизи та землевпорядкування
Ольга СТОЛЯРЕНКО - к.пс.н., доцент, завідувач кафедри соціальної роботи, психології та соціокультурної діяльності ім. Т.Сосновської
Фаєрчук Вадим, Галунька Богдан, Лисик Марія, Шпак Марта, Петришин Наталія - студенти ФКІТ ЗУНУ

МЕТОДИ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІЗ ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ ДАНИХ

Кулина Сергій
PhD, доцент кафедри кібербезпеки
sersks@wunu.edu.ua
Соколік Максим
здобувач вищої освіти, гр. КБм-11
sokmax1@gmail.com
Західноукраїнський національний університет
Гарматюк Валентин
аспірант
gar.val.2000@gmail.com
Західноукраїнський національний університет

Традиційні методи автентифікації, такі як паролі, PIN-коди та фізичні токени, стикаються зі значними проблемами безпеки та зручності. Ці методи вразливі до широкого спектру атак, включно з крадіжками, фішингом та атаками методом перебору [1]. Крім того, вони створюють значне навантаження на користувачів, вимагаючи запам'ятовування та управління численними складними обліковими даними, що часто призводить до використання слабких або повторюваних паролів [3]. Ця вразливість і незручність підкреслюють нагальну потребу в більш надійних та зручних рішеннях для ідентифікації.

У відповідь на ці виклики біометричне розпізнавання стало переконливою альтернативою. Воно використовує унікальні фізіологічні характеристики людини, такі як відбитки пальців, обличчя або райдужна оболонка ока, або поведінкові риси, наприклад, голос або ходу. Цей підхід докорінно змінює парадигму автентифікації з "того, що ви маєте" або "того, що ви знаєте" на "того, ким ви є" [2].

Біометричні системи пропонують низку переваг, що робить їх привабливими для широкого впровадження. Вони забезпечують підвищений рівень безпеки, оскільки біометричні дані значно складніше підробити або викрасти, ніж традиційні облікові дані. Процес автентифікації є швидким та зручним, що забезпечує безперешкодний доступ до захищених систем, місць або послуг. Крім того, біометрична автентифікація надає сильніший рівень безвідмовності, що ускладнює заперечення особами своєї участі або дій, оскільки їхні унікальні біометричні ознаки слугують доказом їхньої присутності або залучення до конкретних видів діяльності.

Існують два основні режими роботи біометричних систем: автентифікація та ідентифікація, а біометричні показники, які можна застосовувати у якості підтвердження прийнято називати біометричними

реагування на інциденти, зменшили середній час виявлення загроз на 68% та значно покращили точність їх класифікації [7].

Шкідливий вміст в електронних листах – це не лише технологічне, але й психологічне явище, а боротьба з ним повинна бути багаторівневою та містити наступні етапи:

Перший етап – запобігання підробці, де перевірка адреси відправника забезпечує базову фільтрацію спуфінгу.

Другий етап полягає у глибокій автентифікація, яка визначає справжність намірів відправника та репутацію домену.

Третій етап відповідає за сам аналіз змісту повідомлень та є найкритичнішим. Саме тут у випадку атаки проявляється справжній намір зловмисника, а саме: змусити користувача перейти за посиланням, ввести дані або завантажити файл.

Використання сучасних інструментів, таких як PhishTool робить боротьбу із загрозами та їх аналіз не лише глибоким, а й системним. Це дозволяє не просто реагувати на окремі інциденти, а й вивчати тренди атак, формувати політики захисту, попереджати нові загрози. Завдяки чому боротьба із шкідливим вмістом в електронній пошті стає частиною ширшої стратегії кібергігієни та захисту персональних та корпоративних даних.

Список використаних джерел:

1. IBM Security Report 2023. URL: https://www.ibm.com/reports/data-breach.
2. Proofpoint Human Factor Report 2024. URL: https://www.proofpoint.com/us/resources/threat-reports.
3. Google Cloud Blog – How Gmail uses DMARC. URL: https://cloud.google.com/blog/products/identity-security/gmail-dmarc.
4. EmailRep.io API Docs 2024. URL: https://emailrep.io.
5. BIMI Group – Implementation Guide 2023. URL: https://bimigroup.org/implementation-guide/.
6. IBM X-Force Threat Intelligence Index 2024. URL: https://www.ibm.com/reports/threat-intelligence.
7. Digital Forensics Lab. Comparative Review of Phishing Analysis Tools, 2024. URL: https://df-lab.org/phishing-analysis-review.




ЗАХІДНОУКРАЇНСЬКИЙНАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
КАФЕДРА КІБЕРБЕЗПЕКИ
ГРОМАДСЬКА ОРГАНІАЦІЯ «КІБЕРБЕЗПЕКА І АВТОМАТИЗАЦІЯ»

Матеріали
науково-практичного симпозіуму

"ЗАХИСТ'ІНФОРМАЦІЇ'2025"

28 листопада 2025
Тернопіль

Збірник матеріалів науково-практичного симпозіуму «Захист інформації'2025», Тернопіль, 2025. – 118с.

Редакційна колегія:

Яцків В.В. – доктор технічних наук, професор;
Касянчук М.М.- доктор технічних наук, професор;
Сегін А.І.- кандидат технічних наук, доцент;
Стефурак Н.А. - кандидат фізико-математичних наук;
Якименко І.З.- кандидат технічних наук, доцент;
Яцків Н.Г. - кандидат технічних наук, доцент;
Івасьєв С.В.- кандидат технічних наук, доцент;
Цаволик Т.Г.- кандидат технічних наук, доцент;
Кулина С.В. – PhD.
Давлетова А.Я.

Адреса редакції:
Громадська організація «Кібербезпека і автоматизація»
м. Тернопіль
Контактний телефон: (066)043-42-10
e-mail: conferencekb@gmail.com

УДК 004.93

Максим СОКОЛІК, Сергій КУЛИНА

Західноукраїнський національний університет

АНАЛІЗ СУЧАСНИХ АЛГОРИТМІВ ВИДІЛЕННЯ ОЗНАК В БІОМЕТРІЇ

Вступ. У сучасному інформаційному суспільстві обсяги та важливість обробки даних стрімко зростають. Організації та окремі учасники оперують різноманітними даними, що потребують захисту – персональними даними, бізнес–інформацією, державними або науковими таємницями. У той же час зростає кількість кіберзагроз – фішинг, злом облікових записів, атаки «людина посередині», злочини із використанням витоків паролів, соціальна інженерія та інші [1]. Одним із методів забезпечення необхідного рівня доступу є застосування багатофакторної автентифікації (MFA). Її основою є те, що користувач має надати два або більше незалежних факторів підтвердження особи перед тим, як отримати доступ до ресурсу або системи [2]. Одним із таких факторів підтвердження є біометрична ідентифікація, яка застосовує риси унікальні для кожного користувача.

Метою дослідження є підвищення рівня захищеності систем доступу до даних та швидкодії їх роботи шляхом аналізу та покращення існуючих алгоритмів виділення ознак в біометриці.

1. Дослідження існуючих біометричних модальностей

Біометричні ідентифікатори, або як їх ще називають модальності, класифікуються на основі характеристик, які вимірюються. Вони поділяються на дві основні категорії [3]:

1. Фізіологічні модальності, категорія охоплює статичні, вроджені риси, пов'язані з формою та структурою тіла людини.

2. Фізіологічні риси, які демонструють високі показники унікальності та постійності протягом життя, так звані поведінкові модальності. Вони можуть бути менш постійними, оскільки на них можуть впливати інші фактори.

У таблиці 1 представлено аналіз біометричних модальностей, ключовим для яких є висока універсальність кожного із методів.

Таблиця 1 - Порівняльний аналіз біометричних модальностей

Модальність	Унікальність	Постійність	Збираність	Прийнятність	Захист
Відбиток пальця	Висока	Висока	Висока	Середня	Середня
Обличчя	Середня	Середня	Висока	Висока	Низька
Райдужна оболонка	Дуже висока	Дуже висока	Середня	Низька	Висока
Голос	Середня	Середня	Висока	Висока	Середня
Геометрія долоні	Середня	Висока	Висока	Висока	Середня
Хода	Низька	Середня	Висока	Висока	Середня
ДНК	Дуже висока	Дуже висока	Низька	Низька	Дуже висока

Отже, як бачимо з таблиці 1, кожну із модальностей можна характеризувати по одному із параметрів:

– унікальність – це оцінка того, наскільки кожна із розглянутих модальностей унікальна для користувача;

– постійність – це оцінка того, наскільки модальність користувача змінюється протягом життя;

– збираність – це оцінка того, наскільки складно зібрати зразок модальності;

– прийнятність – це оцінка того, наскільки система є задовільною, доречною та бажаною для використання у конкретному контексті;

– захист – це оцінка того, наскільки складно підробити саму модальність, а отже яким чином можливо її підробити.

Аналіз таких критеріїв виявляє що не існує "ідеальної" модальності, яка б мала найвищі бали за всіма сімома показниками. Така відсутність єдиного, простого, миттєвого чи чудодійного рішення для складної проблеми є основною рушійною силою для двох основних напрямків досліджень в біометрії, а саме:

1) розробки мультимодальних систем, які комбінують сильні сторони різних модальностей (наприклад, обличчя та голос);

2) постійного вдосконалення алгоритмів виділення ознак та зіставлення з метою максимізації ефективності та унікальності легкодоступних модальностей.

Окрім цього будь–яка біометрична система, незалежно від модальності, функціонує в одному з двох режимів: верифікація або ідентифікація. Його вибір визначає основне питання, на яке відповідає система, та має кардинальні наслідки для архітектури, обчислювальної складності та вимог до точності.

2. Аналіз сучасних алгоритмів виділення ознак

Процес біометричної ідентифікації складається з двох основних етапів: виділення ознак та зіставлення ознак. Виділення ознак – це процес перетворення вхідних необроблених даних (наприклад, зображення обличчя або відбитка пальця) у компактний числовий вектор (відомий як вектор ознак або шаблон). Цей вектор має бути достатньо інформативним, щоб бути унікальним для кожної особи, але водночас достатньо стабільним, щоб залишатися незмінним при незначних варіаціях (наприклад, різне освітлення або кут огляду). Історично, цей процес еволюціонував від "рукотворних" алгоритмів до підходів, що базуються на глибокому навчанні. Традиційні алгоритми виділення ознак покладаються на знання експертів у предметній галузі для розробки алгоритмів, які виділятимуть специфічні, заздалегідь визначені патерни. До таких алгоритмів відносять: виділення Мінуцій з відбитків, локальні бінарні шаблони та гістограми орієнтованих градієнтів. Традиційні методи (HOG, LBP, мінуції) базуються на інженерії ознак – процесі, де експерт вручну розробляє алгоритм, базуючись на припущеннях про те, які ознаки є важливими (наприклад, "градієнти важливі" або "текстура важлива"). На відміну від них, згорткові нейронні мережі (CNN) представляють фундаментальний зсув до навчання ознакам. Замість того, щоб програмувати екстрактор ознак вручну, CNN автоматично вивчає оптимальну ієрархію ознак безпосередньо з необроблених пікселів під час процесу навчання.

В таблиці 2 представлено порівняння ключових характеристик для традиційних метрик та згорткових нейронних мереж.

Таблиця 2 - Порівняння парадигм виділення ознак

Метрика	Традиційні методи	CNN
Принцип реалізації	Інженерія ознак	Навчання ознакам
Необхідність знань	Висока	Низька
Потреба в даних	Низька / Середня	Дуже висока
Обчислювальна складність	Низька	Висока
Енергоефективність	Висока	Низька
Потенційна точність	Середня / Висока	Дуже висока
Стійкість до перенавчання	Висока	Низька

Вибір між традиційними методами та CNN не є вибором між старою технологією та новою, це більше компроміс, що базується на трьох факторах.

1. Точність CNN полягає в тому, що зазвичай цей метод забезпечує вищу точність при складних завданнях.

2. Обчислювальна вартість. Традиційні методи, такі як HOG, є *значно* ефективнішими з точки зору енергоспоживання. Дослідження [4] вказує на "значну різницю у споживанні енергії" між CNN та HOG. Енергоспоживання та енергозаощадження є критично важливим для вбудованих та мобільних пристроїв, де час роботи від батареї є пріоритетом.

3. CNN потребують *великих* наборів даних для ефективного навчання. CNN "вигідні переважно для великих баз даних", оскільки на *малих* наборах даних добре налаштований алгоритм LBP або HOG може показати кращі результати через значно менший ризик перенавчання.

Висновок. Проведене дослідження показало, що методи біометричної аутентифікації є необхідним та доступним шдяхом покращення захищеності систем та даних, а для покращення їх швидкодії необхідно оптимізовувати методи виділення ознак. При практичній реалізації перед розробниками постає багато додаткових проблем, що є неявними при теоретичних дослідженнях. Відповідно, потужні CNN, є кращим вибором для *серверних* 1:N систем з великими об'ємами даних, де точність системи є пріоритетом. Натомість традиційні методи та спеціалізовані CNN є необхідними для *клієнтських* 1:1 систем з обмеженими ресурсами.

Перелік використаних джерел.

1. Яіцький А.О.(2022). Ефективні методи та засоби захисту фішингових атак.Problems of science and practice, tasks and ways to solve them, 417–419.

2. Suleski T, Ahmed M, Yang W, Wang E. A review of multi–factor authentication in the Internet of Healthcare Things. Digital Health. 2023; 9. doi:10.1177/20552076231177144.

3. Єжова, Є. (2025). Методи Захисту Від Атак На Біометричні Системи Аутентифікації. Міжнародна науково–практична конференція Інформаційні технології та комп'ютерне моделювання, 161–163.

4. Klingler, N. (2024). MobileNet – Efficient deep learning for mobile vision. [Ектронний ресурс].– Режим доступу: https://viso.ai/deep–learning/mobilenet–efficient–deep–learning–for–mobile–vision/