МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ПРОГРАМУВАННЯ

До захисту допускається
Завідувач кафедри ПМ
д.т.н., доцент О. І. Захожай
«____»_____ 2025 р.

ДИПЛОМНИЙ ПРОЕКТ (РОБОТА) БАКАЛАВРА
ПОЯСНЮВАЛЬНА ЗАПИСКА

НА ТЕМУ:

«Аналіз і покращення безпеки методів автентифікації та ідентифікації в біометричних системах»

Освітній ступінь «бакалавр»
Спеціальність 121 « Інженерія програмного забезпечення»

Керівник проекту: _____ (підпис) Д. В. Ратов (ініціали, прізвище)

Рецензент: _____ (підпис) В. О. Лифар (ініціали, прізвище)

Здобувач вищої освіти: _____ (підпис) Д. Д. Козиренко (ініціали, прізвище)

Група: ІПЗ-21д

Київ 2025

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет інформаційних технологій та електроніки
Кафедра інформаційних технологій та програмування
Освітній ступінь бакалавр
Спеціальність 121 «Інженерія програмного забезпечення»

«**ЗАТВЕРДЖУЮ**»
Завідувач кафедри
ПМ
д.т.н., доцент О. І. Захожай

_____
“____” _____ 2025 року

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Козиренко Даніїл Дмитрович
(прізвище, ім’я, по-батькові)

1. Тема проекту (роботи): «Аналіз і покращення безпеки методів аутентифікації та ідентифікації в біометричних системах» затверджена наказом по університету №67/15.15-С від «27» травня 2025 р.

2. Строк здачі студентом закінченого проекту (роботи): 15.06.2024 р.

3. Вихідні дані проекту (роботи): матеріали переддипломної практики

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити): аналіз загроз та уразливостей сучасних біометричних систем; визначення найбільш ефективних методів автентифікації, зокрема — аналіз систем на основі відбитків пальців, алгоритми та вибір технологій реалізації; виявлення напрямів покращення точності і захисту біометричних даних.

5. Перелік графічного матеріалу (з точною назвою обов’язкових креслень):

Електронні плакати

6. Консультанти роботи, з вказівкою розділів, що до них відносяться

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

7. Дата видачі завдання ____01.04.2025р._____

Керівник ___Д. В. Ратов_____
(підпис)

Завдання до виконання прийняв _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітки
1.	Отримання завдання та збір матеріалів	01.04.25 – 24.04.25	Виконано
2.	Огляд предметної області	25.05.25 –28.05.25	Виконано
3.	Аналіз загроз та уразливостей сучасних біометричних систем	28.05.25 – 30.05.25	Виконано
4.	Визначення найбільш ефективних методів автентифікації	31.05.25– 02.06.25	Виконано
5.	Виявлення напрямів покращення точності і захисту біометричних даних	02.06.25– 08. 06.25	Виконано
6.	Оформлення пояснювальної записки	08.06.25– 10.06.25	Виконано
7.	Підготовка та подання роботи до захисту	10.06.25– 16.06.25	Виконано

Здобувач вищої освіти _____ Д. Д. Козиренко
(підпис) (ініціали, прізвище)

Керівник _____ Д. В. Ратов
(підпис) (ініціали, прізвище)

РЕФЕРАТ

Пояснювальна записка до дипломного проекту бакалавра містить 96 сторінок, 56 рисунків, 6 таблиць, та 25 джерел посилань.

У дипломному проекті проведено аналіз програмного забезпечення для біометричних систем автентифікації та ідентифікації, яке забезпечує підвищену безпеку та точність ідентифікації користувачів. Проаналізовано загрози і методи захисту біометричних даних, а також досліджено різноманітні методи автентифікації та ідентифікації з акцентом на біометричні технології.

Особливу увагу приділено використанню відбитків пальців як засобу автентифікації з високим рівнем безпеки та надійності. Здійснено математичне моделювання процесів ідентифікації та автентифікації. У проекті також враховано нормативні вимоги з охорони праці: забезпечено відповідність умов праці чинним стандартам, розглянуто аспекти пожежної безпеки, мікроклімату, освітлення та інші ергономічні фактори, що сприяють створенню оптимального робочого середовища для користувачів системи.

Дипломний проект демонструє впровадження інноваційних технологій у сфері біометричної ідентифікації, забезпечуючи високий рівень безпеки та захисту персональних даних.

АВТЕНТИФІКАЦІЯ, ІДЕНТИФІКАЦІЯ, БІОМЕТРІЯ, ВІДБИТКИ ПАЛЬЦІВ, ЗАХИСТ ДАНИХ, ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ, ОХОРОНА ПРАЦІ.

Умови отримання дипломного проекту:

СНУ ім. Володимира Даля, м. Київ, вул. Чигоріна, 18

ЗМІСТ

ВСТУП

У сучасну епоху стрімкої цифровізації значне місце займають біометричні технології, які активно впроваджуються в різних сферах — від банківської справи та медицини до транспорту і державного управління. Суть біометрії полягає у використанні неповторних фізіологічних або поведінкових характеристик людини для ідентифікації та автентифікації особи. Завдяки цьому такі системи забезпечують високий рівень захисту й зменшують ризик несанкціонованого доступу до конфіденційної інформації чи ресурсів.

Втім, як і будь-які інші цифрові рішення, біометричні системи не позбавлені недоліків. Кіберзлочинці постійно розробляють нові способи обходу захисту, зокрема шляхом підробки біометричних шаблонів або використанням програмних уразливостей. У зв’язку з цим виникає нагальна потреба в глибокому аналізі існуючих методів автентифікації та ідентифікації, а також у вдосконаленні механізмів, що гарантують надійність та стійкість до зовнішніх загроз.

В українському контексті, де цифрова трансформація та електронне урядування є ключовими напрямками розвитку, питання кібербезпеки біометричних систем стає надзвичайно актуальним. Надійні та ефективні біометричні рішення можуть значно покращити захист персональних даних громадян, підвищити якість державних сервісів і сприяти більшій довірі населення до цифрових послуг.

Потреба в цьому дослідженні зумовлена швидкими темпами розвитку інформаційних технологій і постійно зростаючими вимогами до рівня їх безпеки. Аналіз наукової літератури та практичних реалізацій виявляє певні прогалини у збереженні цілісності й конфіденційності біометричних даних, що актуалізує потребу у створенні нових, більш захищених рішень. Розробка інноваційних підходів до біометричної автентифікації має стати відповіддю на сучасні виклики кіберпростору.

Метою роботи є підвищення надійності та безпеки біометричних методів ідентифікації та автентифікації шляхом створення і перевірки системи, здатної ефективно протидіяти загрозам і забезпечувати точну ідентифікацію користувачів.

Для досягнення цієї мети були визначені наступні завдання:

- провести аналіз потенційних ризиків для існуючих біометричних систем, визначити основні типи атак і можливості їх запобігання;
- дослідити роль різних методів автентифікації в забезпеченні захищеності, зокрема оцінити ефективність технології відбитків пальців;

В основі запропонованого рішення лежить комплексний підхід, що включає вдосконалені алгоритми обробки та розпізнавання відбитків пальців, що дозволяє досягти високої точності ідентифікації. Окрема увага приділяється захисту від підробок та фальсифікацій, що критично важливо для об'єктів із підвищеними вимогами до безпеки. Гнучкість системи забезпечується можливістю використовувати різні типи біометричних даних, що робить її придатною як для державного, так і для корпоративного використання.

Новизна дослідження полягає у впровадженні механізмів покращеної обробки біометричної інформації, зокрема методів “живої перевірки” відбитків пальців, що дозволяють надійно відрізняти справжні біометричні дані від підроблених. Це забезпечує адаптивність системи до змін середовища та підтримує високий рівень інформаційної безпеки.

РОЗДІЛ 1 Теоретичні основи автентифікації та ідентифікації.

1.1 Поняття автентифікації та ідентифікації

Визначення і сутність понять

Ідентифікація та автентифікація — це фундаментальні процеси у сфері інформаційної безпеки, які забезпечують контроль доступу користувачів до інформаційних систем.

Ідентифікація — це процес визначення або встановлення особи користувача, тобто присвоєння унікального ідентифікатора (ID), наприклад, логіна, номера користувача або іншої унікальної інформації. Ідентифікація відповідає на питання: *Хто ти?* Ідентифікація виконується при спробі увійти в будь-яку систему (наприклад, в операційну систему або в сервіс електронної пошти). Мета ідентифікації — перевірити, чи відомий індивід системі. Ідентифікатором може бути: номер телефону, номер паспорта, e-mail, номер сторінки в соціальній мережі і т.д. Коли нам дзвонять з невідомого номера, що ми робимо? Запитуємо "Хто це", тобто дізнаємося ім'я. Ім'я в даному випадку і є ідентифікатор, а відповідь вашого співрозмовника - це буде ідентифікація.

Автентифікація — це процес перевірки справжності заявленої особи, підтвердження, що користувач дійсно є тим, за кого себе видає. Автентифікація відповідає на питання: *Чи є ти тим, ким ти себе називаєш?*

Важливо розуміти, що ідентифікація — це лише заявка, а автентифікація — підтвердження.

Тож, після ідентифікації проводиться **аутентифікація** - це процедура перевірки автентичності (перевірка справжності). Це процес розпізнавання користувача

системи і надання йому певних прав та повноважень. Його суть — визначити, чи справді індивід є тією особою, якою він або вона себе називає.

Аутентифікація - це процес перевірки облікових даних користувача (зазвичай імені та пароля). Іншими словами введені облікові дані звіряються з даними, що зберігаються в базі даних (користувача перевіряють за допомогою пароля, лист перевіряють по електронного підпису і т.д.)

Способи аутентифікації

- Парольна (здійснюється на основі володіння користувачем певної конфіденційної інформації)
- Біометрична (основана на унікальності певних антропометричних характеристик людини)

Щоб визначити чиюсь справжність, можна скористатися трьома факторами:

- Пароль - то, що ми знаємо (слово, PIN-код, код для замка, графічний ключ): об’єкт може продемонструвати знання якого-небудь загального для сторін секрету

- Пристрій - то, що ми маємо (пластикова карта, ключ від замка, USB-ключ)
- Біометрика - то, що є частиною нас (відбиток пальця, портрет, сітківка ока)

Парольна аутентичність

Більшість мережевих систем на даний час продовжують використовувати парольну аутентифікацію, оскільки вона простіше і дешевше. Перевірка автентичності користувача звичайно здійснюється операційною системою. Користувач ідентифікується своїм ім'ям, а засобом аутентифікації служить пароль.

Конструкція пароля: Для розумної ефективності паролі повинні складатися не менше ніж з 6-8 символів, не бути легко згадувані і змінюватися не рідше, ніж кожні 90 днів.

Чим довше пароль, тим більше складнощів для зловмисника, щоб його вгадати або обчислити. Можна стверджувати, що збільшення довжини пароля тільки на один символ помітно збільшує безпечний час: якщо очікуваний безпечний час для пароля з трьох символів становить близько трьох місяців, безпечний час для пароля з чотирьох символів становить сімдесят вісім місяців.

Так само важлива форма пароля. Користувач повинен бути в змозі впевнено його пам’ятати (і не відчувати незручностей від неможливості його записувати), але пароль також повинен бути дуже складним для вгадування іншими. Телефонний номер шкільної подруги або назва вулиці – приклади правильних форм

Біометрична аутентифікація

Системи біометричного захисту використовують унікальні для кожної людини вимірювані характеристики для перевірки особи індивіда.

Біометричний захист ефективніший ніж такі методи як, використання смарт-карток, паролів, PIN-кодів.

До біометричних засобів захисту інформації відносять системи аутендифікації за:

- Параметрами голосу.

- Візерунком райдужної оболонки ока і карта сітчатки ока.
- Рисами обличчя.
- Формою долоні.
- Відбитками пальців.
- Формою і способом підпису.

Біометричні системи складаються з двох частин: апаратних засобів і спеціалізованого програмного забезпечення.

Для того, щоб біометрична система змогла надалі аудентифікувати користувача, в ній необхідно спочатку зареєструвати відомості про його ідентифікатори. Під час процедури реєстрації в базу даних системи заносяться характеристики користувачів, необхідні для встановлення їх автентичності.

Апаратні засоби включають в себе біометричні сканери і термінали. Вони фіксують той чи інший біометричний параметр (відбиток пальця, райдужну оболонку очей, малюнок вен на долоні або пальці) і перетворять отриману інформацію в цифрову модель, доступну комп'ютера. А програмні засоби ці дані обробляють, співвідносять з базою даних і виносять рішення, хто постав перед сканером.

Приклади стандартів і протоколів автентифікації

FIDO (Fast IDentity Online)

- Стандарт, що визначає методи безпарольної автентифікації з використанням біометрії, апаратних токенів та криптографії.
- Включає FIDO U2F (Universal 2nd Factor) та FIDO2, що дозволяють реалізувати багатофакторну автентифікацію.

- Принцип — ключі зберігаються локально, а сервер підтверджує автентичність через криптографічний протокол.

OAuth 2.0

- Протокол авторизації, який часто поєднують з автентифікацією.
- Дозволяє стороннім додаткам отримувати обмежений доступ до ресурсів користувача без передачі пароля.

OpenID Connect

- Надбудова над OAuth 2.0, що забезпечує автентифікацію користувача.
- Широко застосовується для єдиного входу (SSO) на різних сайтах.

Kerberos

- Протокол мережевої автентифікації, що базується на симетричному криптографічному ключі.
- Забезпечує захищений обмін ключами між користувачем і сервером.

1.2 Дослідження потенційних загроз біометричних систем

Біометричні системи являють собою комплекси технологій, які використовують унікальні фізіологічні або поведінкові риси людини для визначення її особи або підтвердження ідентичності. Такі системи здійснюють збір та аналіз одного або декількох біометричних параметрів. До фізіологічних ознак належать, зокрема, відбитки пальців, контури обличчя, зображення сітківки ока, візерунки вен, форма вуха та інші особливості анатомії. Поведінкові ознаки включають індивідуальні особливості манери друкування на клавіатурі, голос, стиль ходи, підпис та інші поведінкові характеристики, що унікальні для кожної людини. Хоча біометричні системи є ефективними інструментами для підвищення безпеки і точної ідентифікації, вони також можуть бути вразливими до різноманітних загроз і викликів. На рисунку 1.1 наведено схему основних категорій загроз, що можуть впливати на біометричні системи.

Рисунок 1.1 – Діаграма розподілу основних загрози для біометричних систем

Загрози, з якими можуть стикатися біометричні системи, поділяють на кілька ключових груп:

- **Фізичні атаки.** Ця категорія включає спроби отримання несанкціонованого доступу через фізичне втручання, наприклад, крадіжку або пошкодження біометричних сенсорів, таких як сканери відбитків пальців.
- **Атаки з обманом.** Зловмисники можуть застосовувати фальшиві біометричні дані, наприклад, виготовлені відбитки пальців або маски обличчя, щоб обійти систему безпеки.
- **Технічні вразливості.** До цієї групи належать помилки або уразливості програмного забезпечення, яке управляє біометричними системами, наприклад, недосконалі алгоритми обробки даних або програмні баги, які можуть бути використані хакерами для втручання в процес автентифікації.
- **Внутрішні загрози.** Пов'язані з ризиком недобросовісної поведінки співробітників, які мають доступ до біометричних систем і можуть, наприклад, незаконно копіювати або змінювати біометричні дані.
- **Загрози приватності та конфіденційності**. Незаконне збирання, зберігання або передача біометричних даних, відсутність захисту персональних даних згідно з законами GDPR, CCPA та іншими.

Забезпечення надійного захисту є одним із найважливіших аспектів при створенні та експлуатації біометричних систем. Біометрична система, яка не оснащена ефективними заходами безпеки для запобігання несанкціонованому доступу, втрачає свою практичну значущість і надійність.

Автентифікація (authentication) є фундаментальним елементом безпеки будь-якої інформаційної системи, оскільки вона передбачає процес перевірки достовірності наданих користувачем даних [3]. Хоча автентифікація відрізняється від процесів ідентифікації та авторизації, всі три етапи разом утворюють комплексний механізм захисту. Спочатку відбувається ідентифікація — розпізнавання користувача за допомогою певної інформації, наприклад, логіна або пароля. Наступним кроком є автентифікація — підтвердження достовірності цієї

інформації. І на завершення виконується авторизація, яка визначає рівень доступу користувача до системи або ресурсів.

Рисунок 1.2 – Етапи перевірки користувача в біометричній системі

У контексті біометричних систем аутентифікація необхідна для підтвердження особи шляхом аналізу унікальних фізіологічних або поведінкових характеристик. Коли користувач звертається до системи або сервісу, вона порівнює надані біометричні дані із збереженими зразками, щоб упевнитися, що особа, яка намагається отримати доступ, є дійсно тією, за кого себе видає. Це забезпечує надійний контроль доступу і запобігає проникненню сторонніх осіб до конфіденційної інформації або ресурсів.

Основними компонентами процесу аутентифікації є:

- **Суб'єкт (користувач).** Людина, яка намагається увійти до системи або отримати доступ до ресурсів;
- **Характеристика суб'єкта.** Дані, які користувач надає для підтвердження своєї особистості (наприклад, біометричні ознаки);
- **Власник системи (адміністратор).** Організація чи особа, що управляє контролем доступу до системи чи ресурсів;
- **Механізм аутентифікації.** Процедура або технологія, що перевіряє подані користувачем дані на відповідність з існуючими записами;

- **Механізм авторизації.** Система, що визначає права доступу користувача після успішного підтвердження особи.

Таким чином, аутентифікація є ключовим засобом захисту, що забезпечує перевірку справжності користувача шляхом порівняння наданих ним даних із збереженими відомостями, дозволяючи гарантувати безпеку інформаційної системи та запобігати несанкціонованому доступу.

1.3 Види методів автентифікації.

При вивченні різних способів аутентифікації та ідентифікації користувачів важливо враховувати різноманітність механізмів підтвердження особи, які дозволяють отримати доступ до системи або ресурсів. На рисунку 1.3 зображено класифікацію основних методів автентифікації та ідентифікації.

Рисунок 1.3 – Основні методи аутентифікації та ідентифікації користувачів

До найпоширеніших і найбільш використовуваних методів належать:

Логін і пароль. Це один із найпростіших і найпоширеніших способів підтвердження особи, що базується на введенні унікального ідентифікатора (логіну) та секретного коду (пароля). Користувач вводить свої дані, які порівнюються із записами в базі системи. У разі збігу користувач отримує доступ до ресурсів. Однак цей метод вразливий до атак методом підбору пароля (brute force) або фішингу, що вимагає впровадження додаткових заходів безпеки.

Двофакторна аутентифікація (2FA). Цей підхід передбачає використання двох незалежних факторів для підтвердження особи. Зазвичай це комбінація «щось, що користувач знає» (наприклад, пароль) і «щось, що користувач має» (одноразовий код з SMS або спеціального додатку, наприклад Google Authenticator). Використання 2FA значно підвищує безпеку системи, оскільки навіть у випадку компрометації пароля, без другого фактора доступ залишається недоступним.

Біометрична аутентифікація. Цей метод заснований на унікальних фізичних або поведінкових характеристиках особи — відбитках пальців, геометрії обличчя, голосі, рукописному підписі тощо. Біометрія вважається ефективною через складність підробки таких даних. Проте існують певні ризики, пов’язані з технічними помилками, наприклад, хибнопозитивними або хибнонегативними результатами, а також можливістю обходу систем шляхом використання підроблених або записаних біометричних зразків.

Токени. У цьому випадку користувачу видається апаратний або програмний пристрій — токен, який генерує одноразові коди доступу (One-Time Password, OTP) для кожної спроби входу. Токени широко застосовуються у банківській сфері та корпоративних мережах. Навіть якщо код буде перехоплений, його можна використати лише один раз, що значно знижує ризик несанкціонованого доступу.

Смарт-карти. Це фізичні карти з інтегрованим чипом, які містять зашифровані дані для ідентифікації користувача, сертифікати чи криптографічні ключі. Власник карти повинен вставити її у зчитувач або застосувати безконтактний метод, після чого система підтверджує його особу. Цей метод часто використовується в урядових та корпоративних структурах з підвищеними вимогами до безпеки.

Ці методи можуть застосовуватися як поодинці, так і у різних комбінаціях, залежно від рівня необхідної безпеки та специфіки інформаційної системи. Для прикладу, в банках часто поєднують пароль, смс-код і біометрію, щоб досягти максимальної надійності. Адміністратори систем мають відповідально підходити до вибору і налаштування методів аутентифікації, щоб забезпечити баланс між безпекою та зручністю для користувачів.

1.4 Аналіз біометричних методів автентифікації

Біометрична аутентифікація — це процес підтвердження та перевірки особи шляхом зчитування її біометричних даних та їх подальшого оброблення за визначеним протоколом. Цей метод доступу до системи вважається надійним і зручним, оскільки він базується на унікальних біологічних характеристиках, які властиві кожній людині й практично не можуть бути втрачені або передані іншим особам. У разі необхідності біометричні дані можна видалити або замінити, що підвищує безпеку їх використання.

Для ефективності та прийнятності біометричних параметрів існує ряд ключових критеріїв:

Унікальність — біометричні дані повинні бути унікальними для кожної особи, щоб виключити можливість співпадіння параметрів між різними людьми. Це дозволяє системі точно ідентифікувати користувача, знижуючи ризик помилкових збігів.

Універсальність — методи біометричної аутентифікації повинні бути доступні для застосування усіма користувачами без винятку. Враховуючи різноманітність населення, обрані характеристики мають бути ефективними в усіх групах.

Вимірність — система має забезпечувати точне і надійне вимірювання біометричних параметрів для коректного збирання та обробки даних під час реєстрації та подальшої аутентифікації.

Прийнятність — соціальний аспект використання біометричних технологій є важливим, тому суспільство та користувачі повинні приймати збір і використання

своїх біометричних даних без значних заперечень, почуватися комфортно та впевнено під час взаємодії з системою.

Стійкість — біометричні характеристики повинні залишатися відносно стабільними протягом тривалого часу. Система має враховувати можливі фізіологічні або зовнішні зміни, щоб підтримувати високу точність аутентифікації.

Складові біометричних систем

Біометричні системи складаються з двох основних компонентів: апаратних засобів та спеціалізованого програмного забезпечення.

Для можливості подальшої аутентифікації користувача в системі спочатку необхідно зареєструвати його біометричні дані. Під час процедури реєстрації відомості про унікальні ідентифікатори користувача заносяться у базу даних системи, що забезпечує можливість встановлення його автентичності у майбутньому.

До апаратних засобів відносяться біометричні сканери та термінали, які здійснюють зчитування певного біометричного параметра — наприклад, відбитків пальців, райдужної оболонки ока, малюнку вен на долоні чи пальці. Отримані дані перетворюються у цифровий формат, доступний для подальшої обробки комп’ютером. Програмне забезпечення виконує аналіз цих даних, порівнює їх із записами у базі та приймає рішення про підтвердження особи, яка звернулася до системи.

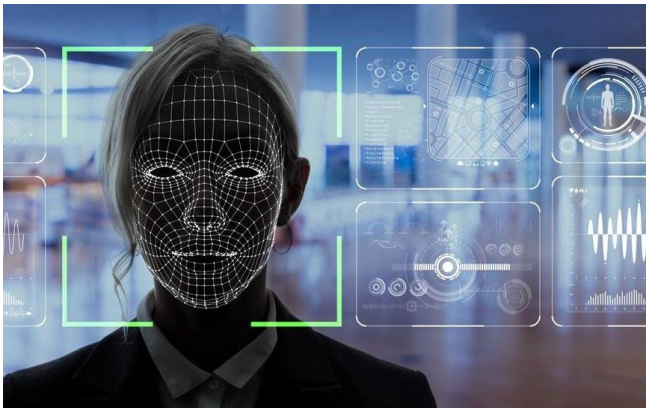
Аутентифікація за райдужною оболонкою ока

Райдужна оболонка ока є унікальним біометричним показником для кожної людини. Під час аутентифікації зображення ока відокремлюється від загального зображення обличчя, після чого на нього накладається спеціальна маска, що кодує особливий "штрих-код". Результатом є унікальна матриця, яка індивідуальна для кожного користувача.

Аутентифікація за зображенням обличчя

Технології розпізнавання обличчя широко застосовуються для ідентифікації осіб на відстані. Для визначення особи враховуються такі характеристики, як форма обличчя, колір шкіри та волосся, а також положення ключових точок (очі, брови, ніс, вуха, рот, контур обличчя), які відповідають за зміну контрасту.

Алгоритм роботи системи полягає у зчитуванні зображення за допомогою відеокамери та аналізі отриманого портрета. Програмне забезпечення порівнює це зображення з еталонним, збереженим у базі. Сучасні системи розпізнавання обличчя можуть також здійснювати безперервну аутентифікацію користувача протягом усього часу роботи з комп’ютером.



Аутентифікація за геометрією долоні

Для ідентифікації людини використовують геометричні характеристики руки — розмір і форму долоні, а також унікальні ознаки на тильній стороні кисті, такі як малюнки вен або складки шкіри. Сканери, що працюють за цим принципом, застосовуються у високозахищених об’єктах, таких як аеропорти, банки, атомні електростанції.

Розпізнавання базується на аналізі тривимірного зображення кисті руки. Однак варто зазначити, що форма долоні може змінюватися з часом, а для якісного сканування потрібне обладнання великого розміру, що підвищує вартість системи

Аутентифікація за відбитками пальців

Оптичні сканери для зчитування відбитків пальців широко інтегруються в ноутбуки, комп’ютерні миші, клавіатури, флеш-накопичувачі, а також використовуються як автономні пристрої в терміналах банків і аеропортів. Якщо зразок відбитка пальця не відповідає записам у базі, доступ до системи не надається.

Аутентифікація за голосом

Ідентифікація особи за голосом є одним із традиційних методів біометрії. Інтерес до цього підходу зростає у зв’язку з розвитком голосових інтерфейсів в операційних системах та пристроях. Голосова аутентифікація базується на унікальних акустичних характеристиках мовлення конкретної людини.

Біометричні системи можуть використовувати різні параметри для аутентифікації користувачів, зокрема: відбитки пальців, структуру рогівки ока, геометрію обличчя, термограму, тембр голосу, рукописний підпис та інші. Вибір конкретного методу залежить від специфіки та вимог інформаційної системи, а також від переваг і недоліків кожного способу.

Для більш наочного порівняння основних методів біометричної аутентифікації наведено таблицю 1.1.

Таблиця 1.1 – Порівняння методів біометричних систем

Метод	Необхідне обладнання	Плюси	Мінуси	Галузь застосування
1	2	3	4	5
По відбитку пальців	Сканувальна панель з багаторівневим фотоелементом, у дорогих апаратах з датчиком ступеня натискання та температурним датчиком	Швидкість аутентифікації, великий вибір апаратів сканування, простота використання, спеціалізовані модулі	Мало точок для побудови шаблонної моделі, можна обдурити фізичною копією пальця	Телефони, ноутбуки, біометричні замки
По рогівці ока	Камера швидкісної зйомки, вбудована в модуль сканування	Швидкість та точність сканування, високий захист від спроб підробки оригінального об'єкту	Вартість, складність обладнання та його обслуговування	Об'єкти, що схильні до високого рівня небезпеки
За сітківці ока	Сканер сітківки ока з інфрачервоним випромінюванням низького ступеня інтенсивності	Індивідуальність об'єкта сканування, висока точність сканування	Зміна сітківки протягом життя, незручність використання, шкода організму	Надсекретні об'єкти (корпорації, військові тощо)
За геометрії кисті	Скануючий модуль з камерою та освітлювальним елементом для створення тривимірної моделі	Швидкість сканування та обробки запиту, багато параметрів перевірки, простота використання, вартість	Висока ймовірність пошкодження сканованої частини тіла	Замки в бізнес-центрах, контрольно-пропускні пункти

По термо-грамі обличчя	Скануючий елемент з інфрачервоними камерами для створення об'ємної теплової моделі обличчя	Точність використовуваного методу, не можна обдурити навіть людям з ідентичною зовнішністю, захист від старіння та зміни об'єкта	Мала зацікавленість у даному методі, вартість спеціального обладнання, складність роботи з обладнанням	Охоронні системи, військові об'єкти
По геометрії обличчя	Камера або модуль, що дозволяє знімати і створювати тривимірну модель	Швидкість автентифікації та простота використання, високий ступінь точності	Виникнення проблем при частковій закритості обличчя, можливість обдурити при використанні пластичного втручання	Державні служби, смартфони, банки
За голосом	Мікрофон, обладнання для обробки голосу	Швидкість та простота використання, швидкість сканування	Низький рівень безпеки, при хворобі користувача можуть виникнути проблеми з автентифікацією	Смартфони, двері, сейфи, банки
За руко-писним підписом	Сканер із сенсорною панеллю з датчиком сили натискання	Простота використання, швидкість сканування	Можливість підробки, низький рівень безпеки	Бізнес підприємства, державні служби, банки

Біометричні системи автентифікації використовують різноманітне обладнання та методи для забезпечення безпеки, кожен з яких має свої специфічні переваги та обмеження. Методи автентифікації по відбитку пальців та по геометрії обличчя є популярними завдяки їхній швидкості, простоті використання та доступності обладнання. Проте, методи, як-от сканування сітківки ока, хоча й дорожчі та складніші у використанні, забезпечують вищий рівень безпеки, що

робить їх незамінними для застосування на об'єктах з високими вимогами до захисту інформації.

1.5 Математичне моделювання процесу розпізнавання відбитків пальців

Процес обробки відбитків пальців складається з кількох ключових етапів, що забезпечують точну ідентифікацію особи на основі її біометричних характеристик. Після зчитування зображення відбитка за допомогою сенсора, система проводить його обробку з метою виділення індивідуальних рис, які використовуються для подальшого порівняння з еталонними зразками. Основні етапи цього процесу включають:

Бінаризація

На першому етапі обробки вихідне зображення відбитка перетворюється в бінарне за допомогою відповідного алгоритму. Бінаризація дозволяє відокремити гребені відбитка (представлені темними пікселями) від долин (світлі пікселі), що значно спрощує подальший аналіз. Метою є підвищення контрастності зображення та усунення фону.

Скелетизація

Отримане бінаризоване зображення проходить етап скелетизації, під час якого гребені зображення зменшуються до однопіксельної ширини. Це зберігає топологію лінійного малюнка відбитка та зменшує обсяг оброблюваних даних, дозволяючи зосередитися на його структурних особливостях.

Виділення характерних точок

Після скелетизації проводиться аналіз структури гребенів для виявлення мінуцій — характерних точок, таких як:

розгалуження (вилки) — місця, де один гребінь розділяється на два;

завершення гребеня — точка, де гребінь обривається.

Ці точки є унікальними для кожної людини та слугують основними орієнтирами для подальшого порівняння.

Порівняння за мінуціями

На заключному етапі система порівнює набір виявлених мінуцій із шаблонами, що зберігаються в базі даних. Аналізуються не лише типи мінуцій, але й їх просторове розташування та відносна орієнтація. Якщо кількість і точність співпадінь перевищує певний поріг, система підтверджує ідентичність користувача.

Ці етапи створюють основу для надійного функціонування біометричних систем автентифікації, які використовують відбитки пальців.

Приклад результату бінаризації відбитка наведено на рис. 1.4.

Рисунок 1.4 – Початкове зображення відбитка; бінарне зображення

Скелетизація зображення відбитків пальців

Скелетизація є критичним етапом у процесі обробки зображень відбитків пальців, оскільки дозволяє зменшити обсяг даних, зберігаючи при цьому ключові геометричні та топологічні характеристики папілярного візерунка. Завдяки цьому процесу стає можливим ефективне виділення характерних точок, зокрема завершень гребенів і їхніх розгалужень, що суттєво впливає на точність ідентифікації особи.

У комп'ютерній графіці скелет фігури визначається як множина точок, що рівновіддалені від контурів об'єкта. Такий підхід дозволяє виокремити структуру, яка описує топологічну суть фігури: її зв’язність, напрямки та геометричні

властивості. У контексті біометричної автентифікації, скелет відбитка є спрощеним представленням папілярних ліній, що забезпечує зменшення шумів і підвищення точності наступних етапів аналізу.

Алгоритми скелетизації

Існує кілька підходів до реалізації скелетизації бінарних зображень. Початково вони були розроблені для задач розпізнавання текстів та символів, однак згодом знайшли широке застосування у сфері біометрії. Серед найбільш відомих алгоритмів можна виділити:

Хвильовий алгоритм (wavefront method) — побудова скелета шляхом моделювання поширення хвилі з контуру фігури;

Алгоритм витончення (thinning) — послідовне видалення пікселів з країв фігури без порушення її топології;

Шаблонний метод (template matching method) — застосування фіксованих шаблонів для виявлення пікселів, які слід зберегти або видалити.

Шаблонний метод вважається одним із найефективніших у контексті біометрії. Він забезпечує стабільність результату навіть за наявності шумів, а також високу швидкість обробки.

Формалізація шаблонного методу

Шаблонний метод реалізується як послідовна перевірка кожного пікселя бінарного зображення f(x,y)∈{0,1}f(x,y) \in \{0,1\}f(x,y)∈{0,1}, де значення 1 означає належність до папілярного візерунка. Для оцінки пікселя використовується індекс KKK, що розраховується за формулою:

K=∑i=−11∑j=−11f(x+j,y+i)⋅h(i,j)(1.1)K = \sum_{i=-1}^{1} \sum_{j=-1}^{1} f(x+j, y+i) \cdot h(i, j) \tag{1.1}K=i=−1∑1j=−1∑1f(x+j,y+i)⋅h(i,j)(1.1)

де:

- f(x,y)f(x,y)f(x,y) — значення пікселя у позиції (x,y)(x,y)(x,y),
- h(i,j)h(i,j)h(i,j) — вагова маска для кожного з 8 сусідніх пікселів.

Маска h(i,j)h(i,j)h(i,j) має вигляд:

h=[128643216084218421](1.2)h = \begin{bmatrix} 128 & 64 & 32 \\ 16 & 0 & 8 \\ 4 & 2 & 1 \end{bmatrix} \tag{1.2}h=128164640232381(1.2)

Значення KKK може варіюватися від 0 до 255 і виступає як індекс для звернення до таблиці шаблонів. Таблиця шаблонів містить набір правил, де кожен шаблон відповідає певній дії, яку потрібно виконати: зберегти піксель, видалити його, або пропустити (нічого не робити). Це дозволяє забезпечити точне формування скелета при збереженні важливих точок малюнка.

У реалізації на мовах програмування, зокрема C#, розрахунок індексу K часто виконується за допомогою побітових операцій (bit shifting), що дозволяє значно оптимізувати продуктивність.

Приклад операції за індексом

Одна з найпоширеніших операцій, яка виконується при скелетизації — видалення центрального пікселя, якщо шаблон околиці відповідає заданому з таблиці. Наприклад, на рис. 1.5 наведено приклад такої операції, коли піксель, що розташований у центрі, відповідає умові для видалення згідно з шаблонним правилом.

Рисунок 1.5 – Видалення центрального пікселя

Ще однією операцією, яка може виконуватись у процесі шаблонної скелетизації, є **перенесення інформативного пікселя** в іншу позицію навколо центрального пікселя. При цьому сам центральний піксель обнуляється, а важлива

інформація переноситься у нове місце. Такий підхід дозволяє зберегти цілісність структури папілярного візерунка за умов деформацій або неповного зчитування.

На рис. 1.6 схематично зображено приклад перенесення пікселя в одну з восьми навколишніх позицій:

Рисунок 1.6 – Перенесення центрального пікселя

Метод скелетизації функціонує ітеративно, послідовно обробляючи кожен піксель бінаризованого зображення. Протягом кожної ітерації алгоритм аналізує локальне оточення пікселя згідно з таблицею шаблонів і, за необхідності, виконує відповідну операцію (видалення, збереження або перенесення). Ітерації повторюються доти, поки на зображенні не залишиться жодних пікселів, які потрібно модифікувати. Таким чином, коли протягом цілої ітерації не відбулося жодної зміни — алгоритм завершує свою роботу, що гарантує досягнення стабільного результату.

Фінальним продуктом цього процесу є **скелетизоване зображення**, що містить лише центральні осі папілярних ліній без надлишкової інформації. Приклад такого результату наведено на рис. 1.7:

Рисунок 1.7 – Результат роботи алгоритму шаблонної скелетизації

Такий підхід дозволяє не тільки сформувати компактне представлення відбитка, але й значно полегшує наступний етап — **виділення особливих точок**, до яких належать:

- **кінцеві точки** (termination points) — місця завершення гребенів,
- **розгалуження** (bifurcations) — точки поділу гребеня на два або більше відгалужень,
- **точки перетину** — області складної топології, наприклад при накладанні ліній.

Ці особливі точки визначаються координатно, а також за напрямом гребенів у їх околі. Вони є критичними для **процесів верифікації та ідентифікації**, оскільки саме за сукупністю цих параметрів система формує унікальний біометричний шаблон особи.

Таким чином, скелетизація не лише зменшує обсяг даних для аналізу, але й виступає ключовим етапом у побудові ефективних та точних біометричних систем автентифікації.

1.6 Висновки до розділу 1

У межах цього розділу було здійснено комплексний аналіз основних понять, принципів та компонентів біометричної аутентифікації та ідентифікації. Розглянуто ключові аспекти безпеки, включаючи потенційні загрози для біометричних систем — від фізичних та соціоінженерних атак до технічних вразливостей і внутрішніх ризиків. Це дозволило глибше осмислити роль аутентифікаційних механізмів у побудові надійного захисту інформації.

Особливу увагу було приділено порівнянню традиційних методів аутентифікації — таких як логін/пароль, двофакторна аутентифікація, токени та смарт-карти — із біометричними технологіями, які базуються на фізіологічних або поведінкових ознаках користувача.

Біометричні методи було проаналізовано з урахуванням їхніх основних властивостей: **унікальності**, **універсальності**, **вимірюваності**, **прийнятності** та **сталості**, що є визначальними критеріями для ефективного функціонування таких

систем. Серед розглянутих методів ідентифікації особлива увага приділялася технології розпізнавання **відбитків пальців**, яка вирізняється високою надійністю, неможливістю передачі біометричних ознак, стабільністю даних у часі та високим ступенем унікальності.

Окремо було розглянуто алгоритмічні етапи обробки зображень відбитків пальців: **бінаризацію**, **скелетизацію**, **виділення особливих точок**, а також математичне моделювання процесів розпізнавання з використанням оцінок **FAR (False Acceptance Rate)** та **FRR (False Rejection Rate)**. Це створює підґрунтя для подальших розробок і досліджень у наступному розділі, де буде запропоновано методи вдосконалення біометричних технологій, спрямованих на підвищення **точності**, **надійності** та **економічної доцільності** їх використання в реальних умовах.

РОЗДІЛ 2 Традиційні методи автентифікації.

2.1 Традиційні методи автентифікації.

Традиційні методи автентифікації є основою інформаційної безпеки у більшості комп’ютерних систем і засновані на трьох основних принципах: **те, що користувач знає** (наприклад, пароль), **те, що він має** (наприклад, смарт-карта або токен), або **те, ким він є** (біометрія, яка розглядається у наступних підрозділах).

До найпоширеніших традиційних методів належать:

1. Паролі та логіни

Найбільш широко використовуваний метод автентифікації, який полягає у введенні пари "логін–пароль". Користувач повинен ввести унікальний ідентифікатор та відповідний до нього пароль, який перевіряється системою на відповідність записам у базі даних.

Переваги:

- простота реалізації;
- невисока вартість;
- сумісність з більшістю існуючих систем.

Недоліки:

- користувачі часто створюють слабкі паролі;
- можливість фішингових атак;
- паролі можуть бути викрадені або перехоплені шкідливим ПЗ;
- потреба у регулярному оновленні паролів.

2. PIN-коди

PIN-коди використовуються переважно у банкоматах, банківських картах та мобільних пристроях. Це короткий числовий код, який вводиться користувачем для підтвердження своєї особи.

Переваги:

- швидкість та зручність введення;
- підтримка пристроями з обмеженим інтерфейсом.

Недоліки:

- обмежена довжина коду;
- вразливість до підглядання (shoulder surfing);
- низький рівень захисту без додаткових заходів безпеки.

3 Смарт-карти

Смарт-карта — це фізичний носій із вбудованим чипом, що зберігає криптографічні ключі, сертифікати чи інші дані для ідентифікації користувача. Взаємодіє з комп’ютером через спеціальний зчитувач.

Переваги:

- високий рівень захисту інформації;
- можливість використання у багатофакторній автентифікації;
- підтримка шифрування та електронного підпису.

Недоліки:

- потреба у додатковому обладнанні (зчитувачах);
- ризик втрати або пошкодження;
- складність в адмініструванні при великій кількості користувачів.

4. Апаратні токени

Апаратні токени (наприклад, OTP-генератори) створюють одноразові паролі, які використовуються разом із основним паролем. Вони часто застосовуються в банківських системах та корпоративному середовищі як елемент двофакторної автентифікації.

Переваги:

- підвищений рівень захисту;
- одноразові паролі зменшують ризик перехоплення.

Недоліки:

- вартість придбання та обслуговування пристроїв;
- можливість втрати або викрадення токена;
- залежність від зовнішнього пристрою.

Традиційні методи автентифікації, попри свою популярність, мають обмеження з точки зору безпеки, зручності та захисту від сучасних атак. Зі зростанням складності інформаційних загроз постає потреба у впровадженні більш надійних методів, таких як біометричні системи, які забезпечують вищу точність і унікальність при ідентифікації особи.

2.2 Інформаційне забезпечення систем контролю доступу

Інформаційне забезпечення систем контролю доступу є невід'ємною частиною архітектури безпеки сучасних інформаційних систем. Воно охоплює сукупність даних, правил, процедур та програмних засобів, які забезпечують належну обробку, збереження, передачу та захист інформації, що використовується для ідентифікації, автентифікації та авторизації користувачів.

Основні компоненти інформаційного забезпечення:

1. Бази даних ідентифікаційної інформації

База даних є центральним елементом, де зберігаються профілі користувачів, що включають:

- унікальні ідентифікатори (ID);

- облікові записи;
- паролі або їх хеші;
- біометричні шаблони (відбитки пальців, сітківка ока тощо);
- рівні доступу та ролі;
- логи подій і журнал автентифікації.

Для безпеки бази даних використовуються методи шифрування, контроль доступу до записів, а також регулярне резервне копіювання.

2. Механізми автентифікації

Це програмні засоби, які реалізують логіку перевірки особи користувача. До них належать:

- алгоритми хешування (SHA-256, bcrypt тощо);
- протоколи автентифікації (LDAP, Kerberos, RADIUS);
- двофакторна та багатофакторна автентифікація;
- обробка біометричних шаблонів.

3. Політики доступу

Політики визначають, хто і до чого має доступ, на яких умовах і з якими правами. Основні моделі:

- **Дискреційна модель (DAC)** — доступ залежить від власника об’єкта;
- **Мандатна модель (MAC)** — доступ визначається політикою безпеки системи;
- **Рольова модель (RBAC)** — права надаються відповідно до ролі користувача;
- **Атрибутна модель (ABAC)** — доступ базується на множині атрибутів.

4. Програмне забезпечення систем контролю доступу

Ці програми реалізують:

- інтерфейс користувача;
- управління користувачами та ролями;
- обробку запитів на автентифікацію;
- ведення журналів подій;
- візуалізацію активності системи;
- інтеграцію з іншими модулями IT-інфраструктури.

5. Модулі аналізу та звітності

Ці компоненти забезпечують:

- аудит безпеки;
- моніторинг спроб несанкціонованого доступу;
- генерацію звітів для адміністраторів безпеки;
- оцінку ефективності системи автентифікації.

Вимоги до інформаційного забезпечення:

- **Надійність** — стійкість до збоїв та атак;
- **Конфіденційність** — захист персональних даних;
- **Цілісність** — недопущення модифікації даних без авторизації;
- **Доступність** — гарантований доступ до системи авторизованим користувачам;
- **Масштабованість** — можливість розширення системи за потреби.

Дактилоскопія, або ідентифікація за відбитками пальців, становить найбільш вдосконалену та широко впроваджену на сьогоднішній день технологію біометричної ідентифікації особи. Вона використовується як у цивільних системах безпеки (банківських, мобільних, прикордонних), так і в правоохоронній та криміналістичній практиці, що підкреслює її надійність і ефективність.

Основи дактилоскопічної ідентифікації

Ключовим фактором, що забезпечує унікальність дактилоскопічного методу, є папілярні візерунки на подушечках пальців, які формуються ще до народження людини і залишаються незмінними протягом усього життя. Ці візерунки складаються з ліній, які можуть створювати дуги, петлі, завитки, розгалуження або бути перерваними.

Ідентифікація ґрунтується на аналізі таких характерних елементів:

- **гребені та долини** (лінії та проміжки між ними),
- **кінцеві точки гребенів**,
- **розгалуження (біфуркації)**,
- **ізольовані точки або "острівці"**,
- **морфологічна структура** візерунка (форма дуг, наявність замкнених ліній, симетрія, тощо).

Алгоритми обробки відбитків, які застосовуються у сучасних системах, виконують:

- попередню обробку зображення (фільтрація шумів, покращення контрасту),
- бінаризацію і скелетизацію (перетворення зображення до лінійної структури),
- виділення характерних точок (мінут),
- формування унікального **коду відбитка** (вектор, шаблон),
- порівняння з базою даних за допомогою спеціальних метричних алгоритмів (наприклад, за допомогою евклідової або геймінгової відстані).

Зберігання і використання шаблонів

Після виділення ключових ознак, система формує **уніфікований цифровий шаблон**, який зберігається у зашифрованому вигляді в базі даних. Ці шаблони містять лише мінімальну кількість інформації, необхідну для порівняння, що мінімізує ризик компрометації персональних даних у разі витоку.

У більшості систем використовуються **пороги подібності** (threshold), які визначають, чи вважається збіг достатнім для ідентифікації. Цей підхід дозволяє

враховувати незначні спотворення зображень, викликані тиском, вологістю чи кутом прикладання пальця.

Рисунок 2.1 – Класи відбитків пальців за натуральним розподілом (Зображення ілюструє три основні класи: *дуги*, *петлі* та *завитки*) Дактилоскопія залишається одним з найнадійніших методів біометричної автентифікації завдяки своїй стабільності, малій ймовірності помилкових збігів, ефективності в обробці та простоті використання. Вона продовжує вдосконалюватись шляхом застосування новітніх алгоритмів машинного навчання та високоточних сенсорів.

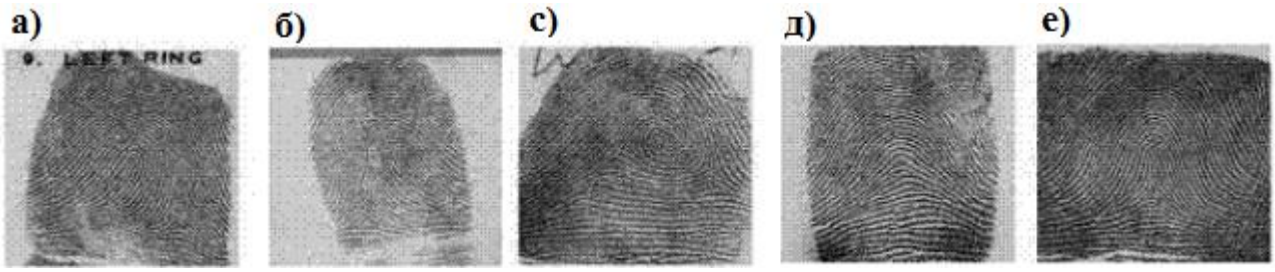


Рисунок 2.1 – Класи відбитків пальців з врахуванням натурального розподілу: а) ліва петля, б) права петля, с) завиток, д) дуга, е) півсфера

Кожен відбиток пальця містить у собі унікальний набір характеристик, які поділяються на дві основні групи: **глобальні** та **локальні ознаки**. Їхня сукупність дозволяє точно ідентифікувати особу в рамках біометричної системи.

Глобальні ознаки

Глобальні ознаки — це загальна структура візерунка на подушечці пальця. До них належать:

- **Папілярний узор** — унікальний малюнок, сформований виступами (гребенями) та западинами (долинами) шкірного рельєфу;
- **Виступ (гребінь)** — опукла лінія, що проходить по поверхні шкіри;
- **Западинка (долина)** — улоговина між двома виступами;

- **Центр (ядро)** — центральна точка узору або область з максимальною кривизною ліній;
- **Дельта** — точка, де три лінії візерунка з'єднуються або розходяться (схожа на трикутну область);
- **Область інтересу** — фрагмент зображення, який містить більшість інформативних ознак і використовується для ідентифікації.

У дактилоскопії прийнято класифікувати відбитки пальців на три основні типи:

- **Дуги** (~5% населення),
- **Петлі** (~65%),
- **Завитки** (~30%).

Кожен із цих типів додатково розподіляється на підтипи залежно від симетрії, кількості дельт, напряму та форм ліній.

Локальні ознаки

Локальні або мінутні ознаки — це дрібні, але унікальні деталі папілярного узору. Вони мають критичне значення в процесі порівняння відбитків:

- **Унікальні точки**: кінці ліній, роздвоєння (біфуркації), переривання, точки відгалуження тощо;
- **Орієнтація** кожної такої точки фіксується разом з її **точними координатами**;
- В одному відбитку може міститись **до 70 локальних ознак**, які утворюють унікальний шаблон.

Для підвищення точності порівняння, в базах даних зазвичай зберігається **декілька варіантів одного і того ж відбитка**, що враховують можливі варіації положення пальця (обертання, зсув, натиск).

Практичні аспекти використання

Всі відбитки, зібрані за допомогою спеціалізованих сканерів або сенсорів, проходять обробку та кодування у вигляді **цифрових шаблонів**, які використовуються для подальшого порівняння з еталонними записами в системі.

Переваги дактилоскопічної системи:

- Швидка ідентифікація (займає лише кілька секунд),

- Висока точність,
- Простота у використанні,
- Компактність пристроїв.

Обмеження:

- Близько **1% людей** не можуть бути ідентифіковані через вроджені чи набуті дефекти шкіри;
- У разі **тимчасових ушкоджень** пальців (опіки, порізи) ідентифікація ускладнюється, однак можлива після повного загоєння;
- За необхідності реєструється **резервний відбиток** з іншого пальця.

Розповсюдження технології

Системи на основі відбитків пальців є одними з найпоширеніших біометричних технологій у світі. Їх активно розробляють і вдосконалюють компанії з США, Швеції, Угорщини та інших країн. Сканери інтегруються у широкий спектр пристроїв:

- ноутбуки,
- комп'ютерні миші та клавіатури,
- флеш-накопичувачі,
- зовнішні пристрої та термінали, які є складовими **AFIS-систем** (Automated Fingerprint Identification Systems).

2.3 Процеси автентифікації за допомогою відбитків пальців

Автентифікація за допомогою відбитків пальців є однією з найнадійніших та широко впроваджених форм біометричної перевірки особи. Цей процес ґрунтується на унікальності папілярного візерунка шкіри пальців, який залишається незмінним протягом усього життя людини. У біометричних системах автентифікація за відбитком пальця проходить кілька послідовних етапів, які можна умовно поділити на дві основні фази: **реєстрацію (енролмент)** та **верифікацію (ідентифікацію)**.

Етап 1. Реєстрація (Enrollment)

У фазі реєстрації користувач вперше взаємодіє з біометричною системою. Цей етап включає:

Сканування відбитка пальця за допомогою спеціального сенсора (оптичного, ємнісного, ультразвукового тощо);

Передобробку зображення, яка включає:

- підвищення контрастності;
- шумозаглушення;
- нормалізацію зображення;

Виділення ключових ознак, таких як:

положення та орієнтація локальних особливостей (кінці ліній, роздвоєння тощо);

глобальні характеристики візерунка;

Формування шаблону (template) – компактного математичного представлення відбитка;

Збереження шаблону у базі даних або на носії (наприклад, на смарт-карті).

Цей шаблон не є зображенням у прямому вигляді, що забезпечує захист персональних біометричних даних.

Етап 2. Верифікація або Ідентифікація

Після реєстрації система може виконувати дві основні операції:

- **Верифікація** (1:1) – перевірка, чи відповідає представлений шаблон заявленому користувачу (наприклад, при вході в систему);
- **Ідентифікація** (1:N) – пошук шаблону у базі даних, щоб визначити особу користувача серед багатьох інших.

Процес включає:

- **Повторне сканування відбитка** користувача;
- **Обробку зображення** з виділенням ознак;

- **Порівняння шаблону** з одним (верифікація) або кількома (ідентифікація) збереженими шаблонами;
- **Прийняття рішення** на основі встановленого порогу схожості (threshold);
- **Видача результату** – підтвердження або відмова в доступі.

Технічні аспекти та надійність

У процесі автентифікації система враховує **допуски на похибки**, що виникають через:

- незначне зміщення пальця;
- зміни тиску;
- неякісне сканування (волога або суха шкіра, подряпини);
- зовнішні фактори (температура, освітлення тощо).

Для оцінки ефективності процесу використовуються такі метрики:

FAR (False Acceptance Rate) – ймовірність помилкового прийняття;

- **FRR (False Rejection Rate)** – ймовірність помилкової відмови;
- **EER (Equal Error Rate)** – точка, в якій FAR і FRR рівні; чим вона нижча, тим точніша система.

Приклади використання

Біометричні системи автентифікації за відбитками пальців застосовуються у:

- системах фізичного доступу до приміщень;
- електронних пристроях (смартфони, ноутбуки);
- банківській сфері (банкомати, мобільний банкінг);
- паспортному контролі та імміграційних службах;
- державних системах обліку (ID-картки, вибори).

На сучасному етапі технологія ідентифікації за допомогою відбитків пальців є однією з найбільш уживаних у біометричних системах контролю доступу. Цей метод заснований на принципі унікальності папілярних візерунків, які присутні на пальцях кожної людини. Кожен такий візерунок має свої неповторні характеристики, що дозволяють використовувати їх для точної ідентифікації особи.

Процес ідентифікації розпочинається зі сканування відбитка пальця, під час якого папілярний візерунок фіксується і перетворюється у цифровий образ. Цей цифровий образ далі конвертується в унікальний цифровий код, який зберігає всі особливості візерунка. Отриманий код вноситься до бази даних, де він зберігається для майбутнього використання.

При кожній спробі доступу до системи, новий відбиток сканується і також перетворюється в цифровий код, який потім порівнюється з вже існуючими кодами в базі даних. Якщо знайдено відповідність між новим кодом і одним з зареєстрованих кодів, доступ до системи надається. Цей метод ідентифікації є високоефективним завдяки своїй точності та надійності в розпізнаванні осіб.

2.3 Біометричний контроль доступу за допомогою відбитків пальців

Біометричний контроль доступу, що базується на використанні відбитків пальців, має ряд суттєвих переваг, які забезпечили його широку популярність у різних галузях:

- **Простота використання** — користувачеві достатньо прикласти палець до сенсора, що не потребує спеціальної підготовки;
- **Комфорт** — швидка і безконтактна процедура ідентифікації;
- **Висока надійність та достовірність** — відбиток пальця є унікальним та стабільним біометричним параметром;
- **Відносно низька вартість обладнання** — сучасні сканери відбитків пальців стали доступними і компактними.

Ці фактори сприяють широкому застосуванню таких систем у сфері безпеки, банківських послуг, державних установ, а також у персональних гаджетах.

Недоліки та обмеження

Водночас існують певні технічні та фізіологічні обмеження:

- **Мінімальні пошкодження шкіри**, такі як подряпини, порізи або опіки, можуть ускладнювати зчитування папілярного візерунка;
- **Вплив хімічних речовин** іноді призводить до деформації шкіри та порушення точності сканування;
- **Суха шкіра** може перешкоджати якісному зчитуванню відбитків деякими типами сенсорів.

Показники точності

Середній рівень помилкової відмови в системах розпізнавання відбитків пальців (FAR — False Acceptance Rate) становить близько **0,001%**, що є високим показником для біометричних технологій. Ефективність зберігається стабільною при чисельності персоналу до 300 осіб.

Сучасний стан ринку

Системи ідентифікації на основі відбитків пальців займають понад половину світового ринку біометричних технологій, що свідчить про їхню затребуваність і високу довіру користувачів.

Безпека і зручність

Використання відбитків пальців для аутентифікації значно полегшує користувачам процес доступу, у порівнянні з традиційними методами, що вимагають пам’ятати та захищати паролі. Це робить технологію бажаною як для комерційних організацій, так і для державних структур.

Технології розпізнавання

Існує кілька популярних архітектурних підходів до обробки відбитків пальців:

- **Match-on-Host** — у цій технології сенсор лише зчитує дані відбитка і відправляє їх на зовнішній процесор (хост) для обробки та порівняння з шаблонами. Всі обчислення виконуються на платформі хоста.
- **Match-in-Sensor** — це компактна система на кристалі (SoC), яка виконує всі операції — від реєстрації відбитків до зберігання шаблонів і біометричного порівняння — безпосередньо всередині сенсора.

Вимоги до сенсорів

Основна функція сенсора полягає у забезпеченні позитивної ідентифікації користувача шляхом точного порівняння захищеного шаблону із зчитаним відбитком. Сенсор застосовується на етапі реєстрації для створення запису та під час кожної наступної спроби доступу для порівняння нового зразка відбитка з наявним шаблоном (рисунок 2.2).

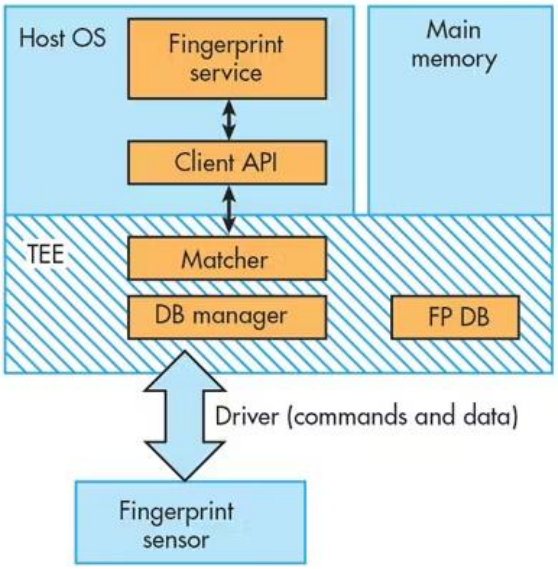


Рисунок 2.2 – Аутентифікація за технологією «Match-on-Host»

Архітектури розпізнавання відбитків пальців: Match-on-Host та Match-in-Sensor

Сучасні біометричні системи розпізнавання відбитків пальців здебільшого базуються на двох основних архітектурах: **Match-on-Host** та **Match-in-Sensor**, кожна з яких має свої особливості, переваги й обмеження.

Архітектура Match-on-Host з оточенням довіри (Trusted Execution Environment, TEE)

У архітектурі Match-on-Host процес порівняння відбитків пальців виконується у захищеній області пам’яті — довіреному середовищі виконання (TEE), яке працює в межах загальної системи хоста (смартфон, планшет, ПК чи спеціалізований пристрій). Сенсор відбитків пальців відповідає лише за захоплення

зображення відбитка, тоді як всі операції ідентифікації, створення та зберігання шаблонів, а також порівняння здійснюються процесором хоста.

До функцій програмного забезпечення у цій архітектурі належать:

- Виявлення та ідентифікація характерних ознак відбитка;
- Формування захищеного біометричного шаблону;
- Безпечне зберігання шаблонів;
- Порівняння нових відбитків із збереженими шаблонами;
- Використання антиспуфінгових технологій для виявлення спроб підробки біометричних даних.

Хостова система відповідає за захист цілісності і конфіденційності біометричних даних та за запобігання атакам з підробкою (спуфінгом).

Основні переваги архітектури Match-on-Host — це:

- Відносно низька вартість впровадження;
- Короткий цикл розробки;
- Легкість інтеграції відбиткових сенсорів у різні пристрої.

Ці фактори сприяли широкому поширенню цієї архітектури та розвитку суміжних стандартів, таких як Universal Authentication Framework (UAF) від альянсу FIDO.

Проте, незважаючи на переваги, з точки зору інформаційної безпеки ця архітектура є менш надійною у порівнянні з Match-in-Sensor через те, що критичні операції відбуваються поза межами сенсора, що потенційно збільшує вразливість до атак.

Архітектура Match-in-Sensor

На відміну від Match-on-Host, архітектура Match-in-Sensor інтегрує весь процес ідентифікації безпосередньо в сенсор відбитків пальців. Інтегральна схема сенсора містить:

- Високошвидкісний мікропроцесор;
- Пам’ять для зберігання інструкцій і даних;
- Механізми захищеного зв’язку;
- Вбудовані криптографічні модулі високої продуктивності.

Ця інтеграція реалізована у вигляді системи на кристалі (SoC), що забезпечує високий рівень безпеки завдяки виконанню всіх біометричних операцій у захищеному та ізольованому середовищі всередині самого сенсора (рисунок 2.3).

Архітектура Match-in-Sensor значно знижує ризики втручання або компрометації біометричних даних, оскільки відсутня необхідність передачі необроблених або частково оброблених даних відбитка на зовнішні пристрої до моменту їх порівняння. Це робить таку архітектуру найбільш безпечною та перспективною для застосування в умовах високих вимог до конфіденційності.

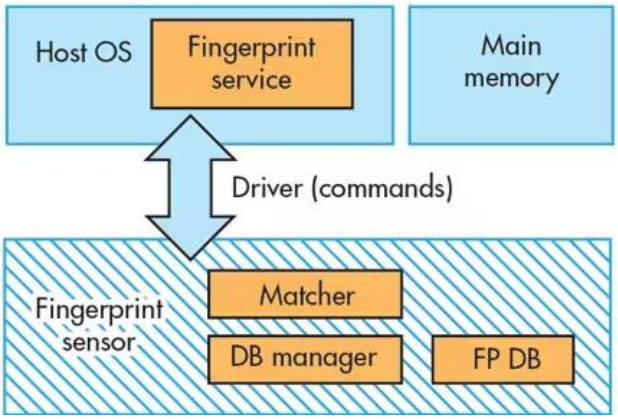


Рисунок 2.3 – Аутентифікація за технологією «Match-in-Sensor»

Переваги архітектури Match-in-Sensor для безпеки біометричних систем

Архітектура **Match-in-Sensor** ізолює операції з відбитками пальців від операційної системи хоста безпосередньо в самому сенсорі. Хоча інтеграція кількох функцій в одному модулі є звичною для сучасних інтегральних схем, рівень додаткової безпеки, що забезпечується повною інтеграцією зчитування та порівняння відбитків, має вагомий вплив на галузь.

Основні переваги Match-in-Sensor для системної безпеки:

- Фізична ізоляція відбиткових даних і середовища виконання сенсора від операційної системи хоста запобігає впливу шкідливого ПЗ і вторгненням у систему.

- Сенсор виконує біометричну ідентифікацію автономно, без залежності від зовнішніх вхідних даних, які можуть бути скомпрометовані.
- Вхідні біометричні дані захоплюються, шифруються, обробляються і зберігаються безпосередньо на чіпі сенсора.
- Результат ідентифікації підписується приватним ключем, що генерується апаратними засобами сенсора, що підвищує достовірність автентифікації.
- Криптографічні ключі для цифрових ідентифікаційних даних створюються, зберігаються та керуються безпосередньо сенсором, захищаючи дані від підробок.

Навіть у разі повної компрометації хост-системи, сенсор унеможливлює створення хибного позитивного результату або маніпуляції даними, що забезпечує збереження безпеки ідентифікації.

Щодо захисту біометричних даних користувача:

- Всі характеристики та шаблони відбитка обробляються виключно вбудованим процесором і пам’яттю сенсора.
- Біометричні дані не передаються на хост і фізично ізольовані.
- База даних шаблонів зберігається у приватній флеш-пам’яті, доступній лише сенсору.
- Шаблони шифруються та підписуються за допомогою власних алгоритмів і криптографічних ключів перед зберіганням.

Таким чином, навіть при повній компрометації хоста, неможливо викрасти біометричну інформацію користувача, що є ключовою перевагою для запобігання крадіжці особистих даних.

Сучасні виробники, зокрема компанія Synaptics, впроваджують передові сертифіковані за стандартом FIDO рішення Match-in-Sensor, які забезпечують:

- Надійне зчитування відбитків під різними кутами;
- Візуальний або вібраційний зворотний зв’язок для користувача;
- Оптимізацію під різні пристрої та застосунки;
- Відсутність потреби передавати біометричні дані між сенсором і хостом, що усуває ризики їх крадіжки.

2.3.1 Типологія сканерів відбитків пальців

На сьогоднішній день сканери відбитків пальців поділяються на три основні типи, кожен з яких має свої унікальні особливості та переваги:

– оптичні сканери відбитків пальців працюють за принципом використання світла для отримання зображення папілярних ліній;

– напівпровідникові сканери використовуються для отримання тривимірного зображення відбитка пальця, використовуючи технології вимірювання ємності або опору;

– ультразвукові сканери відбитків пальців використовують звукові хвилі для створення тривимірної моделі внутрішньої структури пальця.

2.3.2 Огляд оптичних сканерів

Оптичні сканери відбитків пальців ґрунтуються на застосуванні фізичних принципів оптики для отримання високоякісного зображення папілярного візерунка. В залежності від принципу дії, виділяють кілька основних методів зчитування:

Основні методи оптичного сканування

1. **Оптичний метод на відображення**
   Заснований на використанні джерела світла (зазвичай світлодіодного), яке освітлює палець. Світло відбивається від нерівностей шкіри, і зображення формується за допомогою матриці (наприклад, CMOS або CCD-матриці). Папілярні лінії відбивають менше світла, ніж проміжки між ними, завдяки чому створюється чітке зображення.
2. **Оптичний метод на просвіт**
   Передбачає просвічування пальця з одного боку та реєстрацію зображення на іншому за допомогою детектора. Цей метод дозволяє побачити структуру шкіри зсередини, що підвищує точність і складність підробки.

3. **Оптичні безконтактні сканери**

   Зчитують зображення без прямого дотику до сканувальної поверхні. Це підвищує гігієнічність, пришвидшує процес і зменшує зношення пристрою.

Альтернативні технології сканування

4. **Ємнісні сканери**

   Вимірюють зміни електричної ємності між поверхнею сенсора та пальцем. Кожна точка сенсора сприймає різну ємність залежно від рельєфу шкіри, формуючи електронну "карту" відбитка.

5. **Радіочастотні (RF) сканери**

   Використовують радіохвилі для проникнення під поверхню шкіри. Це дозволяє отримати зображення навіть при забрудненнях чи незначних пошкодженнях епідермісу.

6. **Тискочутливі сканери**

   Визначають малюнок папілярних ліній за змінами сили тиску, який чинить палець на сенсор. Метод менш точний, але може бути корисним у спеціалізованих сферах.

7. **Термосканери**

   Створюють зображення на основі температурних відмінностей між виступами та заглибленнями шкіри. Точність залежить від температурного контрасту.

8. **Ультразвукові сканери**

   Застосовують звукові хвилі високої частоти, які проникають в шкіру і відбиваються від різних шарів тканин. Це забезпечує створення тривимірного зображення високої точності, стійкого до підробки.

Контактні сканери та ефект повного внутрішнього відбиття

Найбільш поширені **контактні оптичні сканери** використовують принцип **повного внутрішнього відбиття**. Палець прикладається до скляної або акрилової пластини, яка освітлюється з боків. Якщо світловий промінь падає під певним кутом, і не відбувається проходження в інше середовище, відбувається повне внутрішнє відбиття.

У місцях, де палець торкається поверхні (вершини папілярних ліній), відбивання світла порушується, і частина світла поглинається. У заглибленнях (між лініями) світло повністю відбивається. Так створюється контрастне зображення відбитка (рис. 2.4).

Цей метод дає змогу отримати якісне, стійке до шуму зображення, проте потребує фізичного контакту з пристроєм, що може бути обмеженням у деяких сценаріях використання (наприклад, у медичній сфері або за умов підвищеної стерильності).

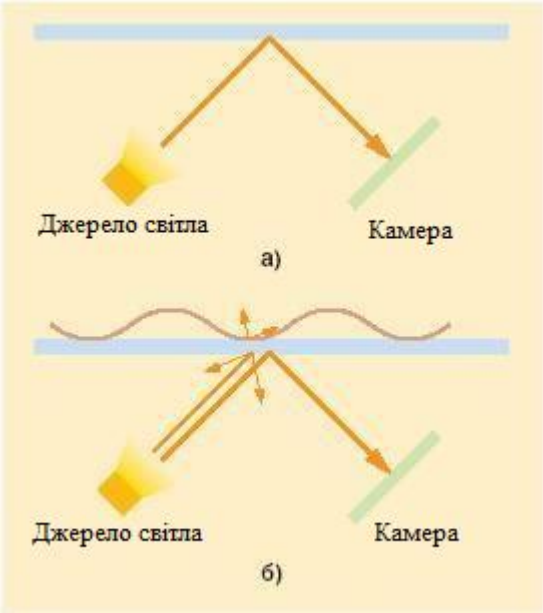


Рисунок 2.4 – Принцип роботи методу відображення

Ефект повного внутрішнього відбиття

У контексті роботи оптичних контактних сканерів важливим є явище **повного внутрішнього відбиття**. Коли палець торкається скануючої поверхні (зазвичай — скла або пластику), світловий пучок, що поширюється в середовищі з більш високим показником заломлення, досягає межі з повітрям або шкірою. Якщо кут падіння менший за критичний, пучок світла **пройде через межу**, а якщо більший — **повністю відбивається**. Однак у місцях дотику папілярних ліній, де поверхня

шкіри притиснута до скла, цей ефект порушується — частина світла поглинається або розсіюється, утворюючи тіньову ділянку на зображенні.

Таким чином, світло відбивається лише в тих місцях, де між шкірою та поверхнею сканера залишається повітря, тобто **між папілярними лініями**. Це дозволяє чітко розрізняти структуру відбитка на отриманому зображенні (рис. 2.4).

Переваги оптичного методу відображення:

- **Висока якість зображення.**
  Оптичні сканери забезпечують високу роздільну здатність, що дозволяє точно зафіксувати особливості папілярного візерунка для подальшої ідентифікації.
- **Надійність.**
  Більшість моделей не потребують тиску чи глибокого контакту, що дозволяє працювати навіть за незначного забруднення пальця.
- **Швидкість сканування.**
  Обробка зображення відбувається майже миттєво, що підвищує ефективність у місцях з великим потоком користувачів (аеропорти, підприємства тощо).
- **Безпека для здоров’я.**
  Сканери не випромінюють радіацію чи інші шкідливі сигнали, тому є цілком безпечними для тривалого використання.

Недоліки оптичного методу відображення:

- **Вразливість до впливу середовища.**
  Надмірна вологість, пил або жир на поверхні сканера можуть значно знизити якість зчитування.
- **Необхідність фізичного контакту.**
  Контакт із поверхнею може бути неприйнятним у медичних закладах або в умовах, що вимагають стерильності.

- **Проблеми з пошкодженими пальцями.**
  Подряпини, мозолі або надмірно суха шкіра можуть спотворювати структуру відбитка.
- **Залежність від освітлення.**
  Якість роботи сканера може залежати від стабільності внутрішнього підсвічування, а також умов навколишнього освітлення.

Безконтактні оптичні сканери

Безконтактні оптичні сканери є перспективним напрямом біометричних технологій, що дозволяє уникнути недоліків, пов'язаних з фізичним дотиком до пристрою. Ці системи використовують **комбінований оптичний підхід**, що включає:

- **Систему підсвічування.**
  Джерела світла (світлодіоди) розміщуються під різними кутами, забезпечуючи рівномірне освітлення поверхні пальця, що розміщується над сканером.
- **Оптичну лінзову систему.**
  Лінза або система дзеркал фокусує відбиті світлові промені, що формують проекцію папілярного візерунка.
- **Камеру.**
  Цифрова матриця (CMOS або CCD) фіксує зображення, яке далі обробляється спеціалізованим програмним забезпеченням (рис. 2.5).

Переваги безконтактних сканерів:

- Вища гігієнічність (відсутність прямого контакту).
- Менше зношення пристроїв.
- Зменшення ризику пошкодження поверхні сенсора.
- Придатні для використання у сфері охорони здоров'я та державних структур.

Обмеження:

- Складніша оптична схема.
- Залежність від стабільного освітлення навколо.
- Вища вартість порівняно з контактними пристроями.

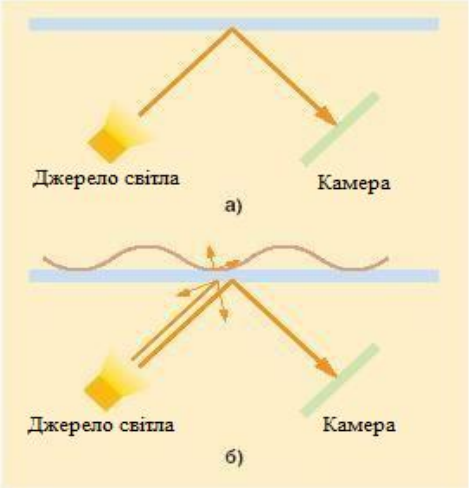


Рисунок 2.5 – Принцип роботи безконтактного сканера

Оптичні безконтактні сканери функціонують без фізичного дотику пальця до сенсорної поверхні. Це досягається за рахунок використання спеціальної оптичної системи, яка фіксує зображення папілярного візерунка за допомогою світлових променів та високочутливих камер. Такий підхід дозволяє отримати **детальне та якісне зображення відбитка**, не створюючи прямого контакту з шкірою.

Переваги оптичних безконтактних сканерів:

- **Збереження гігієни.**
  Відсутність фізичного контакту знижує ризик перенесення бактерій або вірусів між користувачами, що особливо важливо у громадських або медичних закладах.
- **Зручність використання.**
  Безконтактне сканування є швидшим і комфортнішим для користувача, не вимагає прикладання пальця під певним кутом чи з певною силою.
- **Висока точність.**
  Завдяки вдосконаленим оптичним компонентам сканери здатні фіксувати дрібні деталі папілярного візерунка, що підвищує точність ідентифікації.
- **Універсальність.**
  Пристрої можуть ефективно працювати з різними типами шкіри, а також в умовах змінного освітлення, що робить їх придатними для широкого спектра застосувань.

Недоліки оптичних безконтактних сканерів:

- **Чутливість до вологості.**
  Вологі або пітні пальці можуть спотворювати зображення, знижуючи ефективність розпізнавання.
- **Залежність від умов освітлення.**
  Для точного зчитування зображення потрібно забезпечити стабільне, якісне освітлення — його нестача або надлишок можуть ускладнити сканування.
- **Похибки при русі.**
  Якщо користувач рухає пальцем під час сканування, це може спричинити розмиття зображення або помилки у визначенні візерунка.
- **Обмеження відстані.**
  Більшість безконтактних сканерів мають оптимальний діапазон відстані між пальцем і сенсором. Порушення цього інтервалу знижує якість результату.

Загальна оцінка:

Оптичні безконтактні сканери демонструють значні переваги, зокрема збереження гігієни, високу точність та зручність. Водночас їх ефективність залежить від умов експлуатації — вологість, нестабільне освітлення або швидкі рухи можуть вплинути на точність розпізнавання.

2.3.3 Аналіз напівпровідникових сканерів

Напівпровідникові сканери

Напівпровідникові сканери базуються на принципі зміни електричних властивостей матеріалу сенсора при взаємодії з папілярним візерунком пальця. Коли палець прикладається до поверхні сканера, виникає контакт між шкірою та сенсорною поверхнею, що змінює електричну провідність або відбивну здатність мікроструктур напівпровідника.

Сканер фіксує ці зміни, аналізуючи структуру поверхні шкіри та будуючи високоточно деталізоване зображення відбитка пальця. Завдяки прямій електричній взаємодії, ці сканери демонструють високий рівень точності та мають переваги в

умовах, де оптичні методи можуть давати збої (наприклад, при сильному зовнішньому освітленні).

Переваги напівпровідникових сканерів:

- **висока точність і деталізація;**
- **стійкість до забруднень поверхні;**
- **можливість мініатюризації пристрою;**
- **низьке енергоспоживання.**

Однак такі сканери можуть бути чутливими до температури навколишнього середовища та стану шкіри користувача.

Ємнісні сканери

Ємнісні сканери відбитків пальців є найбільш поширеними у мобільних пристроях, таких як смартфони та планшети. Їхня робота базується на використанні електростатичного поля для зчитування мікрорельєфу шкіри.

Усередині сканера розміщений масив мікроскопічних **конденсаторів**, кожен з яких вимірює **зміну ємності** при дотику пальця. Папілярні лінії, які знаходяться ближче до сенсора, спричиняють меншу ємність, ніж западини між ними. Таким чином формується електрична карта відбитка, яка з високою точністю відображає структуру шкіри.

Переваги ємнісних сканерів:

- **висока точність зображення;**
- **невеликий розмір і зручність інтеграції в мобільні пристрої;**
- **надійність і швидкість обробки;**
- **низький рівень енергоспоживання.**

Недоліки:

- **зниження точності при наявності вологи або бруду на пальці;**
- **можливість зношення сенсорної поверхні з часом.**

На **рис. 2.6** зображено схематичну модель роботи ємнісного сканера, яка демонструє принцип фіксації мікроскопічного рельєфу шкіри через вимірювання змін у електричному полі.

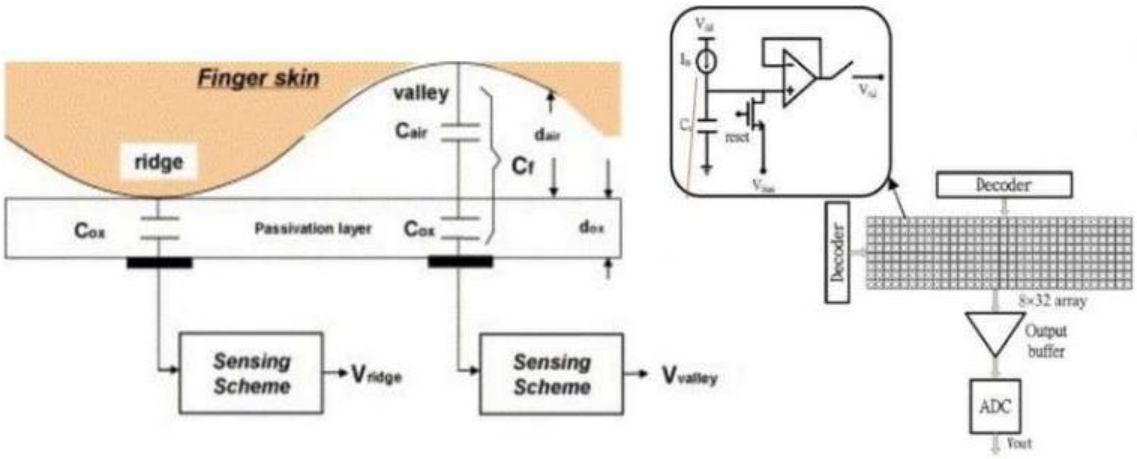


Рисунок 2.6 – Принцип роботи ємнісного сканеру

Коли палець наближається до поверхні ємнісного сканера, його **папілярні виступи** торкаються сенсорної зони, змінюючи **ємність вбудованих конденсаторів** саме в тих місцях, де відбувається контакт. У свою чергу, **впадини** між виступами не торкаються поверхні, залишаючи відповідні ємності **незмінними**. Такий розподіл ємностей створює **матрицю відмінностей**, яка зчитується електронним інтегратором на базі операційного підсилювача. Саме він перетворює фізичні зміни у поверхневій ємності на **електричний сигнал**.

Після цього сигнал обробляється **аналогово-цифровим перетворювачем (АЦП)**, який перетворює аналогові значення ємностей у цифрові дані. Ці цифрові значення передаються до обчислювального модуля системи, де відбувається аналіз та реконструкція **цифрового зображення відбитка пальця**.

Завдяки цьому процесу, ємнісні сканери здатні формувати точні та стабільні зображення відбитків, що робить їх ефективним інструментом у сучасних біометричних системах.

Переваги ємнісних сканерів:

- **Висока точність сканування.** Здатність фіксувати мікроскопічні особливості папілярного візерунка.
- **Менша чутливість до рухів.** У порівнянні з оптичними сканерами, ємнісні моделі рідше видають помилки при незначному русі пальця.

- **Висока швидкість.** Дані зчитуються практично миттєво, що дозволяє використовувати їх у системах з високою пропускною здатністю.
- **Сумісність із різними умовами експлуатації.** Сканери можуть працювати з різними типами шкіри та в умовах різного освітлення.

Недоліки ємнісних сканерів:

- **Чутливість до вологи й забруднень.** Наявність води, жиру або бруду на пальці чи сканері може знижувати якість зображення.
- **Вразливість до зносу.** Часте використання може призводити до механічного зношення сенсорної поверхні.
- **Обмеження відстані.** Палець має бути в безпосередньому контакті з поверхнею для коректного зчитування.
- **Вартість.** Технологія ємнісного сканування зазвичай дорожча за базові оптичні рішення, що може бути важливо у великомасштабному впровадженні.

Отже, ємнісні сканери поєднують **високу точність, швидкодію та зручність інтеграції** в сучасні пристрої, однак їх ефективність може знижуватись при недотриманні умов експлуатації.

Термосканери

Термосканери функціонують на основі вимірювання **температурного профілю поверхні пальця**. При дотику пальця до сенсора тепло передається від шкіри до пристрою. Завдяки різній **температурі папілярних ліній і впадин**, на сканері утворюється температурний малюнок, що відображає рельєф шкіри.

Термочутливі елементи (як правило, терморезистори або пірометричні матриці) фіксують різницю температур, а отримані дані обробляються мікроконтролером для створення теплового зображення відбитка. Такий метод може бути **ефективним при слабкому зовнішньому освітленні** або навіть у темряві, оскільки він не залежить від світла.

На **рис. 2.7** наведено принцип дії термосканера, що ілюструє, як тепло передається до сенсорної поверхні та формується температурна карта відбитка.

Переваги термосканерів:

- **Не залежать від освітлення.** Можуть працювати у темних або нестабільно освітлених умовах.
- **Безконтактне або мінімально контактне сканування.**
- **Швидка реакція на зміну температури.**

Недоліки:

- **Чутливість до зовнішніх джерел тепла.** Нагріта поверхня сканера або холодні пальці можуть спотворити результат.
- **Менш деталізоване зображення.** У порівнянні з оптичними чи ємнісними методами, термокарта може бути менш точною.
- **Висока залежність від часу дотику.** Надто короткий або довгий контакт може призводити до похибок.

Таким чином, термосканери є перспективним методом, особливо у специфічних умовах, але потребують **ретельного калібрування** та **контролю температурного фону** для досягнення високої точності.

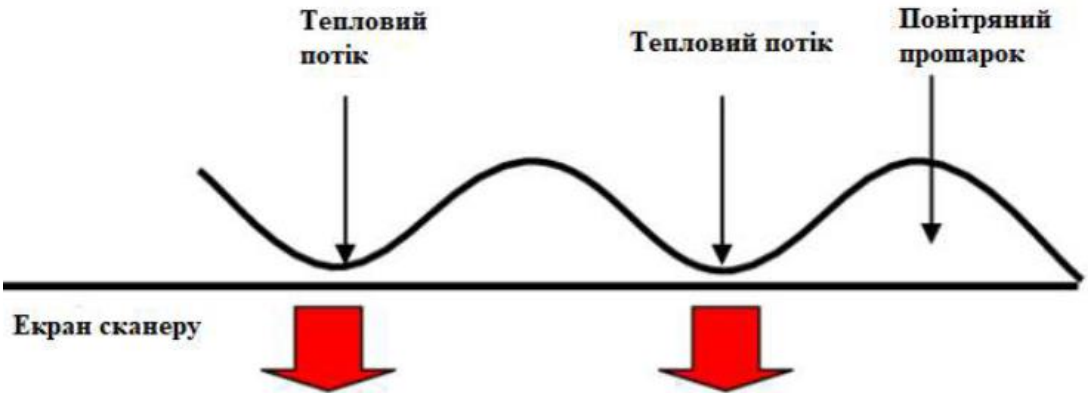


Рисунок 2.7 – Принцип роботи термосканера

Контактна поверхня термального сканера обладнана сіткою мікроскопічних піроелектричних сенсорів. У момент дотику пальця до пристрою, виступи папілярного візерунку (так звані гребені) передають тепло безпосередньо на ці чутливі елементи. У місцях, де між шкірою й сенсорною поверхнею залишаються

порожнечі (тобто в западинах), теплове випромінювання значно слабшає через наявність повітряного проміжку.

Піроелектричні сенсори реагують на ці теплові коливання, генеруючи електричні сигнали, які відповідають температурному розподілу на зоні дотику. Надалі ці сигнали оцифровуються та обробляються для побудови термографічного зображення відбитка пальця. Таким чином, формується **теплова карта**, яка відтворює індивідуальний рельєф шкіри та дозволяє провести біометричну ідентифікацію користувача з високою точністю.

Переваги термальних сканерів:

- **Стійкість до зовнішніх впливів.** Термальні сканери надійно функціонують у складних середовищах, включаючи вологі приміщення, забруднене повітря чи значні температурні коливання.
- **Мінімальний фізичний контакт.** У багатьох випадках пристрій здатен зчитувати дані без прямого дотику, що зменшує зношення компонентів і підвищує гігієнічність використання.
- **Висока точність сканування.** Технологія дозволяє розпізнавати унікальні термальні властивості шкіри, що підвищує надійність автентифікації.
- **Працездатність у темряві.** Оскільки зчитування базується на тепловому випромінюванні, пристрої не залежать від джерел зовнішнього світла.

Недоліки термальних сканерів:

- **Висока собівартість.** Виготовлення сенсорних елементів і супутніх систем обробки сигналів потребує складних інженерних рішень, що впливає на кінцеву ціну пристрою.
- **Температурна вразливість.** Експлуатація за межами допустимого температурного діапазону може вплинути на точність або навіть працездатність сканера.
- **Питання конфіденційності.** Використання термограм може викликати занепокоєння щодо захисту персональних біометричних даних, особливо в разі збереження зображень або передачі їх через мережу.

- **Чутливість до вологи або жирів.** Надмірна вологість шкіри або наявність жирної плівки можуть ускладнити передачу тепла й знизити точність формування зображення.

Отже, термосканери забезпечують високу надійність і точність у складних експлуатаційних умовах, але потребують ретельного врахування технічних параметрів і потенційних витрат. Їхня ефективність особливо помітна в середовищах, де традиційні контактні методи зчитування виявляються малопридатними.

2.3.4 Використання ультразвукових сканерів

Ультразвукові біометричні сканери є однією з найсучасніших технологій у сфері ідентифікації особи за відбитком пальця. Ці пристрої працюють на основі принципу передавання ультразвукових хвиль на шкірну поверхню користувача та подальшого аналізу відбитих сигналів, які залежать від мікроструктури папілярного візерунка.

Під час сканування сенсор генерує високочастотні звукові імпульси, які проходять крізь шкіру та частково відбиваються залежно від її рельєфу та внутрішньої будови. Ультразвуковий сигнал, що повертається назад до приймача, містить інформацію про тривимірну структуру гребенів і западин пальця. Отримані дані обробляються за допомогою спеціального алгоритму, який формує високоточне зображення відбитка пальця (рис. 2.8).

На відміну від традиційних методів, які зчитують лише поверхневі характеристики шкіри, ультразвукові сканери дозволяють створити детальну карту як поверхневого, так і підшкірного шару. Завдяки цьому вони демонструють високу стійкість до спроб підробки, наприклад, за допомогою силіконових або паперових копій відбитків.

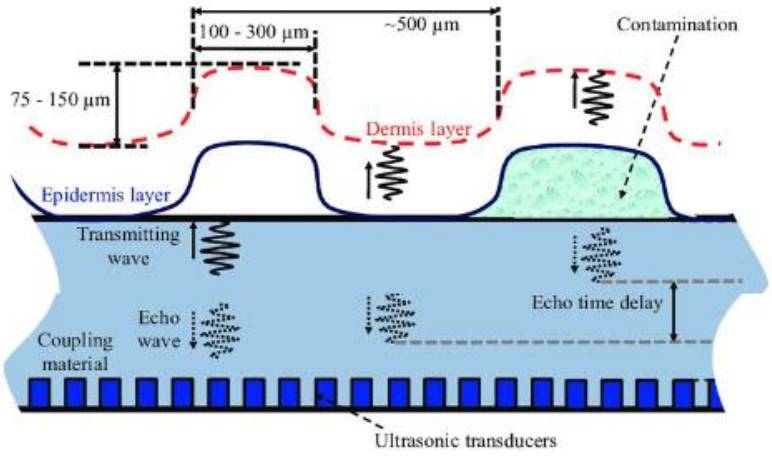


Рисунок 2.7 – Принцип роботи ультразвукового сканеру

Під час взаємодії ультразвукової хвилі з поверхнею пальця, сигнал по-різному відбивається від папілярних ліній. Виступи (гребені) знаходяться ближче до передавача й першими відбивають хвилю, тоді як западини, розташовані глибше, створюють затримку у поверненні сигналу. Ці відмінності у часі відбиття акустичних імпульсів фіксуються приймачем сканера та перетворюються в електронні сигнали, які далі обробляються для створення цифрової моделі відбитка.

Така технологія дозволяє зчитувати мікроскопічні особливості шкіри, що недоступні для традиційних оптичних або ємнісних сканерів. Завдяки глибшому проникненню ультразвуку, формується тривимірне зображення, яке характеризується високою деталізацією. Ультразвукові сканери демонструють підвищену точність і ефективність, що робить їх оптимальним рішенням для систем, де необхідна надійна автентифікація.

Основні переваги ультразвукових сканерів:

- **Точність ідентифікації.** Завдяки глибокому аналізу структури шкіри, сканери забезпечують високий рівень достовірності при розпізнаванні особи.
- **Стійкість до зовнішніх факторів.** Пристрої залишаються функціональними в умовах підвищеної вологості або забруднення шкіри, що розширює їх застосування в складних середовищах.
- **Швидкодія.** Сканування відбувається за лічені миті, що дозволяє інтегрувати ці системи в сценарії з високими вимогами до швидкості доступу.
- **Незалежність від освітлення.** Ультразвук не залежить від світлових умов, тому сканери ефективно працюють як у яскраво освітлених, так і в темних приміщеннях.

Недоліки ультразвукової технології:

- **Висока собівартість.** Складність конструкції та потреба в точному обладнанні роблять виробництво таких сканерів затратним.
- **Зниження точності при вологих пальцях.** Хоча сканери і можуть працювати у вологому середовищі, надмірна вологість або жирність шкіри можуть знизити якість зчитування.
- **Можливі помилкові спрацьовування.** У певних випадках пристрої можуть хибно розпізнати користувача або відмовити у доступі.

- **Енергоспоживання.** Деякі моделі потребують значного джерела живлення, що обмежує їх застосування в автономних чи мобільних пристроях.

2.4 Аппаратні токени та смарт-карти.

Апаратні токени та смарт-карти як засоби автентифікації

У контексті сучасних інформаційних систем, особливе місце займають апаратні засоби автентифікації, серед яких найпоширенішими є **апаратні токени** та **смарт-карти**. Ці пристрої забезпечують високий рівень безпеки, оскільки реалізують принцип *двохфакторної автентифікації* — поєднання фізичного носія інформації з паролем або біометричним параметром користувача.

Апаратні токени

Апаратний токен — це компактний пристрій, який зберігає криптографічні ключі, цифрові сертифікати або одноразові паролі (OTP). Його основна функція — генерування унікального коду для входу в систему, який змінюється з певним інтервалом часу або генерується на основі запиту.

Існують два основних типи токенів:

- **Токени OTP (One-Time Password)** — генерують одноразові паролі, які користувач вводить разом з логіном. Прикладом є пристрої типу RSA SecurID.
- **Криптотокени (PKI-токени)** — зберігають особисті ключі користувача і використовуються для цифрового підпису або шифрування. Найчастіше мають вигляд USB-пристрою та інтегруються з криптографічним програмним забезпеченням (наприклад, CryptoPro, OpenSC).

Переваги апаратних токенів:

- високий рівень захисту ключів (зберігаються лише на пристрої);
- складність для копіювання чи підробки;

- можливість інтеграції з системами цифрового підпису, VPN, email та іншими сервісами.

Недоліки:

- фізична втрата пристрою може призвести до недоступності сервісів;
- потреба в спеціальному програмному забезпеченні та драйверах;
- порівняно висока вартість (особливо у великій інфраструктурі).

Смарт-карти

Смарт-карта — це пластикова картка з вбудованим мікропроцесором або мікроконтролером, що здатний виконувати криптографічні операції. Вона може містити захищену пам’ять, операційну систему та апаратний генератор випадкових чисел.

Смарт-карти найчастіше використовуються у:

- банківській сфері (банківські картки з чипом);
- національних ID-картах;
- системах цифрового підпису;
- контролі фізичного доступу до об'єктів;
- державних та корпоративних інфраструктурах PKI.

Для зчитування інформації із смарт-карти використовується спеціальний рідер (пристрій зчитування), що може підключатися до комп’ютера через USB, або бути інтегрованим у клавіатуру, термінал чи інший пристрій.

Переваги смарт-карт:

- висока безпека даних завдяки апаратній криптографії;
- підтримка багаторазового використання;

- можуть комбінувати з біометричними методами (наприклад, смарт-карта + відбиток пальця).

Недоліки:

- потребують сумісного зчитувача;
- уразливість до фізичних пошкоджень;
- необхідність керування сертифікатами та оновленням ПЗ.

Порівняння

Характеристика	**Апаратні токени**	**Смарт-карти**
Форма	Зазвичай USB або брелок	Пластикова карта з чипом
Основна функція	Генерація OTP або зберігання ключів	Зберігання ключів та сертифікатів
Потреба в зчитувачі	Залежно від моделі	Так
Захист від копіювання	Високий	Високий
Простота використання	Висока (plug and play)	Залежить від інфраструктури
Додаткові функції	Підпис, автентифікація	Підпис, автентифікація, доступ

Апаратні токени та смарт-карти є ефективними інструментами для забезпечення безпечної автентифікації. Вони значно підвищують захист інформаційних систем, дозволяючи уникнути вразливостей, притаманних лише парольним системам. Вибір

між токеном і смарт-картою залежить від особливостей системи безпеки, інфраструктури організації та вимог до мобільності та зручності.

2.5 Аналіз переваг і недоліків застосування біометрії. Особливості безпеки

Біометричні технології стають дедалі популярнішими у сфері ідентифікації та автентифікації завдяки їх здатності надійно і швидко підтверджувати особу користувача. Проте, як і будь-яка технологія, біометрія має як сильні сторони, так і певні обмеження, які слід враховувати при впровадженні.

Переваги біометрії

1. **Висока точність і надійність**
   Біометричні системи базуються на унікальних фізичних або поведінкових характеристиках людини — відбитках пальців, райдужній оболонці ока, голосі тощо. Це забезпечує високу ступінь точності при розпізнаванні, що суттєво знижує ризик помилкової ідентифікації.
2. **Зручність використання**
   На відміну від традиційних методів, таких як паролі чи картки, біометрія не вимагає запам’ятовування складних комбінацій або носіння додаткових носіїв. Користувачі можуть підтвердити свою особу простим дотиком або поглядом.
3. **Складність підробки**
   Підробити або викрасти біометричні параметри набагато складніше, ніж паролі або токени. Це підвищує загальний рівень безпеки системи.
4. **Автоматизація та швидкість**
   Біометричні системи дозволяють швидко та автоматично проводити ідентифікацію, що зменшує час на обробку даних і покращує користувацький досвід.
5. **Незалежність від фізичних носіїв**
   Відсутність необхідності мати при собі окремий пристрій або карту зменшує ризик втрати або крадіжки.

Недоліки біометричних систем

1. **Питання конфіденційності**

   Збір та зберігання біометричних даних викликає занепокоєння щодо захисту персональної інформації. Зловмисники, які отримають доступ до таких даних, можуть використати їх для шахрайства або порушення приватності.

2. **Помилки розпізнавання**

   Біометричні системи не є абсолютно безпомилковими. Існують два основні види помилок:

   - *Помилка першого роду* (False Acceptance Rate, FAR) — коли система помилково ідентифікує невідповідну особу як допустиму;
   - *Помилка другого роду* (False Rejection Rate, FRR) — коли законний користувач відхиляється системою. Ці помилки можуть бути критичними в залежності від сфери застосування.

3. **Вплив зовнішніх факторів**

   Якість та точність розпізнавання може погіршуватися через забруднення сенсорів, пошкодження шкіри, зміну зовнішнього вигляду, освітлення чи вологість.

4. **Вартість впровадження**

   Встановлення та обслуговування біометричних систем часто потребують значних фінансових вкладень у спеціалізоване обладнання, програмне забезпечення та навчання персоналу.

5. **Питання адаптивності**

   Біометричні характеристики можуть змінюватися з часом через старіння, травми або захворювання, що може ускладнити підтримку актуальності бази даних.

Біометричні технології мають значний потенціал для підвищення безпеки та зручності у процесі ідентифікації користувачів. Водночас, для ефективного впровадження необхідно ретельно зважити можливі ризики, пов’язані з конфіденційністю, помилками системи та технічними обмеженнями. Оптимальним підходом є поєднання біометричних методів з іншими засобами аутентифікації (багатофакторна автентифікація), що дозволяє мінімізувати недоліки та максимально використовувати переваги.

Особливості безпеки біометричних систем

Біометричні системи, незважаючи на свою зростаючу популярність і високу ефективність у ідентифікації користувачів, мають ряд суттєвих ризиків, пов’язаних із захистом біометричних даних.

Однією з головних проблем є те, що біометричні характеристики — відбитки пальців, сітківка ока, зображення обличчя — є унікальними й незмінними для конкретної особи. На відміну від паролів або токенів, які можна замінити у разі компрометації, біометричні дані залишаються незмінними протягом усього життя. Тому викрадення або підробка таких даних має серйозні наслідки, оскільки відновити або «перевипустити» їх неможливо.

Зловмисники можуть здійснювати різноманітні атаки на біометричні системи, зокрема:

- **Спуфінг (підробка біометричних ознак).** Використання підроблених відбитків пальців, фотографій або масок для обходу системи. Такі атаки можуть вводити в оману сенсори, якщо вони не оснащені механізмами захисту, наприклад, детекцією живої тканини.
- **Атаки на сенсори та інтерфейси.** Перехоплення даних на стадії сканування, наприклад, через інтерфейси зв’язку або маніпуляції з апаратним забезпеченням.
- **Викрадення біометричних шаблонів з баз даних.** Якщо база даних, де зберігаються цифрові шаблони біометричних характеристик, буде скомпрометована, зловмисники отримають можливість використовувати ці дані для несанкціонованого доступу або створення підроблених облікових записів.

Забезпечення безпеки біометричних даних вимагає реалізації комплексних заходів:

- Шифрування біометричних шаблонів у базах даних та при передачі.
- Використання захищених протоколів комунікації.
- Впровадження механізмів виявлення підробок і визначення живих тканин.
- Контроль доступу до системи і журналювання дій.
- Регулярне оновлення програмного забезпечення і апаратних компонентів.

Таким чином, захист біометричних систем є багатошаровим процесом, що включає як технічні, так і організаційні аспекти. Відсутність належного рівня безпеки може призвести до серйозних порушень конфіденційності та зловживань, що ставить під загрозу як користувачів, так і організації, що використовують ці системи.

2.6 Висновки до розділу 2

У другому розділі було проведено детальний аналіз основних методів автентифікації та ідентифікації, зокрема біометричних систем, їх принципів роботи та технологічних особливостей. Розглянуто різноманітні види сканерів відбитків пальців, включно з оптичними, термосканерами, ультразвуковими та іншими типами, а також їх переваги і недоліки. Було виявлено, що кожен із методів має свої унікальні властивості, які впливають на рівень безпеки, точність розпізнавання та зручність використання.

Зокрема, оптичні та термосканери відзначаються високою точністю, проте можуть бути чутливими до зовнішніх умов, таких як вологість або освітлення. Ультразвукові методи забезпечують глибше сканування, але вимагають складнішого обладнання. Аналіз переваг і недоліків показав, що жоден із методів не є універсальним ідеалом, тому для підвищення надійності аутентифікації часто застосовуються комбіновані рішення.

Також було підкреслено важливість врахування факторів конфіденційності, захисту персональних даних і технічних обмежень при розробці та впровадженні біометричних систем. Загалом, для забезпечення максимальної безпеки та ефективності аутентифікації необхідно обирати методи відповідно до конкретних умов застосування, а також розробляти заходи для мінімізації їхніх слабких сторін.

Оцінено різні типи сканерів, включаючи оптичні, напівпровідникові та ультразвукові, щодо їхньої здатності забезпечити надійне зчитування відбитків. Особлива увага приділяється технологіям, що дозволяють виявляти "живі" відбитки для запобігання шахрайству за допомогою фальсифікованих відбитків.

Аналіз заходів безпеки показав, що поєднання організаційних та технічних підходів істотно підвищує рівень захищеності інформаційних систем. Застосування багаторівневої аутентифікації та сучасних алгоритмічних методів значно ускладнює несанкціонований доступ і зменшує ризик помилкових спрацьовувань. Вивчення сильних і слабких сторін біометричних методів дозволило виділити ключові напрямки для покращення, серед яких — підвищення стабільності розпізнавання та ефективне використання обчислювальних ресурсів.

Отримані результати підтверджують необхідність подальших досліджень у сфері вдосконалення інтеграції біометричних рішень та підвищення їх продуктивності. Це стане основою для розробки практичних рекомендацій, спрямованих на збільшення надійності систем, оптимізацію витрат і впровадження інноваційних технологій у галузі біометричної ідентифікації.

РОЗДІЛ 3 ТЕОРЕТИЧНІ ОСНОВИ АЛГОРИТМІВ ТА МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ

Алгоритмічне забезпечення та технології обробки в біометричних системах

Біометричні системи ідентифікації та аутентифікації користувачів є однією з найперспективніших технологій сучасного інформаційного суспільства, спрямованих на забезпечення безпеки доступу до ресурсів та інформації. Вони ґрунтуються на використанні унікальних фізіологічних або поведінкових характеристик особи, що робить процес аутентифікації більш надійним у порівнянні з традиційними методами, такими як паролі чи ключі. Однак надійність біометричних систем суттєво залежить від коректного застосування алгоритмів обробки біометричних даних, методів вилучення ознак, захисту даних та ефективності процедур порівняння. Цей розділ присвячений детальному аналізу алгоритмічних основ, методів обробки зображень та сучасних підходів до підвищення надійності біометричних систем.

3.1 Архітектура біометричного процесу

Біометричні системи аутентифікації та ідентифікації функціонують на основі послідовного виконання кількох ключових етапів, що забезпечують точність та надійність розпізнавання особистості. Основні етапи включають:

1. Захоплення біометричних даних (Data Acquisition): Використовується відповідне сенсорне обладнання (сканери відбитків пальців, камери для обличчя, мікрофони для голосу), яке забезпечує отримання цифрового зображення або аудіосигналу високої якості. Якість зображення безпосередньо впливає на точність наступних етапів.
2. Передобробка (Preprocessing): Спрямована на покращення якості отриманих даних — видалення шумів, корекція освітлення, нормалізація розміру та орієнтації. Це дозволяє уніфікувати вхідні дані для подальшого аналізу.

3. Виділення ознак (Feature Extraction): Визначення унікальних характеристик біометричного зразка, які відрізняють одну особу від іншої. Для відбитків пальців це мінуції — кінці та розгалуження папілярних ліній, для обличчя — геометричні параметри або ключові точки, для голосу — спектральні характеристики.
4. Формування шаблону (Template Creation): Перетворення вилучених ознак у компактне цифрове подання, що зберігається в базі даних або порівнюється з наявними записами.
5. Порівняння шаблонів (Matching): Визначення ступеня схожості між вхідним зразком і шаблоном з бази даних за допомогою відповідних алгоритмів.
6. Прийняття рішення (Decision Making): На основі результатів порівняння визначається результат аутентифікації або ідентифікації — прийняття або відмова у доступі.

Ця архітектура є базовою для більшості біометричних систем та визначає порядок взаємодії компонентів системи.

[Сенсор] → [Передобробка] → [Вилучення ознак] → [Формування шаблону] → [Порівняння] → [Рішення]

Схема 3.1 Архітектура біометричної системи

3.2 Алгоритми вилучення ознак

Виділення унікальних ознак біометричних зразків є критично важливим етапом, що значною мірою визначає точність розпізнавання. Найпоширенішими алгоритмами для обробки зображень відбитків пальців та інших біометричних ознак є:

- **Методи на основі мінуцій (minutiae-based methods) —** виявлення характерних точок, таких як кінці та розгалуження папілярних ліній, які формують унікальний малюнок відбитка (рисунок 3.2 ілюструє цей процес).

Рис. 3.2 Виявлення основних точок (мінуцій) відбитку

- **SIFT (Scale-Invariant Feature Transform) —** алгоритм, що забезпечує інваріантність до масштабу, повороту та освітлення, використовується для виділення ключових точок.
- **SURF (Speeded-Up Robust Features) —** оптимізована версія SIFT, що забезпечує швидшу обробку без значної втрати точності.
- **ORB (Oriented FAST and Rotated BRIEF) —** швидкий та ресурсозберігаючий алгоритм, який застосовується у мобільних пристроях.
- **Фільтри Габора (Gabor Filters) —** частотні фільтри, що імітують процеси обробки зорової кори, ефективно підсилюють структури папілярних ліній.

3.3 Методи порівняння шаблонів

Порівняння шаблонів — це процес визначення міри подібності між двома наборами ознак. Існують різні підходи:

- **Кореляційний аналіз (Cross-correlation):** Використовується для виявлення подібних ділянок у двох зображеннях шляхом обчислення ковзної кореляції.
- **Метричні відстані:** Евклідова, Манхеттенська та косинусна відстані дозволяють оцінити розбіжність між векторними поданнями шаблонів.

Евклідова відстань: $$d(A,B) = \sqrt{\sum_{i=1}^{n}(A_i - B_i)^2}$$

Манхеттенська відстань: $$d(A,B) = \sum_{i=1}^{n}|A_i - B_i|$$

Косинусна схожість: $$\cos(\theta) = \frac{A \cdot B}{\|A\|\|B\|}$$

- **Графові методи:** Побудова графів, де вершинами є мінуції, а ребрами — відстані чи кути між ними, що дозволяє порівнювати топологічну структуру шаблонів.
- **Імовірнісні методи:** Визначення ймовірності належності вхідного шаблону до певного класу.
- **Хешування шаблонів:** Перетворення біометричних даних у хеш-коди для швидкого пошуку та порівняння.

Для оцінки схожості часто використовують комбіновані підходи для підвищення точності.

3.4 Реєстрація відбитка пальця у базі даних і проходження автентифікації та ідентифікації

Автентифікація користувачів у інформаційній системі за допомогою відбитків пальців передбачає попередню реєстрацію унікальних відбитків кожного користувача в системі. Для ефективної ідентифікації необхідно створити унікальний профіль, який базується на відбитках пальців користувача.

Процес реєстрації відбитка пальця у базі даних інформаційної системи включає наступні послідовні кроки:

1. **Сканування відбитка пальця**
   Використовується спеціалізований сканер для отримання високоякісного цифрового зображення відбитка пальця.
2. **Передача зображення у систему**
   Отримане цифрове зображення передається від сканера до центральної оброблювальної системи через захищений канал зв’язку для подальшої обробки.
3. **Аналіз зображення та виділення характерних ознак**
   Система аналізує зображення для виявлення папілярних ліній, проводить їх тонке витончення та виділяє унікальні характеристики відбитка.

4. **Створення шаблону відбитка пальця**

   На основі виділених особливостей формується шаблон — компактне та унікальне представлення відбитка для збереження та подальшого порівняння.

5. **Перетворення шаблону у цифровий формат**

   Шаблон кодується у стандартизований цифровий формат, оптимізований для ефективного зберігання і швидкого пошуку в базі даних.

6. **Збереження шаблону у базі даних**

   Цифровий шаблон, разом з оригінальним зображенням відбитка та додатковими ідентифікаційними даними користувача, зберігається у базі даних інформаційної системи.

7. **Надання прав доступу користувачу**

   Після успішної реєстрації користувачу надаються відповідні права доступу до ресурсів та сервісів інформаційної системи.

Завершальним результатом даного процесу є створення унікального профілю користувача в базі даних системи, що забезпечує подальшу надійну ідентифікацію за відбитками пальців згідно з алгоритмом, представленим на рис. 3.2.

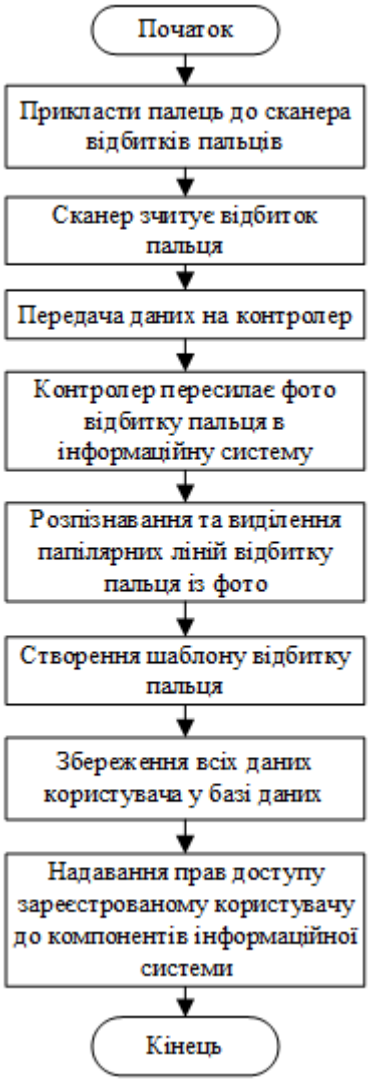


Рисунок 3.2 – Алгоритм реєстрації відбитків пальця у системі

Таким чином, система забезпечує точну та надійну аутентифікацію користувачів на основі їх відбитків пальців.

Процес аутентифікації користувача у інформаційній системі подано у вигляді алгоритму, що показаний на рис. 3.3.

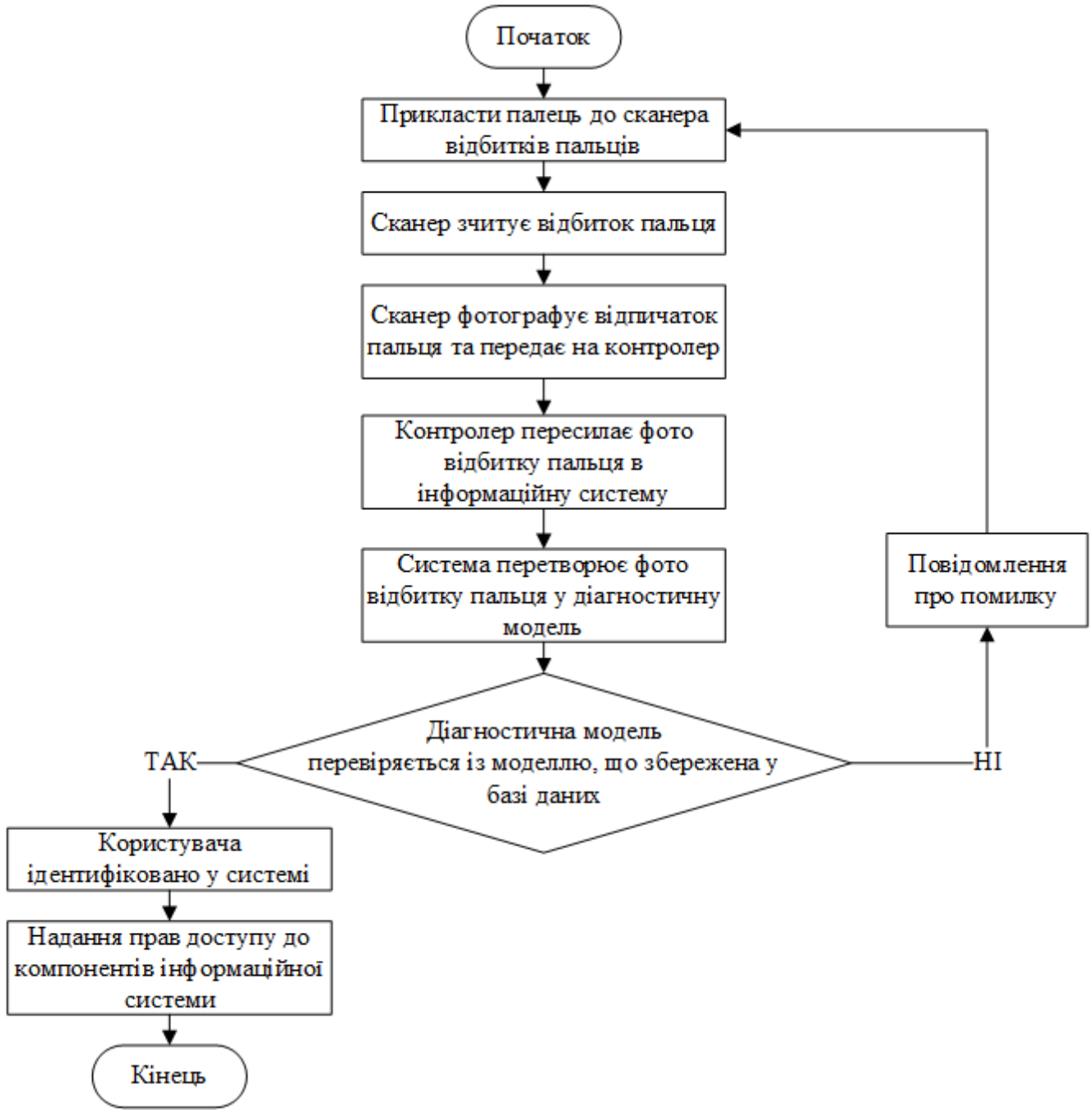


Рисунок 3.3 – Алгоритм аутентифікації користувача

Аутентифікація користувача в інформаційній системі з використанням відбитків пальців складається з послідовного виконання наступних ключових кроків:

1. **Застосування сканера відбитків пальців**

   Користувач прикладає палець до сканера, призначеного для зчитування відбитків.

2. **Зчитування відбитку пальця**
   Сканер фіксує відбиток та перетворює його у цифрове зображення високої якості.
3. **Передача зображення відбитка**
   Отримане цифрове зображення передається від сканера до контролера, який відповідає за подальшу обробку біометричних даних.
4. **Передача даних у інформаційну систему**
   Контролер відсилає зображення відбитка в основну інформаційну систему для проведення ідентифікації.
5. **Перетворення відбитка у діагностичну модель**
   Інформаційна система аналізує зображення та формує діагностичну модель, що відображає унікальні характеристики відбитка пальця.
6. **Порівняння моделі з базою даних**
   Отримана діагностична модель порівнюється з шаблонами відбитків, які збережені у базі даних системи, для пошуку збігів.
7. **Надання або відмова в доступі**

- Якщо модель відбитка співпадає з однією з моделей у базі даних, користувачу надається доступ до інформаційної системи відповідно до його прав доступу.
- Якщо ж збігів не знайдено, система повідомляє про відмову в доступі.

Ця послідовність дій забезпечує високу точність, надійність і безпеку процесу аутентифікації, що дозволяє ідентифікувати користувачів за їхніми біометричними ознаками з мінімальним ризиком помилок.

3.5 Алгоритм процесу обробки зображення

На рис. 3.4 представлено схему процесу зчитування даних із фотодатчика та їх подальшої обробки. Ключовим елементом цього процесу є регістр PixelData, що має адресу 0x48. Структура цього регістру включає два управляючі біти (SOF і DataValid) та шість біт, які відповідають за кодування яскравості пікселя (PixelNumb).

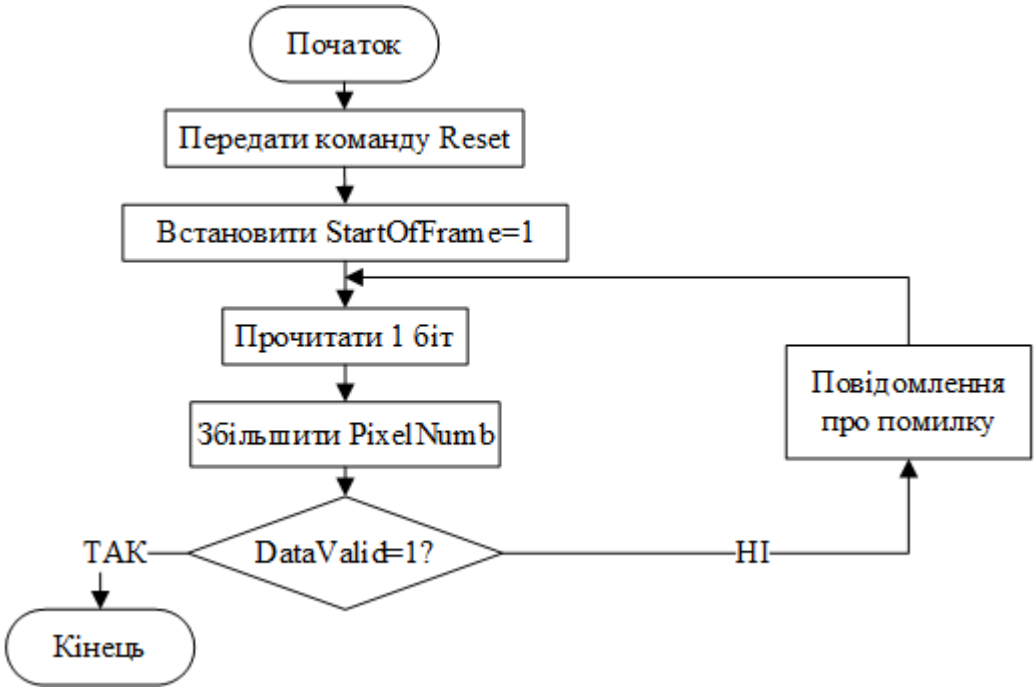


Рисунок 3.4 – Алгоритм зчитування та обробки зображення

Біт StartOfFrame (SOF) встановлюється в положення "1" відразу після ініціалізації пристрою, сигналізуючи про готовність до зчитування даних. Біт DataValid приймає значення "1" тільки після того, як буде зчитано останній біт даних зображення, вказуючи на те, що всі дані є валідними і можуть бути оброблені. Шість біт PixelNumb використовуються для кодування яскравості кожного пікселя в діапазоні від 0 до 63, де "0" відповідає мінімальній яскравості, а "63" — максимальній.

Алгоритм зчитування та обробки зображення (Рисунок 3.4) включає наступні кроки:

- ініціалізація SOF. Встановлення біта StartOfFrame у стан "1", що засвідчує початок передачі даних;
- зчитування першого пікселя. Визначення яскравості першого пікселя імедіатно після ініціалізації SOF;

- інкрементація лічильника пікселів. Збільшення лічильника пікселів на одиницю після кожного зчитування, для переходу до наступного пікселя;
- перевірка DataValid. Моніторинг стану біта DataValid після кожного зчитування. Якщо біт встановлено у "1", це означає, що всі пікселі були успішно зчитані, і процес можна завершувати. В іншому випадку, процес зчитування продовжується до наступного пікселя.

Ці кроки забезпечують ефективне зчитування та обробку зображень, що є критично важливим для забезпечення точності та надійності системи ідентифікації особи за відбитками пальців.

3.5 Алгоритм розпізнавання зображення

Обробка зображень на етапі перед вилученням ознак забезпечує усунення шумів і покращення якості. Основні методи:

- **Гаусове розмивання:** Фільтрація, що знижує випадкові шуми, згладжуючи зображення.
- **Вирівнювання гістограми (Histogram Equalization):** Покращення контрасту за рахунок перерозподілу інтенсивності пікселів.
- **Бінаризація (Otsu Thresholding):** Автоматичне перетворення зображення у двокольорове (чорно-біле) для виділення контурів.
- **Детектор країв Кані (Canny Edge Detector):** Виявлення країв із застосуванням багатокрокового процесу зниження шуму, визначення градієнтів і видалення незначущих контурів.
- **Морфологічні операції:** Ерозія та дилатація, що видаляють дрібні артефакти і покращують структуру зображення.

Ці методи забезпечують високу якість вхідних даних для алгоритмів вилучення ознак. Ідентифікація особистості за допомогою відбитків пальців виконується послідовно за такими ключовими кроками:

1. **Сканування відбитка пальця**

   Використовується спеціалізований сканер для отримання високоякісного цифрового зображення відбитка.
2. **Розпізнавання та виділення папілярних ліній**

   Аналіз зображення для виявлення основних характеристик – папілярних ліній, які є унікальними елементами відбитка.
3. **Виділення папілярних візерунків**

   Детальне визначення візерунків (петлі, дуги, спіралі), що додають індивідуальності відбитку.
4. **Завантаження бази даних шаблонів у оперативну пам’ять**

   Шаблони відбитків, які зберігаються у базі даних, підвантажуються для швидкого та ефективного порівняння.
5. **Порівняння з шаблонами**

   Новий відбиток пальця послідовно порівнюється з кожним шаблоном у базі даних доти, доки не буде знайдено збіг або не буде переглянутий увесь список.
6. **Ідентифікація або відмова в доступі**

   Якщо знайдено відповідний шаблон, система підтверджує ідентичність користувача та надає йому доступ. У разі відсутності збігів — доступ відмовляється.

На рис. 3.5 наведено візуальне відображення цього алгоритму, що ілюструє кожен крок — від сканування до остаточного зіставлення відбитків у базі даних.

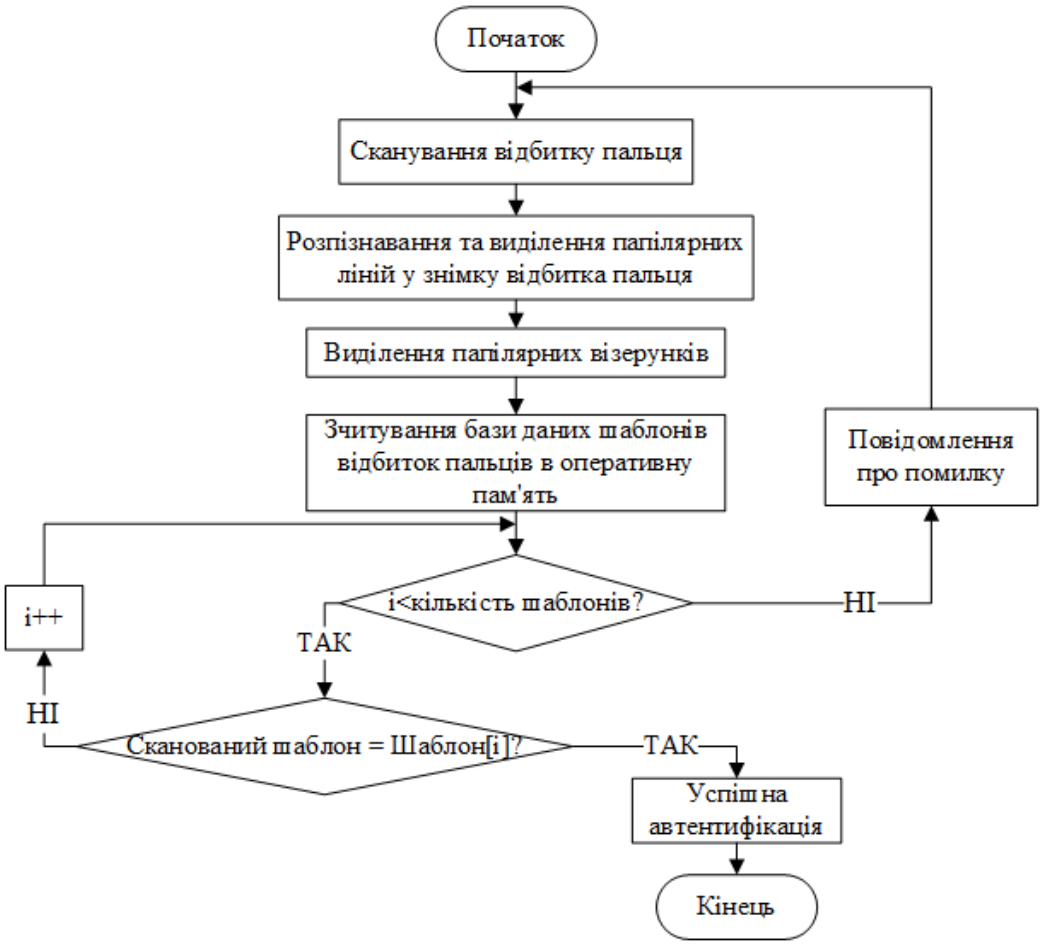


Рисунок 3.5 – Алгоритм розпізнавання зображення

Цей алгоритм визначає логічну послідовність дій, яка є важливою для забезпечення точності та надійності системи ідентифікації особи за відбитками пальців.

3.6 Методи підвищення достовірності

Для запобігання підробкам і покращення точності застосовуються спеціальні методики:

- **Liveness Detection:** Виявлення «живості» біометричного зразка за допомогою аналізу фізіологічних ознак — тепловий режим, кровообіг, рухи.
- **Спуфінг-протекція:** Захист від підробок за допомогою штучних відбитків, фотографій або відеозаписів, застосування складних сенсорів і алгоритмів.

- **Мультимодальні системи:** Використання двох або більше типів біометричних ознак (наприклад, обличчя і голосу) для підвищення надійності.
- **Постійна аутентифікація:** Безперервний контроль особи під час роботи з системою для запобігання несанкціонованому доступу.

3.7 Захист біометричних даних

Захист інформації є критично важливим аспектом:

- **Криптографічне шифрування:** Використання алгоритмів AES, RSA, ECC для захисту шаблонів при зберіганні і передачі.
- **Hash-based protection:** Застосування хеш-функцій із додаванням сольових значень для запобігання відтворенню шаблонів.
- **Cancelable Biometrics:** Модифікація шаблонів, яку можна замінити у випадку компрометації.
- **Захист каналів:** Впровадження протоколів TLS/SSL для захищеної передачі даних між пристроями та серверами.

Використання штучного інтелекту та машинного навчання

Застосування сучасних методів ШІ дозволяє значно покращити ефективність біометричних систем:

- **Convolutional Neural Networks (CNN):** Глибокі нейронні мережі, що автоматично вилучають характерні ознаки з біометричних зображень, особливо для обличчя та райдужки.
- **Підтримувані векторні машини (SVM):** Використовуються для класифікації шаблонів у дві чи більше категорій.
- **Випадкові ліси і дерева рішень:** Для комбінування ознак та прийняття рішень.

- **Autoencoders:** Застосовуються для зменшення розмірності та очищення вхідних даних.
- **Transfer Learning:** Використання заздалегідь навчених моделей для швидкої адаптації до нових даних.

Стандартизація та протоколи

Стандарти відіграють важливу роль у забезпеченні сумісності та безпеки біометричних систем:

- **ISO/IEC 19794-2:** Формат збереження шаблонів відбитків пальців.
- **ISO/IEC 30107-3:** Методики тестування захисту від підробок (Presentation Attack Detection).
- **ANSI/NIST ITL:** Стандарти обміну біометричними даними.
- **FIDO2/WebAuthn:** Протоколи безпарольної аутентифікації з використанням біометрії.

Оцінка якості та точності систем

Для оцінки ефективності застосовуються стандартні метрики:

- **FAR (False Acceptance Rate):** Частка випадків помилкового прийняття.
- **FRR (False Rejection Rate):** Частка помилкових відмов.
- **EER (Equal Error Rate):** Значення, при якому FAR = FRR.
- **ROC-крива:** Відображає співвідношення між FAR і FRR при різних порогах.
- **DET-крива:** Логарифмічне відображення помилок.

Оцінка точності є основою для порівняння та вибору алгоритмів.

3.8 Контролер й компоненти системи

Для створення ефективної системи автентифікації за допомогою відбитків пальців критично важливо підібрати належний контролер і ключові компоненти. Це вимагає аналізу ринкових аналогів для вибору найбільш підходящих рішень.

Контролер mbed NXP LPC1768 виробництва ARM є відмінним вибором для розробки прототипів завдяки своїм високим продуктивним характеристикам. Вбудований процесор NXP LPC1768 Cortex-M3, який працює на частоті 96 МГц та має 512 КБ ППЗУ флеш-пам'яті та 32 КБ SRAM, значно перевершує багато 8-бітних платформ. До того ж, mbed LPC1768 включає периферійні пристрої, які зазвичай відсутні у менш продуктивних платформах, зокрема Ethernet, USB OTG, 12-бітний АЦП, 10-бітний ЦАП та стандартні інтерфейси як UART, SPI, I2C, та CAN. Ці периферійні можливості разом із зручним 40-контактним DIP-форм-фактором із стандартними піновими роз’ємами забезпечують легкість інтеграції з макетними та монтажними платами.

Особливу цінність mbed додає його бібліотека, яка пропонує API-орієнтований підхід до програмування, мінімізуючи необхідність розробки на низькому рівні. Це дозволяє розробникам швидко створювати код з високим рівнем абстракції, що сприяє якості та надійності розробки. Крім того, унікальна онлайн-платформа для C++ компіляції та IDE, що працює безпосередньо у браузері без необхідності завантаження додаткового програмного забезпечення, забезпечує доступність і зручність використання.

На рис. 3.10 представлено контролер mbed NXP LPC1768 від ARM, який демонструє його важливість для розробки сучасних систем автентифікації.

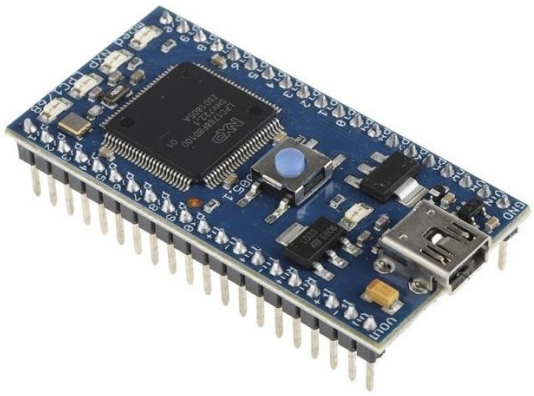


Рисунок 3.10 – Зовнішній вигляд контролера mbed NXP LPC1768 від ARM

Специфікація:

– мікроконтролер: LPC1768;

– тактова частота: 96 МГц;

– завантажувач: mbed;

– пам'ять: ППЗП (Flash Memory): 512 КБ та ОЗП (SRAM): 32 КБ;

– канали введення/виводу: 40 (включаючи 6 ШІМ та 6 аналогових вхідних каналів);

– вбудовані світлодіоди для зворотного зв'язку;

– послідовний порт через USB для налагодження;

– живлення від USB або зовнішнього джерела (4.5 - 9 В, з загальною безпечною напругою до 12 В);

– форм-фактор: 40-контактний DIP з кроком 2.54 мм;

– розміри: 54 х 26 х 14 мм;

– вага: 12 гр.

Цей мікроконтролер є ідеальним для створення прототипів високопродуктивних проектів завдяки своїм широким можливостям та легкості інтеграції з різними розробницькими інструментами.

Teensy 3.2, оснащений 32-бітним ARM-процесором Cypress MK20DX256 з ядром Cortex-M4 та тактовою частотою 72 МГц, забезпечує значні ресурси для розробки складних програм (рис. 3.11). Завдяки 64 кБ оперативної пам'яті та 256 кБ

енергонезалежної Flash-пам'яті, цей контролер ідеально підходить для таких завдань, як обробка звуку, керування роботами та розпізнавання образів.

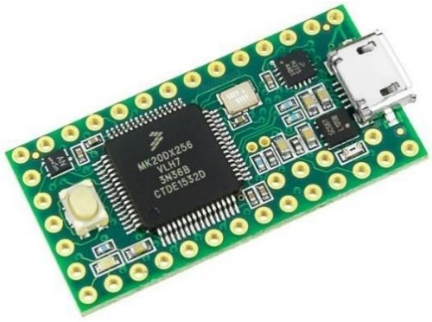


Рисунок 3.11 – Зовнішній вигляд контролера Teensy 3.2

Процесор оснащений розширеним DMA-контролером, що дозволяє здійснювати передачу даних безпосередньо між периферією і пам'яттю, мінімізуючи навантаження на процесор. Наприклад, можливе одночасне отримання зображення через SPI та його виведення на дисплей, звільняючи процесор для інших завдань.

Teensy 3.2 також оптимізовано для енергоефективної роботи, зокрема у режимі сну, де споживання становить менше 0,25 мА, що дозволяє працювати від одного літієвого акумулятора на 3,3 В протягом кількох місяців без підзарядки.

Основні характеристики Teensy 3.2:

- процесор: Cypress MK20DX256;
- ядро: ARM Cortex-M4, 72 МГц;
- пам'ять: 64 кБ оперативної, 256 кБ Flash, 2 кБ EEPROM;
- введення-виведення: 34 лінії (всі 5V-толерантні);
- аналогові та цифрові канали: 21 АЦП, 12 ШІМ;
- комунікаційні інтерфейси: 3 UART, 2 I²C, 1 SPI, 1 CAN;
- живлення: 3.3-5.5 В, з можливістю видачі 250 мА на 3.3V пін;
- розміри: 17×35 мм.

Arduino Leonardo, заснована на мікроконтролері ATmega32u4, є просунутою версією попередників Arduino UNO (рис. 3.12). На платі використовується ATmega32u4 з тактовою частотою 16 МГц та 32 кб пам'яті. Ця модель також оснащена 20 портами вводу/виводу, що дозволяє підключати зовнішні датчики та інші пристрої.

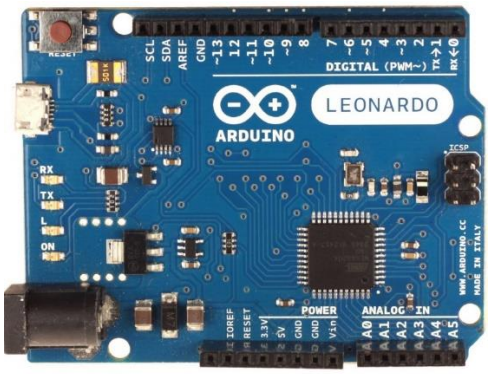


Рисунок 3.12 – Зовнішній вигляд контролера Arduino Leonardo

Arduino Leonardo можна живити через USB або зовнішнє джерело живлення. При використанні зовнішнього живлення важливо врахувати споживання підключених модулів, оскільки плата може працювати від напруги від 6 до 20 В на контакт Vin.

Основні характеристики Arduino Leonardo [19]:

– мікроконтролер: ATmega32u4;

– тактова частота: 16 МГц;

– флеш-пам'ять: 32 Кб (512 байт з яких використовуються для завантажувача);

– ОЗУ (RAM): 2 Кб;

– EEPROM: 1 Кб;

– цифрові входи/виходи: 20 шт., з яких 6 можуть використовуватися як виходи ШІМ і 6 як аналогові входи;

– робоча напруга: 4.5-5.5 В;

- максимальний струм на пін: 40 мА;
- струм на виведенні при живленні від 3.3 В: 50 мА;
- робоча напруга на Vin: 7-15 В;
- максимальна вхідна напруга: 6-20 В.

Цей контролер ідеально підходить для проектів, що потребують різноманітного підключення і гнучких параметрів живлення, забезпечуючи високу продуктивність та адаптивність для широкого спектру застосувань.

В процесі підготовки до вибору оптимального мікроконтролера для реалізації проекту було важливо провести детальний аналіз і порівняння основних характеристик кожного з розглядуваних контролерів. Для цього, у таблиці 3.3, було зібрано і систематизовано всі ключові параметри, що дозволяють оцінити потенціал кожного пристрою для конкретних потреб проекту.

Табл. 3.3 слугує інструментом для об'єктивного порівняння мікроконтролерів, включаючи такі параметри, як тактова частота, обсяг оперативної та постійної пам'яті, кількість входів/виходів, наявність периферійних інтерфейсів, а також рівень енергоспоживання. Це дозволяє не тільки оцінити загальну продуктивність кожного мікроконтролера, але й визначити його спроможність впоратись зі специфічними вимогами проекту.

Таблиця 3.3 – Порівняння мікроконтролерів для розробки пристрою

Характеристика	LPC1768	Teensy 3.2	Arduino Leonardo
ППЗП (Flash Memory)	512 КБ	256 КБ	32 КБ
Ядра	1	1	1
Частота ядра	96 МГц	72 МГц	16 МГц
Ціна	$145,15	$29.97	$8
ОЗП	32 КБ	64 КБ	2 КБ
Wi-Fi	–	–	–

Ці дані вказують на значні відмінності у продуктивності та вартості між моделями. LPC1768 вирізняється високою продуктивністю з великою кількістю пам'яті та швидкістю процесора, але має вищу ціну. Teensy 3.2 пропонує баланс між ціною і продуктивністю, забезпечуючи помірну ціну при добрих показниках пам'яті та частоти. Arduino Leonardo є найбільш доступним варіантом, має значно нижчі характеристики за інших та для використання у системі його характеристик достатньо.

Для сканування відбитків пальців один з кращих варіантів є оптичний сканер FPM10A, який є бюджетним рішенням і базується на мікроконтролері ARM Cortex M 32-bit від Synochip (AS608, FPM10A) (рис. 3.13).

Рисунок 3.13 – Сканер відбитків пальців FPM10A

Цей сканер підтримує функції шифрування даних та зберігає базу відбитків прямо у вбудованій пам'яті, дозволяючи проводити швидке порівняння відбитків за заздалегідь збереженими шаблонами.

Сканер FPM10A можна інтегрувати з різними мікроконтролерами, налаштування проводиться через спеціалізовані утиліти від виробника або через скетчі для Arduino. Відрізняється низьким енергоспоживанням, а час обробки зображення відбитка становить менше 1 секунди, що забезпечує високу швидкість роботи.

Основні характеристики сканера FPM10A:

- напруга живлення: 3.6 - 6.0 В;
- струм споживання: 120 мА (140 мА макс.);
- час обробки зображення: менше 1 секунди;
- сенсор: оптичний;
- розмір сенсора: 14 мм х 18 мм;
- розмір сигнатури: 256 байт;
- розмір шаблону: 512 байт;
- ємність пам'яті: до 300 записів;
- рівні безпеки: 1-5;
- інтерфейс: UART TTL;
- швидкість передачі: налаштовується 9600, 19200, 28800, 38400, 57600 (за замовчуванням 57600);
- робоча температура: від -20°C до +50°C;
- допустимий рівень вологості: 40% - 85% RH;
- габаритні розміри: 45 х 26 х 19 мм;
- вага: 15 г.

Цей сканер є відмінним вибором для проектів, де потрібне надійне і швидке сканування відбитків пальців за доступною ціною.

3.9 Висновки до розділу 3

Розглянуті теоретичні основи, алгоритми та методи створюють комплексне підґрунтя для розробки надійних біометричних систем. Синтез сучасних методів обробки зображень, алгоритмів вилучення ознак, машинного навчання та стандартів безпеки формує високий рівень захисту та точності. Подальший розвиток біометричних технологій пов’язаний із впровадженням гібридних систем та новітніх криптографічних методів, що забезпечать безпечну і зручну аутентифікацію у майбутньому.

Також було розглянуто архітектуру системи, яка включає трьохрівневий підхід, забезпечуючи чітке розділення логіки, представлення і доступу до даних, що дозволяє підвищити масштабованість та зручність обслуговування системи. Значну увагу приділено інтеграції та налаштуванню компонентів системи, включаючи вибір Arduino Leonardo як основного контролера через його вартісну ефективність та легкість використання. Вибір Wi-Fi як протоколу передачі даних підкреслює акцент на високій швидкості та надійності комунікацій в рамках системи.

ВИСНОВКИ

Даний дипломний проєкт присвячений розробці та аналізу біометричних систем аутентифікації та ідентифікації з метою підвищення безпеки методів контролю доступу. В ході дослідження були вивчені основні компоненти біометричних систем, потенційні загрози, які впливають на їх роботу, а також запропоновані ефективні способи їх мінімізації.

У першому розділі здійснено детальний огляд технологій і методів, що застосовуються в біометричних системах, включаючи різноманітні способи аутентифікації та ідентифікації. Окрему увагу приділено аналізу можливих загроз та розробці стратегій захисту з використанням біометричних характеристик, таких як відбитки пальців.

Другий розділ містить поглиблений аналіз сучасних процесів аутентифікації за відбитками пальців, з особливим акцентом на методах виявлення "живих" відбитків і захисту від підробок. Розглянуто питання стандартизації процедур роботи з біометричними шаблонами, а також описано стандарти й методики, що підвищують надійність біометричної автентифікації.

У третьому розділі було здійснено комплексний теоретичний аналіз алгоритмічного забезпечення біометричних систем ідентифікації та автентифікації. Розглянуто повний життєвий цикл обробки біометричних даних — від моменту зчитування фізіологічних ознак користувача до прийняття рішення на основі зіставлення шаблонів. Особливу увагу приділено питанням ефективності, безпеки, достовірності та стійкості систем до зовнішніх загроз і спроб шахрайства.

Було детально проаналізовано етапи передобробки сигналу та виділення ознак для різних типів біометричних характеристик, таких як відбитки пальців, обличчя, райдужна оболонка, голос, динаміка підпису тощо. Розглянуто методи покращення якості зображень, алгоритми вилучення унікальних ознак та порівняння шаблонів із застосуванням різноманітних метрик подібності.

Значну увагу приділено сучасним засобам захисту біометричних шаблонів, включаючи технології шифрування, диференційного захисту, біометричного

хешування, а також інноваційні підходи на основі гомоморфного шифрування та багатоагентних обчислень. Окремим напрямом дослідження є технології розпізнавання "живих" біометричних ознак (Liveness Detection), що суттєво знижують ризики фальсифікації.

Четвертий розділ присвячений організаційно-технічним заходам, спрямованим на забезпечення безпеки робочих місць та покращення умов праці в контексті застосування біометричних систем. Особлива увага приділялась охороні праці, електро- та пожежній безпеці, а також створенню сприятливих мікрокліматичних умов і відповідного рівня освітлення.

Проведена робота демонструє комплексний підхід до розробки та аналізу біометричних систем, що забезпечує не лише технічну надійність, але й відповідність вимогам безпеки і комфорту користувачів.

Розроблені рішення можуть бути ефективно застосовані у широкому спектрі сфер, де потрібна надійна аутентифікація та ідентифікація, зокрема:

- банківська сфера та фінансові установи — для забезпечення безпеки транзакцій і контролю доступу до рахунків;
- державні установи — у паспортних сервісах, реєстрації виборців та інших органах, де важливо перевіряти особистість;
- системи фізичного контролю доступу — в офісах, промислових об’єктах і зонах обмеженого доступу;
- охоронні системи — для підвищення рівня безпеки об’єктів;
- медичні установи — для захисту конфіденційності пацієнтських даних і контролю доступу до медичної інформації;
- IT-інфраструктура — для охорони критично важливих даних і ресурсів від несанкціонованого доступу;
- освітні заклади — для контролю доступу студентів і викладачів до навчальних ресурсів та приміщень.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Різник О. «Біокон» – система біометричної ідентифікації користувача комп'ютерної мережі / О. Різник, Д. Дзюба, А. Чернодуб // Системи підтримки прийняття рішень. Теорія і практика: зб. доп. наук.-прак. конф. з міжнар. участю. «СППР 2009». – Київ, 2009. – 516 с.

2. Чередниченко В. Б. Біометричні методи у системах захисту інформації [Текст] / В.Б. Чередниченко, К.Е. Чередниченко // Системи обробки інформації. – 2012. 354 с.

3. Грищук Р.В. Основи кібернетичної безпеки / Р.В. Грищук, Ю.Г. Даник – Житомир: ЖНАЕУ, 2016 – 616 с.

4. Мороз А.О. Біометричні технології ідентифікації людини. Огляд систем. [Текст] / А.О. Мороз // Математичні машини і системи. – 2011. – 498 с.

5. Юдін О.К., Корченко О.Г., Конахович Г.Ф. Захист інформації в мережах передачі даних. Київ : Вид-во DIRECTLINE, 2019. – 714 с.

6. О. Корченко, А. Давиденко, О. Висоцька, «Метод автентифікації користувачів інформаційних систем за їх рукописним почерком з багатокроковою корекцією первинних даних», Захист інформації, 2019. – 319 с.

7. Precision Verification: Effect of Experiment Design on False Acceptance and False Rejection Rates. - Режим доступу: https://academic.oup.com/ajcp/article/156/6/1058/6296072?login=false (дата звернення 24.04.2024).

8. Low false reject rate and false accept rate multi-step fire detection method. - Режим доступу: https://www.sciencedirect.com/science/article/abs/pii/S0030402613007389 (дата звернення 24.04.2024)..

9. Шведова О. В. Дактилоскопічні дослідження : Навч. посіб. для студ. ВНЗ – К. : КНТ, 2010. – 208 с.

10. What's the Difference Between Match-on-Host and Match-in-Sensor Fingerprint Authentication? - Режим доступу: https://www.electronicdesign.com/technologies/embedded/article/ 21801072/whats-the-difference-between-match-on-host-and-match-in-sensor-fingerprint-authentication (дата звернення 24.04.2024)..

11. Мартинова, Л.Є. Дослідження та порівняльний аналіз методів аутентифікації [Текст]/ Л. Є. Мартинова, М.Ю. Умніцин, К.Є. Назарова // Молодий вчений. - 2016. - 518 с.

12. Сокольський І.О. Дослідження та розробка засобів демонстрації аутентифікації за відбитками пальців / І.О. Сокольський // Всеукраїнська конференція студентів та молодих вчених. – 2020. – 329 с.

13. Пелешко Д.Д., Теслюк В.М. Об'єктні технології С++: навчальний посібник/ МОН України, Національний університет "Львівська політехніка". – Львів, 2013. – 360 с.

14. Придатко О. В., Бурак Н. Є., Хлевной О. В. Основи програмування (мовою Java) : курс лекцій. – Львів : ЛДУ БЖД, 2019. – 180 с.

15. Ріхтер Д. CLR via C#. – К.: Видавнича група "Буква", 2018. – 896 с.

16. Трирівнева архітектура. URL: https://javarush.com/ua/quests/lectures/ua.questservlets.level14.lecture01 (дата звернення 23.04.2024).

17. Feedback control system based on a remote operated PID controller implemented using mbed NXP LPC1768 development board. URL: https://iopscience.iop.org/article/10.1088/1742-6596/659/1/012028/meta (дата звернення 24.04.2024).

18. Teensy® 3.2 Development Board. URL: https://www.pjrc.com/store/teensy32.html (дата звернення 24.04.2024).

19. Development of a Low-Cost Air Quality Data Acquisition IoT-based System using Arduino Leonar. URL: https://www.mecs-press.net/ijem/ijem-v9-n3/IJEM-V9-N3-1.pdf (дата звернення 24.04.2024).

20. Alat Pendeteksi Data Vaksinasi Sensor FPM10A dan NODEMCU ESP8266 Menggunakan Metode Sequential Searching. URL: http://journal.lembagakita.org/index.php/jtik/article/view/528 (дата звернення 24.04.2024).

21. Третьяков О. В. Охорона праці: навч. посіб. з тестовим комплексом на CD / О. В. Третьяков, В. В. Зацарний, В. Л. Безсонний – Київ : Знання, 2010. – 167 с. + компакт-диск.

22. Основи охорони праці: підручник / К. Н. Ткачук, М. О. Халімовський, В. В. Зацарний та ін. – Київ : Основа, 2011. – 474 с.

23. Управління охороною праці: навч. посіб. / К. Н. Ткачук, Я. О. Мольчак, С. Ф. Каштанов та ін. – Луцьк : 2012. – 287 с.

24. Психологія праці та її безпеки: навч. посіб. / К. Н. Ткачук, Г. С. Калда, С. Ф. Каштанов та ін. – Хмельницький : 2011. – 135 с.

25. Ткачук К.Н., Халімовський М.О. Основи охорони праці: Підручник. – К.: Основа, 2003 – 403 с.