МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 20__ р.

На правах рукопису
УДК 004.056.5:510.22(043.3)

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: **Система біометричного захисту об'єкту інформаційної діяльності**

Виконавець: В. В. Білак
Керівник: к.т.н., доцент С. В. Єгоров
Нормоконтролер: к.т.н., доцент С. В. Єгоров

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп’ютерної та програмної інженерії

Кафедра: Комп’ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«__» _____ 20__ р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Білак Вікторії Володимирівни

1. Тема: *Система біометричного захисту об'єкту інформаційної діяльності* затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.
2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.
3. Вихідні дані: проаналізувати існуючі методи та методики біометричного захисту; проаналізувати переваги та недоліки розглянутих методів; сформувати критерії та показники для біометричного аналізу вхідних даних; на основі вибраного типу та методу біометричного захисту розробити прототип системи для біометричного захисту об'єкту інформаційної діяльності.
4. Зміст пояснювальної записки: аналіз предметної області; застосування методів і засобів для біометричної ідентифікації та автентифікації; створення прототипу системи для біометричного захисту об’єкту інформаційної діяльності.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	19.04.2021	*Виконано*
2.	Аналіз літературних джерел	20.04.2021	*Виконано*
3.	Обґрунтування вибору рішення	25.04.2021	*Виконано*
4.	Збір інформації	01.05.2021	*Виконано*
5.	Дослідження методів і засобів для біометричної ідентифікації та автентифікації	03.05.2021	*Виконано*
6.	Розробка вимог та структури системи для біометричного захисту об'єкту інформаційної діяльності	07.05.2021	*Виконано*
7.	Розробка прототипу системи для біометричного захисту об’єкту інформаційної діяльності	13.05.2021	*Виконано*
8.	Апробація роботи на XVII Міжнародна науково-технічна конференція «Проблеми інформатизації – 2021»	19.05.2021	*Виконано*
9.	Оформлення і друк пояснювальної записки	20.05.2021	*Виконано*
10.	Оформлення презентації	23.05.2021	*Виконано*
11.	Перевірка на антиплагіат	03.06.2021	*Виконано*
12.	Отримання рецензій від рецензента	08.06.2021	*Виконано*

Здобувач вищої освіти В. Білак

(підпис, дата)

Керівник дипломної роботи С. Єгоров

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, складає 66 сторінок і має 29 рисунків, 9 таблиць та 1 додаток.

Метою роботи є підвищення рівня захищеності об'єкту інформаційної діяльності за рахунок впровадження біометричної ідентифікації та автентифікації.

В роботі встановлено вимоги та розроблена архітектура, а також прототип системи для захисту об'єкту інформаційної діяльності з використанням відповідного методу біометричної автентифікації.

Розроблений метод та програмне забезпечення відносяться до галузі інформаційної безпеки і можуть бути використані для підвищення рівня захищеності.

Можливі напрямки розвитку цієї роботи пов’язані із розширенням моделі і удосконалення алгоритму програмного забезпечення відповідно до вимог міжнародних стандартів, наприклад ISO 27001, для більш повного аналізу та оцінки ризиків.

Ключові слова: біометричний захист, показники, моделі, методи, біометрична автентифікація, програмне забезпечення.

ЗМІСТ

ПЕРЕЛІК ПРИЙНЯТИХ СКОРОЧЕНЬ

ЕЦП – електронний цифровий підпис

ОС – операційна система

ІКС – інформаційно-комунікаційна система

БД – база даних

ПЗ – програмне забезпечення

ВСТУП

Актуальність теми. За довгі роки розвитку сформувалися і отримали в даний час широке поширення інформаційні системи біометричної ідентифікації особи, які здійснюють контроль фізичного доступу і доступу до конфіденційної інформації. Як біометричного ідентифікатора використовують людський голос, почерк, райдужну оболонку очей, відбитки пальців.

Завдання біометричної верифікації та ідентифікації особистості, а також завдання безпечної біометричної аутентифікації, є ключовими для багатьох важливих додатків та систем захисту. Це пов'язано з дедалі більшим поширенням біометричних даних в інформаційних системах і процесах, розвитком інфраструктури інтернету і хмарних технологій, орієнтацією на кінцевого користувача інтернет-сервісів і Web-додатків.

Окрім класичних задач верифікації та ідентифікації, досить затребуваними стають нові завдання захищеної передачі біометричних даних, захисту біометричних даних від підробок, розробки систем захищеної біометричної аутентифікації користувачів, створення біометричних систем шифрування і біометричної цифрового підпису в зв'язку з необхідністю захисту персональних даних в різного роду інформаційних системах.

Об’єкт дослідження – процес ідентифікації та автентифікації користувача у системі захисту інформації.

Предмет дослідження – методи та моделі ідентифікації та аутентифікації користувачів в захищених інформаційно-комунікаційних системах.

Мета роботи – підвищення рівня захищеності об'єкту інформаційної діяльності за рахунок впровадження біометричної ідентифікації та автентифікації.

Завдання бакалаврської роботи:

- Аналіз існуючих методів та методик біометричного захисту, їх переваги та недоліки
- Дослідження методів і засобів для біометричної ідентифікації та

автентифікації

- Розробка вимог та структури системи для біометричного захисту об'єкту інформаційної діяльності
- Розробка прототипу системи для біометричного захисту об’єкту інформаційної діяльності

Методи дослідження – аналіз експлуатаційної документації, звітів світових конференцій та засад з інформаційної безпеки, теорія біометричної ідентифікації та аутентифікації та проведення досліджень з використанням спеціалізованого ПЗ.

Практична цінність. Розроблений метод та програмне забезпечення відносяться до галузі інформаційної безпеки і можуть бути використані для підвищення рівня захищеності. Можливі напрямки розвитку цієї роботи пов’язані із розширенням моделі і удосконалення алгоритму програмного забезпечення відповідно до вимог міжнародних стандартів, наприклад ISO 27001, для більш повного аналізу та оцінки ризиків.

Галузь використання – інформаційна безпека.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Міжнародні стандарти по криптографічним протоколам ідентифікації/автентифікації

Основним міжнародним стандартом для протоколів криптографічної автентифікації є Міжнародна організація зі стандартизації та Міжнародна електротехнічна комісія ISO / IEC 9798 - Інформаційні технології - Методи безпеки - Механізми автентифікації суб'єктів господарювання, що складаються з п'яти частин:

ISO / IEC 9798-1 - "Загальна модель";

ISO / EEC 9798-2 - "Механізми, що використовують симетричні алгоритми шифрування";

ISO / EEC 9798-3 - "Аутентифікація суб’єкта з використанням алгоритму відкритих ключів";

ISO / IEC 9798-4 - "Механізми, що використовують функцію криптографічного контролю";

ISO / IEC 9798-5 - Механізми, що використовують технологію нульових знань.

У цих протоколах заявник і верифікатор мають симетричний секретний ключ або парний вибірковий ключ зв'язку. Для їх отримання в режимі реального часу можна використовувати надійний сервер.

ISO / IEC 9798-2 визначає три методи автентифікації:

1. Одностороння автентифікація на основі позначки часу (рис. 1.1). Якщо заявник та рецензент мають системний годинник, подавати заявку не потрібно. Заявник може негайно надіслати повідомлення із позначкою часу, а інспектор може перевірити позначку часу, прочитавши годинник.

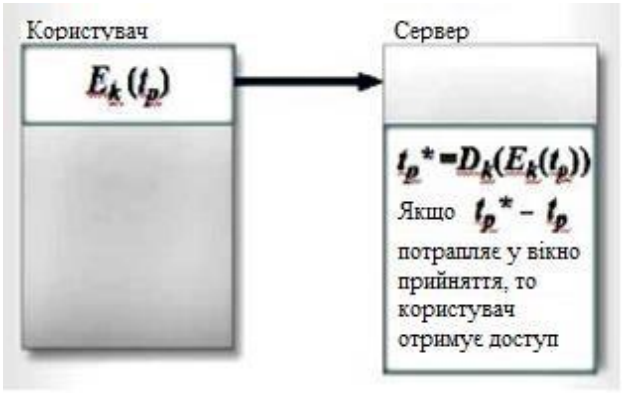

Рис. 1.1. Одностороння аутентифікація, заснована на мітці часу

1. Одностороння автентифікація за випадковими числами (рис. 1.2). За запитом сертифікат надсилає випадкове число, сформоване генератором псевдовипадкових чисел. Отримавши запит, заявник обчислює відповідь на нього - шифрує отримане випадкове число та (за необхідності) ідентифікатор, використовуючи алгоритм симетричного шифрування. Сертифікат розшифровує отриманий зашифрований текст і перевіряє структуру запиту. Якщо вона правильна, ви приймете заявника.

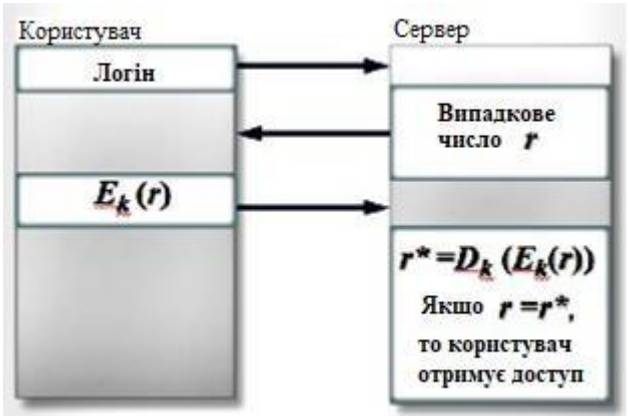

Рис. 1.2. Одностороння аутентифікація з використанням випадкових чисел

3. Взаємна автентифікація за випадковими числами (рис. 1.3). Різниця між цим протоколом та попереднім полягає в тому, що тут учасники по черзі виконують ролі рецензента та заявника, доводячи автентичність один одного.

Протокол взаємної автентифікації - це, по суті, два односторонні протоколи автентифікації, «загорнуті» у три повідомлення. Через їх симетрію такі протоколи

називаються протоколами рукостискання. Цей протокол дозволяє запускати шифр за допомогою хеш-функції за допомогою ключа, як зазначено у ISO / IEC 9798-4. Для підвищення надійності протоколу до переданого повідомлення можна додати мітки часу.

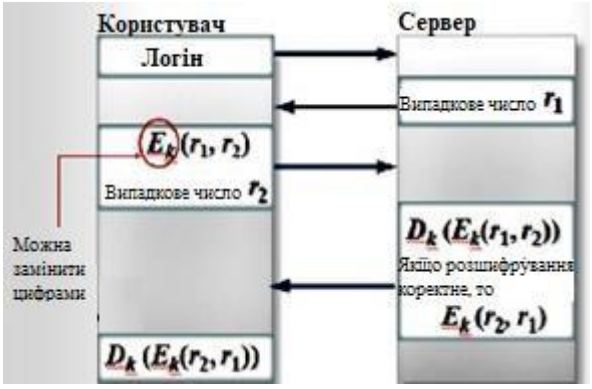

Рис. 1.3. Взаємна аутентифікація з використанням випадкових чисел

4. Протоколи «запит - відповідь» з використанням асиметричних криптосхем. Такі протоколи можна розділити на дві групи: протоколи з використанням ЕЦП і протоколи з використанням схем відкритого шифрування. В стандарті ISO / IEC9798-3 рекомендовані:

1) Протоколи з використанням схем-цифрового підпису (рис.1.4):

Рис. 1.4. Протоколи з використанням схем-цифрового підпису

Опис протоколів включає нотації certA сертифікатів відкритого ключа для цифрового підпису відповідних учасників протоколу, тобто структури даних, що

містять їх ідентифікатори, відкриті ключі та іншу службову інформацію, яку використовує орган сертифікації. Метод автентифікації відкритих ключів буде розглянуто більш детально далі. Протоколи, подібні до описаних вище, також використовуються стандартом МСЕ X.509 Міжнародного союзу електрозв'язку. Описує протоколи автентифікації та протоколи обміну ключами.

2) Протоколи, що використовують відкриті схеми шифрування (рис. 1.5).

Загрози безпеки ICS можна розділити на мережеві атаки (інформація з віддаленого клієнта) та локальні атаки, які надходять від шкідливих програм, вже встановлених у клієнтській системі, таких як троянські програми, руткіти тощо. Часто оцінювання безпеки автентифікації зосереджуються переважно на мережевих атаках, припускаючи, що термінал користувача (тобто портативний комп'ютер, ноутбук або мобільний пристрій) є захищеною платформою. Однак нерідкі випадки, коли зловмисники отримують повний доступ до комп’ютера жертви за допомогою прихованих комунікаційних процесів, які залишаються поза шкідливими програмами, які використовують вразливості неліцензійного програмного забезпечення.

Рис. 1.5. Протоколи з використанням схем відкритого шифрування

Типові методи атаки на протоколи автентифікації включають:

1. Аутсорсинг (видавання себе за іншу особу) - одна схожа на іншу.

2. Повторне відтворення (атака відтворення) - повторна передача

попередніх облікових даних будь-якими користувачами.

3. Зміну сторони біржі аутентифікації (Interleaving attack) - зловмисник може змінити трафік, що проходить через атаку.

4. Рефлексивну атаку - одна з можливостей фейкової атаки, коли зловмисник повертає захоплену інформацію в рамках цього сенсу.

5. Примусову затримку - зловмисник фіксує певну інформацію та пересилає її через деякий час.

6. Атакування виділенням тексту (виділена текстова атака) - зловмисник перехоплює трафік і намагається отримати інформацію з клавіш.

1.2 Біометрична ідентифікація/автентифікація користувачів

На сьогодні є кілька технологій ідентифікації та автентифікації користувачів в інформаційно-комунікаційних системах (рис.1.6).

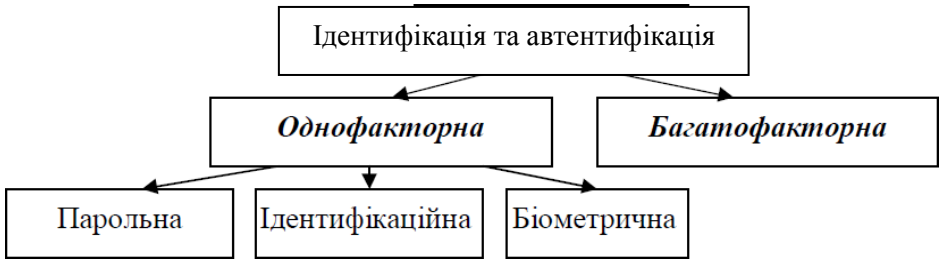

Рис.1.6. Система технологій ідентифікації та автентифікації

Кожна має свої переваги та недоліки, завдяки чому одні технології придатні для використання в одних комп’ютерних системах, а інші - для інших. Однак у багатьох випадках чітко визначеного рішення не існує. Тому як розробники програмного забезпечення, так і користувачі повинні самі вирішити, який метод автентифікації використовувати у власній ІКС.

Біометрія - це ідентифікація людини на основі єдиних біологічних характеристик, які властиві лише їй. Тобто, можна сказати, що спочатку були розроблені біометричні технології для точного встановлення особистості людини. Тому рішення щодо використання в галузі інформаційної безпеки видається цілком логічним. Більше того, цей напрямок розвивається дуже активно. Сьогодні

використовується більше десятка різних біометричних характеристик. Більше того, для найпоширеніших з них (відбитки пальців та райдужної оболонки ока) існує безліч сканерів, які відрізняються за своєю роботою.

Отже, для користувачів, які вирішили використовувати біометричну ідентифікацію, існує безліч варіантів вибору. Біометрична ідентифікація / автентифікація - це один із способів ідентифікації особи на основі певних біометричних характеристик, властивих цій людині. Сучасний рівень техніки в галузі комп'ютерних технологій дозволив використовувати такі сигнали для встановлення можливості ідентифікації людини та доступу до ресурсів комп'ютерних систем.

Серед механізмів біометричної ідентифікації можна виділити такі:

1) за статичними характеристиками - те, що практично не змінюється від народження (фізіологічні характеристики);

2) за динамічними сигналами - поведінковими характеристиками, тобто тими, що базуються на характеристиках підсвідомих рухів у процесі відтворюючої дії.

Динамічні сигнали можуть змінюватися з часом, але не раптово, а поступово.

Статичні методи ідентифікації користувачів комп'ютерних систем включають:

1. Ідентифікація за відбитками пальців (рисунок 1.7). Цей метод заснований на унікальності папілярного малюнка пальців. Ідентифікація будується наступним чином: зображення відбитка пальця отримується за допомогою сканера, а потім це зображення перетворюється у спеціальний цифровий код за допомогою складного алгоритму. Потім цей код порівнюється з контрольними кодами, що зберігаються в базі даних.

Рис.1.7. Пальцевий та долонний дактилоскопічні сканери

1. Ідентифікація на основі розташування вен на долоні. Пристроєм зчитування інформації в цьому випадку є інфрачервона камера. Як результат, малюнок вен на людській руці з’являється на вході програми, коли генерується цифровий код. Для сканування не потрібен контакт людини з пристроєм. Він має високі показники достовірності та надійності.

2. Ідентифікація за сітківкою ока (рисунок 1.8). У цьому випадку досліджується картина судин очного дна, фіксована структура яких з часом не змінюється. Очевидно, що цю закономірність можна спостерігати лише за певних умов: під час сканування людина дивиться на віддалене джерело світла, а спеціальна камера сканує очне дно, що в свою чергу може викликати у людини неприємні відчуття. Один з найнадійніших біометричних методів.

3. Ідентифікація з райдужкою ока (рисунок 1.6).

Візерунок райдужки є унікальним для кожної людини. У цьому методі важлива не тільки гарна камера, але й надійне програмне забезпечення. Адже, вони використовують програмне забезпечення, щоб виділити в райдужній оболонці зображення. Цей метод є одним з найбільш точних серед біометричних методів.

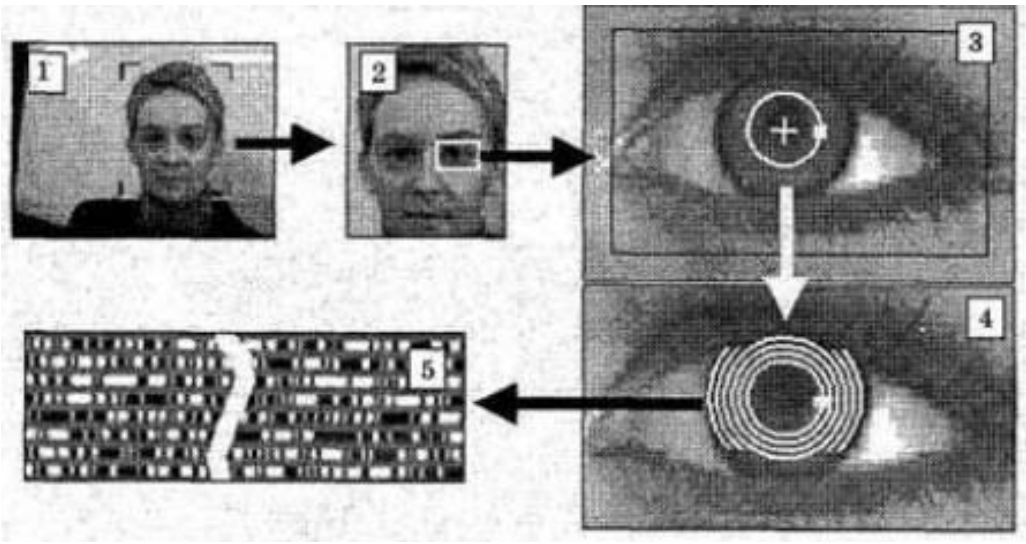

Рис. 1.8. Аутентифікація за райдужною оболонкою ока

1. Ідентифікація по формі кисті руки. Цей метод базується на розпізнаванні геометричних особливостей кисті руки. Спеціальний сканер формує тривимірний малюнок кисті. Під час аналізу даного малюнка виконуються вимірювання, за допомогою яких формується певний цифровий код.

2. Ідентифікація за формою обличчя (рис.1.9).

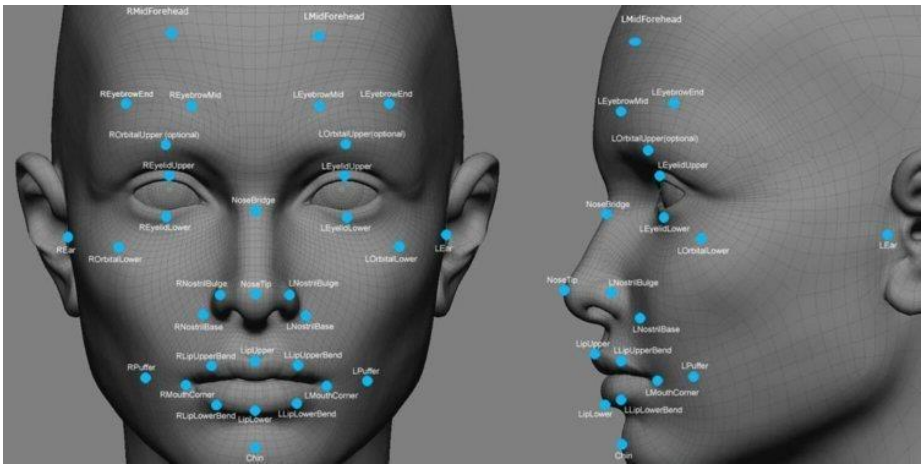

Рис. 1.9. Аутентифікація за формою обличчя

На практиці використовуються як 2D, так і 3D зображення. Більше того, двовимірне розпізнавання обличчя є одним із найефективніших методів біометричних даних на сьогодні, а тому має обмежений обсяг або використовується лише спільно з іншими методами. Розпізнавання обличчя за тривимірним зображенням чимось схоже на метод ідентифікації форми руки. Тут

також побудовано тривимірне зображення обличчя. Спеціальне програмне забезпечення витягує з цього зображення контури очей, губ та інших частин обличчя. Потім проводяться точні вимірювання між зазначеними контурами. Цифровий код складається з цих даних.

До динамічних методів, що використовуються для ідентифікації особи користувача, належать:

1. Голосова ідентифікація. Сьогодні існує безліч програм для розпізнавання голосу. У методі розпізнавання голосу важливі частотні характеристики людського голосу. Цифрова модель побудована відповідно до частотних характеристик.

2. Рукописне засвідчення особи. При ідентифікації за допомогою цього методу, як правило, перевіряється підпис особи. Перевіряються такі динамічні характеристики, як: графічні параметри, тиск, що чиниться на поверхню, швидкість підпису. На основі цих характеристик будується цифровий код.

3. Аутентифікація за допомогою почерку на клавіатурі. Цей метод схожий на ідентифікацію рукописного вводу, але замість того, щоб підписувати автограф, потрібно ввести кодове слово. Цифровий код базується на динаміці набору певного слова чи фрази.

Окрім теоретичного різноманіття можливих біометричних методів, методів, що застосовуються на практиці, небагато. Існує три основних методи - розпізнавання відбитків пальців, розпізнавання обличчя (двовимірне або тривимірне), райдужка і сітківка. Сьогодні всі біометричні технології є імовірнісними, і цей факт часто є основою біометричної критики.

Важко не погодитися з тим, що біометричні технології - це надійні та зручні заходи безпеки, які широко використовувались дотепер. Незважаючи на потужні зусилля в останні роки щодо розробки та вдосконалення методів ідентифікації користувачів для контролю доступу до ресурсів інформаційних систем, надійність та стабільність існуючих систем недостатня для сучасних потреб. Головною перевагою біометричної технології є її висока надійність. Насправді всім відомо, що в природі не існує двох людей з однаковим відбитком пальців. Правда, зараз

відомо багато методів, які обманюють зчитувачі відбитків пальців.

Наприклад, потрібні відбитки пальців можна передати на плівку або використати фотографію пальця зареєстрованого користувача. Однак ми повинні визнати, що сучасні пристрої набагато стійкіші до таких підробок.

Основним недоліком біометричної ідентифікації є вартість обладнання. Насправді вам потрібно придбати власний сканер для кожного комп'ютера в системі. Звичайно, ціна біометричних приладів останнім часом неухильно падає. Крім того, нещодавно з'явилися миші та клавіатури з вбудованими зчитувачами відбитків пальців.

У розглянутих системах для визначення особистості користувача використовується лише один фактор. Однак такі процеси сьогодні не можна назвати надійними. Останнім часом набула поширення комплексна або багатофакторна ідентифікація.

1.3 Багатофакторна ідентифікація/автентифікація користувачів

Багатофакторну автентифікацію / автентифікацію не можна виділити як окремий тип. Однак у таких системах одночасно використовується кілька параметрів для визначення ідентифікації користувача в ICS. Причому ці параметри можна комбінувати в будь-якому порядку.

Однак у переважній більшості випадків сьогодні використовується лише декілька: захист паролем та токен. У цьому випадку користувач не може побоюватися, що хакер вгадає його пароль (він не буде працювати без електронного ключа) і викраде токен (він не буде працювати без пароля). Деякі системи використовують найнадійніші методи автентифікації, які одночасно використовують паролі, токени та біометричні характеристики людини.

Впровадження комбінованих систем збільшить кількість ідентифікаційних функцій і, отже, підвищить рівень безпеки. Сьогодні розрізняють такі типи комбінованих систем:

- систему на основі безконтактних смарт-карт та USB-ключів;
- систему на базі гібридних смарт-карт;

- біоелектронну систему.

Безконтактні смарт-карти та USB-ключі. Антена та мікророз'єм вбудовані в корпус брелока USB для створення безконтактного інтерфейсу. Це дозволяє організувати контроль доступу до кімнат та комп'ютера за допомогою посвідчення особи. Цей шаблон використання посвідчення може усунути ситуацію, коли працівник залишає своє робоче місце і залишає ключ USB у роз'ємі на комп'ютері, що дозволяє йому працювати під своїм посвідченням. У випадку, коли неможливо вийти з кімнати без використання безконтактного посвідчення особи, цієї ситуації можна уникнути. Сьогодні двома найпоширенішими ідентифікаторами цього типу є:

- RfiKey - Rainbow Technologies;

- eToken PRO RM - Aladdin Software Security R.D.

Цифрові підписи, такі як: eToken RM - USB-ключі та смарт-карти eToken PRO у комплекті з пасивними RFID-мітками. Технологія RFID (ідентифікація радіочастот, ідентифікація радіочастот) є найпопулярнішою технологією безконтактної ідентифікації сьогодні. Ідентифікація радіочастот виконується за допомогою так званих RFID-міток, прикріплених до об'єкта, які несуть ідентифікаційну та іншу інформацію. З сімейства USB-ключів eToken лише eToken PRO / 32K може бути доповнений тегом RFID.

Гібридні смарт-карти. Гібридні смарт-карти містять різні чіпи. Один чіп підтримує контактну поверхню, інший - без контакту. Як і гібридні USB-ключі, гібридні смарт-карти мають дві функції: кімнатну та комп'ютерну. Крім того, на картці можна розмістити логотип компанії, фотографію працівника або магнітну смужку, що забезпечує повний обмін знайомими місцями та доступ до єдиного «електронного входу». Ці типи смарт-карт розробляються рядом компаній: HID Corporation, Axalto, GemPlus, Indala, Aladdin Knowledge Systems та іншими. У Росії технологія Aladdin Software Security RD була розроблена для виробництва гібридних смарт-карт eToken Pro / SC RM. Вони мають мікрозв'язки з інтерфейсом eToken Pro і вбудовані в безконтактні смарт-карти. Смарт-карти EToken PRO можна доповнити HID / ISOProx II, EM-Marine (частота 125 кГц),

Cotag (частота 122/66 кГц), Angstrem / Kiby-002 (частота 13,56 МГц), Mifare та інші пасивні RFID-мітки. компанії. Вибір варіанту поєднання визначається замовником.

Біоелектронні системи (рисунок 1.10). Як правило, для захисту комп'ютерних систем від несанкціонованого доступу використовується комбінація двох систем - контакт на основі біометричних та смарт-карт або USB-ключів. Системи розпізнавання відбитків пальців найчастіше використовуються як біометричні системи.

Рис.1.10. Багатофакторний біометричний термінал

Якщо відбиток пальця відповідає шаблону, доступ дозволений. До недоліків цього методу ідентифікації можна віднести можливість використання фіктивного друку. Підвищення надійності та точності автоматизованих систем ідентифікації користувачів можна досягти, поєднуючи використання біометричних характеристик із традиційними методами ідентифікації користувачів (наприклад, захист паролем, PIN-код, використання різних карток тощо).

Актуальною проблемою є розробка та вивчення складних систем, які використовують кілька біометричних характеристик користувача для прийняття рішення про доступ до інформаційних систем (наприклад, вони використовують

почерк та голосові характеристики клавіатури, динаміку роботи користувача з мишею). маніпулятор або використання кількох відбитків пальців тощо).). Кілька виробників вже почали інтегрувати два методи розпізнавання облич, включаючи 2D та 3D зображення.

Висновки по розділу

В даному розділі описані основні стандарти по криптографічних протоколів ідентифікації/автентифікації. Наведений опис біометричної ідентифікації та її складові.

РОЗДІЛ 2
ЗАСТОСУВАННЯ МЕТОДІВ І ЗАСОБІВ ДЛЯ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ТА АВТЕНТИФІКАЦІЇ

2.1. Принцип біометричної автентифікації

Для автентифікації за допомогою біометричного алгоритму суб’єкт повинен дослідити одну або кілька фізіологічних (відбиток пальця, райдужну оболонку, сітківку, риси обличчя тощо) або поведінкових характеристик (підпис, почерк на клавіатурі, шаблон голосу). Цей метод зазвичай використовується у критично важливих об'єктах та системах із спеціальним обладнанням.

Система працює за таким алгоритмом:

1. Користувач зчитує біометричні дані за допомогою біометричного зчитувача.

2. Дані зчитування надсилаються на сервер, де вони порівнюються з довідковими даними, що зберігаються в базі даних.

3. Якщо дані збігаються з еталонним варіантом, аутентифікація вважається успішною, і доступ до системи надається, якщо ні, то суб'єкт повертається до першого кроку. Алгоритм автентифікації пароля показаний на (рис. 2.1).

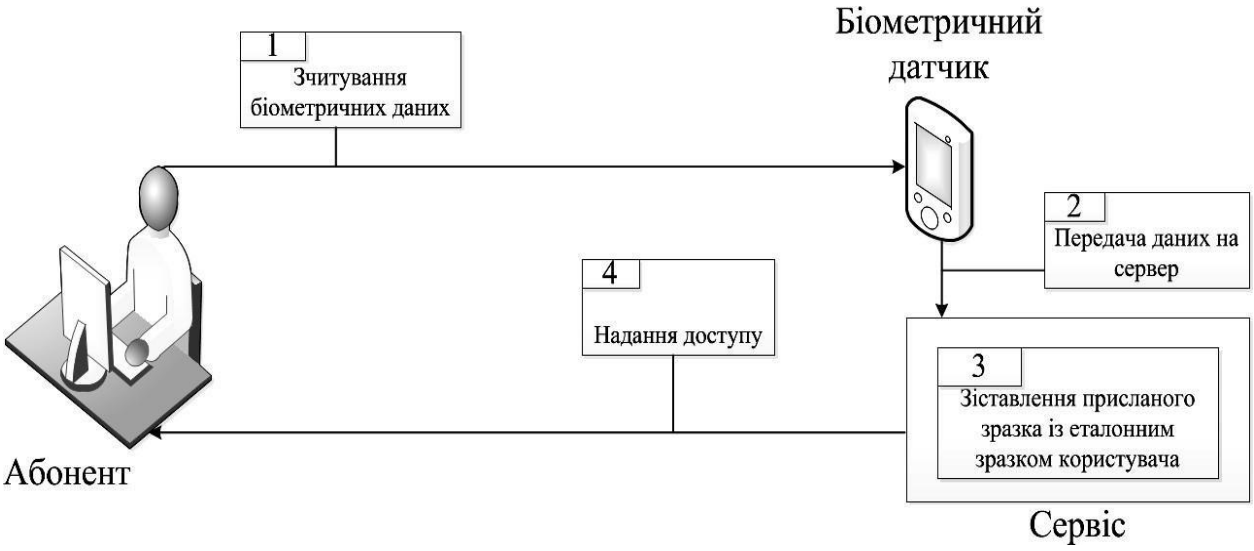

Рис. 2.1. Схема алгоритму біометричної аутентифікації

2.2. Біологічні дані, що використовуються в біометрії та особливості роботи з ними

Відбитки пальців

В останні роки метод біометричного розпізнавання відбитків пальців людини поширився з високою швидкістю і став найбільш перспективним методом серед інших біометрій. На думку дослідників, цей метод ідентифікації є номером один на корпоративному ринку, і в найближчому майбутньому лише метод розпізнавання райдужної оболонки зможе конкурувати за лідерство з цією технологією.

Уряд та громадянське суспільство у всьому світі постійно використовують біометричні системи, засновані на порівнянні відбитків пальців, як основний спосіб автентифікації та розпізнавання людей. І це не дивно, адже такий параметр, як його друк, економія обробки та значна точність результатів процесу, є найефективнішими параметрами, які можна використовувати для управління в комп'ютерних системах. Ця технологія застосовується у США, наприклад, департаментами транспортних засобів кількох державних адміністрацій, Mastercard, ФБР, Секретною службою, Агенцією національної безпеки, Міністерством фінансів та Міністерством оборони тощо. Цей метод, впроваджений компанією як система захисту доступу, значно підвищує ефективність адміністрування мережі, оскільки співробітникам більше не доводиться використовувати паролі, тому більше не виникає проблем, таких як втрата пароля та, як наслідок, найм обслуговування клієнтів [6].

Як загальне правило, біометричні технології для ідентифікації відбитків пальців людини поділяються на дві групи: перша використовується для ідентифікації, а друга для перевірки. Перша група використовує всі десять відбитків пальців для розпізнавання обличчя у своїй роботі. Такі технології широко поширені в судовій системі. Системи другої групи найчастіше використовують для перевірки відбитки одного пальця, а іноді і параметри кількох пальців. Як правило, існує три типи технологій сканування: оптична,

ультразвукова та на основі мікрочіпів.

Ключовими особливостями ідентифікації відбитків пальців, які зробили цей метод лідером на ринку підприємств, є практичність, простота використання та значний рівень безпеки. Відбитки пальців на обличчі деталізовані, майже унікальні, важкі в обігу та стабільні в житті людини, що робить їх придатними для ролі маркерів розпізнавання обличчя до 40 років. Існує два основних способи перевірки відбитків пальців: відповідно до певних ділянок (характерних точок) та рельєфу всієї поверхні пальця. Перший спосіб полягає в тому, що спеціальний сканер видаляє лише деякі деталі, які стосуються лише цього відбитка пальця, і обчислює їх відносне розміщення на пальцях. Відповідно, другий спосіб видаляє всю поверхню пальця та аналізує весь відбиток пальця. Сьогодні біометричні технології часто в різній мірі використовують обидва методи разом. Такий підхід дозволяє позбутися недоліків кожного алгоритму та підвищити точність процесу розпізнавання.

Зняття відбитка пальця на обличчі за допомогою оптичного сканера не витрачає багато часу. Зображення відбитка робиться за допомогою невеликої CCD-камери, яка може бути як окремим технічним пристроєм, так і легко інтегруватися в клавіатуру. Потім за допомогою певних алгоритмів візерунок відбиття кодується і перетворюється на цифрове зображення - схематично наносячи розташування характерних точок відбитка, які є унікальними перетинами ліній і заломлень відбитка. Це схематичне зображення точок знову кодується і зберігається в базі даних біометричної системи розпізнавання обличчя. Таке цифрове зображення може містити до сотні мікроточок. Таким чином, система записує не відображення, а унікальні мікротипи з їх розташування, тому користувачам цієї технології не доведеться турбуватися про конфіденційність своїх ідентифікаційних параметрів, оскільки зображення відбитків пальців не можна відтворити за допомогою таких шаблонів [10].

Вагомим плюсом ультразвукового сканування є те, що цей метод дозволяє видалити необхідні параметри без спотворення брудом на поверхні пальця. Крім того, можна навіть охарактеризувати ультразвук відбитків пальців за допомогою

гумових рукавичок. Слід сказати, що в даний час біометричні технології також захищені від підробки відбитків пальців так само, як і порізані пальці, оскільки спеціальні мікросхеми пристроїв здатні аналізувати фізичні характеристики шкіри. Сьогодні понад 50 різних виробників беруть участь у розробці таких технологій.

Використання відбитків пальців для розпізнавання людини є найбільш зручним з усіх біометричних методів. При перевірці справжності граней можливість помилки значно менша, ніж при інших методах біометричної перевірки. Однак на точність зображення відбитків пальців і правильність аналізу системою впливає стан поверхні пальця, а також положення пальця щодо пристрою для видалення. Вплив цих характеристик відбитків пальців на кінцевий результат залежить від вартості системи та вибраного типу перевірки відбитків пальців. Наприклад, якщо на поверхні пальця є бруд, ідентифікація з кожним мікроблоком ускладнюється. Тип перевірки відбитків пальців шляхом сканування всієї поверхні пальця не несе такого сильного ефекту бруду, але цей метод вимагає досить точного положення пальця на скануючому пристрої. Технічні засоби розпізнавання відбитків пальців людини не займають багато місця; може бути інтегрована у звичайну комп’ютерну мишу або клавіатуру [1].

Методи зняття відбитків пальців

В даний час розробляється велика кількість інструментів та методів електронних відбитків пальців. Найпоширеніші з них - оптичний, ємнісний, радіо-, тисковий, мікроелектромеханічний та температурний.

Оптичний метод

Цей метод справляє враження завдяки технологіям, які працюють як цифрова камера. Поверхня пальця розміщується на скляній поверхні, освітленій особливим чином. Все, що вам потрібно, - це необхідна лінза, вона може бути так близько до об’єкта зйомки. Потрібна картинка отримується завдяки наявності сучасної матриці та інших спеціальних технологій. Потім отримані дані перетворюються на чорно-білий малюнок із відтінками сірого (зазвичай 2-16

переглядів є задовільною кількістю). Одним з недоліків цього методу є те, що привертають увагу сліди відбитків пальців можуть залишатися на скляному аркуші, куди був поміщений палець, що надає зловмисникові несанкціонований доступ. Ще одним недоліком є те, що цей метод важко розпізнати справжнім пальцем за ретельно підготовленою підробкою [3].

Існує кілька типів оптичних відбитків пальців, які описані нижче.

Метод оптичного відбивання використовує фізичний ефект, такий як порушення повного внутрішнього відбиття. Суть ефекту полягає в тому, що коли світло падає на межу між двома середовищами, енергія світла ділиться на дві частини - одна відбивається від кордону, інша проникає через кордон до іншого середовища. Співвідношення відбитої енергії залежить від кута падіння світлового потоку. Починаючи з певного значення даного кута, вся світлова енергія відбивається від інтерфейсу. Це явище називається тотальним внутрішнім відображенням. Цей метод використовується оптичними сканерами FTIR (рис. 2.2).

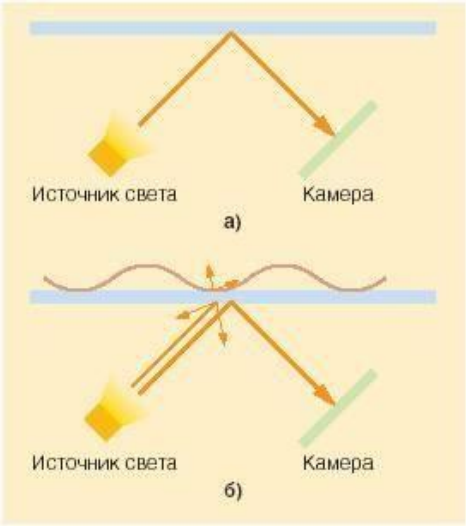

Рис. 2.2 Принцип роботи FTIR сканерів

У разі контакту між більш щільним оптичним середовищем (поверхнею пальця) і менш щільним оптичним середовищем промінь світла проходить через цю межу в точці повного внутрішнього відбиття. Таким чином, від кордону відбиваються лише ті промені світла, які впали до певних точок повного внутрішнього відбиття, до яких не був застосований сосочковий малюнок пальця.

Для захоплення отриманої фотографії поверхні пальця використовується матриця спеціального призначення.

Недоліки способу:

• Можливість помилкового підкріплення у разі помилкового всмоктування

• Чутливий до бруду.

Сканери, що використовуються в технології оптичної передачі, являють собою волоконно-оптичний масив, в якому всі вихідні хвилеводи підключені до фотодатчиків (рис. 2.3).

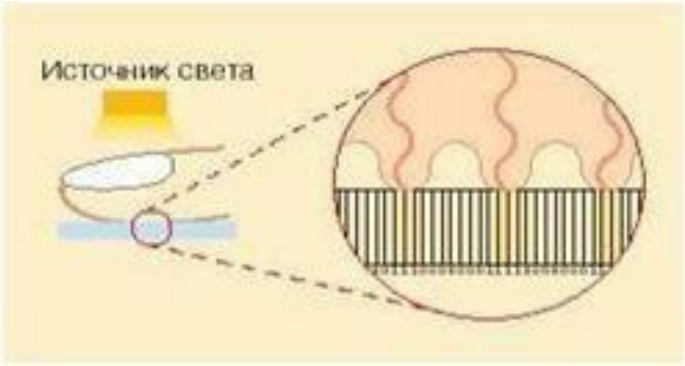

Рис. 2.3 Принцип функціонування оптоволоконних сканерів

Чутливість кожного датчика дозволяє виявити залишкове світло, що проходить крізь палець у місці контакту пальця з поверхнею матриці. Зображення всього відбитка формується відповідно до даних, зчитаних від кожного фотодатчика.

Цей метод має багато інших переваг:

• Високу надійність зчитування

• Стійкість до обману.

Однак у цього методу також є суттєвий недолік - складність реалізації.

В оптичному безконтактному методі використовуються оптичні контактні сканери, які не вимагають повнометражного запису на поверхню пристрою камери. Палець вдавлюють у спеціальні отвори, кілька світлодіодів висвітлюють його поверхню з різних кутів, а в центрі пристрою розміщується лінза, яка збирає дані та передає їх на спеціальну камеру, яка вже оцифровує зібрану інформацію. креслення відбитків пальців (рис. 2.4) [8].

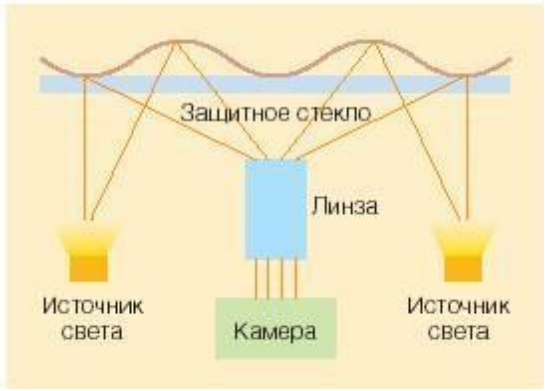

Рис. 2.4 Загальна схема роботи безконтактного сканера

Ємнісний метод

Метод заснований на принципі, що поверхня пальця розміщується на спеціальному пристрої, що містить матрицю елементів, схильних до електричного заряджання. Оскільки виступи та поглиблення на поверхні пальця мають різну електропровідність (вода, яка з'являється на шкірі, містить воду, а поглиблення - лише повітря), ємність елементів матриці змінюється. Це явище дає можливість визначити місце випинань і западин і сформувати шаблон цифрового друку. Цей метод є одним із найпоширеніших, хоча така технологія відбитків пальців має певні недоліки, такі як чутливість приладу до електростатичних розрядів та різних блукаючих електричних полів.

Радіо метод

У тому випадку, коли радіохвилі низької щільності проводяться на поверхні пальця, можна дізнатися розташування виступів і западин шкіри за допомогою пристрою, що має правильно налаштовані елементи антени. Для цього потрібно, щоб поверхня пальця була прикладена до спеціального датчика, частина якого випромінює радіохвилі. Цей метод знову заснований на фізіологічних особливостях шкіри, і тому майже неможливо отримати несанкціонований доступ підробленим пальцем. Недоліком цієї технології є те, що потрібно бути обережним, коли палець піднімається до пристрою, випромінююча частина якого має властивість нагріватися, що впливає на комфорт використання.

Нажимний метод

Для отримання характеристик відбитків пальців можна використовувати пристрої, п’єзоелектрична матриця яких чутлива до напруги. Ці технології мають досить слабкі місця, такі як низька чутливість батарейок, неможливість відрізнити палець користувача від підробки, можливість пошкодження через надмірну силу тощо. Однак є виробники біометричних приладів, які все ще розробляють пристрої, засновані на цій технології.

Мікроелектромеханічний метод

Ці технології все ще розвиваються, проходячи фазу розвитку та досліджень, але поступово інтегруються для аналізу їх ефективності. Цей метод також фіксує розміщення кінчиків пальців і вдавлення за допомогою вдосконаленого мікроелектромеханічного масиву датчиків. Хоча важко зробити висновки щодо стабільності елементів відповідного пристрою та точності інформації, цей метод можна отримати, але неможливість ідентифікації пристрою з накладним пальцем вже може бути додана до списку недоліків .

Температурний метод

Метод заснований на тому, чи здатні піроелектричні елементи виробляти деяку напругу зі зміною температури. Це явище використовується в процесі роботи інфрачервоних сканерів. Спеціальний датчик, що контактує з поверхнею пальця, працює відповідно до цього способу пристрою, дозволяє отримувати значення температури при стикуванні елементів пристрою з виступами і западинами на шкірі.

Ця технологія має ряд переваг, серед яких можна виділити відсутність впливу на роботу пристрою електростатичного розряду та велику зручність використання, оскільки палець не відчуває випромінювання. Крім того, пристрої, засновані на цьому методі, дозволяють отримувати точну інформацію на поверхні пальця при будь-якій температурі навколишнього середовища та виявляти помилковий палець, з яким не може впоратися достатня кількість методів.

Єдиним недоліком цього методу є те, що отримане цифрове зображення пальця користувача є досить нестабільним і його потрібно швидко зафіксувати.

Це пов’язано з тим, що в той момент, коли поверхня пальця поміщається на пристрій, різниця температур викликає певний ступінь напруги, але це поступово згасає за дуже короткий час (менше десятої секунди), оскільки температура пальця та сканера досягти рівноваги [1].

Інформаційні ознаки відбитків пальців

Для кожного відбитка пальця виділяють дві групи характеристик - глобальну та локальну.

Глобальні сигнали - це ті, які можна побачити без використання спеціальних пристроїв:

- Папілярні візерунки.
- Область зображення - найбільша частина роздруківки, що містить усі фрагменти інформації.
- Ядро - точка посередині друку або конкретного фрагмента.
- Точка "дельта" є початковою точкою. Це може бути місце відділення або зрощення канавок папілярних ліній, або воно може бути досить невеликим за розміром.
- Тип лінії - визначається двома найбільшими лініями, які проходять спочатку паралельно, а потім виходять по краю всієї області зображення.
- Лічильник ліній - визначає кількість ліній у всій області зображення та між ядром і точкою “дельта”.

Рис. 2.5 Типи папілярних рисунків

1 - 4 - креслення типу "петля" (лівий, правий, середній, подвійний), 5 і 6 - креслення "дельта" або "дуга" (простий і гострий), 7 і 8 - креслення форми «Спіраль» (центральна та змішана).

Друга група функцій - локальна. Це називається мінус - унікальні параметри відбитка, що характеризують точки, де змінюється форма сосочкових ліній (наприклад, закінчення, роздвоєння, переломи тощо), і включають розміщення цих ліній та точок, описаних річ. Будь-який відбиток складається приблизно із сімдесяти Minucias [11].

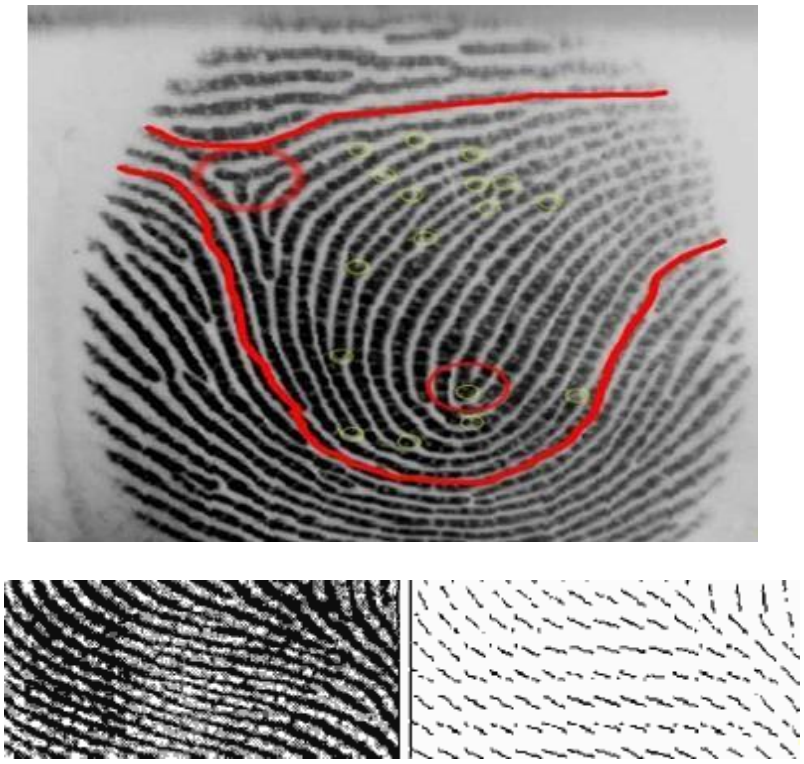

Рис. 2.6 Установлення поля орієнтації папілярних ліній

Аналізуючи відображений друк, ви можете помітити наступні параметри:

- два рядки - "тип рядка"; Площа зображення може бути будь-якою між цими рядками, але в багатьох випадках аналізується вся область друку;

- червоне коло зліва - елемент "дельта"; червоне коло внизу - це серцевина;

- мінуція позначена жовтими колами.

Глобальні характеристики деяких облич можуть бути невиразні, тому виявлення користувачів на основі цих параметрів неефективно. Однак дані мінуції

від різних людей завжди є унікальними, тому глобальні сигнали зазвичай використовуються для поширення бази даних до певної міри та на перших рівнях ідентифікації. Мікроточки використовуються на останньому рівні розпізнавання[3].

Стандарти на відбитки пальців

Сьогодні, як правило, використовують ANSI (Американський національний інститут стандартів) та американські стандарти ФБР. Для підвищення ефективності ідентифікації прийнято одночасно зберігати кілька зображень у сховищі шаблонів. Допускаються відмінності між малюнком малих поворотів та зсувами. У цьому випадку співвідношення сторін зображень залишається незмінним, оскільки відбитки зроблені з одного і того ж пристрою [1].

Принципи порівняння відбитків за локальними ознаками Збіг відбитків пальців ділиться на такі етапи:

- Етап 1: Покращення властивостей відсканованого зображення. Покращено межі рядків друку.
- Етап 2: Розрахунок розташування папілярних ліній. Креслення поділено на квадратні блоки зі сторонами не менше 4 точок і кут розміщення лінії розраховується для кожного відбитка.
- Етап 3 Розробка напівтонового малюнка. За допомогою спеціальних алгоритмів малюнок буде чорно-білим.
- Етап 4: Витончення ліній отриманого візерунка друку. Розрідження застосовують до тих пір, поки товщина лінії не стане 1 пікселем (рис. 2.7).

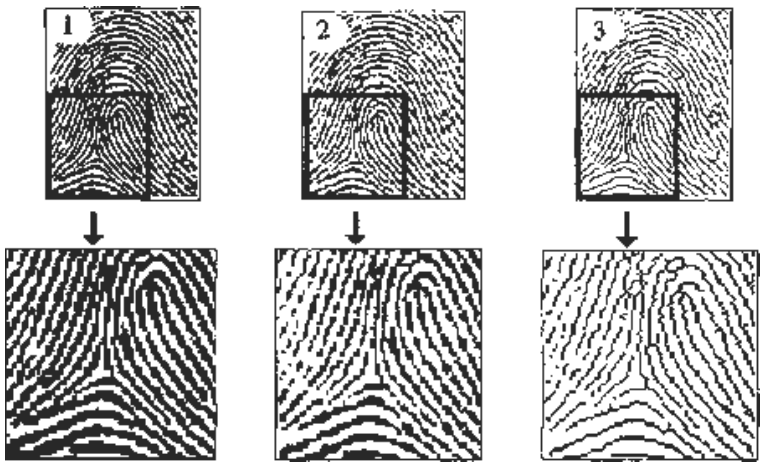

Рис. 2.7 Етап 4. Витончення ліній відбитку

• Етап 5. Акцентування мінуцій. Спочатку малюнок ділиться на квадратні блоки зі стороною 9 пікселів. Потім за допомогою алгоритмічного опрацювання технологія знаходить кількість чорних пікселів, які розміщуються в центральній зоні. Такий піксель називається мінуцією, у випадку коли він сам чорний та поряд з ним знаходяться один (тип «кінцівка») або два (тип «подвоєння») чорних пікселі (рис. 2.8).

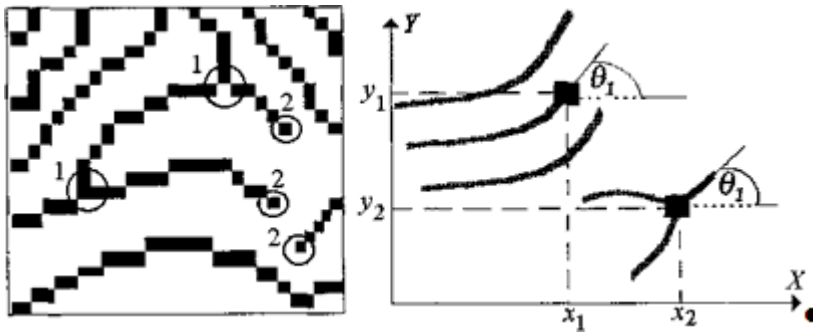

Рис. 2.8 Етап 5. Акцентування мінуцій

Координати знайдених мікроточок, їх кути положення та загальна кількість розраховуються на основі певної векторної формули, і ця конкретна формула зберігається в системі як шаблон для даних даного користувача. Під час ідентифікації формула визначає дійсність відбитка пальця [12].

Крок 6. Порівняння мікроточок

Два користувачі можуть мати різні зміщення своїх двох відбитків пальців

відносно один одного, не кажучи вже про інтерфейс між пальцем і пристроєм, навіть якщо обличчя тисне на диск. Тому неможливо перевірити відбиток пальця людини за допомогою стандартного методу порівняння. Отже, робота пристрою шляхом порівняння параметрів друку повинна проходити через кожну мікропланшет шаблону та отримане зображення. Цей розділ дотримується наступного алгоритму:

• Реєстрація параметрів.

• Знайдіть пару відповідних мінуцій.

• Визначення ідентичності відбитків.

На момент реєстрації можуть бути знайдені характеристики розміщення (кут повороту, масштаб та зсуви), беручи до уваги, чи співпадає певна мікроточка з одного вектора з певною Minucia з іншим.

Для будь-якої мікроточки слід враховувати до тридцяти кутових обертань (від -15 градусів до +15 градусів), 500 значень переміщення (від -250 пікселів до +250 пікселів - однак, іноді обмеження вибирають дещо менших розмірів і 10 значень шкали (0,5-1,5 0,1 на крок.) Загалом до 150 000 таких чисел можна застосувати до будь-якої з 70 можливих мікроточок. Але не всі параметри обліку використовуються в технології обробки друку, оскільки після враховуючи можливі особливості розміщення одного мікропростору, отримані результати застосовують розрахунки до інших для цього друку. В іншому випадку, при багатьох обчисленнях, ви можете зв’язати майже всі свої відбитки пальців один з одним.

У випадку, якщо збіг кількості хвилин перевищує 65%, система підтверджує справжність відбитка пальця. (Відсоток збігів, необхідний для підтвердження, може змінюватися залежно від рівня безпеки, достатнього для замовника.) Система, що працює для цілей контролю, вимкнеться після отримання результату. Якщо потрібна ідентифікація, слід порівняти всі відбитки пальців, що зберігаються в системі. Далі ми знаходимо шаблон, з яким ступінь збігу є найбільшим серед інших. Ступінь ідентичності в цьому випадку перевищує 65% [1].

Інші методи зіставлення відбитків.

Описана технологія є дуже точною та ефективною, але біометричні системи активно розвиваються, тому досліджуються нові методи узгодження параметрів відбитків пальців, які згодом можуть виявитися більш ефективними. Так, наприклад, при використанні **глобального методу, заснованого на ознаках**, спочатку визначаються глобальні характеристики відбитків пальців (наприклад, ядро, дельта та інші). Потім тип вибірки визначається кількістю та відносним розміщенням цих параметрів. Перевірка та ідентифікація здійснюються за допомогою місцевих таблиць. Менше обчислень, які система повинна виконати, щоб узгодити відбитки пальців таким чином, а значить, вони працюють швидше.

Метод, що використовує графи, а 2.8. працює за алгоритмом, наведеним на рисунку. Отриманий шаблон друку (1) стає схематичним зображенням розташування папілярних ліній (2). Крім того, знайдені фрагменти, що мають подібні лінії та межі між такими фрагментами (3). Потім створюються центри фрагментів, щоб отримати графік (4). У розділі, позначеному стрілкою (d), отримана інформація про друк обличчя зберігається в системі. Порівняння відбитків та оцінка їхньої ідентичності у квадраті (5). Крім того, технологія працює так само, як і попередній метод - мікродотальна ідентифікація.

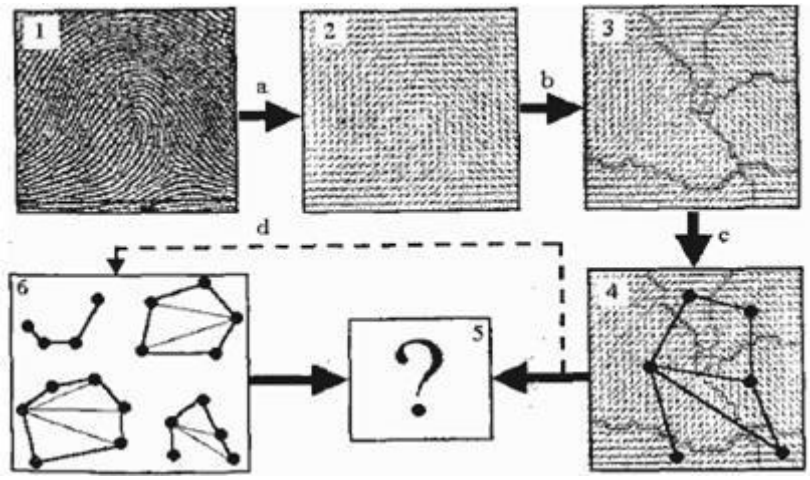

Рис. 2.9 Метод з використанням графів

Методи обходження такої системи доступу

1. Конденсація. У деяких випадках, якщо ви дихаєте на контактній поверхні,

ви можете побачити сліди лицьової відбутки, саме для цього ви використовували пристрій. Цей метод може працювати лише з пристроями з оптичним сканером. Для напівпровідників такі хитрощі неможливі.

2. Можна сфальсифікувати друк іншої людини клейкою стрічкою, проте, як і раніше - метод можливий лише при використанні оптичних сканерів.

3. Для виготовлення підробки можна використовувати жувальну гумку, але цей спосіб не спрацює, оскільки надруковане зображення буде видалено як дзеркальне. Але, можливо, навчені фахівці зможуть сфальсифікувати відбиток такого матеріалу.

4. Використання відрізаного пальця не дасть результату, оскільки мертва тканина відразу почне втрачати свій попередній вигляд. Крім того, деякі системи використовують технологію, яка сприймає такі параметри, як температура, частота серцевих скорочень тощо, однак вони коштують значно дорожче. Надійність системи доступу можна підвищити, запровадивши додаткові технології, такі як розпізнавання райдужної оболонки ока.

2.3. Переваги та недоліки методів

Оцінка біометричної системи ідентифікації за відбитками пальців

Переваги:

1. Не потрібно використовувати логін та пароль, тому вам не доведеться турбуватися про їх втрату.

2. Створити манекен дуже важко (співвідношення ціни та надійності дуже велике).

3. Невеликий розмір скануючих пристроїв дозволяє їх застосовувати навіть на мобільних пристроях. Такі технології будуть дуже ефективні сьогодні, коли переважна більшість людей мають мобільні телефони та USB-накопичувач. Якщо ви крадете пристрої з вбудованою біометричною системою, вам не доведеться турбуватися про те, що особисті дані стануть доступними для незнайомця.

Обмеження:

1. Вважається, що дані, зібрані за відбитками пальців деяких систем, будуть використовуватися правоохоронними органами без відома осіб, яким вони

належать.

2. Неможливо розпізнати характеристики відбитка пальця у разі пошкодження шкіри пальця.

3. Надійність перевірки ускладнюється також наявністю бруду на поверхні пальця.

Зовнішні риси особистості

Це сучасний метод розпізнавання людини, який зазнав значного розвитку за останні роки, заснований на появі визначення обличчя. Забезпечити ефективність такої системи - завдання не з простих. Розробляючи таку технологію, ми витратили багато часу на те, щоб дізнатися, як отримати необхідні дані за допомогою фото- чи відеокамер. Уряди США та Німеччини навіть надали фінансову допомогу ряду організацій, що розробляють такі системи. Відповідно, на початку розробки такі технології планувалось запровадити для підвищення ефективності роботи правоохоронних органів, але згодом подібні системи були введені і в інших сферах. Прилади, що працюють за цим принципом, дозволяють проводити сканування індивідів будь-де та в будь-який час. Спеціальні камери, підключені до відповідних комп’ютерів, знімають фото людини и технологія підтверджує або спростовує відповідність особи з тією, характеристики якої зберігаються в системі. Методика процесу ідентифікації по зовнішності базується на новітніх способах перетворення зображень у цифрові дані, які у своєму складі мають такі характеристики обличчя як взаємне розташування, форма та розміри очей, носа, губ і таке інше. Такі оцифровані дані виконують роль мінуцій при ідентифікації за відбитками пальців, тобто являють собою унікальні мікрокрапки, які є неповторними для кожного користувача. Зазвичай для надійного розпізнавання достатньо визначити близько 40 таких точок обличчя, в той час як технологія знаходить близько 2 тисяч таких характеристик. Система може знайти так багато оригінальних параметрів особи за допомогою аналізу її обличчя, що точність та достовірність отриманої інформації не залежить від повороту голови, використання косметики чи окулярів.

Біометричні технології ідентифікації особи за зовнішністю діляться на два

види. Системи першого виду грунтуються на статистичному методі: знімається зображення людини, за допомогою певних алгоритмів отримується оцифрований шаблон який представлений набором чисел, які визначають конкретного індивіда. Така технологія дуже популярна, проте результати розпізнавання виходять не достатньо точні.

Системи другого виду здатні підлаштовуватися до факторів мінливості зовнішності людини. Вони враховують наявність бороди на обличчі, окулярів та навіть вік. Це означає що такі технології дозволять для розпізнавання застосовувати і застарілі фото особи. Деякі системи здатні обчислювати необхідні дані навіть за рентгенівськими знімками. Ефективність даного способу обумовлена тим, що він користується принципом, аналогічним до того, як сама людина аналізує іншу з метою розпізнати її. Встановлення достовірності людини за її зображенням на паспорті, як і за унікальним підписом, являється одним з найзручніших та ефективних способів.

Такі методи доцільно застосовувати і в цілях контролю доступу до інформації, тому що вони не займають багато часу та розпізнавання відбувається за відсутності безпосереднього контакту користувача з біометричним приладом, що, знову ж таки, досить зручно.

Технології ідентифікації/верифікації особи за її зовнішністю можливо застосовувати в різних сферах: від пошуку певної особи, порівнюючи його зображення, відзняте з камер спостереження, з шаблоном, збереженим в системі, до звичайного контролю доступу. Такі методи встановлення достовірності користувача втрачають ефективність тільки в тому випадку, коли відбулись великі зміни в зовнішності (як приклад, через певний нещасний випадок), що приводить до неможливості розпізнати людину навіть іншим особам.

Як ми вже знаємо, усі біометричні технології в залежності від параметрів які вони застосовують мають як свої переваги, так і недоліки. Тому немає сенсу гадати, що певна технологія досягне більш високої ефективності для будь-якої ситуації. Проте серед біометричних систем існують найбільш універсальні технології, такі як встановлення особи за відбитками пальців, райдужній оболонці

ока або зовнішності, і людина повинна сама, враховуючи конкретну ситуацію, обрати придатну для неї систему.

Технологія встановлення персони індивіда за його зовнішністю у своїх перевагах має той факт, що людині не потрібно тісно взаємодіяти з біометричним пристроєм та виконувати певні дії.

Варто наголосити, що ідентифікація людини за неповторними рисами обличчя – один з небагатьох біометричних методів встановлення персони, в процесі використання якого немає необхідності у специфічних приладах. Метод використовує близький до людського підхід, адже ми впізнаємо знайомих нам людей завдяки рисам зовнішності, а не займаємося зіставленням відбитків пальців та звірянням райдужної оболонки ока. Цей спосіб відомий вже досить давно, за часів, коли застосування фото для встановлення персони було одним з єдиних на той час методів біометричної ідентифікації. Саме тому впроваджувати цей метод у сучасні технології досить просто, адже представлення про нього вже давно закоренилося у свідомості людей.

Технологія ідентифікації людини на основі її зовнішнього вигляду є найкращим біометричним методом для встановлення справжності людини також для багаторазового використання. Якщо розпізнавання обличчя використовується іншими методами головним чином для доступу або порівняння даних із даними, що зберігаються в системі, метод розпізнавання зовнішнього вигляду дозволяє негайно використовувати характеристики людини, знятої на камеру, і ігнорувати отримане зображення, якщо це не потрібно. Якщо ми говоримо про спроби обійти таку систему, то вбудована технологія ІЧ-випромінювання здатна відрізнити маску від справжнього обличчя людини. Біометрична система виявляє шкіру та міміку людини та негайно сповіщає вас, активуючи спеціальний сигнал про підозру на манекен. Процес зйомки зовнішнього зображення відбувається непомітно, на певній відстані від об’єкта, часто без його відома. Звичайно, це суттєвий параметр роботи правоохоронних органів. Але правозахисники висловлюють своє невдоволення цими методами, покладаючись на порушення права людини на анонімність. Однак розробники біометричних пристроїв мали

справу з подібними скаргами. Права людини не порушуються, оскільки у випадку, якщо технологія не підтверджує автентичність особи тим, що має бути визначено, вона автоматично видаляє всі отримані дані людини, знятої у відеозоні, камерою [3].

Крім того, розробники забезпечать використання традиційних камер відеоспостереження в технологіях виявлення, характеристики яких вже давно визначені чинним законодавством. Наприклад, в даний час існує правило, згідно з яким відповідні попередження розміщуються в місцях із відеоспостереженням.

Такі технології розпізнавання обличчя використовують служби безпеки переважної більшості різних організацій, не кажучи вже про державні установи.

Практика використання розпізнавання обличчя

Спосіб ідентифікації людини за її зовнішністю, безсумнівно, набув звання однієї з найефективніших технологій. Цим методом користуються такі установи, як Банк Німеччини, Європейський центр ядерних досліджень, Microsoft Corporation, Siemens та багато інших. Більшість атомних електростанцій та суворо зашифровані контрольовані території також використовують ці біометричні системи. Завдяки цифровій фотобазі даних із першими технологіями ідентифікації, представленими ZN Vision Technologies, багато служб безпеки в різних країнах досягли величезного підвищення ефективності пошуку зловмисників.

Геометрія руки

Ці типи біометричних технологій працюють за принципом використання пристрою, створюючи ідентичність шляхом порівняння унікальних характеристик пальми. Під час розпізнавання система враховує понад 90 параметрів, таких як розмір долоні, показники довжини і ширини пальця, характеристики суглобів тощо. На практиці застосування цього методу розпізнавання обличчя можна знайти в законодавстві, міжнародних аеропортах, лікарнях, імміграційних службах тощо. Позитивні сторони використання таких технологій мають таку ж точність і швидкість обробки, що і в системах, що використовують відбитки пальців, але недоліком є те, що пристрої для зчитування ручної інформації не

настільки компактні, як цього вимагають деякі випадки [1].

Геометрична карта судин долоні

Науково-технічний журнал IEEE Spectrum присвятив статтю про використання систем біометричної ідентифікації при оплаті в Японії за допомогою геометричної карти долонь. З 2005 року банки країни впровадили «біометричні дані» в 80 000 банкоматів, а також у комерційні термінали та інші пристрої. Технологія настільки добре зарекомендувала себе, що новою технологією зацікавились банки не лише Японії, але й Бразилії, Польщі та Туреччини.

Системи, незалежно запропоновані Hitachi та Fujitsu, засновані на скануванні зображення вени руки. У кожної людини є суто унікальний малюнок вен, артерій та капілярів, це ідентифікує людину краще, ніж відбиток пальця.

На відміну від сканерів райдужної оболонки, судинні сканери швидкі та легкі, а сам пристрій набагато дешевший.

Компанії Hitachi та Fujitsu роками працюють над комерційним впровадженням таких систем - кожна зі своїм впровадженням, різними методами сканування рук, але сканери Hitachi оглядають лише пальці, а не цілі долоні. На даний момент капілярний сканер лише доповнює (або навіть замінює) PIN-код картки, але в майбутньому можна буде обміняти всю картку, тобто товари можна оплатити, роздавши машину. Це буде повноцінна біометрична платіжна система: новий рівень розуміння грошей - це абстракція.

Така система є набагато складнішою, ніж поточна реалізація, оскільки замість простої перевірки ідентичності буде потрібно повна ідентифікація особи. Нещодавно компанія Fujitsu поділилася результатами експерименту, в якому взяли участь 5 мільйонів користувачів: система правильно розпізнає людей в середньому за 1,34 секунди.

Першим європейським банком, який дозволив клієнтам знімати гроші зі свого рахунку на основі біометричних даних, був польський BPS SA, який використовував технологію Finger Vein, розроблену Hitachi. Кожен біометричний банкомат має сканер, який збирає унікальні дані про систему кровоносних судин

пальця для кожної людини.

У вересні 2012 року японський банк Ogaki Kyoritsu запустив першу в світі нову біометричну платіжну систему: вам не потрібна пластикова картка для зняття грошей з банкомата, вам достатньо провести руку до сканера, ввести свій PIN-код і дату народження .

Природні катастрофи того часу змусили японський банк пришвидшити роботу із впровадження нової технології на практиці, залишивши десятки тисяч людей без документів та банківських карток.

Сканери також можна використовувати у торгових автоматах. Наприклад, якщо ви хочете придбати пляшку мінеральної води у торговому автоматі, все, що вам потрібно зробити, це торкнутися сканера рукою, і ви отримаєте товар.

термограма на обличчі

Метод ідентифікації людини за допомогою термограми заснований на дослідженнях, які показали, що термограма обличчя є унікальним параметром для кожної людини.

Термограма виготовляється за допомогою інфрачервоних камер. Метод має перевагу перед системами розпізнавання зовнішності, оскільки він може розрізнити близнюків. Застосування спеціальних масок, пластична хірургія, старіння людського тіла, температура тіла, охолодження шкіри обличчя в холодну погоду не впливають на точність термограми. Через низьку якість ідентифікації, метод в даний час не використовується широко [1].

Райдужна оболонка ока

Цей тип системи також є одним з найбільш ефективних. Це пов’язано з тим, що райдужна оболонка ока - це унікальний особистий параметр для кожної людини, який відрізняється навіть для близнюків. Почалося обстеження райдужної оболонки ока з суто медичних цілей - вивчення симптомів деяких захворювань. Вчені, між іншим, дійшли висновку, що певні захворювання спричиняють появу різних пігментів на райдужці. Враховуючи цей фактор, біометричні технології, засновані на цьому методі, використовують чорно-білі малюнки.

У методології роботи біометричної технології вона використовує спеціальну тканину як основний визначальний параметр для створення шаблону; плід розвивається до восьмого місяця вагітності, і в результаті стає помітним розподіл райдужки в променевих секторах. Інші параметри включають такі характеристики, як окремі кільця, борозенки, веснянки та область коронки. За допомогою райдужки 11 мм біометричні системи можуть знаходити приблизно 3-4 біти цифрових даних на 2 мм2 площі. Ірис містить до 266 специфічних мікроточок, які використовуються для розпізнавання, на відміну від більшості біометричних технологій, які працюють від 10 до 60 мікродів. Тому системи, що використовують такі методи, переконливо ведуть біометричний ринок, оскільки можна з упевненістю стверджувати, що ефективність таких технологій є однією з найкращих.

Давайте розглянемо, як відбувається процес розпізнавання особистості, здійснюваний райдужкою в біометричній системі. Сканування ока і отримання зображення здійснюється спеціальним пристроєм, і робиться це навіть на відстані одного метра. Для вивчення та розрахунку параметрів ока наступні процеси можна розділити на наступні етапи: процес захоплення райдужки, процес ізоляції зіниць, процес аналізу та розрахунку характеристик райдужки та встановлення результати тесту. Перший та другий процеси його роботи працюють з такими факторами: круглою формою райдужки та зіниці та високим ступенем контрастності в білій частині ока. В даний час існує кілька методів швидкого визначення кіл на кресленні, але одним з найпопулярніших є метод, заснований на перетворенні Хафа. Щоб отримати результат розпізнавання обличчя, технологія використовує шаблони зареєстрованих користувачів, збережені в базі даних, щодо яких перевіряють параметри обличчя, яке потрібно перевірити. Кількість ознак, за якими відбувається розпізнавання, залежить від мети такої перевірки, тобто типу визнання, що має місце - перевірки або ідентифікації.

Таким чином, як уже зазначалося раніше, біометричні системи, що працюють за принципом унікальності параметрів райдужки, характеризуються високим рівнем захисту. Ось кілька статистичних даних, які найкраще

ілюструють надійність таких технологій. Величина другого типу індикатора несправності, коли особа, яка не має достатніх прав, перевіряється та отримує несанкціонований доступ, виражається ймовірністю 1 200 000 випадків ідентифікації цього типу технології.

Сучасні пристрої можуть виявити обличчя навіть у разі затінення (або пошкодження) хребетної оболонки, коли величина таких змін становить 2/3 площі оболонки або менше. За цих обставин ймовірність рівня помилки розпізнавання обличчя в 100 000 процесів ідентифікації становить 1. Говорячи про здатність цих систем протистояти різним методам обману, біометрія, заснована на видаленні ознак райдужки ока, має кілька рівнів захисту, таких як : визнання манекена зіниці; зчитування даних, виявлених на рогівці; визначення наявності контактних лінз, використання інфрачервоного світла для перевірки стану тканин ока. Тому дуже важко описати ситуації, коли зловмисникам вдалося обійти цю біометричну систему.

Недоліком цих технологій є висока вартість пристроїв, але вони відповідають своїм параметрам якості та ефективності [1].

Сітківка ока

Рівень захисту, що забезпечується цим типом біометричної системи, порівнянний із методом ідентифікації райдужки. Принцип реєстрації параметрів сітківки ока досить складний (ви повинні мати спеціальний пристрій, щоб зробити бажані властивості видимими за допомогою інфрачервоного світла), однак цей метод відомий давно для розпізнавання людини. Дослідники Саймон і Гольдштейн виявили картину кровоносних судин на будь-якому очному дні в 1935 році. Потім стало відомо, що цей параметр є особистим і унікальним, включаючи близнюків.

Якщо не брати до уваги певні типи захворювань очей та випадки травм голови, картина малюнка судин залишатиметься досить стабільною протягом усього життєвого циклу людини.

Поширення цього методу розпізнавання зупиняється тим, що він досить складний і процес взаємодії між пристроєм та користувачем не такий зручний, як

при використанні інших систем. За статистикою, лише 85% від загальної кількості людей схильні проходити першу спробу фіксувати параметри сітківки. У цьому випадку обличчя повинно підходити до ока за допомогою спеціального скануючого пристрою, відстань між оком і поверхнею сканування не повинна перевищувати 1-1,5 сантиметра. У момент, коли робиться знімок, людина фокусує свій погляд на маленькому зеленому світлодіоді, який обертається навколо своєї осі. На відміну від методу перевірки відбитків пальців у людей, де використовується приблизно від 30 до 40 мікроточок, пристрій специфічності сітківки зчитує, обчислює та створює із свого зображення зображення, яке зберігається в базі даних системи і згодом використовується для розпізнавання обличчя. Ось чому цей тип біометричної системи характеризується надійністю, яка перевершує різні способи розпізнавання людини.

Якщо говорити про статистичні показники помилок при використанні цих систем, то у випадку другого типу помилок (для забезпечення доступу несанкціонованих осіб) значення надійності становить 0,0001%, що свідчить про високий рівень безпеки для цього технології. Однак перший тип показника несправності (який не забезпечує доступу уповноважених осіб) набагато вищий - до 0,1%. Такі дані пов’язані з тим, що подібні технології були виготовлені для використання у військових організаціях на початку розробки методу, тому основним завданням створеної системи було усунення можливості несанкціонованого доступу до об’єкта та зручності за допомогою методу було відсунуто на другий план. Він розроблений таким чином, що оскільки вірогідність помилкового відхилення є достатньо високою для системи доступу, людина зможе виконати процес перевірки кілька разів. Враховуючи описані фактори, ця технологія поки що не широко поширена серед цивільних споживачів систем контролю доступу.

До недоліків методу належать певні незручності, з якими усувається процес збору даних із сітківки ока, і, як і у випадку ідентифікації з райдужкою ока, висока вартість пристроїв становить близько 4000 доларів. Цікаво, що в сучасному світі комп’ютерні технології еволюціонували до такої міри, що вони

можуть не тільки бачити та розрізняти обличчя на задньому плані навколишнього середовища, а й розпізнавати людську особу та виконувати функції доступу [1].

Голос і мова

Багато компаній розробляють біометричні системи, які можуть розпізнавати обличчя на основі його голосових характеристик. Метод базується на таких характеристиках, як частотні характеристики, інтонація, висота звуку тощо. До переваг таких систем можна віднести відсутність використання дорогих пристроїв, ідентифікація можлива лише за допомогою звукової карти та мікрофона.

Однак, незважаючи на простоту використання, ця технологія не така точна, як інші системи. Пацієнт, голос якого змінився в результаті, не може отримати підтвердження при врученні сертифіката. Взагалі, людський голос підпорядковується низці фізіологічних та психологічних факторів; тому основним недоліком системи цього типу є низька надійність оцінки розпізнавання. Але це не заважає впровадженню таких біометричних технологій в системах доступу для об’єктів з низькою конфіденційністю [1].

Підпис

Підпис обличчя є унікальним особистим параметром, хоча і не є невід'ємною частиною його фізіології. Це більш відомий метод розпізнавання особи, оскільки його використання не викликає асоціацій у сфері кримінального правосуддя, ніж у випадку з відбитками пальців. Цей метод є досить ефективним, принцип ідентифікації заснований на характеристиках параметрів рукописного руху обличчя на момент написання. Методи розпізнавання осіб за літерними параметрами можна розділити на два типи: перевірка отриманого підпису за допомогою стандартного шаблону та більш складна динамічна перевірка. Метод першого типу не відрізняється від точності результатів аудиту, оскільки простий аудит із шаблоном, що зберігається в системі, не є повністю ефективним. Людина може подавати один і той самий підпис різними способами, тому така перевірка цілком ймовірно припуститься помилки. Другий тип систем розпізнавання підписів використовує значно більше факторів і використовує у своїй методології

такі характеристики введення підпису, як характеристики руху людської руки в певні моменти письма, сили тиску та тривалості кожного виходу. фрагмент підпису. Ось чому навіть професіонал, який імітує підписи, не зможе обдурити таку систему, оскільки надзвичайно важко повторити підсвідомий рух будь-якої людини з точністю та детальністю.

Людина, що використовує традиційний оцифровщик та ручку, тихо вводить свій особистий підпис, і в даний час технологія фіксує орфографічні характеристики та перевіряє їх за допомогою шаблону, що зберігається в системі. Якщо характеристики збігаються з тими, що зберігаються в базі даних, технологія додає до документа, що підписується, ім'я користувача, електронна пошта, посада, поточний час і дата, характеристики введення підпису, багато характеристик руху (швидкості) запису, прискорення , напрямок, тиск тощо. Отримана інформація шифрується за спеціальною формулою, обчислюється контрольна сума і формується біометрична мітка. Щоб налаштувати систему, людина повинна ввести підпис кілька разів (від 5 до 10), щоб створити більш досконалий шаблон.

Використання систем біометричного розпізнавання на основі перевірки підпису не має сенсу, якщо метою реалізації є захист доступу до певної кімнати чи комп’ютерної системи. Але в організаціях, які завжди мають робочий процес із великим обсягом конфіденційної інформації у своїх операціях (наприклад, банківський сектор), такий метод перевірки автентичності особи може стати чудовим вибором для зручності та порівняно простим у впровадженні [1].

Висновки по розділу

На сьогодні є багато систем біометричної ідентифікації людини, які працюють по-різному і мають різний ціновий діапазон і ефективність (стійкість до взлому). Все залежить від типу використання біометричних даних. Біометричні системи доступу можуть використовувати біометричні дані таких типів: відбитки пальців, зовнішність людини, геометрія руки, геометрична карта судин долоні, термограма особи, райдужна оболонка ока, сітківка ока, голос та мова, підпис.

Кожна біометрична система може використовувати як один певний тип, так і декілька типів біометричних даних. Особливу увагу було виділено біометричному методу ідентифікації на основі відбитків пальців та на основі фото, так як даний методи являються домінуючим на корпоративному ринку.

РОЗДІЛ 3
СТВОРЕННЯ ПРОТОТИПУ СИСТЕМИ ДЛЯ БІОМЕТРИЧНОГО ЗАХИСТУ ОБ'ЄКТУ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

3.1. Технічне завдання

Згідно з НД ТЗІ 1.6-005-2013 під ***об'єктом інформаційної діяльності будемо розуміти*** інженерно-технічну споруду (приміщення), транспортний засіб, де здійснюється озвучення та/або обробка технічними засобами інформації з обмеженим доступом.

Відповідно до ГОСТ 34.602- 89 технічне завдання на автоматизовані системи (АС) виглядає наступним чином:

1. Загальні відомості

- повне найменування системи та її умовне позначення – «Система біометричного захисту об'єкту інформаційної діяльності»;

- найменування розробника/замовника системи – Національний авіаційний університет;

2. Призначення системи

Система призначена для створення біометричних шаблонів на основі біометричних характеристик і подальшого біометричного розпізнавання за допомогою створених шаблонів.

Система повинна поширюватися у вигляді бібліотеки динамічного компонування з мінімумом додаткових залежностей, яка містить всі функції, необхідні для інтеграції сервісів біометричної ідентифікації і перевірки в інші програмні продукти.

3. Вимоги до системи

Система повинна містити кілька модулів з різним функціоналом:

• Основні поняття - базова інформація про алгоритми, структури і контейнери.

• Виявлення - орієнтоване на виявлення облич людей в анфас.

• Відстеження - дозволяє відстежувати обличчя в відеопотоці.

• Визначення ключових точок - визначення 68 ключових точок обличчя.

• Розпізнавання - технологія біометричного розпізнавання, заснована на методах глибокого навчання.

• Портретні характеристики - деякі популярні характеристики обличчя, такі як різкість, освітлення, геометричні властивості та інші.

• Верифікація живої людини - електронний інструмент або метод, який перевіряє, чи належить взятий біометричний зразок живій людині. Така технологія допомагає запобігти так званий «спуфінг», наприклад використання раніше зроблених фотозображень, голосових записів або відеофайлів для перевірки.

3.2. Встановлення вимог до системи

Вимоги до програмних засобів

Система повинна підтримувати наступні ОС (тільки 64-розрядні):

- Windows 10, Server 2016 року;

- CentOS 7;

- Ubuntu 18.04.

Вимоги до ОС Windows:

- Microsoft Visual Studio 2013 SP1 ч64 або більш нові версії;

- Microsoft Visual C ++ Redistributable for Visual Studio 2017 x64.

Вимоги до ОС Linux:

- Набір компіляторів GCC 4.8 (або більш нова версія);

- Для CentOS: пакети glibc.i686, initscripts, libgomp;

- Для Ubuntu: пакети Iibc6-i386, ffmpeg, libgtk2.0.

Вимоги до технічних засобів

Для установки системи необхідно дотримуватися наступних них вимог:

Процесор: lntel®Core ™ x64 / lntel®Xeon®x64 з підтримкою набору команд AVX2;

- Оперативна пам'ять: не менше 8 GB;

- Жорсткий диск: не менше 10 GB;
- USB порт (для локального ключа HASP);
- Ethernet з'єднання (якщо використовується ключ Net HASP).

Вимоги до вхідних даних

Підтримуються наступні формати файлів зображень:

- Формати Windows - .bmp;
- файли JPEG - .jpeg, .jpg;
- Portable Network Graphics - -png;
- формати .pbm, .pgm, .ppm;
- формати SUN- .sr, .ras;
- файли TIFF - .tiff, .tif.

Підтримуються наступні формати відео:

- CentOS - *.MJPEG;
- Ubuntu - всі формати, підтримувані ffmpeg, встановлені в ОС;
- Windows - всі формати, підтримувані FFmpeg 3.x;
- файли QuickTime- *.mov.

3.3. Архітектура системи

Всі дані отримані системою управління доступом (дані про всі проходи - час, дата, П.І.Б. та посада працівника або відвідувача) повинні зберігатися в одному місці, тобто в одній базі даних. З вищесказаного можна зробити висновок, що найбільш відповідною архітектурою для розроблюваної системи буде архітектура клієнт-сервер (рис. 3.1).

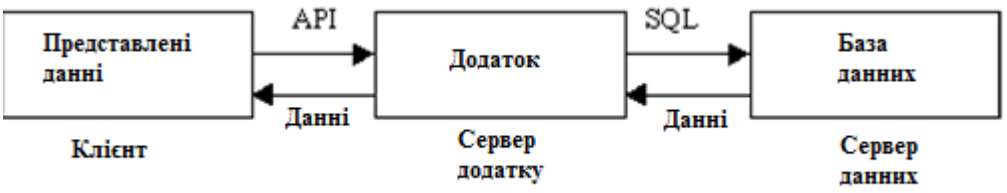

Рис. 3.1. Архітектура клієнт-сервер

Основними критеріями, що висуваються до інформаційної БД є:

– простота і зручність в створенні БД і подальшій роботі з нею;

– доступ до будь-якої інформації, а також оперативно змінювати інформацію в БД;

– відображення результатів пошуку потрібної інформації;

У базі даних будуть міститися відомості:

– про рівень доступу (номер доступу);

– про робоче місце (номер кабінету);

– про користувачів (П.І.Б., адреса, телефон, фото, відбитки пальців, паспортні дані, дата народження);

– про перехід (час проведений, перехід з, перехід в, індикатор вдалого переходу, причина заборони, час входу, час виходу);

– про кімнату (номер кімнати, рівень доступу);

– про поверхи (номер поверху);

– про будівлю (адреса, номер будинку);

Оскільки створюється реляційна БД, то виділення об'єктів предметної області - це один з важливих етапів проектування БД.

Процес моделювання полягає у виділенні сутностей ПЗ, установлення властивостей виділених сутностей і виявлення існуючих між ними зв'язків. На основі проведеного аналізу предметної області була побудована ER–діаграма (рис. 3.2).

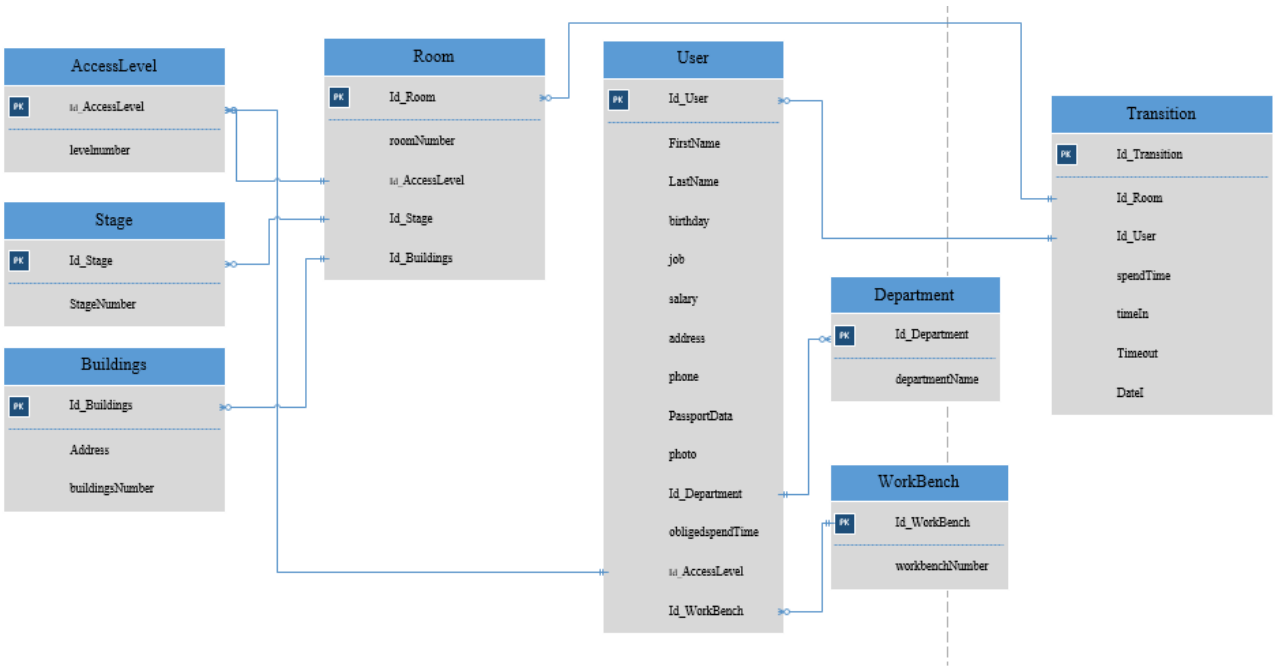

Рис. 3.2. ER-Діаграма

Процес виділення інформаційних об'єктів предметної області може здійснюватися двома підходами: аналітичним і інтуїтивним.

Аналітичний підхід - спочатку визначаються основні завдання, для вирішення яких будується база, виявляються сукупність даних і різних відомостей про об'єкти і процеси, що характеризують дану область, перелік документів, що містять ці дані. Основним джерелом даних є довідкові, планові і оперативно - облікові документи, і, визначивши склад і структуру інформаційного об'єкта, створюємо зв'язку між ними.

Інтуїтивний підхід - відразу встановлюються типові об'єкти предметної області та їх взаємозв'язку.

В отриманих об'єктах всі описові реквізити логічно пов'язані. Також, в проектовану БД необхідно ввести ще: «Відділ», «Рівень доступу», «Робоче місце», «Користувач», «Перехід», «Кімната», «Поверх» і «Будівля» описані в таблицях 3.1-3.8.

Таблиця 3.1

Опис таблиці «Department»

Ім'я стовпця	***Тип***	***Обмеження***	***Призначення***
Id_Department	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор групи користувачів.
departmentName	Varchar(255)	not null	Назва відділу

Таблиця 3.2

Опис таблиці «AccessLevel»

Ім'я стовпця	***Тип***	***Обмеження***	***Призначення***
Id_AccessLevel	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор рівня доступу.
Levelnumber	bigint(20)	not null	Рівень доступу до кімнаті

Таблиця 3.3

Опис таблиці «WorkBench»

Ім'я стовпця	***Тип***	***Обмеження***	***Призначення***
Id_WorkBench	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор робочого місця.
workbenchNumber	bigint(20)	not null	Номер приміщення – що є робочим місцем

Таблиця 3.4

Опис таблиці «User»

Ім'я стовпця	***Тип***	***Обмеження***	***Призначення***
Id_User	int	not null	Первинний ключ, унікальний ідентифікатор працівника.
FirstName	Varchar(255)	not null	ім'я співробітника
LastName	Varchar(255)	not null	Прізвище співробітника
Birthday	Date	not null	дата народження
Job	Varchar(255)	not null	Посада співробітника
Salary	Bigint(20)	not null	Ставка
Address	Varchar(255)	not null	Домашня адреса
Phone	Varchar(10)	not null	Телефон
PassportID	Varchar(10)	not null	Серія та номер паспорта
Photo	Varchar(255)	not null	Шлях до фотографії на сервері
Fingerprint	Varchar(255)	not null	Шлях до фотографії з відбитком пальців
Id_Department	bigint(20)	not null	Ідентифікатор групи користувачів.
obligedspendTime	Bigin(20)	not null	Обов'язкове час проведений на робочому місці
obligedspendTime	bigint(20)	not null	Ідентифікатор рівня доступу.
Id_WorkBench	bigint(20)	not null	Ідентифікатор робочого місця.

Таблиця 3.5

Опис таблиці «Transition»

Ім'я	***Тип***	***Обмеження***	***Призначення***

стовпця			
Id_Transition	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор проходу.
Id_Room	bigint(20)	not null	Ідентифікатор приміщення.
Id_User	bigint(20)	not null	Ідентифікатор працівника.
spendTime	Bigint(20)		Проведений час в приміщенні
timeIn	Date	not null	час входу
Timeout	Date	not null	час виходу
DateI	Date	not null	День проходу

Таблиця 3.6

Опис таблиці «Room»

Ім'я стовпця	***Тип***	***Обмеження***	***Призначення***
Id_Room	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор приміщення.
roomNumber	Int(11)	not null	Номер кімнати
Id_AccessLevel	Int(11)	not null	Рівень доступу
Id_Stage	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор поверху.
Id_Buildings	bigint(20)	not null	Унікальний ідентифікатор лікарняного.

Таблиця 3.7

Опис таблиці «Stage»

Ім'я стовпця	***Тип***	***Обмеження***	***Призначення***
Id_Stage	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор поверху.
StageNumber	Int(11)	not null	Номер поверху

Таблиця 3.8

Опис таблиці «Buildings»

Ім'я стовпця	***Тип***	***Обмеження***	***Призначення***
Id_Buildings	bigint(20)	not null	Первинний ключ, унікальний ідентифікатор корпусу.
Address	Varchar(255)	not null	Адреса корпусу.
buildingsNumber	Int(11)	not null	Номер корпусу

Лістинг коду створення таблиці "User"

```
Create table USER (
ID_User int Primary Key,
First name varchar (255) Not Null,
Last Name varchar(255) Not Null,
Birthday Date Not Null,
Job Varchar(255)
Salary Bigint(20)
Address Varchar(255)
Phone Varchar(10)
PassportID Varchar(10) Unique,
Photo Varchar(255) Not Null
Fingerprint Varchar(255) Not Null
```

```
ID_Department Bigint(20)
obligedspendTime Bigint(20) Not Null
obligedspendTime Bigint(20) Not Null
Id_WorkBench Bigint(20) Not Null
)
GO
```

3.4. Алгоритми роботи програмного засобу

Наведемо реалізацію біометричної ідентифікації на прикладі ідентифікації по фото.

Мінімальний дозвіл для обличчя на зображенні становить приблизно 35 пікселів на ширину обличчя. Для кращої якості виявлення рекомендується не менше 60 пікселів. Хоча рекомендовано зображення обличчя в анфас, допустимі і деякі відхилення. Відхилення під будь-яким кутом (з вертикального огляду, вгору / вниз або по тангажу) від позиції в анфас має бути не більше 70 градусів. У разі якщо умови освітлення контрольовані, необхідно дотримуватися наступних вимог:

- уникати тіней в області обличчя;

- уникати відблисків на окулярах або блиску шкіри;

- уникати сонячного світла;

- умови освітлення повинні бути аналогічні умовам, при яких проводилися етапи реєстрації та перевірки.

Для будь-якої людини на кожному кадрі модуль надає наступне:

• положення;

• унікальний ID;

• оцінка впевненості (якість зображення особи).

Набір положень з однаковим ID називається треком. Кілька треків можуть відповідати одній людині. Остаточна оцінка достовірності обчислюється за допомогою засобу перевірки осіб.

Алгоритм відстеження заснований на локальних функціях, які називаються двійковими дескрипторами. Ці риси обчислюються по орієнтирам обличчя.

Виконано цей проект за допомогою «Open Source Computer Vision

Library», OpenCV . Так як OpenCV був розроблений для ефектного обчислення і роботи в реальному часі - він ідеально підходить для розпізнавання осіб в реальному часі за допомогою камери.

Щоб створити повний проект по розпізнаванню осіб, ми повинні працювати на 4 різних етапах:

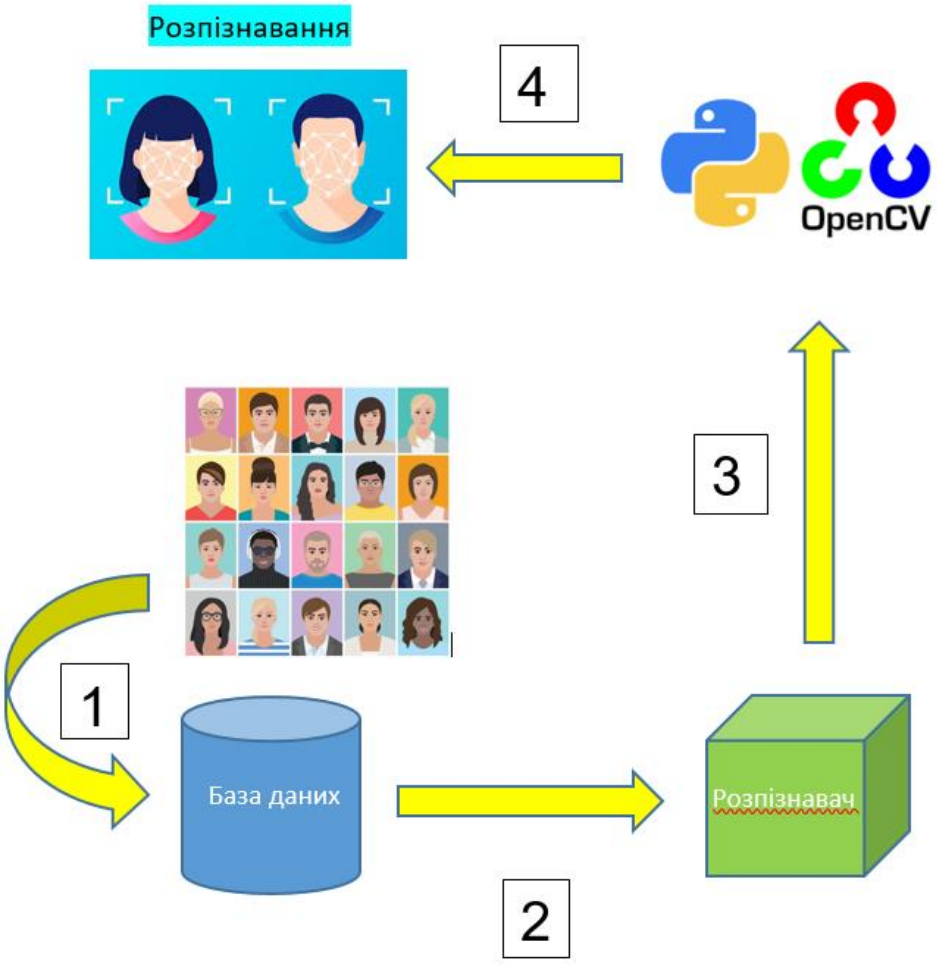

Рис. 3.3 Алгоритм розпізнавання користувача

1 – Збірка даних (фото) облич, які підлягають ідентифікуванню

2 – Передача даних облич та ідентифікатора кожного обличчя в розпізнавач

3 – Опрацювання даних

4 – Розпізнавання

Завантажуємо пакет OpenCV.

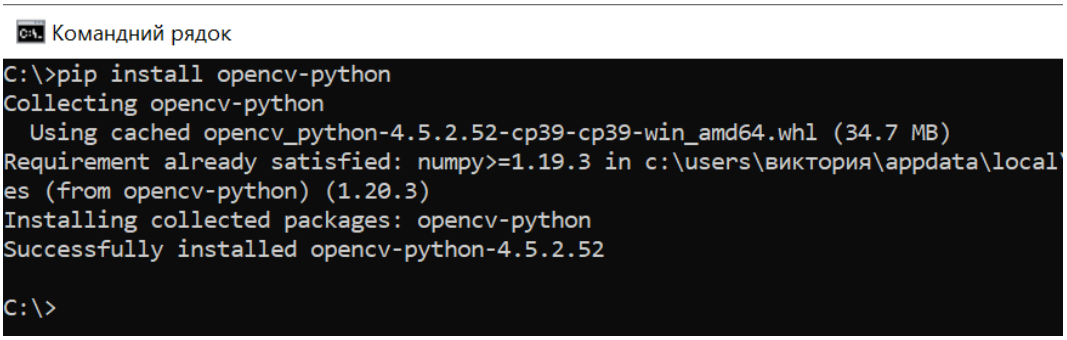

Рис. 3.4 Завантаження бібліотеки OpenCV

Використовуємо програмне забезпечення VisualStudio.

При написанні програмної реалізації використовуємо бібліотеку face_recognition. Face_recognition - бібліотека Python з відкритим вихідним кодом для розпізнавання осіб з глибоким навчанням на основі dlib.

Впровадження face_recognition для реалізації розпізнавання облич:

1. Надаємо зображення (фото) особи, яке хочемо розпізнати і закодувати (кожній людині потрібен тільки один), і складаємо список цих різних кодувань особи. Кодування фактично відображає зображення обличчя в 128-мірний вектор ознак.

2. Opencv відео зчитує і зациклює кожен кадр зображень, 128-мірний вектор ознак кожного кадру кодування зображення і внутрішній продукт кожного вектора в раніше введеному списку кодування бібліотеки осіб.

3. Результатом є виявлення розпізнаного обличчя.

Під час встановлення face_recognition ми отримуємо дві прості програми командного рядка:

- face_recognition - розпізнає обличчя на фотографії або в папці, з фотографіями.
- face_detection - дозволяє знайти місце розташування (піксельні coordinatates) будь-яких осіб в зображенні.

```python
import face_recognition
import cv2
import numpy as np


# Створюємо посилання на веб-камеру (за замовчуванням)
video_capture = cv2.VideoCapture(0)

# Завантажуємо зразок картинки, щоб програма її розпізнала
vika_image = face_recognition.load_image_file("perso1.jpg")
vika_face_encoding = face_recognition.face_encodings(vika_image)[0]

lesha_image = face_recognition.load_image_file("person2.jpg")
lesha_face_encoding = face_recognition.face_encodings(lesha_image)[0]


# Створюємо масиви даних розпізнаних облич
known_face_encodings = [
    lesha_face_encoding,
    vika_face_encoding
    ]
known_face_names = [
    "Alexey",
    "Viktoria"
]
```

Рис. 3.5 Фрагмент коду для реалізації розпізнавання облич

OpenCV циклічно зчитує кожне зображення кадру в відео, кодує його та визначає аналогічне зчитування по внутрішньому продукту один за іншим з вектором ознак з попереднього кодування бібліотеки осіб відповідно до граничних значень та визначає, чи це одна і та ж особа.

Завантажуємо фото особи, яка буде підлягати перевірці на ідентифікацію. Перша особа – студент університету, тому йому доступ ми маємо відкрити.

Рис. 3.6. Зразок фото першої особи, яка підлягає перевірці

Наступним кроком буде створення масивів відомих кодувань облич та імен осіб, які підлягають ідентифікації та ініціалізації змінних. (див. Додаток А)

Результат виконання програми:

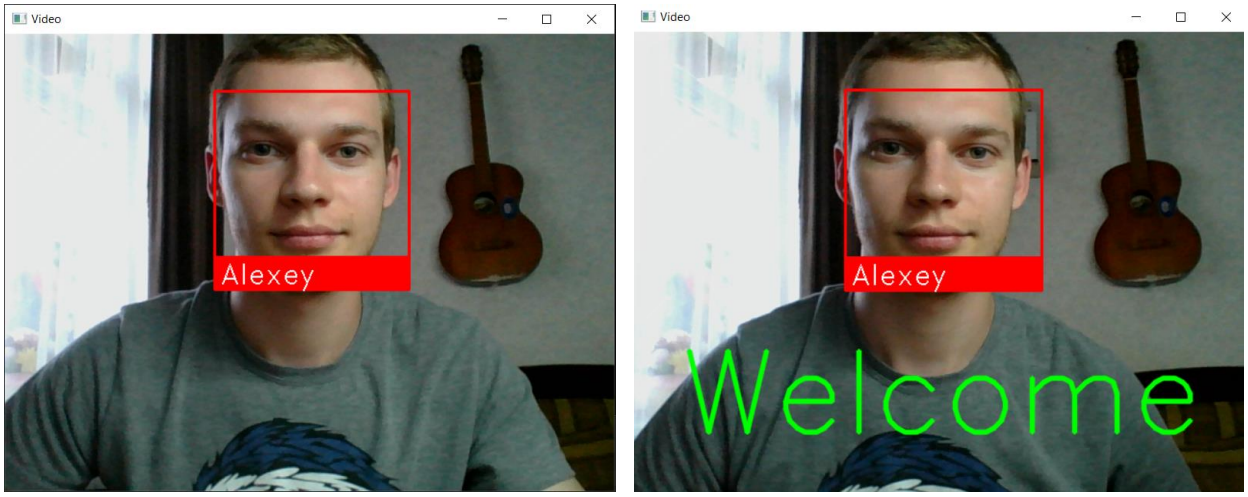

Рис. 3.7 Розпізнавання особи та надання доступу до інф. об’єкту

Як бачимо, робота програми є коректною, так як розпізнавання успішне. Суб’єкту (Alexey), фото якого ми внесли в базу, доступ до інформаційного об’єкту надається.

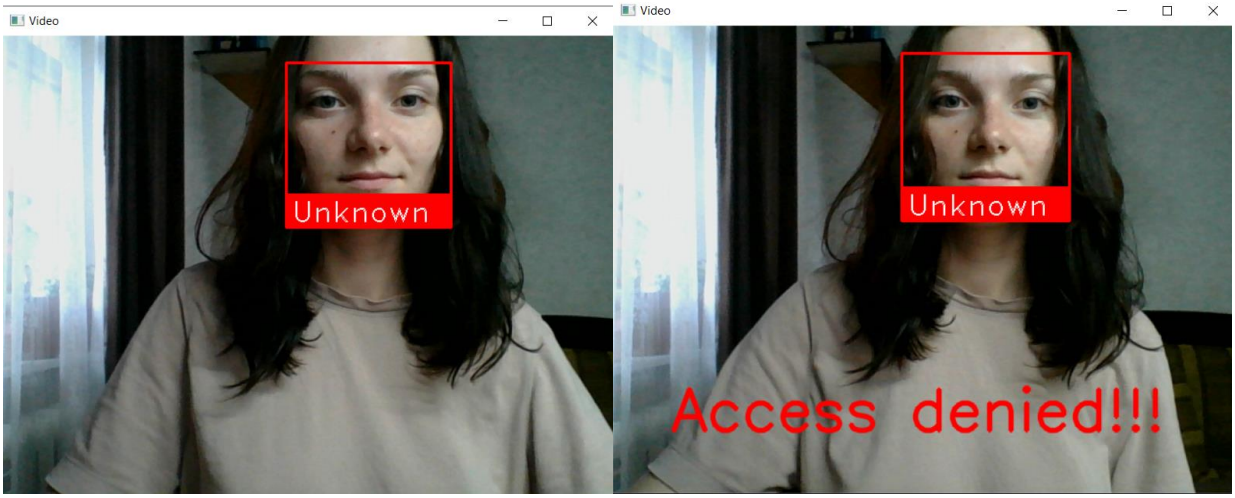

Рис. 3.8 Помилка в розпізнаванні та заборона доступу до об'єкту

В даному випадку, наведено приклад ситуації, коли особи в базі немає (тобто не завантажене зображення, по якому можна було б ідентифікувати особу). Тому даному суб’єкту, якого в базі інформаційного об’єкту немає - в доступі навпаки відмовлено.

Спробуємо внести вищезгадану особу (Unknown) до бази інформаційного

об’єкту та надати доступ до неї. Аналогічно як і з першою персоною, завантажуємо фото в базу інформаційного об’єкту. Тепер, досі невідома особа – студентка НАУ (Viktoria). Вносимо необхідну інформацію та запускаємо програму знову – для розпізнавання осіб.

Рис. 3.9 Зразок фото другого суб'єкта, якого потрібно внести в базу

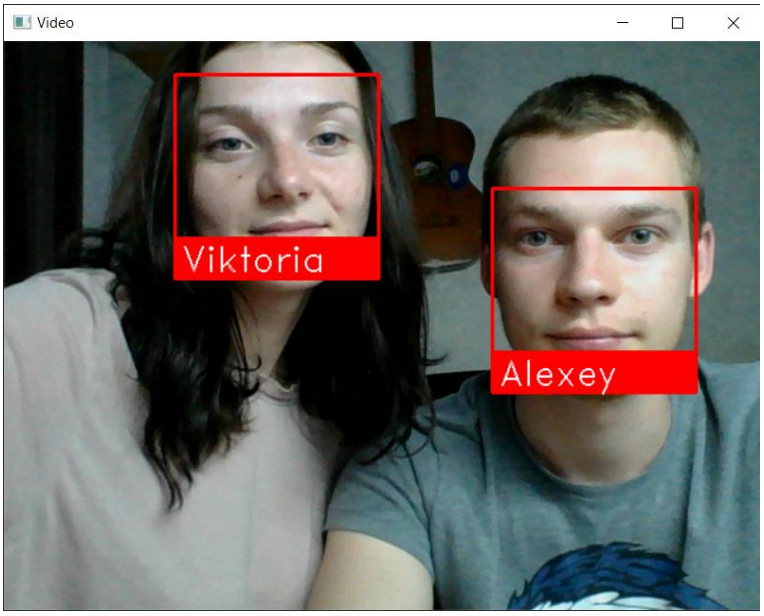

Рис. 3.10 Успішне розпізнавання облич, занесених в базу

Результатом виконання програмної реалізації – розпізнавання суб’єктів, які занесені до бази інформаційного об’єкта та надання їм доступу до нього.

Висновки до третього розділу

В даному розділі наведено проектування програмної системи для біометричної ідентифікації особи за її зображенням (фото). Крім цього у розділі описані основні вимоги, які висуваються до системи такого роду та наведено лістинг коду для реалізації основного функціоналу системи.

ВИСНОВКИ

Основним завданням впровадження біометричних технологій у системи контролю доступу є покращення ефективності розпізнавання особи шляхом автоматизації процесу верифікації/ідентифікації. Базові вимоги що висуваються до таких систем – відсутність можливості надання несанкціонованого доступу неуповноваженій особі та мінімальна вірогідність похибок перевірки користувачів, за яких відбувається помилкова відмова у доступі уповноваженим особам. Відносно застарілих систем надання доступу, методи яких оперують паролями та картками, біометричні технології пропонують значно більший степінь захисту.

У дипломній роботі були розглянуті та вирішені такі цілі:

1) Проаналізовано основні стандарти криптографічних протоколів ідентифікації/автентифікації.

2) Розглянуто основні типи біометричних систем.

Біометричні системи за базовими параметрами, які застосовуються в процесі розпізнавання особи, діляться на дві групи - фізіологічні та психологічні (поведінкові). Перша група досліджує наступні унікальні характеристики людини: риси обличчя, структура ока, особливості відбитків пальців і т.п. Параметри, які аналізує друга група біометричних технологій - голос людини, специфіка підпису, особливості введення тексту з клавіатури та інші.

3) Що дозволило більш якісно розглянути використання та роботу біометричних систем ідентифікації. А також виконати аналіз їх переваг та недоліків.

На даний час є безліч біометричних систем, які працюють по-різному і мають різну стійкість до взлому. Біометричні системи доступу можуть використовувати біометричні дані таких типів: відбитки пальців, геометрія особи, геометрія руки, геометрична карта судин долоні, термограма особи, райдужна оболонка ока, сітківка ока, голос і мова, підпис. Біометричні системи можуть використовувати як один певний тип біометричних даних, так і складатися із

декількох типів біометричних даних. Кожна біометрична система в залежності від методу, на якому базується її функціонування, має як свої переваги, так і недоліки. Ознайомившись із основними методами біометричної ідентифікації та їх характеристиками, такими як швидкість процесу ідентифікації, зручність даної процедури з точки зору користувача, вірогідність помилок першого та другого роду, коштовність необхідного обладнання, було проведено аналіз кожної з біометричних систем, внаслідок чого виконана робота, описана в наступному пункті.

4) В результаті спроектовано програмний засіб для біометричної ідентифікації особи за її зображенням.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Пентланд А. Распознавание лиц для интеллектуальных сред // Открытые системы. – 2000. – № 3. – С. 17 – 20.

2. Обработка и анализ изображений в задачах машинного зрения / Ю.В. Визильтер, С.Ю. Желтов, А.В. Бондаренко и др. – М.: Физматкнига, 2015. – 672 с.

3. Кухарев Г.А. Системы распознавания человека по изображению лица / Г.А. Кухарев, Н.Л. Щеголева. – СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2016. – 176 с.

4. Хомяков М.Ю. Принципы построения пакета программ для моделирования систем распознавания изображений лиц / М.Ю. Хомяков, Г.А. Кухарев // Известия СПбГЭТУ «ЛЭТИ». – 2010. – № 7. – С. 41–46.

5. NI Vision Assistant Tutorial [Электронный ресурс]. – Режим доступа: http://www.ni.com/pdf/manuals/372228a.pdf

6. International biometrics and idenity association [Електронний ресурс] – Режим доступу до ресурсу: www.ibia.org.

7. Biolink біометричні системи [Електронний ресурс] – Режим доступу до ресурсу: www.biolink.ru.

8. Biometric terminals add security to a variety of processes [Електронний ресурс] – Режим доступу до ресурсу: www.bioscrypt.com

9. From identity and secure access to biometric identity [Електронний ресурс] – Режим доступу до ресурсу: www.crossmatch.com

10. Everywhere Identity Matters [Електронний ресурс] – Режим доступу до ресурсу: www.identix.com

11. Конахович Г.Ф., Корченко О.Г., Юдін О.К., Захист інформації в мережах передачі даних: Підручник. – К.: Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714с., іл.

12. Сарбуков А. Аутентификация в Компьютерных Системах / А. Сарбуков А. Грушо // Системы безопасности. – 2003. - №5 (53). – С. 25-29.

13. Чепиков О. Особенности применения Двухфакторной аутентификации / О. Чепиков // Информационная безопасность. – 2005. – №3. – С.35-41.

14. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. – М.: ДМК Пресс, 2012. – 544 С.

15. Шрамко В. Н. Защита компьютеров: электронные системы идентификации и аутентификации / В. Н. Шрамко // PCWeek/RE. – 2004. - №12.

16. BioAPI [Електронний ресурс] – Режим доступу до ресурсу: www.bioapi.org

17. Новые системы паролей. [Електронний ресурс] – Режим доступу до ресурсу: www.windows2008.At.Ua.

18. Системы идентификации [Електронний ресурс] – Режим доступу до ресурсу: www.acoder.org

Додаток А

Програмна реалізація розпізнавання та ідентифікації осіб

```
import face_recognition
import cv2
import numpy as np


# Створюємо посилання на веб-камеру (за замовчуванням)
video_capture = cv2.VideoCapture(0)

# Завантажуємо зразок картинки, щоб програма її розпізнала
vika_image = face_recognition.load_image_file("perso1.jpg")
vika_face_encoding = face_recognition.face_encodings(vika_image)[0]

lesha_image = face_recognition.load_image_file("person2.jpg")
lesha_face_encoding = face_recognition.face_encodings(lesha_image)[0]


# Створюємо масиви даних розпізнаних облич
known_face_encodings = [
    lesha_face_encoding,
    vika_face_encoding
    ]
known_face_names = [
    "Alexey",
    "Viktoria"
]
```

```
while True:
    # Запускаємо зчитування по веб-камері
    ret, frame = video_capture.read()

    # Змінюємо розмір кадру відео до 1/4 для швидшої обробки розпізнавання облич
    small_frame = cv2.resize(frame, (0, 0), fx=0.25, fy=0.25)

    # Перетворюємо зображення з кольору BGR (який використовує OpenCV) на колір RGB (який використовує розпізнавання обличчя)
    rgb_small_frame = small_frame[:, :, ::-1]

    # Оброблюємо лише кожен другий кадр відео, щоб заощадити час
    if process_this_frame:
        # Знаходимо усі обличчя та кодування облич у поточному кадрі відео
        face_locations = face_recognition.face_locations(rgb_small_frame)
        face_encodings = face_recognition.face_encodings(rgb_small_frame, face_locations)

        face_names = []
        for face_encoding in face_encodings:
            # Перевіряємо, чи відповідає особа відомому обличчю
            matches = face_recognition.compare_faces(known_face_encodings, face_encoding)
            name = "Unknown"

            # Порівняємо список кодувань осіб з відомим кодуванням і отримаємо Евклідову відстань для кожної порівнювальної особи
            # Відстань говорить вам, наскільки схожі особи
            face_distances = face_recognition.face_distance(known_face_encodings, face_encoding)
            best_match_index = np.argmin(face_distances)
            if matches[best_match_index]:
                name = known_face_names[best_match_index]

            face_names.append(name)

    process_this_frame = not process_this_frame
```

Продовження додатку А

```
    # Відображуємо результати
    for (top, right, bottom, left), name in zip(face_locations, face_names):
        # Масштабуємо резервні копії місць обличчя, оскільки кадр, який ми виявили, був зменшений до 1/4 розміру
        top *= 4
        right *= 4
        bottom *= 4
        left *= 4


        # Намалюємо квадрат навколо обличчя
        cv2.rectangle(frame, (left, top), (right, bottom), (0, 0, 255), 2)


        # Намалюємо ярлик з іменем під обличчям
        cv2.rectangle(frame, (left, bottom - 35), (right, bottom), (0, 0, 255), cv2.FILLED)
        font = cv2.FONT_HERSHEY_DUPLEX
        cv2.putText(frame, name, (left + 6, bottom - 6), font, 1.0, (255, 255, 255), 1)

        # Перевіряємо чи допущена особа
        if (face_encoding == known_face_names):
            frame = cv2.putText(frame, 'Welcome', (50, 415), cv2.FONT_HERSHEY_SIMPLEX, 4, (0, 255, 0), 4, cv2.LINE_AA)
        else:
            frame = cv2.putText(frame, 'Access denied!!!', (60, 415), cv2.FONT_HERSHEY_SIMPLEX, 2, (0, 0, 255), 3, cv2.LINE_AA)

    # Відображуємо отримане зображення
    cv2.imshow('Video', frame)


    # Натискаємо "q" на клавіатурі, щоб вийти!
    if cv2.waitKey(1) & 0xFF == ord('q'):
        break

video_capture.release()
cv2.destroyAllWindows()
```