Харківський національний університет імені В.Н. Каразіна
Факультет комп'ютерних наук
Безпека інформаційних систем і технологій

«Допущено до захисту»

Зав.кафедрою БІСТ

Сватовський І.І._____
« » червня 2023р.

Пояснювальна записка
до кваліфікаційної роботи бакалавра
спеціальність: 125 Кібербезпека

на тему: «Автентифікація за допомогою біометричних даних»

оцінка « »

Голова ЕК

Лемешко О.В._____

Керівник доц.Мелкозьорова О.М.
(прізвище та ініціали/підпис)

Рецензент Д.т.н Краснобаєв В.А.
(прізвище та ініціали/підпис)

Виконавець студент групи КБ-42

Юрченко В.А.
(прізвище та ініціали/підпис)

Харків – 2023

РЕФЕРАТ

Структура роботи: робота складається з вступу, трьох розділів, а саме теоретичного огляду, розробки та тестування програми системи ідентифікації за відбитками пальців, висновку, списку використаних джерел та додатків. Текстовий матеріал, який утримує основний зміст роботи, представлений на 49 сторінках.

Мета роботи: визначення особливостей біометричної ідентифікації за відбитками пальців, розробка та тестування власної системи.

Методи дослідження і апаратура: Для досягнення мети дослідження та виконання поставлених завдань було застосовано наступні методи дослідження:

- теоретичні (аналіз, порівняння, узагальнення та систематизація інформації з наукової літератури);
- ПК з необхідним програмним забезпеченням;
- Сканер відбитків пальців.

Результати роботи та їх новизна: В ході дослідження було встановлено, що використання біометричної системи ідентифікації на основі відбитків пальців є ефективним методом розпізнавання особи. Була розроблена власна система ідентифікації, яка проявила високу точність в ідентифікаційних процесах. Оригінальністю цієї роботи є використання алгоритму глибинного навчання для розпізнавання відбитків пальців.

Теоретична значущість дослідження: полягає у вивченні фундаментальних принципів і методів розпізнавання особи на основі відбитків пальців. Це дозволяє розробляти більш точні та надійні алгоритми та моделі для ідентифікації людей, що має важливе значення в багатьох галузях, таких як безпека, правоохорона, медицина та банківська справа.

Практична значущість дослідження: ще більш вагома, оскільки цей метод ідентифікації вже широко застосовується в різних сферах життя. Наприклад, системи контролю доступу на підприємствах, в установах охорони здоров'я, в аеропортах, на митницях та інших місцях використовуються для ідентифікації працівників, пасажирів та інших осіб.

Припущення про можливі напрямки розвитку або продовження досліджень, що були виконані: У подальшому можна провести подальші дослідження у сфері біометричної ідентифікації, зосередившись на розробці нових алгоритмів обробки зображень та методів визначення схожості відбитків пальців. Крім цього, розглянути можливість використання інших біометричних характеристик, таких як відбитки обличчя, з метою досягнення більш точної ідентифікації користувачів.

Ключові слова: БІОМЕТРИЧА СИСТЕМА ІДЕНТИФІКАЦІЇ, АУТЕНТИФІКАЦІЯ, БЕЗПЕКА, РОЗПІЗНАВАННЯ, ПОВЕДІНКА, ВІДБИТКИ ПАЛЬЦІВ, АЛГОРИТМИ ОБРОБКИ, ТОЧНІСТЬ ІДЕНТИФІКАЦІЇ, БЕЗПЕКА.

ABSTRACT

Work structure: The work consists of an introduction, three sections, namely theoretical overview, development and testing of a fingerprint identification system program, conclusion, list of references and appendices. The main text of the work is presented in 49 pages.

Work objective: to determine the peculiarities of biometric identification using fingerprints, to develop and test our own system.

Research methods and equipment: To achieve the research objective and tasks, the following research methods were used:

- theoretical (analysis, comparison, generalization, and systematization of information from scientific literature);

- personal computers with necessary software;

- fingerprint scanner.

Results of the work and their novelty: During the research, it was determined that using a biometric identification system based on fingerprints is an effective method of person recognition. A proprietary identification system was developed, demonstrating high accuracy in the identification processes. The novelty of this work lies in the utilization of deep learning algorithms for fingerprint recognition.

The theoretical significance of the research lies in studying the fundamental principles and methods of person recognition based on fingerprints. This allows for the development of more accurate and reliable algorithms and models for identifying individuals, which is of great importance in many fields such as security, law enforcement, medicine, and banking.

Practical significance of the research is even more substantial, as this method of identification is already widely used in various spheres of life. For example, access

control systems in enterprises, healthcare facilities, airports, customs and other places are used for identifying employees, passengers, and other individuals.

Assumptions regarding possible directions for future research: In the future, further research can be conducted in the field of biometric identification, focusing on the development of new image processing algorithms and methods for determining the similarity of fingerprint patterns. Additionally, the possibility of utilizing other biometric characteristics, such as facial recognition, can be considered to achieve more precise user identification.

Keywords: BIOMETRIC IDENTIFICATION SYSTEM, AUTHENTICATION, SECURITY, RECOGNITION, BEHAVIOR, FINGERPRINTS, PROCESSING ALGORITHMS, IDENTIFICATION ACCURACY, SECURITY.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

Init	запуск периферійних систем та системи обробки переривань
Handshake	перевірка стану сканера
GetImage	ініціювання процесу отримання зображення відбитку пальця зі сканера
DrawImage	відображення зображення на LCD дисплеї за допомогою функції виводу
Interpolate	функція, яка виконує інтерполяцію зображення
Filtering	застосування фільтра Лапласа для фільтрації зображення
ReInit	функція автоматичної переініціалізації системи при виявленні помилки в роботі
CheckUSART	функція автоматичної переініціалізації блоку USART
CheckDMA	функція автоматичної переініціалізації блоку DMA
ErrorMessage	функція передачі повідомлення про аварійне завершення роботи системи
end	завершення виконання програми

ВСТУП

На даний момент все більше зростає потреба у забезпеченні безпеки та захисту інформації, що призводить до складних викликів, пов'язаних з ідентифікацією особи. Біометричні системи ідентифікації стають дедалі популярнішими у реалізації цієї мети в сучасних умовах. Зокрема, біометрична система ідентифікації за відбитками пальців є однією з найбільш поширених та ефективних технологій, яка дозволяє точно визначати особу за її унікальним відбитком пальця.

Щоб оцінити сучасний стан проблеми, проведено аналіз вітчизняної та зарубіжної науково-технічної літератури та патентного пошуку, що дозволило виявити як практично вирішені завдання, так і існуючі прогалини знань у цій предметній галузі. З'ясовано, які провідні фірми, вчені та спеціалісти працюють у даній галузі, а також проаналізовано світові тенденції вирішення схожих задач.

Біометрична ідентифікація за відбитками пальців є однією з найбільш точних і надійних методів ідентифікації особи. Це метод, який використовує особливості геометричної будови рук, відбитків пальців, а також інших біометричних характеристик для ідентифікації особи.

Актуальність дослідження біометричної ідентифікації за відбитками пальців полягає в тому, що цей метод використовується в багатьох галузях, таких як безпека, медицина, соціальна сфера, фінанси тощо. Застосування біометричної ідентифікації за відбитками пальців дозволяє ефективно вирішувати завдання з ідентифікації особи та підтвердження її прав на доступ до різних ресурсів.

Однак, на жаль, існують певні проблеми з біометричною ідентифікацією за відбитками пальців, такі як можливість зламування та підробки даних. Тому дослідження у цій галузі має велике значення, щоб знайти способи покращення та захисту біометричних систем від небажаних втручань.

Отже, дослідження біометричної ідентифікації за відбитками пальців має велике значення у сучасному світі, тому що цей метод є надійним та ефективним, але також має свої недоліки, які потрібно вирішувати.

Біометрична ідентифікація за відбитками пальців є ефективним та надійним способом ідентифікації людей, який може бути успішно використаний в різних сферах, таких як охорона здоров'я, правоохорона, банківська справа та інші.

У наукових дослідженнях, пов'язаних з біометричною ідентифікацією за відбитками пальців, досліджувалися різні аспекти цієї технології. Наприклад, досліджувалася точність і надійність різних алгоритмів обробки відбитків пальців, розроблялися нові методи збору та обробки біометричних даних, а також вивчалися можливості застосування цієї технології в різних сферах, таких як фінансові послуги, медицина, безпека тощо.

Крім того, біометрична ідентифікація за відбитками пальців також вивчалася в контексті захисту персональних даних та приватності. Дослідження показали, що використання цієї технології може становити загрозу для приватності особи, якщо не забезпечувати відповідний рівень захисту даних та контроль над їх використанням. Тому, дослідження в цій області також спрямовані на розробку та вдосконалення механізмів захисту персональних даних в біометричних системах ідентифікації за відбитками пальців.

1 ТЕОРЕТИЧНІ АСПЕКТИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ЗА ВІДБИТКАМИ ПАЛЬЦІВ

1.1 Огляд біометричних технологій ідентифікації

Біометрична ідентифікація за відбитками пальців – це процес визначення особи, що ґрунтується на унікальності папілярних ліній та точок на поверхні пальців. Цей метод є одним з найбільш поширених у біометричній ідентифікації людини [8]. Велика кількість наукових праць присвячена теоретичним аспектам цієї технології, які пов'язані з розробкою та вдосконаленням біометричних систем ідентифікації за відбитками пальців. Однією з головних теоретичних проблем є відображення папілярних ліній та точок на поверхні пальців у вигляді математичних моделей, які можуть бути збережені та використані для порівняння з іншими відбитками пальців [6]. Крім того, важливо вирішувати проблему захисту біометричних даних від незаконного доступу та зберігання їх у надійному місці.

Біометрична ідентифікація за відбитками пальців – це процес використання унікальної структури папіллярних ліній на пальцях для ідентифікації людини [32]. Відбитки пальців вважаються одним з найбільш надійних біометричних ідентифікаторів, оскільки кожна людина має унікальну структуру папіллярних ліній на пальцях, яка не змінюється протягом життя.

Процес біометричної ідентифікації за відбитками пальців зазвичай включає наступні кроки:

1) Збір відбитків пальців: цей процес включає сканування папіллярних ліній на поверхні пальців за допомогою спеціального сканера або приладу.

2) Обробка відбитків пальців: після збору відбитків пальців, дані переходять до комп'ютера, де вони обробляються та аналізуються для виявлення унікальних рис.

3) Порівняння з базою даних: отримані дані порівнюються зі збереженою базою даних відбитків пальців для встановлення ідентичності або невідповідності.

Біометрична ідентифікація за відбитками пальців використовується у багатьох галузях, таких як урядові служби, банківський сектор, аеропорти, в'їзд на території промислових підприємств та багато інших. Вона дозволяє забезпечити високий рівень безпеки та надійності ідентифікації, що дуже важливо в різних сферах діяльності.

Дослідження в галузі біометричної ідентифікації за відбитками пальців, як зарубіжні, так і вітчизняні, мають на меті вирішення теоретичних проблем та поліпшення методів і алгоритмів ідентифікації. Також вони досліджують питання стандартизації, оцінки якості та ефективності біометричних систем ідентифікації за відбитками пальців [22, 31].

Деякі з головних напрямів досліджень в цій галузі включають наступні:

- Розробка нових методів збору та обробки відбитків пальців: дослідники працюють над розробкою нових методів сканування та обробки відбитків пальців, щоб покращити точність та швидкість ідентифікації.
- Вивчення впливу зовнішніх факторів: дослідження в галузі біометричної ідентифікації за відбитками пальців включають вивчення впливу зовнішніх факторів, таких як вік, стать, здоров'я шкіри та інші, на точність та надійність ідентифікації.
- Розробка нових алгоритмів ідентифікації: дослідники працюють над розробкою нових алгоритмів ідентифікації, щоб покращити точність та надійність ідентифікації, особливо в умовах шуму та інших випадкових чинників.
- Розробка стандартів та протоколів: дослідники працюють над розробкою стандартів та протоколів для біометричної ідентифікації за

відбитками пальців, щоб забезпечити сумісність та інтеграцію між різними системами та пристроями.

- Вивчення проблем безпеки: дослідження в галузі біометричної ідентифікації за відбитками пальців включають вивчення проблем безпеки, таких як можливість підробки тощо.

Ця технологія зустрічається дуже часто в банківському секторі, на митницях, в аеропортах та на багатьох інших об'єктах, де використовуються високі вимоги до безпеки [7].

Відбитки пальців представляють собою неповторний біометричний параметр, який можна використовувати для ідентифікації людини. При цьому цифрове збереження відбитків пальців забезпечує їх використання в автоматизованих системах безпеки.

Провідні компанії, які займаються створенням та виробництвом біометричних систем ідентифікації за відбитками пальців, грають важливу роль в розвитку цієї галузі. Біометричні технології ідентифікації є одними з найбільш ефективних і надійних методів визначення особистості. Ці технології базуються на використанні неповторних біологічних особливостей людини, таких як відбитки пальців, обличчя, структура рогівки, голос і т.д. Відбитки пальців є одними з найпоширеніших і найнадійніших біометричних характеристик.

Узагальнюючи, з технічної точки зору, можна стверджувати, що існують різноманітні біометричні технології ідентифікації, які використовують різноманітні біологічні характеристики людини. Наприклад, для розпізнавання особи за обличчям використовуються комп'ютерні системи, які досліджують різні параметри, такі як форма, розмір та риси обличчя. Для ідентифікації особи за голосом використовуються системи, які аналізують звукові характеристики голосу, зокрема тональність та частоту.

Однак, на практиці, системи ідентифікації за відбитками пальців є найбільш поширеними та надійними, через їхню простоту та достатню точність. Дані системи використовують для контролю доступу, ідентифікації злочинців, а також для розблокування різноманітних пристроїв, таких як смартфони чи банківські рахунки.

Під час дослідження ідентифікації людини за допомогою відбитків пальців виявлено, що однією з найголовніших проблем є підробка відбитків, для якої можуть використовуватися різні методи. Оптичні сканери та сканери на основі відбивання з використанням ультразвукових хвиль є найбільш поширеними технологіями збору відбитків пальців, причому оптичні сканери є більш доступними і дешевшими. Сканери на основі відбивання з використанням ультразвукових хвиль використовуються у випадках, коли необхідна вища точність та якість зображення. При використанні відбитків пальців для ідентифікації людини необхідно забезпечити високий рівень захисту інформації та персональних даних, що досягається за допомогою різних методів шифрування та зберігання даних для запобігання несанкціонованому доступу [10].

Отже, незважаючи на безліч різних систем біометричної ідентифікації, системи на основі відбитків пальців є найбільш поширеними та ефективними.

1.2 Відбитки пальців як біометрична характеристика

Відбитки пальців є популярною біометричною характеристикою для ідентифікації людини. Кожна особа має унікальні відбитки пальців, які формуються через складну геометрію поверхні шкіри. Спеціальні сканери зчитують та аналізують риси відбитків, такі як глибина борозен, контурні лінії, розміри чи форма. Відбитки пальців є надійною та зручною біометричною характеристикою для різних застосувань, від логіна на комп'ютері до контролю

доступу до важливих об'єктів та фінансових операцій, а їхній паттерн визначається ще в утробі матері.

Відбитки пальців є зручним та надійним методом біометричної ідентифікації, який широко використовується в правоохоронних органах, банках та інших сферах. Вони стійкі до зносу, не змінюються з часом і не піддаються підробці [13, 25, 35, 36]. Системи ідентифікації за відбитками пальців зазвичай працюють на основі сканування папірних або електронних відбитків пальців та порівняння їх з відбитками пальців у базі даних.

Проте, є деякі недоліки, наприклад, можливість підробки відбитків пальців та необхідність достатньої якості відбитків для точної ідентифікації. Крім того, системи ідентифікації за відбитками пальців не завжди ефективні в разі пошкодження шкіри та не гарантують абсолютної точності ідентифікації [1]. Необхідно також забезпечувати високий рівень захисту даних в біометричних системах для уникнення можливих крадіжок або злому.

Біометричні системи ідентифікації за відбитками пальців зазвичай не зберігають самі відбитки, а замість цього створюють математичні описи їх особливостей, щоб захистити персональні дані користувачів і забезпечити їх конфіденційність.

Крім того, відбитки пальців можуть використовуватися для аутентифікації користувачів, а не лише для ідентифікації. У такому випадку система перевіряє, чи співпадає відбиток пальця з тим відбитком, який зберігається в базі даних, що забезпечує ще вищий рівень безпеки. Навіть якщо хакер зламає систему і здобуде доступ до бази даних з відбитками пальців, він не зможе скористатися цим доступом без наявності пальця справжнього власника.

1.3 Класифікація відбитків пальців

Людина може змінювати свої звички, зовнішність та поведінку, але є ознаки, що залишаються незмінними протягом життя, наприклад, відбитки пальців та кровоносних судин очного дна. Ці та інші ознаки можуть бути використані біометричними системами для ідентифікації особи.

Класифікація відбитків пальців – це метод, який дозволяє віднести відбиток до певного класу на основі його ознак, що забезпечує подальшу ідентифікацію. Класифікація відбитків пальців є важливою складовою ідентифікації особи за її унікальними характеристиками.

Класифікацію відбитків пальців проводять за типом папілярного узору, існує три основних класи відбитків пальців: дугові, петлеві та звиткові [21].

- Дугові – це відбитки з дугоподібним рисунком. Вони зустрічаються меншою часткою, близько 5% від загальної кількості;
- Петлеві – це відбитки з петлеподібним рисунком. Вони складають більшість, приблизно 65% від загальної кількості;
- Звивисті – це відбитки з звивистим рисунком. Вони також становлять значну частку, близько 35% від загальної кількості.

Кожен з цих класів має декілька підкласів, які можуть допомогти уточнити класифікацію відбитка. Наприклад, дугові відбитки поділяються на радіальні та ульнарні відбитки в залежності від того, чи знаходиться початок дуги в районі кисті руки (ульнарний) або в районі зап'ястя (радіальний). Петлеві відбитки можуть бути одиночними або двократними, а звиткові відбитки можуть бути коловими або спіральними.

Рисунок 1.1 – Основні класи відбитків пальців

Важливо зазначити, що для зображення відбитків пальців необхідно дотримуватись певних стандартів [33, 34]. Зазвичай, використовуються стандарти ANSI, які мають ряд вимог до зображень відбитків. Наприклад, для відповідності вимогам, зображення має бути в форматі TIF із роздільною здатністю не менше 500 пікселів на дюйм і містити 256 рівнів яскравості. Крім того, необхідно, щоб кут нахилу відбитка відносно вертикальної осі складав не менше 15 градусів, а головними типами локальних ознак повинні бути кінцеві точки та точки розбіжності. Виконання цих вимог дозволить отримати якісне та точне зображення відбитка пальця, що забезпечить його ефективну ідентифікацію.

Класифікація відбитків пальців є важливою для правоохоронних органів, банківської та фінансової сфер, а також для різних систем ідентифікації та контролю доступу [17, 19, 20]. Відбитки пальців є унікальними для кожної людини, тому класифікація відбитків пальців є важливим елементом в системах ідентифікації та визначення особи.

1.4 Біометрична ідентифікація за відбитками пальців

Система ідентифікації за відбитками пальців є однією з найбільш вживаних технологій ідентифікації людей у світі. Вона базується на неповторності кількості точок на поверхні пальця [3].

Система ідентифікації за відбитками пальців використовується як у приватному, так і у державному секторі для ідентифікації осіб, забезпечення безпеки та протидії шахраївству [9]. Наприклад, відбитки пальців використовуються для контролю доступу до захищених приміщень, банківських рахунків, мобільних пристроїв, комп'ютерів та інших пристроїв, які містять конфіденційну інформацію.

Також системи ідентифікації за відбитками пальців широко використовуються в правоохоронних органах для ідентифікації злочинців та підозрюваних у вчиненні злочинів. Відбитки пальців можуть бути знайдені на місці злочину та порівняні з базою даних відбитків пальців для знаходження можливих підозрюваних.

Кожен відбиток складається з глибинних ліній та точок, що утворюють унікальний «шаблон» для кожної людини. Така система ідентифікації може бути використана в різних сферах, включаючи безпеку, медицину та фінанси. Вона є швидкою та надійною, що допомагає зменшити помилки та збільшити безпеку. В наш час активно працюють над створенням нових біометричних технологій, які використовують інші фізіологічні ознаки [30]:

- ДНК-порівняння є найновішою біометричною технологією, яка дозволяє безпомилково ідентифікувати особу, крім однояйцевих близнюків, які мають однаковий генотип. Цей метод не пов'язаний з дактилоскопією, яка базується на відбитках пальців. Біометричні системи, які використовують ДНК-порівняння, можуть бути введені в дію лише в майбутньому;
- Відбиток долоні – це біометрична технологія, що використовує розташування ліній на долоні людини, аналогічно відбиткам пальців;
- Судинні рисунки – це розташування вен в різних частинах тіла людини, включаючи зап'ястя і тильну сторону долоні;

- Сигнали, що виробляються серцем (мозком, легенями) – ця біометрична технологія використовує датчик «біодинамічного підпису», на який користувач торкається протягом деякого часу, щоб датчик ідентифікував індивідуальні параметри людини.

Таблиця 1.1 – Основні характеристики методів біометричної ідентифікації

Метод отримання біометричних параметрів	Імовірність відмови у доступі, %	Імовірність помилкової ідентифікації «чужого» (без використання муляжу), %	Імовірність помилкової ідентифікації «чужого» (з використанням муляжу), %	Збереження таємниці образу у процесі ідентифікації абонента	Вартість технічної реалізації в грошовому еквіваленті, у.о.
Геометрична будова руки	0,2 – 4	0,2 – 1	10 – 75	Неможливо приховати	600 – 3000
Відбитки пальців	2 – 6	0,0001	10 – 70	Неможливо приховати	60 – 600

Продовження таблиці 1.1

Особливості малюнка сітківки ока	0 – 4	6 – 10	-	Неможливо приховати	4000
Райдужна оболонка ока	0,2 – 2	0,0001	-	Неможливо приховати	500 – 6000
Портрет обличчя	1 – 9	–	-	Неможливо приховати	55000
Рукописний почерк	0,5 – 5	0,5 – 5	0,5…5	8 – 10 – 10 – 40	–
Клавіатурний та комп'ютерний почерк	3 – 9	3 – 9	–	6 – 10 –10 –12	–
Характеристики і особливості мови	0,5 – 5	0,5 – 5	25 – 90 (запис)	10-16 – 10-30	1 – 60

Метод розпізнавання за формою кисті руки використовується для ідентифікації людей на основі їх біометричної характеристики [28]. Для цього використовуються спеціальні пристрої, які сканують форму кисті руки, декількох її пальців і отримують тривимірний образ. Зібрані дані використовуються для створення унікального відбитка, який служить однозначною ідентифікацією

особи. Існує два підходи до використання геометричних характеристик кисті руки: перший заснований на геометрії самої кисті руки, а другий враховує образні особливості, такі як візерунки на стиках між фалангами пальців та малюнки кровоносних судин.

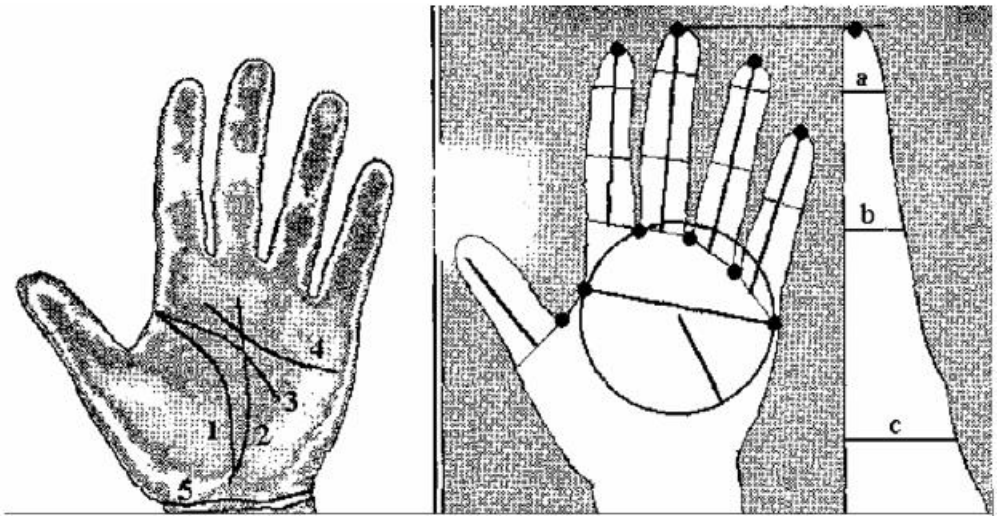

Рисунок 1.2 – Рисунок долоні

На рис. 1.2 показано візерунок на долоні, що є методом ідентифікації. Для цього використовуються п'ять основних ліній на долоні та 17 геометричних ознак руки. Ці ознаки об'єднуються в єдиний вектор значень, який використовується для ідентифікації особи. Під час процесу ідентифікації знімають декілька проекцій руки та формується свій вектор значень для кожної проекції. На основі цих векторів створюється спеціальний клас, де ознаки усереднюються та формуються ознаки еталонного образу. Вихідні образи можуть модифікуватися під час роботи. Для порівняння двох образів використовуються декілька критеріїв, зокрема найменша відстань від досліджуваного образу до еталону. Також можна використовувати складніший метод, який включає аналіз характеристик розмірів та складок шкіри на згинах між фалангами для унеможливлення обдурення пристрою [15].

Розпізнавання за відбитком пальців полягає в тому, що зі сканера отримується зображення відбитку пальця, з якого можна виділити характерні ознаки для ідентифікації. Роздільна здатність сканера дозволяє виділити багато дрібних деталей на поверхні відбитка, але для систем ідентифікації використовуються всього два типи деталей: кінцеві точки, де папілярні лінії закінчуються, та точки розгалуження, де папілярні лінії роздвоюються.

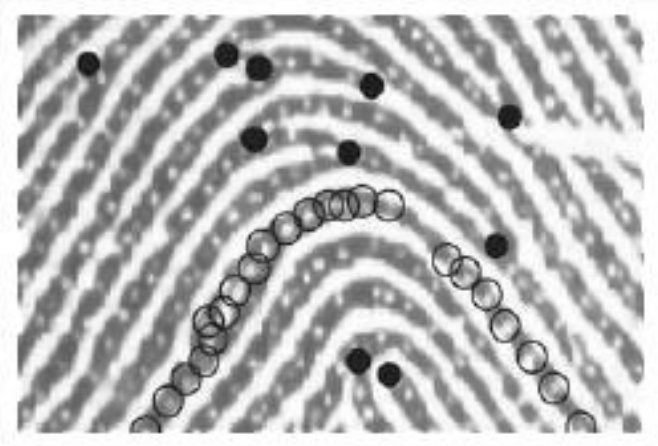

Рисунок 1.3 – Зображення відбитків пальців з позначками пор, точок розгалуження та кінцевих точок

Коли зображення поверхні пальця має роздільну здатність приблизно 1000 dpi, це дозволяє виявити деталі внутрішньої структури папілярних ліній, включаючи пори потових залоз (рис. 1.2, пори позначені порожніми колонками, кінцеві точки і точки розгалуження – чорними колонками). Можна використовувати розташування цих деталей для ідентифікації особи. Проте, цей метод нешироко поширений через складнощі отримання зображень такої високої якості у не-лабораторних умовах.

У процесі автоматизованого розпізнавання відбитків пальців, на відміну від традиційної дактилоскопії, виникає менше проблем, пов'язаних з різними факторами, що можуть впливати на точність розпізнавання [29]. При використанні фарби для отримання відбитків пальців, неможливо повністю

уникнути або максимально зменшити зсув або поворот пальця, зміну тиску, а також зміну якості поверхні шкіри та інші фактори. За допомогою електронних безфарбових сканерів можна отримати зображення відбитку з достатньою якістю для подальшої обробки. Якість отриманого зі сканера зображення папілярного візерунку пальця є ключовим критерієм, який впливає на вибір алгоритму формування згортки відбитку пальця та ідентифікації особи.

Таблиця 1.2 – Реалізація фізіологічних біометричних характеристик

Біометрична характеристика	Реєструючий пристрій	Зразок	Досліджувані риси
Геометрична будова руки	Запатентований настінний пристрій	Тривимірне зображення зверху і з боків кисті	Висота і ширина кісток і суглобів кисті і пальців
Відбиток пальця	Периферійний пристрій комп'ютера, карта стандарту PC card, миша, мікросхема або зчитувальний пристрій у клавіатурі	Зображення відбитку пальців (оптичне, на кремнієвому фотоприймачі, ультразвукове, або безконтактне)	Розташування і напрям гребінчастих виступів і розгалужень на відбитку пальця, дрібні деталі

Висновки до розділу 1

Таким чином, біометрична ідентифікація за відбитками пальців – це процес визначення особи, що ґрунтується на унікальності папілярних ліній та точок на поверхні пальців. Цей метод є одним з найбільш поширених у біометричній

ідентифікації людини. Дослідження в галузі біометричної ідентифікації за відбитками пальців, як зарубіжні, так і вітчизняні, мають на меті вирішення теоретичних проблем та поліпшення методів і алгоритмів ідентифікації.

Відбитки пальців представляють собою неповторний біометричний параметр, який можна використовувати для ідентифікації людини.

Узагальнюючи, з технічної точки зору, можна стверджувати, що існують різноманітні біометричні технології ідентифікації, які використовують різноманітні біологічні характеристики людини.

Система ідентифікації за відбитками пальців є однією з найбільш вживаних технологій ідентифікації людей у світі. Вона базується на неповторності кількості точок на поверхні пальця. Кожен відбиток складається з глибинних ліній та точок, що утворюють унікальний «шаблон» для кожної людини.

Розпізнавання за відбитком пальців полягає в тому, що зі сканера отримується зображення відбитку пальця, з якого можна виділити характерні ознаки для ідентифікації.

2 ОСОБЛИВОСТІ ВИКОРИСТАННЯ ВІДБИТКІВ ПАЛЬЦІВ ДЛЯ ІДЕНТИФІКАЦІЇ ОСОБИ

2.1 Робота біометричної системи ідентифікації за відбитками пальців

На сьогодні ідентифікація за відбитками пальців є найпоширенішою біометричною технологією. За даними International Biometric Group, понад 48% усіх біометричних систем, що використовуються в світі, ґрунтуються саме на розпізнаванні відбитків пальців. Прогнозується, що обсяг продажів таких систем з часом тільки збільшуватиметься [37].

Складно визначити коли з'явилося використання відбитків пальців для ідентифікації. Археологи, які проводять розкопки, часто знаходять зображення відбитків пальців на камені, але не можна з упевненістю стверджувати, що на початку вони використовувалися саме для цієї мети.

У давнину вже використовували відбитки пальців для створення глиняних табличок і печаток в Давньому Вавилоні та Китаї, а в Персії в XIV столітті вони використовувались для підписування державних документів. Це підтверджує той факт, що навіть тоді було зрозуміло, що відбиток пальця є унікальною особливістю людини, яку можна використовувати для її ідентифікації.

Наступним кроком у розвитку технології було застосування відбитків пальців у криміналістиці. У середині XIX століття виникли перші припущення щодо унікальності відбитків кожної людини та методів їх класифікації залежно від різних ділянок папілярного візерунка. Це призвело до створення "системи Генрі" [2] в 1897 році, яка була першою системою класифікації відбитків пальців, розробленою Едвардом Генрі, англійським науковцем під час його перебування в Індії.

До кінця XIX століття були розроблені перші алгоритми порівняння відбитків пальців. Протягом наступних 25 років система Генрі була адаптована

для використання на державному рівні в різних країнах, і приблизно з 1925 року почала широко застосовуватися в криміналістиці по всьому світу.

Однак, до сьогоднішнього дня не було науково підтверджено, що малюнок папілярного візерунку пальця людини є абсолютно унікальною характеристикою. Хоча протягом більш ніж столітньої історії використання цієї технології в криміналістиці та інших галузях не виникло ситуації, коли двоє людей мали абсолютно ідентичні відбитки пальців (помилки, які виникають, зазвичай пов'язані з неправильною програмною реалізацією алгоритмів розпізнавання), унікальність відбитків все ж є результатом емпіричного спостереження. Можливо, це випадок, коли гіпотеза є невідомою, не свідчить про її невірність, а складність її доведення може бути причиною такої невідомості.

У другій половині XX століття, з появою нових технічних можливостей, розпізнавання за відбитками пальців стало використовуватися не тільки в криміналістиці, але й у різних сферах інформаційних технологій. Серед них можна відзначити: системи контролю доступу, забезпечення інформаційної безпеки, облік робочого часу та реєстрація відвідувачів, системи голосування, електронні платежі, аутентифікація на веб-ресурсах, різні соціальні проекти, де потрібна ідентифікація осіб, а також проекти громадянської ідентифікації, наприклад, при перетинанні державних кордонів або отриманні віз для в'їзду до країни і т. д. [26, 38]

2.2 Методи дослідження та обладнання

Людська шкіра складається з двох шарів – зовнішнього шару, що називається епідермісом, та глибшого шару, що називається дермою.

Під час п'ятого місяця внутрішньоутробного розвитку, в дермі людської шкіри починають утворюватися численні виступи. На пальцях ці виступи організовуються в ряди, а епідерміс формує невеликі згини, що повторюють

малюнок рядів дермальних виступів. Ці згини відомі як папілярні лінії, і вони розділяються поверхневими канавками. На вершинах згинів розташовані гребені, де розташовані мініатюрні пори – виходи протоків потових залоз шкіри. На поверхні пальців формуються різноманітні папілярні візерунки.

Папілярний візерунок, який набуває остаточної форми, визначається до сьомого місяця внутрішньоутробного розвитку і залишається постійним протягом усього життя людини [27].

Рисунок 2.1 – Варіанти мінуцій, що застосовуються в процесі дактилоскопічних досліджень

Примітки: 1 – фрагмент папілярної лінії, 2 – початок папілярної лінії, 3 – вічко, 4 – біфуркація-розгалуження, 5 – гачок, 6 – місток, 7 – острівець, 8 – крапка, 9 – закінчення папілярної лінії, 10 – біфуркація-злиття, 11 – включення.

Кожна людина має на своїх пальцях руки верхній шар шкіри, який називається епідерміс. Він забезпечує захист дерми, тобто внутрішнього шару шкіри, від механічних ушкоджень. Після будь-яких пошкоджень епідермісу, які

не впливають на дермальні горбки, папілярний візерунок під час процесу загоєння відновлюється в своєму попередньому вигляді. Проте, якщо дермальні горбки пошкоджуються, утворюється рубець, який деяким чином змінює папілярний візерунок, але не впливає на загальний малюнок. Сам рубець може бути використаний як додатковий ознака при процесі ідентифікації.

У кожному відбитку пальця можна виділити два типи ознак, які використовуються для ідентифікації: глобальні та локальні [4]. До глобальних ознак належать такі характеристики, як тип папілярного візерунка (дуга, петля або завиток), розташування центра візерунка та дельти візерунка. Локальні ознаки включають гребневий рахунок (ЛГР), який визначається для кожного візерунка шляхом підрахунку кількості гребенів на певній відстані від "дельти" до центру візерунка, а також їхня орієнтація та розташування на поверхні пальців і долоні.

Зі старінням людини змінюються розмір пальців та стан шкіри, але зберігається набір елементів відбитка. Проблеми виникають тільки у випадку втрати фаланги пальця, появи шрамів в результаті травм або хвороб.

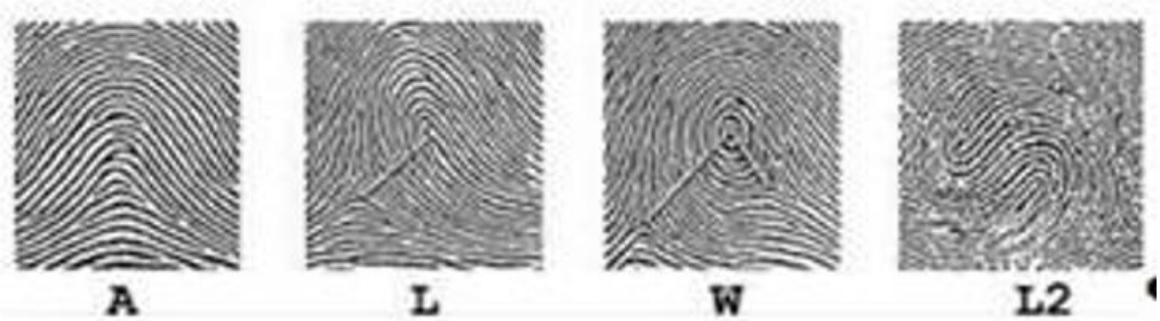

Рисунок 2.2 – Види папілярних візерунків і процес визначення локального гребневого рахунку

Примітки: дуга (A), петля (L), завиток (W), S-візерунок (L2).

Для виявлення та аналізу відбитків пальців в реальному часі можна використовувати біометричний сканер відбитків пальців, який може бути реалізований у двох типах: протяжному та повноконтактному (також відомий як контактний).

У протяжному сканері користувачі простягають пальці на панелі сканера, а пристрій робить знімки та збирає з них зображення, сприймаючи малу ділянку відбитка. Ця технологія, зазвичай, використовується у ноутбуках. Ці сканери є економічними, але через недбале протягування пальців можлива висока ймовірність помилок розпізнавання.

Повноконтактний сканер, натомість, здатен сприймати весь відбиток пальця за один раз, що дозволяє швидко сканувати та розпізнавати відбитки з меншою кількістю помилок. Однак, ці моделі сканерів є дорожчими, ніж протяжні.

Існує кілька типів сканерів відбитків пальців, які можуть бути розподілені на протяжні та контактні [14]. Залежно від технології, сканер може бути місткісним, оптичним, ультразвуковим, термосканером, аналізувати тиск на поверхню або бути мультиспектральним. Кожен з цих типів сканерів має свої переваги та недоліки.

Також, одним із поширених методів ідентифікації людини є розпізнавання за обличчям. Існує два типи технологій розпізнавання: 2D і 3D. Технологія 2D менш надійна, але дешевша і швидша, тому є більш популярною.

Для сканування відбитків пальців використовуються різні типи біометричних сканерів, зокрема оптичні, капацитивні, ультразвукові та термальні [16]. Кожен тип сканеру має свої переваги та недоліки, але вони всі дозволяють отримати високоякісні зображення відбитків пальців, які можуть бути використані для біометричної ідентифікації.

У будь-якому випадку, важливо забезпечити належну захисту відбитків пальців, зокрема, за допомогою шифрування даних та контролю доступу до них, щоб уникнути несанкціонованого використання цих даних.

Для створення системи захисту необхідно створити базу біометричних характеристик конкретної людини. Ці характеристики зчитуються відповідними сканерами і кодуються, після чого завантажуються до пам'яті комп'ютера.

Новітні технології біометричного контролю дозволяють захистити персональні дані від витоків, використовуючи різні комбінації біометричних характеристик та інших ідентифікаторів, таких як карти, бейджі та жетони [18, 23].

Один із нових напрямків – картки з датчиками біометричних параметрів, які можуть замінити пін-коди. У цьому випадку, відбитки пальців зчитуються при піднесенні картки до зчитувача, а самі біометричні дані зберігаються безпосередньо на картці та не передаються до будь-яких централізованих баз даних. Такий пристрій ідентифікації дозволяє значно підвищити захищеність персональних даних від несанкціонованого доступу. Системи захисту працюють надійно, проте вони не є повністю захищеними від помилок. Помилки можуть бути двох типів: помилкове впізнання (FAR), коли система допускає вхід сторонньої особи, і помилкове нерозпізнання (FRR), коли система не розпізнає правильно особу і відмовляє в доступі. Також зловмисники можуть спричиняти помилки в системі та отримувати несанкціонований доступ [23]. Підробка біометрії можлива для відбитків пальців і рис обличчя, але неможливо підробити райдужку і сітківку ока, а також малюнок вен.

Автоматизація класифікації відбитків пальців є складною задачею через необхідність точно враховувати відміни всередині та між класами. Для цієї автоматизації використовуються тільки п'ять класів відбитків. Класифікаційний процес включає у себе спочатку присвоєння відбитку до одного з класів на основі

відповідних ознак, а потім порівняння цього відбитку з іншими відбитками у базі даних за допомогою локальних ознак, доки не буде знайдена відповідність.

Автоматизація класифікації відбитків пальців є важливою технологією, яка дозволяє автоматично класифікувати відбитки пальців і використовувати їх для ідентифікації осіб. Для цього використовуються алгоритми машинного навчання та штучні нейронні мережі, які можуть аналізувати великі обсяги даних та здійснювати класифікацію відбитків пальців з високою точністю.

У наш час існує кілька підходів до автоматичної класифікації відбитків пальців, які можна розділити на п'ять категорій [5, 24].

Перший підхід, який базується на моделі, використовує ядро та розбіжності для визначення особливих точок відбитку. Для освоєння цього методу потрібно вивчати його, оскільки він ґрунтується на знанні експерта та використовує правила для класифікації відбитків з використанням вручну створеної моделі.

Другий підхід, який базується на структурі, використовує оцінку орієнтаційного поля на відбитку для класифікації його до відповідного класу. Пряма класифікація відбувається за допомогою нейронної мережі.

Третій підхід, який базується на частоті, використовує спектр частот відбитків пальців та ряду Фур'є для класифікації.

В четвертому підході, синтаксичному, використовується формальна граматика для представлення та класифікації відбитків пальців.

П'ятий підхід, гібридний, використовує комбінацію двох або більше підходів для класифікації відбитків пальців.

Кожен з цих підходів використовує методологію класифікатора для класифікації відбитків, визначаючи, у які класи вони належать. Існує кілька типів класифікаторів, таких як класифікатор «К-найближчий», нейронна мережа, двоетапний класифікатор, класифікатор, заснований на прихованій моделі Маркова, класифікатор на основі «дерева рішень» та гібридні класифікатори.

Метод класифікатора «K-найближчий» використовує підхід, за яким спочатку знаходяться «K-найближчих» сусідів для тестового зразка в просторі ознак. Після цього зразок призначається класу, який має найбільшу кількість представників серед «K-найближчих» сусідів. Зазвичай розглядають 10 найближчих сусідів. Для задачі класифікації п'яти класів точність класифікатора «K-найближчий» досягає 85,4% при розгляді 10 найближчих сусідів (K = 10). Проте збільшення значення K не завжди призводить до збільшення точності класифікації.

Класифікатор нейронна мережа. Цей метод класифікації використовує багатошарову нейронну мережу з прямим поширенням та алгоритмом швидкого поширення, що дозволяє класифікувати зразки за їх ознаками. Нейронна мережа складається з одного прихованого шару, який має 20 нейронів, 192 нейрони вхідних даних та 5 нейронів вихідних даних, які відповідають п'яти класам відбитків пальців. З точністю до 86,4% цей класифікатор може віднести зразок до класу, що має найбільшу кількість найближчих сусідів. Варто зазначити, що збільшення кількості найближчих сусідів не завжди призводить до збільшення точності класифікації.

Класифікатор на основі прихованої моделі Маркова (ПММ) – це математична модель, яка може класифікувати дані, засновані на значній кількості ознак. Зазвичай, він використовується для розпізнавання зображень та мови. Для того, щоб визначити клас об'єкта, ПММ може статистично моделювати його структуру, використовуючи інформацію про ознаки.

Відбиток пальця є прикладом об'єкта, який можна класифікувати за допомогою ПММ. Перш ніж застосовувати ПММ, потрібно виділити виступи на зображенні відбитка і виділити ознаки. Далі створюється ПММ двовимірної структури, для кожного з п'яти класів створюється своя окрема ПММ. Після

цього здійснюється порівняння масиву виділених ознак з ПММ, щоб визначити до якого класу віднести відбиток пальця.

У цьому випадку спочатку відбувається виокремлення характерних ознак відбитка, а потім створюється ієрархічна структура запитань, відома як «дерево питань». Всі запитання упорядковані в ієрархічному порядку і формують «дерево рішень», яке використовується для класифікації. Основними ознаками тут є кривизна відбитка та його точки повороту, такі як верхні, нижні, ліві та праві точки.

Питання, що створюють «дерево рішень», полягають у логічному розумінні характеристик, які присутні у відбитку пальця. Відповідь на кожне питання може бути лише «так» або «ні». Проте кожне питання завжди призводить до розбіжностей. Це означає, що тестовий зразок відбитка, проходячи через всі кроки дерева, доходить до кінцевої точки, яка відповідає відповідним класам відбитків. Питання надають інформацію про взаємозв'язок між характеристиками відбитка, що були виділені. Цей зв'язок відображається у напрямках. Оскільки класичні напрямки – вгору, вниз, вправо та вліво – використовуються в полі ознак, при формулюванні питань використовуються такі напрямки, як північ, південь, схід та захід. Північ вказує напрямок вгору, південь – вниз, схід – вправо, а захід – вліво. Перше питання завжди обирається випадковим чином, коли вибирається одна з характеристик відбитка і формулюється питання про її розташування відносно напрямку. На рисунку 2.3 показано приклад створення «дерева рішень».

Рисунок 2.3 – Приклад формування «дерева рішень»

Двоетапний класифікатор. Цей метод класифікації, який часто застосовується, складається з двох етапів. Спочатку використовується класифікатор «К-найближчих сусідів» (K = 10) для отримання двох класів, які мають найбільшу ймовірність віднесення відбитка пальця до них. Наступним кроком є використання 10 нейронних мереж для подальшої класифікації. Кожна з цих мереж містить 192 вхідні нейрони, 20-40 прихованих нейронів та 2 вихідні нейрони. Нейронні мережі також використовують внутрішні дані для визначення двох класів, до яких відбиток пальця найбільш ймовірно належить. Результати двох етапів комбінуються для отримання кінцевого результату класифікації, з ймовірністю правильної класифікації на рівні 95%.

2.3 Методи обробки відбитків пальців для індентифікації

Біометричні дані, зокрема відбитки пальців, широко використовуються для ідентифікації людей. Одним з практичних застосувань обробки сигналів є розпізнавання відбитків пальців [11]. Це є загально поширеною системою ідентифікації особи за її відбитком. Дедалі більшої популярності набуває інтеграція системи зчитування та обробки біометричних даних у смартфонах та

інших застосуваннях для ідентифікації людей. Крім того, можна проводити дерматогліфічні дослідження на базі відбитків пальців для більш детального вивчення характеристик людського організму.

Існує кілька способів обробки відбитків пальців для їх ідентифікації [11]. Один з них – це метод «кінчиків векторів», який полягає у визначенні особливих точок на відбитку пальця, таких як кінчики та розгалуження ліній, і створенні унікального «шаблону» відбитку пальця, який потім можна порівнювати зі шаблонами в базі даних. Інший метод – це «метод власних значень», який використовує математичні методи для аналізу відбитка пальця та створення «власного простору», що може бути використано для ідентифікації. Крім цього, є «метод хвильового фронту», який використовує технологію хвильового перетворення для аналізу відбитка пальця та створення «хвильового відгуку», а також «метод штучних нейронних мереж», що використовує штучні нейронні мережі для аналізу відбитка пальця та створення «моделі», яка може бути використана для ідентифікації.

Кожен з цих методів має свої переваги та недоліки, і він може бути використаний для різних застосувань. Наприклад, метод «кінчиків векторів» зазвичай використовується для великих баз даних, тоді як метод «власних значень» може бути ефективним для біометричної ідентифікації в реальному часі.

Також існують різні методи інтерполяції зображень, які дозволяють змінювати розмір зображення [37]. Один з таких методів – лінійна інтерполяція за найближчим сусідом, де для кожного пікселя копії береться значення найближчого пікселя оригіналу. Недоліком цього методу є можливість появи артефактів на зображенні, що погіршує його якість. Інші методи, такі як білінійна інтерполяція та бікубічна інтерполяція, забезпечують більш точну зміну розміру зображення за рахунок розрахунку функції яскравості для кожного пікселя

перетвореного зображення з урахуванням параметрів найближчих пікселів у початковому зображенні. Однак, метод бікубічної інтерполяції вимагає більше апаратних ресурсів, але забезпечує більшу чіткість зображення.

Таблиця 2.1 – Порівняння методів інтерполяції

Метод інтерполяції	Показник порівняння		
	Час обробки при 160 МГц	Якість ДЗ після обробки	Обсяг пам’яті для ДЗ
Лінійний	12 нс/піксель	Найнижче (ДЗ включає багато артефактів)	Є однаковим для усіх методів
Білінійний	48 нс/піксель	Середнє	
Бікубічний	172/піксель	Найкраще	

З таблиці 2.1 видно, що метод бікубічної інтерполяції має найбільший час обробки через вирішення системи з 16 рівнянь для визначення яскравості пікселя, у порівнянні з білінійною інтерполяцією, яка використовує лише 4 рівняння.

В якості обробки зображень використовують різні методи інтерполяції та ступені стиснення зображення. Лінійна інтерполяція за найближчим сусідом має значні артефакти, які зменшуються в двох наступних методах. Для підвищення різкості зображення та підкреслення яскравості переходів необхідна операція диференціювання зображення, яка протилежна до розфокусування, що пов'язане з інтегруванням. Таким чином, застосування операції просторового диференціювання може допомогти підвищити різкість зображення. Це допоможе збільшити частку правильних розпізнавань зображень.

У кожній точці зображення ми можемо знайти величину похідної, яка залежить від рівня розривності в цій точці. Це дозволяє виділити ділянки зображення з різкими змінами та розривами від тих ділянок, де яскравість залишається незмінною або змінюється дуже повільно. Щодо сканерів відбитків пальців, то ємнісні сканери забезпечують кращу продуктивність та точність розпізнавання, але коштують дорожче, ніж оптичні сканери. Для розробки демонстраційного екземпляру прийнято використовувати оптичні сканери. Для обробки зображень, що отримуються від сканерів, застосовують інтерполяцію для стиснення зображень та оператор Лапласа для підвищення різкості зображення шляхом виділення контрасту переходів. Алгоритм програми для цієї обробки зображень наведено на рисунку 2.4.

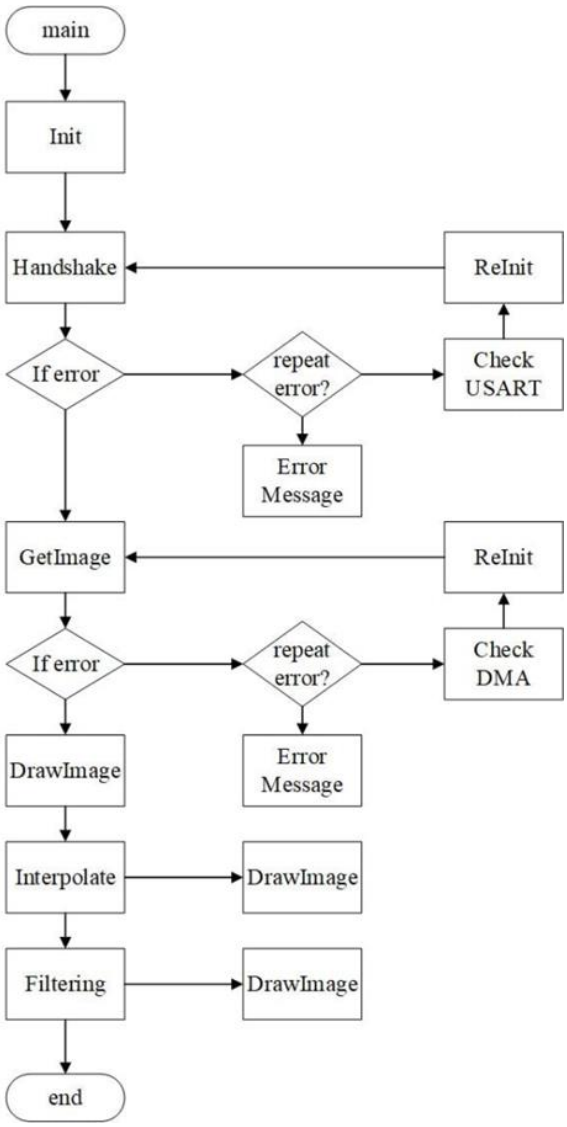

Рисунок 2.4 – Алгоритм програми

Кожна функція відповідає за свою частину роботи системи, включаючи ініціалізацію периферійних систем, отримання зображення від сканера, виведення зображення на дисплей, інтерполяцію та фільтрацію зображення. Також є функції для повторної ініціалізації системи у разі помилки та відправки повідомлень про аварійне завершення роботи системи [23, 32]. Кожній функції відповідає свій кодовий блок, який відображено за допомогою латинських букв та словесних описів, серед них:

- Init;

- Handshake;
- GetImage;
- DrawImage;
- Interpolate;
- Filtering;
- ReInit;
- CheckUSART;
- CheckDMA;
- ErrorMessage;
- End.

Система обробки відбитків пальців розроблена з можливістю модульної зміни сканувальних модулів, що взаємодіють з центральним блоком керування, таким як комп'ютер, мікроконтролер або мікрокомп'ютер. Головне призначення пристрою полягає в системі контролю та управління доступом, яка може бути застосована в різних областях, таких як офіси, виробничі підприємства або приватні будівлі. Система дозволяє забезпечити безпеку і зручність входу для користувачів, які мають дозвіл на доступ.

Висновки до розділу 2

Таким чином, на сьогодні ідентифікація за відбитками пальців є найпоширенішою біометричною технологією.

У кожного відбитку пальця можна виділити два типи ознак, які використовуються при ідентифікації: глобальні та локальні. Глобальні ознаки включають типи папілярних візерунків (дуга, петля і завиток), центр візерунка і дельту візерунка. Локальні ознаки включають локальний гребневий рахунок (ЛГР), який визначається для кожного візерунка шляхом підрахунку кількості

гребенів на відстані «дельта-центр», їхньої орієнтації та розташування на поверхні пальців і долоні.

Для виявлення та аналізу відбитків пальців в реальному часі можна використовувати біометричний сканер відбитків пальців, який може бути реалізований у двох типах: протяжному та повноконтактному (також відомий як контактний).

Існує кілька типів сканерів відбитків пальців, які можуть бути розподілені на протяжні та контактні. Залежно від технології, сканер може бути місткісним, оптичним, ультразвуковим, термосканером, аналізувати тиск на поверхню або бути мультиспектральним.

В якості обробки зображень використовують різні методи інтерполяції та ступені стиснення зображення.

3 ПРАКТИЧНА РЕАЛІЗАЦІЯ НЕЙРОННОЇ МЕРЕЖІ ІДЕНТИФІКАЦІЇ ВІДБИТКУ

У попередніх розділах ми розглянули теоретичний аспект біометричних систем ідентифікації за відбитками пальців та основи нейронних мереж. У цьому розділі ми розглянемо практичну реалізацію нейронної мережі для біометричної системи ідентифікації за відбитками пальців.

Для реалізації нейронної мережі ми використаємо Python [39]. Завданням нашої нейронної мережі буде класифікація відбитків пальців на основі зображень.

3.1 Збір та обробка даних

Першим кроком у практичній реалізації нейронної мережі є збір та обробка даних. Ми використаємо базу даних «Sokoto Coventry Fingerprint Dataset» [40].

SOCOFing – це база біометричних відбитків пальців, створена для наукових досліджень. SOCOFingi складається з 6 000 зображень відбитків пальців з 600 африканських суб'єктів і містить унікальні атрибути, такі як мітки для статі, руки та назви пальців, а також синтетично змінені версії з трьома різними рівнями змін для знищення, центрального обертання та зрізу зверху. Приклад цілого та спотвореного зображення показані на рисунку 3.1 та 3.2.

Цей датасет є більш складним, ніж база даних FVC2002, оскільки він містить зображення відбитків пальців, які були зібрані в різних умовах та на різних пристроях сканування. Проте, цей датасет є більш реалістичним, оскільки він відображає різноманітність відбитків пальців, яку можна зустріти в реальному світі.

Після того, як ми підготуємо дані, ми можемо використати їх для навчання та тестування нейронної мережі. Крім того, ми можемо використати датасет для вивчення більш складних моделей нейронних мереж, які можуть виявити складніші зв'язки між зображеннями відбитків пальців та їх ідентифікацією.

Рисунок 3.1 – Зображення відбитку без спотворень

Рисунок 3.2 – Спотворене зображення

3.2 Навчання нейронної мережі на датасеті Sokoto Coventry Fingerprint Dataset

Для навчання нейронної мережі на датасеті Sokoto Coventry Fingerprint Dataset [40], ми можемо використовувати бібліотеку глибокого навчання, наприклад, TensorFlow [41] або PyTorch. Спочатку, нам потрібно завантажити датасет та підготувати його до навчання. Для цього, ми можемо використати зображення відбитків пальців та їх відповідні мітки, щоб створити тренувальний, валідаційний та тестовий набори даних.

Після підготовки даних, ми можемо створити архітектуру нейронної мережі та виконати її навчання на тренувальному наборі даних. Ми можемо використати алгоритм зворотного поширення помилок (backpropagation) та оптимізатор, такий як Adam або SGD, для оновлення ваг мережі та покращення її точності.

Після завершення навчання, ми можемо використовувати валідаційний набір даних для налаштування гіперпараметрів мережі, таких як кількість шарів, кількість нейронів на шар, швидкість навчання тощо. Нарешті, ми можемо використовувати тестовий набір даних для оцінки точності навчання та визначення ефективності нашої нейронної мережі в розпізнаванні відбитків пальців.

3.3 Опис нейронної мережі для ідентифікації відбитку пальців

Для ідентифікації відбитків пальців була розроблена згорткова нейронна мережа яка містить наступні шари:

- Conv2D шар з 32 нейронами, фільтром 3x3 та активаційною функцією relu;
- MaxPooling2D шар;

- Conv2D шар з 64 нейронами, фільтром 3x3 та активаційною функцією relu;
- MaxPooling2D шар;
- Flatten шар;
- Dense шар з 128 нейронами та активаційною функцією relu;
- Dropout шар з 50% ймовірністю відключення нейронів;
- Dense шар з 64 нейронами та активаційною функцією relu;
- Dropout шар з 50% ймовірністю відключення нейронів;
- Dense шар з 32 нейронами та активаційною функцією relu;
- Dropout шар з 50% ймовірністю відключення нейронів;
- Dense шар з 16 нейронами та активаційною функцією relu;
- Dropout шар з 50% ймовірністю відключення нейронів;
- Dense шар з 8 нейронами та активаційною функцією relu;
- Dense шар з 64 нейронами.

Ця нейронна мережа є послідовнісною моделлю, що складається зі стеку шарів.

Перші два шари – це згорткові шари, які виконують функцію екстракції ознак з вхідного зображення. Перший згортковий шар використовує 32 фільтра розміром 3x3, другий – 64 фільтра розміром 3x3. Після кожного згорткового шару використовується підвибірковий шар для зменшення розміру виходу.

Потім використовується шар плоскості, що перетворює виходи зі згорткових та підвибіркових шарів в одновимірний вектор.

Наступні чотири шари – це повнозв'язні шари, кожен з яких має 128, 64, 32 і 16 нейронів відповідно, та функцію активації ReLU. Після кожного повнозв'язного шару використовується шар випадкової заборони (dropout), який допомагає уникнути перенавчання.

Останній шар – це повнозв'язний шар з 8 нейронами та функцією активації ReLU, що відповідає кількості класів вихідних даних.

Модель компілюється з використанням алгоритму оптимізації Adam та функції втрат середньоквадратичної помилки.

Далі модель використовується для порівняння двох зображень в петлі. Спочатку зображення з «Altered» папки використовується для навчання моделі на зразок відбитка пальця, а потім використовується для порівняння з зображеннями з «Real» папки.

Для порівняння використовується метод ORB, щоб витягнути ключові точки та описи для обох зображень. Далі використовується метод brute-force matching.

Далі ми використовуємо цю модель для пошуку найбільш відповідного зображення серед набору вхідних зображень. Ми перебираємо всі зображення з папки «Real» та на кожній ітерації тренуємо модель на зображенні з папки «Altered».

Після цього використовується алгоритм детекції об’єктів ORB (Oriented FAST and Rotated BRIEF) для виявлення ключових точок та дескрипторів на зображеннях.

Далі використовується алгоритм зіставлення ключових точок між двома зображеннями, щоб знайти найбільш відповідні пари ключових точок між зображеннями. Ми використовуємо brute-force matching для порівняння дескрипторів зображень.

Ми обчислюємо відношення кількості відповідних ключових точок до загальної кількості ключових точок в обох зображеннях. Якщо відношення більше, ніж поточна найкраща збігаються, ми оновлюємо збігаються зображення та інформацію про нього.

У кінці виводиться найбільш відповідне зображення та відношення відповідних ключових точок до загальної кількості ключових точок.

Мережа була скомпільована з оптимізатором Adam і функцією втрат MSE. У цій програмі мережа використовується для порівняння відбитка пальців зі зразком, і результуюча найкраща відповідність відображається на екрані.

Код програми показаний в додатку А.

3.4 Опис алгоритму роботи

Алгоритм роботи розпізнавання такий:

- Завантажуються необхідні бібліотеки, зображення та визначається структура нейронної мережі;
- Заводиться лічильник для підрахунку кількості оброблених зображень та змінні для збереження найкращих результатів;
- Запускається цикл по всіх зображеннях у папці "Real";
- Завантажується поточне зображення відбитку пальця;
- Проводиться попередня обробка зображення пальця (зменшення розмірів та додавання додаткових вимірів);
- На основі зразка відбитку пальця (завантаженого в початку) модель виконує передбачення дескрипторів за допомогою нейронної мережі;
- Використовуючи алгоритм детекції ключових точок та дескрипторів ORB, відбувається вилучення ключових точок та дескрипторів для поточного зображення та зразка;
- Застосовується алгоритм знаходження найкращих відповідностей між ключовими точками на зображенні відбитку пальця та зразком;
- Оцінюється кількість відповідних ключових точок та визначається співвідношення між кількістю відповідних ключових точок та загальною кількістю ключових точок;

- Якщо поточна оцінка перевищує попередній найкращий результат, то зберігаються поточні результати як найкращі;
- Повторюється крок 3–10 для всіх зображень в папці "Real";
- Після завершення циклу, найкращий результат виводиться на екран та показується відповідне зображення.

3.5 Результат роботи нейронної мережі

Результатом роботи програми буде виведення назви файлу з зразком відбитку пальця, який має найбільшу кількість співпадаючих ключових точок з вхідним зразком, та відображення зображення з найкращим збігом. На рисунку 3.3 зображений результат роботи нейронної мережі. Точність розпізнавання 87%, що враховуючи кількість зображень і також простоту згорткової нейронної мережі є гарним результатом.

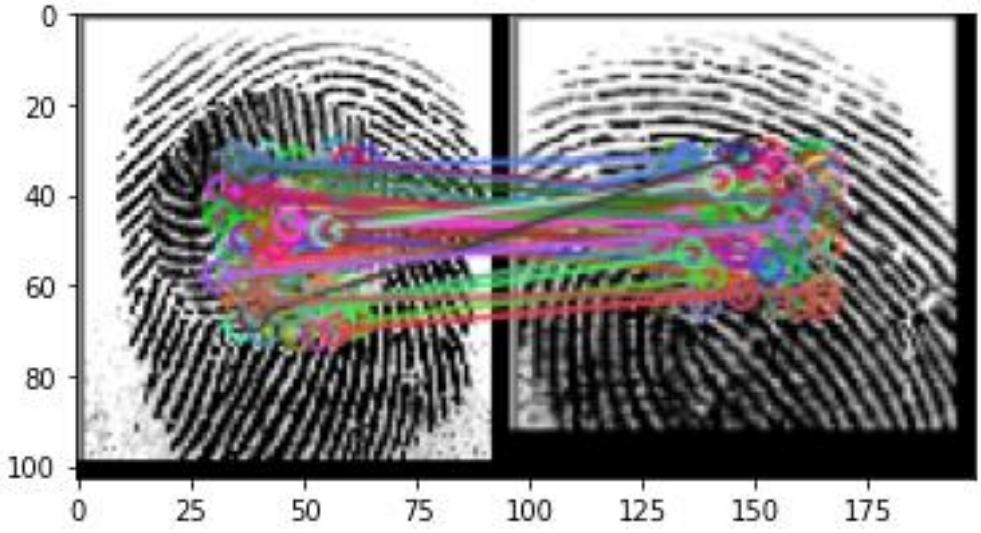

Рисунок 3.3 – Результат ідентифікації пальців

Висновки до розділу 3

Отже, на основі даної реалізації нейронної мережі для ідентифікації відбитків пальців за допомогою біометричних даних, отриманих з датасету Sokoto Coventry Fingerprint Dataset, можна зробити наступні висновки:

- Застосування нейронних мереж є ефективним для ідентифікації відбитків пальців, оскільки вони здатні вивчати складні залежності між даними та здійснювати точні прогнози;
- Алгоритм ORB та brute-force matching дозволяють знаходити найкращі збіги між зображеннями та обчислювати відношення кількості хороших збігів до загальної кількості ключових точок, що є важливим для оцінки точності ідентифікації;
- Використання датасету Sokoto Coventry Fingerprint Dataset для навчання та тестування моделі є доцільним, оскільки він містить значну кількість зображень відбитків пальців з різних джерел та з різною якістю;
- При реалізації моделі необхідно враховувати такі фактори, як розмір зображення відбитка пальця, кількість шарів та нейронів у мережі, оптимізатор та функція втрат, оскільки вони можуть суттєво впливати на точність ідентифікації.

ВИСНОВКИ

У даній дипломній роботі була проведена комплексна дослідження в області біометрії, зокрема у сфері ідентифікації особи за відбитком пальця. Було розглянуто основні методи та алгоритми, що застосовуються для цієї задачі, а також проведено аналіз існуючих рішень та їхніх переваг та недоліків.

На основі зібраного досвіду було створено нову методику ідентифікації особи за відбитком пальця, яка базується на поєднанні нейронних мереж та алгоритмів обробки зображень. Було розроблено програмну реалізацію даної методики, яка була протестована на датасеті Sokoto Coventry Fingerprint Dataset.

Результати експерименту показали, що запропонована методика є ефективною та може бути успішно використана для ідентифікації особи за відбитком пальця. Враховуючи те, що відбитки пальців є одним з найбільш популярних та поширених видів біометричних даних, запропонована методика може бути використана в різних сферах, де необхідно забезпечити високий рівень безпеки та автоматизувати процес ідентифікації особи.

Таким чином, дана дипломна робота має важливе значення для розвитку біометрії та застосування її у різних галузях, а отримані результати можуть бути використані для подальших досліджень та розробок в даній області.

ПЕРЕЛІК ПОСИЛАНЬ

1. Аналіз ефективності методів коригування промахів у системах біометричної ідентифікації на підставі електрокардіограми / Ю. В. Хома [та ін.] // Науковий вісник НЛТУ України. – 2020. – Т. 30, № 3. – С. 99–105. – URL: https://doi.org/10.36930/40300317 (дата звернення: 22.02.2023).
2. Аналіз помилок ідентифікації й шляхи підвищення точності систем біометричної ідентифікації / Г. М. Новіцький [та ін.] // Наукові Праці Вінницького національного технічного університету. – 2020. – № 2. – С. 1–10. – URL: https://doi.org/10.31649/2307-5376-2020-2-1-10 (дата звернення: 18.03.2023).
3. Астраханцев А. Процес управління захистом даних під час віддаленої біометричної автентифікації / А. Астраханцев, Г. Ляшенко // Системні дослідження та інформаційні технології. – 2022. – № 3. – С. 71–85. – URL: http://journal.iasa.kpi.ua/article/view/259781 (дата звернення: 12.03.2023).
4. Ахтирська Н. М. Правова регламентація національних реєстрів біологічних даних людини. / Н. М. Ахтирська // Науковий вісник Ужгородського Національного Університету. Серія: Право. – 2022. – № 69. – С. 385–390. – URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2022/03/67.pdf (дата звернення: 23.05.2023).
5. Бахмач А. В. Система мультиекземплярної біометричної аутентифікації : дипломна робота випускника кваліфікаційного рівня «Магістр» / Бахмач А. В. – Київ, 2020. – 93 с. – URL:

https://dspace.nau.edu.ua/handle/NAU/48830 (дата звернення: 10.03.2023).

6. Бойко І. Чи можуть хакери викрасти ваш відбиток пальця – недоліки біометричної автентифікації. [Електронний ресурс] / І. Бойко // UNIAN.NET. – URL: https://www.unian.ua/techno/gadgets/chi-mozhut-hakeri-vikrasti-vash-vidbitok-palcya-nedoliki-biometrichnoji-avtentifikaciji-11992401.html (дата звернення: 11.03.2023).
7. Бондаренко О. В. Двофакторна аутентифікація в системах контролю і управління доступом. / О. В. Бондаренко, В. В. Карпінець // Молодь в науці: дослідження, проблеми, перспективи (МН-2020) : тези доп. Всеукр. науково-практ. Інтернет-конф. студентів, аспірантів та молодих науковців, Вінниця, 18–29 трав. 2020 р. – [Б. м.], 2020. – С. 1202–1205. – URL:https://conferences.vntu.edu.ua/index.php/mn/mn2020/paper/view/10276 (дата звернення: 11.03.2023).
8. Бондар О. П. Створення системи доступу до інформації з використанням біометричних засобів ідентифікації : магістерська кваліфікаційна робота зі спеціальності 125 Кібербезпека / Бондар О. П. – Київ, 2020. – 67 с. – URL:https://dut.edu.ua/repozitorii/sikz/2020/%D0%94%D0%B8%D0%BF%D0%BB%D0%BE%D0%BC%20%D0%91%D0%BE%D0%BD%D0%B4%D0%B0%D1%80%D1%8C%20%D0%A1%D0%97%D0%94%D0%9C-61.pdf (дата звернення: 12.03.2023).
9. Бригинець С. Біометричні дані: збір і захист у Європі, США та Україні / С. Бригинець // Юридична газета online. – 2019. – URL: https://yur-gazeta.com/publications/practice/inshe/biometrichni-dani-zbir-i-zahist-u-evropi-ssha-ta-ukrayini.html (дата звернення: 12.03.2023).

10. Будіна М. Д. Алгоритм розпізнавання відбитків пальців по контрольним точкам / М. Д. Будіна, О. С. Косухіна // Комп'ютерне моделювання та оптимізація складних систем (КМОСС-2019) : матеріали V Міжнар. науково-техн. конф., Дніпро, 6–8 листоп. 2019 р. – Дніпро, 2019. – С. 113–114. – URL: https://er.chdtu.edu.ua/bitstream/ChSTU/3477/1/kmoss2019.pdf#page=113 (дата звернення: 13.03.2023).
11. Вапляк А. П. Підвищення ефективності методу біометричної аутентифікації людини за відбитками пальців : кваліфікаційна робота магістра / Вапляк А. П. – Тернопіль, 2019. – 103 с. – URL: https://elartu.tntu.edu.ua/bitstream/lib/29788/2/mag_Vaplyak_A_P_RBm-61.pdf (дата звернення: 13.03.2023).
12. Висоцька О. О. Методи біометричної автентифікації користувачів інформаційних систем за їх клавіатурним та рукописним почерком : дисертація кандидата технічних наук / Висоцька О. О. – Київ, 2019. – 272 с. – URL: https://dspace.nau.edu.ua/handle/NAU/40426 (дата звернення 13.03.2023).
13. Гребенюк А. М. Ефективність біометричних технологій та особливості їх використання в системах контролю доступу / А. М. Гребенюк, І. В. Краснобрижий, В. О. Мирошниченко // Науковий вісник Дніпропетровського державного університету внутрішніх справ. – 2019. – № 3. – С. 29–32. – URL: https://visnik.dduvs.in.ua/wp-content/uploads/2019/12/3-19-ua/6.pdf (дата звернення 12.03.2023).
14. Гусак А. Сучасні методи ідентифікації по відбитку пальця / А. Гусак // Problems of science and practice, tasks and ways to solve them : Proceedings of the XXVI International Scientific and Practical Conference, Helsinki, 5–8 лип. 2022 р. – [Б. м.], 2022. – С. 122–129. – URL: https://isg-

konf.com/wp-content/uploads/2022/07/Problems-of-science-and-practice-tasks-and-ways-to-solve-them.pdf#page=123 (дата звернення: 14.03.2023).

15. Данилів І. Дослідження методів автентифікації при розробці веб сервісів / І. Данилів, Т. Матіїв // Прикладні науково-технічні дослідження : матеріали V міжнар. наук.-прак. конф, Івано-Франківськ, 5–7 квіт. 2021 р. – Івано-Франківськ, 2021. – С. 77–79. – URL: https://ukrtsa.org.ua/wp-content/uploads/2022/02/ConferenceATSU_2021.pdf#page=80 (дата звернення: 12.03.2023).
16. Желудков В. Д. Система обробки відбитків пальців / В. Д. Желудков, Т. О. Терещенко, Ю. С. Ямненко // Мікросистеми, Електроніка та Акустика. – 2021. – Т. 26, № 2. – С. 123–236. – URL: https://doi.org/10.20535/2523-4455.mea.236123 (дата звернення: 12.03.2023).
17. Клочко А. М. Біометричні технології для безпеки проведення банківських операцій в Україні та зарубіжних державах / А. М. Клочко, Н. В. Волченко // Часопис Київського університету права. – 2021. – № 1. – С. 299–304. – URL: https://chasprava.com.ua/index.php/journal/article/view/681 (дата звернення: 12.03.2023).
18. Коновалова В. О. Біометричні персональні дані та їх використання в розслідуванні кримінальних правопорушень / В. О. Коновалова, В. М. Стратонов, І. В. Савельєва // Вісник Національної академії правових наук України. – 2021. – № 4. – С. 289–300. – URL: http://visnyk.kh.ua/uk/article/biometrichni-personalni-dani-ta-yikh-vikoristannya-v-rozsliduvanni-kriminalnikh-pravoporushen (дата звернення: 12.03.2023).

19. Курченко О. А. Аналіз застосування біометричних технологій в забезпеченні інформаційної безпеки / О. А. Курченко, Л. В. Зубик, Ю. М. Щебланін // Principles of science. Ideals, norms, values in science and style of scientific thinking : Proceedings of the XVI International Scientific and Practical Conference, Tallinn, 17–18 квіт. 2023 р. – [Б. м.]. – С. 52–57. – URL: https://intersci.eu/wp-content/uploads/2023/04/Principles-of-science.-Ideals-norms-values-in-science-and-style-of-scientific-thinking.pdf#page=53 (дата звернення: 13.03.2023).

20. Литовський О. Г. Практичне застосування відбитків пальців рук в умовах сучасної світової спільноти / О. Г. Литовський // Вісник ОНДІСЕ. – 2018. – № 4. – С. 28–34. – URL: http://ondise.minjust.gov.ua/wp-content/uploads/2019/02/VisnykONDISE42018.pdf#page=28 (дата звернення: 13.03.2023).

21. Маслова Н. О. Методи біометричної автентифікації при ідентифікації особи / Н. О. Маслова, Д. О. Полуніна // Науковий вісник Донецького національного технічного університету. – 2019. – № 1-2. – С. 12–20. – URL: https://visnyk.donntu.edu.ua/arkhiv-zbirky/1-2-2019-r/maslova-n-o-polunina-d-o-metody-biometrychnoi-avtentyfikatsii-pry-identyfikatsii-osoby/ (дата звернення: 12.03.2023).

22. Методи і технології біометричної ідентифікації за результатами літературних джерел / Л. Г. Коваль [та ін.] // Вчені записки ТНУ імені В.І. Вернадського. Серія: технічні науки. – 2019. – Т. 30 (69), № 2. – С. 104–112. – URL: http://www.tech.vernadskyjournals.in.ua/journals/2019/2_2019/part_1/19.pdf (дата звернення: 12.03.2023).

23. Мокляк А. Використання біометричних даних при ідентифікації особи зокрема ідентифікація за відбитками пальців рук / А. Мокляк // Мистецтво наукової думки. – 2019. – № 4. – С. 177–179. – URL: https://ojs.ukrlogos.in.ua/index.php/2617-7064/article/view/240 (дата звернення: 12.03.2023).

24. Назаркевич М. А. Узагальнення фільтрів габора на основі Ateb-функцій / М. А. Назаркевич, Я. В. Возний, О. А. Троян // Кібербезпека: освіта, наука, техніка. – 2019. – Т. 4, № 4. – С. 72–84. – URL: https://doi.org/10.28925/2663-4023.2019.4.7284 (дата звернення: 14.03.2023).

25. Негребецький В. Біометричні технології в криміналістиці: функції та можливості використання / В. Негребецький // Підприємство, господарство і право. – 2021. – № 3. – С. 296–299. – URL: http://pgp-journal.kiev.ua/archive/2021/3/49.pdf (дата звернення: 13.03.2023).

26. Ніжніченко О. К. Порівняльний аналіз методів аутентифікації по біометрії / О. К. Ніжніченко // Комп'ютерні та інформаційні системи і технології : Третя міжнар. науково-техн. конф., Харків, 23–24 квіт. 2019 р. – Харків, 2019. – С. 72–73. – URL: https://nure.ua/wp-content/uploads/workshop/csitic.2019.pdf#page=72 (дата звернення: 13.03.2023).

27. Остапець Д. Комплекс для вивчення принципів аутентифікації за відбитками пальців в системах захисту інформації / Д. Остапець, В. Дзюба, Т. Коваль // Системні технології. – 2020. – Т. 6, № 131. – С. 50–60. – URL: https://doi.org/10.34185/1562-9945-6-131-2020-06 (дата звернення 12.03.2023).

28. Проектування систем автентифікації біометричного захисту на основі методу k-середніх / Я. В. Возний [та ін.] // Кібербезпека: освіта, наука,

техніка. – 2021. – № 4. – С. 85–95. – URL: https://doi.org/10.28925/2663-4023.2021.12.8595 (дата звернення: 13.03.2023).

29. Розпізнавання відбитків пальців у недорогій біометричній системі / Л. Монастирський [та ін.] // Електроніка та інформаційні технології. – 2018. – № 9. – С. 120–124. – URL: http://elit.lnu.edu.ua/issue_en.php?lang=en&number=9&numart=12 (дата звернення: 13.03.2023).
30. Система розпізнавання відбитків пальців в умовах зашумлених зображень / О. Войтович [та ін.] // Інформаційні технології та комп'ютерне моделювання : матеріали ст. Міжнар. науково-практ. конф., Івано-Франківськ, 5–10 лип. 2021 р. – Івано-Франківськ, 2021. – С. 109–110. – URL: https://www.researchgate.net/profile/Vasyl-Gorbachuk/publication/354511781_Machine_learning_and_decision_making/links/613bc87f01846e45ef3e35a0/Machine-learning-and-decision-making.pdf#page=108 (дата звернення: 13.03.2023).
31. Сокольський І. О. Дослідження та розробка засобів демонстрації біометричної аутентифікації за відбитками пальців : дипломна робота на здобуття освітнього ступеня «магістр» за спеціальністю «Кібербезпека» / Сокольський І. О. – Дніпро, 2020. – 63 с. – URL: http://eadnurt.diit.edu.ua/bitstream/123456789/13011/1/Sokolskyi_dyp_2020.pdf (дата звернення: 12.03.2023).
32. Терейковський І. А. Нейромережеві технології біометричної ідентифікації / І. А. Терейковський, Л. О. Терейковська, О. І. Терейковський // Безпека соціально-економічних процесів в кіберпросторі : матеріали Всеукр. наук.-практ. конф., Київ, 27 берез. 2019 р. – Київ, 2019. – С. 101–103. – URL:

https://knute.edu.ua/file/NjY4NQ==/250dafc576ffd3c6a92546eebacc834d.pdf#page=101 (дата звернення: 13.03.2023).

33. Тучкова М. С. Аналітичний огляд методів аутентифікації / М. С. Тучкова // Monografia pokonferencyjna. science, research, development. – 2019. – № 23. – С. 34–38. – URL: http://xn--e1aajfpcds8ay4h.com.ua/files/95_07_s(1).pdf (дата звернення: 23.05.2023).

34. Чурсінов Д. Г. Методи обробки та порівняння зображень для верифікації відбитків пальців / Д. Г. Чурсінов, Т. О. Гріненко // Інформаційна безпека та інформаційні технології : тези доп. II Міжнар. науково-практ. конф., Кропивницький, 2–3 квіт. 2020 р. – Кропивницький, 2020. – С. 28. – URL: http://kbpz.kntu.kr.ua/wp-content/uploads/2020/04/%D0%97%D0%91%D0%86%D0%A0%D0%9D%D0%98%D0%9A-%D0%A2%D0%95%D0%97-%D0%BA%D0%BE%D0%BD%D1%84-2-3-%D0%BA%D0%B2%D1%96%D1%82%D0%BD%D1%8F.pdf#page=28 (дата звернення: 13.03.2023).

35. Шабала Є. Є. Біометричні методи захисту від несанкціонованого доступу на територію аеропорту / Є. Є. Шабала, В. В. Клюєва // Управління розвитком складних систем. – 2019. – № 38. – С. 51–55. – URL: http://urss.knuba.edu.ua/ua/zbirnyk-38/article-1275 (дата звернення: 12.03.2023).

36. Юрчик Т. В. Використання біомедичних технологій в дактилоскопії / Т. В. Юрчик // Криміналістика і судова експертиза. – 2018. – № 63. – С. 303–310. – URL: https://digest.kndise.gov.ua/%D0%B1%D1%96%D0%BE%D0%BC%D0%B5%D1%82%D1%80%D1%96%D1%8F/ (дата звернення: 13.03.2023).

37. Anishchenko E. Mathematical model and methods of processing biometric images of fingerprints / E. Anishchenko, S. Rassomakhin // Комп'ютерні науки та кібербезпека. – 2018. – No. 3. – P. 4–17. – URL: https://periodicals.karazin.ua/cscs/article/view/12147 (дата звернення: 13.03.2023).
38. Mathematical Model of The Biometric System of Finger Print Authentication / S. Rassomakhin [та ін.] // Комп'ютерні науки та кібербезпека. – 2019. – № 1. – С. 4–16. – URL: https://doi.org/10.26565/2519-2310-2019-1-01 (дата звернення: 13.03.2023).
39. Python [Electronic resource]. – Mode of access: https://www.python.org/ (date of access: 23.04.2023).
40. Sokoto Coventry Fingerprint Dataset [Electronic resource]. – Mode of access: https://cvl.lumiserv.net/home (date of access: 20.04.2023).
41. TensorFlow [Electronic resource]. – Mode of access: https://www.tensorflow.org (date of access: 20.04.2023).

ДОДАТОК А

```
import cv2
import numpy as np
import os
import matplotlib.pyplot as plt
import tensorflow as tf

# Load the sample image
sample =
cv2.imread("/kaggle/input/socofing/SOCOFing/Altered/Alter
ed-Hard/100__M_Left_index_finger_CR.BMP")

# Define the custom model
model = tf.keras.Sequential([
    tf.keras.layers.Conv2D(32, 3, activation='relu',
input_shape=sample.shape),
    tf.keras.layers.MaxPooling2D(),
    tf.keras.layers.Conv2D(64, 3, activation='relu'),
    tf.keras.layers.MaxPooling2D(),
    tf.keras.layers.Flatten(),
    tf.keras.layers.Dense(128, activation='relu'),
    tf.keras.layers.Dropout(0.5),
    tf.keras.layers.Dense(64, activation='relu'),
    tf.keras.layers.Dropout(0.5),
    tf.keras.layers.Dense(32, activation='relu'),
    tf.keras.layers.Dropout(0.5),
    tf.keras.layers.Dense(16, activation='relu'),
    tf.keras.layers.Dropout(0.5),
    tf.keras.layers.Dense(8, activation='relu'),
    tf.keras.layers.Dense(64)
])

# Compile the model
model.compile(optimizer='adam', loss='mse')

best_score = counter = 0
filename = image = None

# Loop through all images in the "Real" directory
```

```
for file in
os.listdir("/kaggle/input/socofing/SOCOFing/Real"):
    #if counter % 10 == 0:
        #print(counter)
        #print(file)
    counter += 1

    # Load the fingerprint image
    fingerprint_img =
cv2.imread("/kaggle/input/socofing/SOCOFing/Real/" +
file)

    # Preprocess the fingerprint image
    fingerprint_img = cv2.resize(fingerprint_img,
sample.shape[:2])
    fingerprint_img = np.expand_dims(fingerprint_img,
axis=0)

    # Train the model on the sample image
    sample_desc = model.predict(np.expand_dims(sample,
axis=0))
    model.train_on_batch(fingerprint_img, sample_desc)

    # Extract keypoints and descriptors using ORB
    orb = cv2.ORB_create()
    sample_kp, sample_desc = orb.detectAndCompute(sample,
None)
    fingerprint_kp, fingerprint_desc =
orb.detectAndCompute(fingerprint_img[0], None)

    # Use brute-force matching to find the best matches
between keypoints
    matcher = cv2.BFMatcher(cv2.NORM_L2, crossCheck=True)
    matches = matcher.match(sample_desc,
fingerprint_desc)

    # Sort the matches by distance
    matches = sorted(matches, key=lambda x: x.distance)

    # Select the best matches (with lowest distance)
    num_good_matches = min(len(matches), 50)
```

```
    good_matches = matches[:num_good_matches]

    # Compute the ratio of good matches to total
keypoints in both images
    keypoints_ratio = num_good_matches / len(matches)


    result = cv2.drawMatches(sample, sample_kp,
fingerprint_img[0], fingerprint_kp, good_matches, None)

    # Show the resulting image
    #plt.imshow(result)
    #plt.show()

    # Update the best score and filename if necessary
    if keypoints_ratio > best_score:
        best_score = keypoints_ratio
        filename = file
        image = fingerprint_img
        print(filename)
        print(image)
        plt.imshow(result)
        plt.show()

# Print the best match
print("Best match: {} with keypoints ratio of
{}".format(filename, best_score))



print(filename)
print(image)
plt.imshow(result)
plt.show()
```