

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: «Система ідентифікації за відбитками пальців»

оцінка « » Керівник доцент Мелкозьорова О.М
(прізвище та ініціали/підпис)

Голова ЕК

Рецензент професор Краснобаєв В.А
(прізвище та ініціали/підпис)

Лемешко О.В._____ Виконавець студент групи КБ-41

Золотоверхий Д.В.
(прізвище та ініціали/підпис)

РЕФЕРАТ

Пояснювальна записка містить 54 сторінки, 13 ілюстрацій, 2 додатки, 10 посилань на джерела інформації.

Мета цієї роботи – проаналізувати і дослідити актуальні технології ідентифікації, зокрема сучасні технології біометричної ідентифікації за відбитком пальців, а також створити власну програмну реалізацію системи ідентифікації за відбитками пальців.

У роботі використовувалась база даних відбитків пальців FVC (Fingerprint Verification Competition) 2000-х, 2002-х та 2004-х років. У якості середовища програмної розробки використовувався IntelliJ IDEA Community Edition.

Протягом роботи було практично досліджено технологію ідентифікації відбитків пальців на основі бібліотеки SourceAfis. Було створено програмну реалізацію системи ідентифікації особистості на мові програмування Java.

Дані дослідження можна використовувати при проектуванні або побудові систем біометричної ідентифікації за відбитком пальців з метою більш точного проведення ідентифікації та аналізу відбитків пальців. Створене програмне забезпечення вже можна використовувати для забезпечення безпекою інформації у промислових галузях

Ключові слова: БІОМЕТРИЧНА ІДЕНТИФІКАЦІЯ, МІНУЦІЇ, ВІДБИТКИ ПАЛЬЦІВ, SOURCEAFIS, FVC COMPETITION.

ABSTRACT

The explanatory note contains 54 pages, 13 illustrations, 2 appendices, 10 links to sources of information.

The purpose of this work is to analyze and research current identification technologies, in particular, modern fingerprint biometric identification technologies, as well as to create our own software implementation of the fingerprint identification system.

The FVC (Fingerprint Verification Competition) fingerprint database of 2000, 2002 and 2004 years was used in the work. IntelliJ IDEA Community Edition was used as the software development environment.

During the work, fingerprint identification technology based on the SourceAfis library was practically investigated. A software implementation of the personal identification system was created in the Java programming language.

Research data can be used in the design or construction of fingerprint biometric identification systems for more accurate fingerprint identification and analysis. The created software can already be used to ensure information security in industrial sectors

Key words: BIOMETRIC IDENTIFICATION, MINUTIAE, FINGERPRINTS, SOURCEAFIS, FVC COMPETITION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ	6
ВСТУП	7
1. ДОСЛІДЖЕННЯ ВІТЧИЗНЯНОЇ ТА ЗАРУБІЖНОЇ ЛІТЕРАТУРИ....	11
1.1 Огляд вітчизняної літератури	11
1.2 Аналіз сучасної зарубіжної літератури.....	13
2. ПОРІВНЯННЯ ТА АНАЛІЗ МЕТОДІВ ІДЕНТИФІКАЦІЇ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ	17
2.1 Сучасні методи ідентифікації особистості.....	17
2.2 Біометрична ідентифікація особистості	19
2.2.1 Процес функціонування системи біометричної ідентифікації.....	21
2.3 Система ідентифікації за відбитками пальців	22
2.4 Методологія ідентифікації за відбитками пальців	25
2.4.1 Мінущі.....	25
3. ПРОГРАМА ДЛЯ ВЕРИФІКАЦІЇ ЗА ВІДБИТКАМИ ПАЛЬЦІВ	30
3.1 Підготовка до проведення практичної частини.....	30
3.2 Програмна реалізація.....	32
3.3 Алгоритм роботи програми	34
3.3.1 Відбитки пальців.....	34
3.3.2 Створення програми.....	36
3.3.3 Тестування та експлуатація програмного забезпечення	38
3.4 Результати та перспективи використання мого програмного забезпечення	42

ВИСНОВКИ.....	45
ПЕРЕЛІК ПОСИЛАНЬ НА ЛІТЕРАТУРНІ ДЖЕРЕЛА	46
ДОДАТОК А.....	48
ДОДАТОК Б	51

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ СКОРОЧЕНЬ І ТЕРМІНІВ

FVC	Fingerprint Verification Competition (FVC) — міжнародний конкурс алгоритмів перевірки відбитків пальців, організований у 2000 році Лабораторією біометричних систем (Болонський університет).
ДНК	Це один із двох типів природних нуклеїнових кислот, що забезпечує зберігання, передачу з покоління в покоління і реалізацію генетичної програми розвитку й функціонування живих організмів.
Паттерн	Це повторюваний рішення для постійно виникаючих проблем. Це може бути алгоритм, структура даних, клас або методологія. В об'єктно-орієнтованому програмуванні використовуються паттерни проектування, які допомагають вирішувати певні проблеми проектування.
Фреймворк	Це набір бібліотек, модулів, інструментів та зразків коду, які створюють структуру або "каркас" для побудови програмного забезпечення. Фреймворки розробляються з метою спрощення розробки програмного забезпечення, надаючи загальні функції і можливості, які часто використовуються в конкретній області або для конкретного типу програмного забезпечення.

ВСТУП

У сучасному світі Кібербезпека стає все більш актуальною темою. З кожним днем різноманітні комп'ютерні загрози стають все складнішими і потужнішими, що може створювати значні ризики для безпеки людей і організацій.

Саме тому я вирішив обрати тему дипломної роботи, яка буде описувати та детально розкривати етапи процесу створення та керування системою безпеки. Обрана мною тема дипломної роботи, а саме: "Система ідентифікації за відбитками пальців", надає мені можливість зосередитись на конкретному методі верифікації для того щоб описати його максимально детально.

На сьогоднішній день системи ідентифікації за відбитками пальців є досить поширеними та використовуються в різних галузях, таких як Кібербезпека, криміналістика, медицина, логістика та інші. Аналізуючи вітчизняну та зарубіжну науково-технічну літературу, можна стверджувати, що розробка та вдосконалення систем ідентифікації за відбитками пальців продовжується.

У світі є велика кількість різних виробників систем ідентифікації за відбитками пальців, таких як Crossmatch, Suprema, Fujitsu, NEC, Precise Biometrics, Synaptics, та інші. Кожна з цих компаній пропонує різні технології, алгоритми та пристрої для ідентифікації особи за відбитками пальців.

Також, на сучасному ринку технологій представлені різні програмні та апаратні рішення, які дозволяють використовувати сучасні системи ідентифікації за відбитками пальців у різних галузях діяльності. Однією з головних переваг систем ідентифікації за відбитками пальців є їх висока точність та швидкість ідентифікації. Завдяки цьому, вони широко

використовуються у різних сферах, таких як фінансові установи, урядові органи, наукові дослідження, медицина та інші.

Протягом останніх років, існує певна тенденція до використання систем ідентифікації за відбитками пальців у мобільних пристроях, а саме - в смартфонах та планшетах. Це дозволяє користувачам швидко та зручно захищати свої приватні дані та пристрої, замість використання довгих паролів або інших методів ідентифікації.

Проте, разом з легкістю у використанні, існує ризик порушення конфіденційності та захисту персональних даних користувачів при використанні систем ідентифікації за відбитками пальців. Тому, потрібно дуже активно та доцільно вдосконалювати технології збереження та захисту персональних даних, для того щоб забезпечити максимальний рівень інформаційної безпеки.

Для коректного та більш чіткого застосування систем ідентифікації за відбитками пальців в різних галузях, необхідно розробляти та покращувати технології збирання та обробки відбитків пальців, а також більш якісно забезпечувати стійкість систем до різноманітних атак, що можуть загрожувати безпеці пристрою або даних. Також, для захисту персональних даних та конфіденційності користувачів при використанні систем ідентифікації за відбитками пальців, дуже важливо розробляти і вдосконалювати законодавчу базу, щоб нові протоколи та системи ставали більш безпечними та захищеними від втручання.

У вітчизняній технічно-науковій літературі присутні статті, книги та інші матеріали з дослідження систем ідентифікації за відбитками пальців, які описують процес розробки нових алгоритмів, методів обробки та аналізу відбитків пальців, забезпеченню безпеки даних при збереженні та обробці інформації, а також підвищенню швидкодії та точності систем ідентифікації. Проте, незважаючи на кількість матеріалу, наші вітчизняні розробки у цій галузі, порівняно з зарубіжними, можуть відставати за кількістю та якістю інновацій на декілька років, або навіть на декілька

десяти років. Детальніше поточну ситуацію буде описано у підрозділі 1.1 «Огляд вітчизняної літератури» та підрозділі 1.2 «Аналіз сучасної зарубіжної літератури»

Також патентний пошук показує, що системи ідентифікації за відбитками пальців продовжують розвиватися в різних напрямках, зокрема, з'являються нові методи збору та обробки даних, використання інших біометричних параметрів, таких як форма долоні структура вен та інші, які дозволяють підвищити точність та надійність систем ідентифікації.

З іншого боку, системи ідентифікації за відбитками пальців все ще мають свої недоліки, які стають причиною появи нових технологій та алгоритмів. Наприклад, проблемою є те, що відбитки пальців можуть бути пошкоджені або змінені в результаті травми або впливу погодних умов, що може призвести до помилок у процесі ідентифікації. Також, існує проблема збереження та захисту персональних даних при використанні систем ідентифікації за відбитками пальців.

У цілому, можна зробити висновок, що системи ідентифікації за відбитками пальців продовжують розвиватися та використовуватися в різних галузях діяльності, але є потреба в подальшому вдосконаленні технологій та методів для забезпечення більш високої точності та безпеки.

Мета цієї дипломної роботи - проаналізувати і дослідити актуальні методи створення та керування систем ідентифікації за відбитками пальців, які допоможуть підвищити рівень безпеки в сфері Кібербезпеки. Також, результатом роботи ставиться на меті створити власний прототип системи ідентифікації за відбитками пальців, використовуючи актуальні знання про керування системами безпеки та власні практичні навички, набуті протягом навчального процесу.

Робота зосередиться на розгляді теоретичної бази, підходів до розробки та реалізації таких систем, а також на дослідженні їх можливостей та обмежень.

У ході роботи буде детально проаналізовано різноманітні методи і технології, які застосовуються в системах ідентифікації за відбитками пальців. Дослідження буде включати аналіз попередніх робіт та існуючих систем, а також вивчення сучасних наукових розробок та технологій.

Також, на меті ставиться створення власної програмної реалізації системи ідентифікації особистості за відбитками пальців. Програма повинна мати дослідницький характер та надавати простір для вивчення та аналізу процесів створення та керування системами ідентифікації за відбитками пальців. Крім цього, мені потрібно розробити програму таким чином, щоб її можна було використовувати за призначенням у сучасних системах безпеки.

Отже, дипломна робота "Система ідентифікації за відбитками пальців" відображає важливість технологій Кібербезпеки у сучасному світі, дослідження та розробку нових методів та технологій для забезпечення безпеки ідентифікації користувачів у різних сферах діяльності. Результатом дослідження є прототип системи ідентифікації за відбитками пальців, яка може бути використана в практиці для підвищення рівня безпеки даних та зменшення ризику їх несанкціонованого доступу.

1 ДОСЛІДЖЕННЯ ВІТЧИЗНЯНОЇ ТА ЗАРУБІЖНОЇ ЛІТЕРАТУРИ

1.1 Огляд вітчизняної літератури

Питанням створення та захисту інформаційних систем і баз даних у сучасній вітчизняній технічній та науковій літературі приділено багато уваги. З часом різні методи персональної біометричної ідентифікації стають все більш логічними та загальнозастосовуваними заходами безпеки через їх надійність, конфіденційність та простоту використання. Протягом багатьох років велика кількість вітчизняних наукових досліджень оцінювала різні методи біометричної автентифікації, наводячи приклади особистих досліджень і аналізів, результати практичного впровадження систем, а також основні переваги та недоліки різних систем біометричної ідентифікації.

Наукова робота "Біометричні технології" чиїми авторами є Царьов Р.Ю та Лемежа Т.М. - це огляд основних принципів та технологій біометричної ідентифікації. У роботі розглянуто різноманітні типи біометричних систем, такі як системи розпізнавання обличчя, відбитків пальців, розпізнавання рис характеру та інших фізіологічних та поведінкових ознак.

Автори звертають увагу на актуальну важливість забезпечення безпеки даних при використанні біометричних систем ідентифікації особистості. Також наведені приклади успішного впровадження біометричних систем в різних сферах сучасної діяльності, таких як банківський сектор, державна служба, транспорт і т.д.

У роботі детально описані технічні аспекти біометричної ідентифікації, такі як захист інформації, алгоритми обробки даних, організація та функціонування систем. Крім того, у роботі розглянуто важливість етичних, правових і соціальних аспектів використання біометричних технологій.

Наукова робота "The method of vicinity minutiae decomposition with higher level graphs for fingerprint verification" за авторством Росомахіна С.М., Мелкозьорової О.М. та Нарежного О.П. є загальним оглядом біометричних технологій та їх розвитку. Ця наукова стаття починається з історії біометрії та описує значення використання систем ідентифікації за відбитками пальців у сучасному світі. Автори описують сфери використання систем ідентифікації за відбитками пальців та наводять приклади можливих реалізацій таких систем.

В основній частині наукової статті, основну увагу приділено процесу створення надійної системи ідентифікації та процес збору даних, зображення відбитка пальця, методи обробки та порівняння. Крім того, автори обговорюють застосування біометричних технологій в різних галузях, таких як медицина, банківська справа, державний управління та безпека. Загальна мета цієї статті - описати сучасний стан та перспективи розвитку біометричних технологій та їх застосування в різних галузях, включаючи системи ідентифікації за допомогою відбитку пальців.

Опис систем ідентифікації за відбитками пальців у цій роботі включає детальні пояснення щодо основних етапів роботи даної системи. Починаючи з процесу сканування відбитків пальців, автори описують різні методи та технології, які використовуються для захоплення відбитків, включаючи оптичні, ємнісні та ультразвукові датчики.

Наступним етапом є обробка та збереження отриманих відбитків пальців. Тут автори описують процеси які використовуються для попередньої обробки даних, включаючи видалення шуму, калібрування, і фільтрацію. Далі розглядається процес витягування особливостей відбитків пальців, які використовуються для подальшої ідентифікації. У якості основного засобу ідентифікації у статті використовують процес вилучення мінуцій.

Останнім етапом є використання алгоритмів для порівняння витягнутих особливостей відбитків пальців з тими, що зберігаються у базі

даних. Якщо ідентифікація відбитку пальця успішна, то особа отримує доступ до системи. Якщо ж ідентифікація не пройшла, то доступ забороняється.

Проаналізувавши вищенаведену літературу ми можемо окреслити для себе основні переваги та недоліки систем ідентифікації за відбитками пальців. Серед переваг можемо виділити:

- Високу надійність (статистичні показники цього методу вищі, ніж у методів розпізнавання обличчя, голосу, підпису);
- Низьку вартість обладнання для сканування зображення відбитка пальця;
- Досить просту процедуру сканування відбитків пальців;

Недоліками цього методу будуть:

- Папілярний візерунок відбитків пальців дуже легко пошкоджується дрібними подряпинами, порізами, що може завадити процесу ідентифікації;
- Недостатній захист від підробок зображення відбитків пальців;

З цього ми можемо дійти висновку, що вітчизняна наукова література у наші часи дуже детально описує процес проведення біометричної ідентифікації, зокрема роблячи акцент на створенні систем, що приділяють більшу увагу фільтрації та калібруванню отриманих даних, зменшуючи цим можливу похибку при ідентифікації. Через те що у наші часи системи біометричної ідентифікації використовуються у багатьох сферах навколишньої середовища (мобільні телефони, паспорти, перепустки, тощо), перевагу надають системам, що можуть найбільш точно опрацьовувати інформацію та правильно відображати результати біометричної автентифікації.

1.2 Аналіз сучасної зарубіжної літератури

Аналізуючи актуальну зарубіжну літературу на тему проектування та створення систем біометричної ідентифікації, ми можемо дійти висновку,

що технології про які йде річ в зарубіжних наукових роботах, мають більший потенціал в використанні та кращий рівень актуальної реалізації ніж системи, що були представлені та описані у вітчизняній літературі.

Більша частина зарубіжних технологій та елементів систем ідентифікації за відбитком пальців мають кращі показники діапазону температур, імовірності хибного прийняття та імовірності помилкового відхилення, що надають перевагу даним системам у можливості та якості потенційного використання.

Книга "Biometric Systems: Technology, Design and Performance Evaluation" є одним з ключових джерел, що стосуються біометричних систем і технологій, які використовуються для ідентифікації особистості. Редактори книги James L. Wayman, Anil K. Jain, Davide Maltoni та Dario Maio висвітлюють важливі аспекти створення та вдосконалення біометричних систем, включаючи системи, які використовують відбитки пальців для ідентифікації особистості.

У книзі "Biometric Systems: Technology, Design and Performance Evaluation" описується широкий спектр біометричних систем, включаючи системи ідентифікації за допомогою відбитку пальців, системи розпізнавання обличчя, системи розпізнавання голосу, системи розпізнавання раковини вуха та інші.

Однак, системи ідентифікації за допомогою відбитку пальців були розглянуті досить детально і представляють значний обсяг матеріалу у книзі. Книга містить розділи, присвячені різним аспектам створення систем ідентифікації за допомогою відбитку пальців, такі як:

- Збір даних відбитків пальців та методи їх обробки.
- Розпізнавання відбитків пальців та алгоритми, які використовуються для цього.
- Валідація та оцінка систем ідентифікації за допомогою відбитку пальців.
- Проблеми, пов'язані з захистом даних та приватністю.

Книга також описує різні підходи до реалізації систем ідентифікації за допомогою відбитку пальців, такі як системи з одним сенсором, системи з багатьма сенсорами та системи зі змінними довільними параметрами.

Окрім цього, у роботі надаються розгорнуті інформаційні матеріали про процес тестування та оцінки продуктивності біометричних систем. Редактори наводять докладні інструкції щодо того, як проводити тестування систем ідентифікації з використанням відбитків пальців, як оцінювати ефективність систем, та як забезпечувати надійність і точність.

Роблячи висновки, ми можемо дійти висновку, що як вітчизняна так і зарубіжна література дуже детально описують процес створення та використання технологій біометричної ідентифікації, проте технічні властивості та актуальність методології, що були представлені в сучасній зарубіжній літературі, робить більш надійними та легкими у використанні саме зарубіжні технології.

"Handbook of Biometrics", написана А. К. Jain, F. Patrick та А. Arun, є всеосяжним посібником, що висвітлює широкий спектр тем, пов'язаних із біометрією.

Книга починається з вступного розділу, в якому автори обговорюють загальні принципи біометрії. Вони вводять читача в поняття біометрики, пояснюють, чому це важливий інструмент для сучасної системи ідентифікації, а також розглядають загальні виклики та можливості у цій галузі.

Далі йде обговорення специфічних методів біометрії, включаючи ідентифікацію за відбитками пальців. В цьому розділі автори детально описують, як системи визначення відбитків пальців збирають, обробляють та використовують дані для ідентифікації особи. Їх аналіз включає обговорення алгоритмів, які використовуються для обробки та аналізу даних відбитків пальців.

Автори також присвячують значний час іншим методам біометричної ідентифікації, таким як визначення за голосом, рисами обличчя, сітківкою

ока тощо. Кожен з цих методів аналізується в деталях, пояснюючи технологію, що стоїть за ними, а також їх потенційні переваги та недоліки.

Нарешті, автори звертають увагу на проблеми конфіденційності та безпеки, пов'язані з біометрією. Вони обговорюють, як важливо забезпечити належний захист біометричних даних від несанкціонованого доступу, а також як можуть бути вирішені можливі юридичні та етичні питання.

Загалом, "Handbook of Biometrics" - це детальне і всебічне джерело, яке надає глибоке розуміння біометрії, її методів, викликів та можливостей.

2 ПОРІВНЯННЯ ТА АНАЛІЗ МЕТОДІВ ІДЕНТИФІКАЦІЇ НА ОСНОВІ БІОМЕТРИЧНИХ ДАНИХ

2.1 Сучасні методи ідентифікації особистості

Сьогодні існує багато різних методів ідентифікації особистості, які дозволяють точно та надійно визначити особу. Один з найбільш популярних методів - це біометрія, яка використовує фізичні або біологічні характеристики людини, наприклад відбитки пальців, обличчя, стійкий зір, голос та інші. Крім того, використовуються методи, які базуються на RFID, що вбудовуються в предмети, або ідентифікації за допомогою смарт-карток. Інноваційні методи використовують штучний інтелект та машинне навчання, що дозволяє збільшити точність та швидкість ідентифікації.

В сучасному світі дуже важливо мати надійні методи ідентифікації, особливо в контексті безпеки та протидії злочинності. Проте на вибір конкретного методу впливають різні фактори, такі як вартість, точність, зручність використання та захист від зламу.

Крім того, дуже важливо враховувати етичні аспекти використання методів ідентифікації, зокрема забезпечення конфіденційності та захисту персональних даних. Для цього необхідно розробляти та використовувати методи шифрування та забезпечення безпеки даних.

Найбільш актуальними методами ідентифікації особистості можна назвати Парольну ідентифікацію, Апаратну ідентифікацію та Біометричну ідентифікацію особистості. Кожен з цих методів має свої переваги та недоліки.

Рисунок 2.1 зображує три базових методи ідентифікації та підтипи кожного з цих методів.

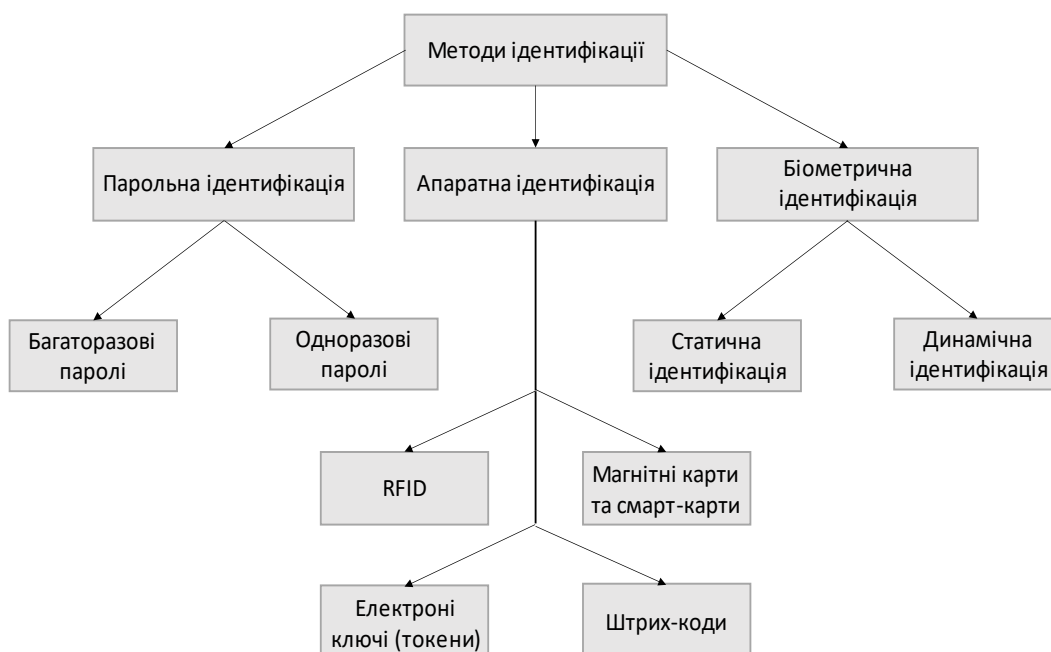


Рисунок 2.1 - Методи ідентифікації особистості

Парольна ідентифікація базується на введенні користувачем певного кодового слова або комбінації конкретних символів, яку він сам встановлює. Основні переваги цього методу - це легкість використання та низька вартість. Крім того, паролі можуть бути змінені або скинуті в разі їх забуття або втрати. Однак, недоліки парольної ідентифікації полягають в тому, що паролі можуть бути легко підібрані або зламані, особливо якщо вони складаються зі слабких символів або користувачі використовують ті ж самі паролі на різних сайтах та сервісах.

Апаратна ідентифікація, також відома як ідентифікація з використанням апаратних ключів, полягає в тому, що користувач використовує спеціальний апаратний пристрій (наприклад, USB-ключ або смарт-карту), щоб підтвердити свою особистість. Головні переваги апаратної ідентифікації полягають в тому, що вона забезпечує високий рівень безпеки та захисту від зламу, оскільки ключі зазвичай мають високу ступінь шифрування та захисту даних. Однак, недоліками цього методу є складність використання та висока вартість апаратного обладнання.

Біометрична ідентифікація базується на використанні фізичних або біологічних характеристик людини, таких як відбитки пальців, обличчя, голос, рухи очей та інші. Цей метод дозволяє встановити ідентичність людини з високою точністю, оскільки кожна людина має унікальні біометричні характеристики.

Перевагами біометричної ідентифікації є висока точність та швидкість ідентифікації, а також відсутність необхідності запам'ятовувати складні паролі або носити прилади із собою. Крім того, біометричні дані не можна загубити або забути, вони є природженими людині.

Однак, біометрична ідентифікація також має свої недоліки. Наприклад, у деяких випадках біометричні дані можуть бути скомпрометовані, наприклад, якщо вони витекли через вразливість системи або були скопійовані. Крім того, зберігання біометричних даних може порушувати приватність та конфіденційність даних.

Окрім того, не всі біометричні технології однаково ефективні для всіх людей. Наприклад, деякі системи розпізнавання обличчя можуть бути менш ефективними для людей з різними етнічними особливостями або які мають зміни в зовнішності (наприклад, зміна волосся або бороди).

З цього ми можемо дійти висновку, що кожен метод ідентифікації має свої переваги та недоліки, і вибір конкретного методу залежить від багатьох факторів, таких як вартість, точність, зручність використання та захист від зламу.

2.2 Біометрична ідентифікація особистості

На 2023 рік методи біометричної ідентифікації є найбільш поширені у використанні в різних сферах нашого життя. Проте, через велику кількість різноманітних методів ідентифікації, кожен з них буде відрізнятися один від одного не лише за технологією використання, а й за легкістю, надійністю та вартістю. Наприклад, технологія ідентифікації за допомогою ДНК можна вважати найточнішою (ідентифікація за допомогою ДНК

забезпечує 100% точність при ідентифікації), проте через важкість використання, необхідний час та вартість процесу, ця технологія використовуються лише у криміналістиці.

Усі методи біометричної ідентифікації можна класифікувати за різними ознаками. Основним критерієм класифікації є вид біометричної характеристики, яку використовують для ідентифікації. Ось декілька видів біометричних ідентифікаторів:

Фізіологічні характеристики:

- Розпізнавання обличчя: включає в себе аналіз геометрії та текстури обличчя;
- Розпізнавання відбитків пальців: використовується для аналізу унікальних ліній та дуг пальців;
- Розпізнавання різноманітних біометричних характеристик, таких як руки, очі, вуха, ДНК, та інші.

Поведінкові характеристики:

- Розпізнавання голосу: аналізується частота, тембр та інші аспекти голосу;
- Розпізнавання почерку: використовується для аналізу унікальних рис почерку, таких як розмір, форма та стиль написання.

Суміш характеристик:

- Розпізнавання мультибіометрики: поєднання кількох різних біометричних характеристик для покращення точності ідентифікації.

Наявність великої кількості методів біометричної та будь-якої іншої системи ідентифікації, надає можливість використовувати кожен з цих методів максимально ефективно. Кожен з цих методів має певні недоліки та переваги над іншими методами біометричної ідентифікації, проте

розглядаючи конкретні сфери використання систем ідентифікації, ми можемо дійти висновку, що деякі методи ідентифікації не ефективно використовувати у певних сферах. Наприклад, метод ідентифікації за допомогою ДНК, неможливо у наш час використовувати у мобільних телефонах через необхідну кількість часу для аналізу.

2.2.1 Процес функціонування системи біометричної ідентифікації

Загалом, біометричні системи працюють на основі наступних принципів наступних принципів. Всі системи спочатку працюють в режимі реєстрації, тобто система повинна спочатку зафіксувати і зберегти певний біометричний ідентифікатор.

Цей ідентифікатор використовується для ідентифікації користувача. Деякі типи систем можуть використовувати більше одного біометричного ідентифікатора (наприклад, коли ідентифікація базується на відбитках пальців або параметрах очей). Після отримання біометричного ідентифікатора система відповідним чином перетворює його в електронний формат. Цей етап системи біометричної ідентифікації називається реєстрацією, під час якої система отримує необхідну початкову інформацію необхідну для подальших операцій. Зазвичай системи біометричної ідентифікації не зберігають такі зображення, як відбитки пальців, сітківка ока або геометрія долоні.

Ці системи зберігають так звані шаблони ідентифікаторів, які являють собою одну або кілька цифрових послідовностей, отриманих під час обробки біометричного ідентифікатора. Це означає, що біометричний ідентифікатор, наданий користувачем за допомогою спеціального записуючого пристрою, зберігається в електронній формі, яка потім обробляється в кілька етапів з використанням різних алгоритмів.



Рисунок 2.2 – Спрощена структурна схема системи біометричної ідентифікації

2.3 Система ідентифікації за відбитками пальців

Станом на 2023 рік системи ідентифікації за відбитками пальців стають усе більш актуальними та починають більше використовуватись в різних сферах, таких як створення біометричних документів, певні технології в медицині, у транспортній промисловості та багатьох інших сферах сучасного соціуму.

Однак, незважаючи на стрімкий розвиток цих систем, продовжують виникати нові проблеми у сфері конфіденційності та безпеки даних користувачів. У найближчому майбутньому найефективнішим вирішенням цієї проблеми може стати вдосконалення технологій шифрування та аутентифікації. Альтернативне рішення - більш контрольоване використання біометричних даних, щоб уникнути вразливостей в системі.

Нові технології, такі як глибоке навчання, штучний інтелект і розподілена обробка даних, також можуть бути використані для підвищення точності систем розпізнавання відбитків пальців. Крім того, багато сучасних компаній, що працюють у цій сфері, активно досліджують нові технології та методи підвищення безпеки інформації користувачів.

Стан ідентифікації за відбитками пальців у 2023 році є дуже просунутим і достатньо придатним для побудови систем захисту комп'ютерної інформації.

Системи розпізнавання відбитків пальців також використовуються у військовій промисловості. Наприклад, в авіаційній і морській безпеці біометрична ідентифікація за відбитками пальців використовується для контролю доступу на судна і літаки.

Також, у сфері банківських технологій системи ідентифікації за відбитками пальців використовуються для ідентифікації та верифікації особи клієнту під час фінансових транзакцій. Дана система може допомогти запобігти шахрайству та будь-яким видам фінансових злочинів. У сфері охорони здоров'я ці системи використовуються для зберігання медичної інформації про пацієнтів та забезпечення конфіденційності.

Державні установи також використовують системи ідентифікації за відбитками пальців для забезпечення безпеки та зручності при перетині кордонів, а в секторі соціального забезпечення - для виявлення злочинів і зловживань.

Однак, існує не так багато скарг на потенційні загрози, пов'язані з використанням систем ідентифікації за відбитками пальців. Однією з них є можливе вторгнення в приватне життя і використання отриманих даних ненадійними сторонами. Це особливо небезпечно, якщо біометричні дані зберігаються у великій базі даних і хакери отримують до неї доступ. Надійність системи також викликає сумніви, оскільки відбитки пальців можуть бути змінені за допомогою хірургічних процедур або створення синтетичних відбитків.

Втім, технологія систем ідентифікації за відбитками пальців значно покращилася за останні роки. Наприклад, більш точні алгоритми зіставлення відбитків пальців, що використовуються в таких системах, дозволяють проводити більш точну і надійну ідентифікацію. Крім того, з'явилися нові технології для підвищення якості сканування і розпізнавання

відбитків пальців, такі як сканери на основі штучного інтелекту і машинного навчання.

Загалом, системи розпізнавання відбитків пальців постійно розвиваються і знаходять нові застосування в багатьох сферах життя. З одного боку, ці системи забезпечують більшу безпеку та надійність у різних галузях, таких як фінанси, охорона здоров'я та національна безпека. З іншого боку, потенційні загрози конфіденційності та надійності цих систем вимагають розробки відповідних заходів для забезпечення безпеки та конфіденційності даних.

Зазвичай, процес ідентифікації за допомогою відбитку пальців складається з кількох етапів:

- 1) Збір відбитка пальця. Для цього використовуються спеціальні сканери або сенсорні екрани, які дозволяють зняти відбиток пальця. Однак, якщо пальці мають порізи, подряпини або інші пошкодження, то сканування може бути ускладнене.
- 2) Обробка відбитка пальця. Зазвичай відбиток пальця обробляється за допомогою алгоритмів обробки зображень, що дозволяє виокремити характеристики, які можуть слугувати основою для подальшої ідентифікації.
- 3) Порівняння збереженого відбитка пальця з базою даних. Після обробки відбитка пальця, система порівнює його з базою даних, яка містить інформацію про відбитки пальців користувачів.
- 4) Прийняття рішення. В залежності від результатів порівняння система приймає рішення щодо ідентифікації або відхилення запиту.

Ідентифікація за допомогою відбитку пальця має кілька переваг порівняно з іншими методами ідентифікації. Вона є надійною та швидкою, а також не вимагає від користувача запам'ятовування складних паролів або використання фізичних токенів для ідентифікації. Крім того, відбиток пальця є унікальним для кожної людини, що забезпечує високий рівень точності ідентифікації.

Однак, існують деякі виклики та ризики, пов'язані з використанням систем ідентифікації за допомогою відбитку пальця. Наприклад, можливість підробки відбитка пальця, а також проблеми з приватністю, які можуть виникнути, якщо система не буде забезпечувати відповідний рівень захисту даних.

2.4 Методологія ідентифікації за відбитками пальців

Станом на 2023 рік існує кілька методів і технологій, які використовуються для збору та аналізу відбитків пальців. Деякі з найбільш поширених методів включають:

- Оптичне сканування - використовується для отримання високоякісного зображення відбитка пальця з використанням оптичної камери.
- Контактне сканування - використовується для отримання відбитка пальця шляхом прямого контакту з сенсором.
- Ультразвукове сканування - використовується для отримання відбитка пальця за допомогою високочастотних звукових хвиль.
- Капацитивне сканування - використовується для вимірювання електричного заряду, який генерується при дотику пальця до сенсора.
- Термічне сканування - використовується для вимірювання теплового випромінювання, яке відбивається від поверхні пальця.

У більшості випадків, системи ідентифікації за відбитком пальця використовують комбінацію кількох з цих методів для збору та аналізу відбитків пальців. Крім того, системи можуть використовувати різні алгоритми обробки даних для забезпечення високої точності ідентифікації.

2.4.1 Мінущі

Більшість вищенаведених систем ідентифікації відбитків пальців використовують мінущі у якості основного елементу навколо якого

будується певний алгоритм який дозволяє проводити ідентифікацію або аналіз відбитків пальців.

Мінуції (англ. Minutiae) - це термін, який використовується в контексті біометричної ідентифікації за відбитком пальця. Він відноситься до невеликих особливостей або деталей, які знаходяться на поверхні пальця та можуть бути використані для ідентифікації особи.

Мінуції включають такі риси, як кінцеві точки ліній, розгалуження та інші особливості, які можуть бути виявлені на відбитку пальця. Ці мінуції збираються з відбитка пальця і використовуються для створення унікального "шаблону" пальця, який може бути порівняно з шаблонами інших відбитків пальців у базі даних для ідентифікації конкретної особи.

Такі мінуції можуть бути виявлені технологіями сканування відбитка пальця, такими як оптичне сканування, контактне сканування, ультразвукове сканування, капацитивне сканування та термічне сканування, які можуть виявляти дрібні особливості на поверхні пальця. Мінуції є важливим елементом для створення точного та безпечного профілю пальцевої біометричної ідентифікації.

З цього ми можемо дійти висновку, що мінуції в біометрії є прикладами локальних розривів папілярного малюнку шкіри на відбитках пальців. Мінуції можуть бути різних типів. Наприклад:

- Кінцева точка (англ. ending ridge) - це точка, де пряма лінія відбитка закінчується.
- Початкова точка (англ. bifurcation) - це точка, де пряма лінія відбитка розгалужується на дві лінії.
- Внутрішня точка (англ. ridge dot) - це невелика точка, яка з'являється на прямій лінії відбитка.
- Кільце (англ. enclosure) - це область, де декілька ліній відбитка оточують певну область.

- Сполучникова точка (англ. short ridge або bridge) - це точка, де дві лінії відбитка з'єднуються дуже короткою лінією.
- Острівець (англ. island) - це невелика область, де лінії відбитка утворюють замкнену область всередині більшої області.
- Двійник (англ. spur) - це відгалуження від основної лінії відбитка.

Ці мінуції зазвичай використовуються в системах біометричної ідентифікації для порівняння відбитків та визначення їхньої унікальності.

Серед різних типів мінуцій на відбитках пальців, кінцеві точки та початкові точки є найбільш поширеними та використовуються в більшості систем біометричної ідентифікації, оскільки вони є більш стійкими та унікальними з точки зору відтворення відбитка пальця.

Внутрішні точки, сполучникові точки та кільця також можуть бути використані для біометричної ідентифікації, але менш часто порівняно з кінцевими та початковими точками.

Острівці та двійники дуже рідко використовуються у біометрії, але можуть бути корисними для визначення рівня деталізації відбитка пальця та стійкості його розпізнавання.

Для того щоб продемонструвати як саме виглядають різні види мінуцій, я звернусь до одного з відбитків пальців з бази даних FVC Competition (детальніше у підрозділі 3.1 «Підготовка до проведення практичної частини»).



Рисунок 2.3 Приклади мінуцій на відбитку пальця

Окрім різновидів самих мінуцій, на даний момент використовується декілька методів для того щоб мінуції вилучати. Станом на 2023 рік є дуже багато методологій, що можуть використовуватись у системах ідентифікації різного рівня складності та комплексності, проте основні методи виглядають наступним чином:

- 1) Порогова бінаризація працює так, що відбиток пальця перетворюється у чорно-біле зображення, і кожна точка аналізується щодо її сусідів. Наприклад, точка може вважатися мінуцією, якщо вона є кінцем лінії (має лише одного сусіда) або є точкою відгалуження (має трьох сусідів).
- 2) Аналіз напрямку рис (з англ. Ridge Flow Analysis) передбачає використання напрямку ліній відбитка пальця (візуалізованого як поле векторів) для виявлення мінуцій. Також до цього методу можна додати засіб вилучення мінуцій на основі циклів Гамільтона.

- 3) Алгоритми машинного навчання використовують машинне навчання та нейронні мережі для виявлення мінуцій. Ці методи можуть бути навчені розпізнавати мінуції на основі великої кількості прикладів відбитків пальців.
- 4) Градієнтний метод використовує величину та напрям градієнтів зображення для визначення мінуцій.

Усі ці методи мають свої плюси та мінуси, і вибір конкретної методології залежить від конкретних вимог до точності та швидкості.

3 ПРОГРАМА ДЛЯ ВЕРИФІКАЦІЇ ЗА ВІДБИТКАМИ ПАЛЬЦІВ

3.1 Підготовка до проведення практичної частини

Для виконання практичної частини мені потрібно було змодельовати послідовний план роботи, що буде описувати кожний етап дослідження.

Такий план в моєму випадку буде виглядати наступним чином:

- Потрібно знайти базу даних відбитків пальців для проведення особистих досліджень
- Розробити систему або програму, що буде виконувати аналіз відбитків пальців на основі створеного алгоритму
- Проаналізувати відбитки пальців та дослідити різні методології процесу для того щоб знайти найбільш точніший та доступніший
- Підвести підсумки досліджень

У рамках першого етапу я звернувся до бази даних відбитків пальців FVC Competition за 2002 та 2004 роки. Fingerprint Verification Competition (FVC) — міжнародний конкурс алгоритмів перевірки відбитків пальців, організований у 2000 році Лабораторією біометричних систем (Болонський університет). Вони встановили загальний еталон, що дозволяє розробникам однозначно порівнювати свої алгоритми, і надали огляд найсучаснішого розпізнавання відбитків пальців. Бази даних відбитків пальців знаходяться у відкритому доступі, тому для завантаження мені потрібно було лише перейти на офіційний сайт конкурсу та обрати ті бази даних, що мені потрібні.

Під час проведення другого етапу, мені потрібно було обрати найбільш зручну у використанні та керуванні систему. Серед варіантів були такі відомі приклади програмного забезпечення як PyFingerprint або NIST Biometric Image Software (NBIS), проте NIST Biometric Image Software наразі не поширюють ліцензію на використання, тому в мене не

було можливості його протестувати. Щодо PyFingerprint, ця бібліотека потребує наявності системи сканування відбитків пальців для коректного використання, тому я вирішив використати у практичній частині бібліотеку SourceAFIS, що працює на мові програмування .NET, проте була адаптована під Java для виконання практичної частини моєї дипломної роботи.

SourceAFIS є відкритим програмним забезпеченням для ідентифікації відбитків пальців. Він надає API для роботи з відбитками пальців, що можуть бути використані в аплікаціях для перевірки автентичності або ідентифікації користувачів.

Основні особливості та функціонал SourceAFIS:

- 1) Ідентифікація та верифікація відбитків пальців: SourceAFIS може використовувати відбитки пальців для ідентифікації окремих осіб, порівнюючи відбиток пальця з базою даних відбитків, або для верифікації, перевіряючи, чи відповідає відбиток пальця вже зареєстрованому відбитку.
- 2) Алгоритми виявлення характеристик: SourceAFIS використовує спеціальні алгоритми для виявлення характеристик відбитків пальців, таких як відрог та закінчення гілок, які є унікальними для кожної особи.
- 3) Порівняння та оцінка подібності: SourceAFIS вміє порівнювати відбитки пальців та оцінювати ступінь подібності між ними. Це може бути використано для визначення, чи належить відбиток палець конкретній особі.

Основні переваги SourceAFIS:

- 1) Відкритий код: SourceAFIS є відкритим програмним забезпеченням, що означає, що ви можете вільно використовувати, копіювати, модифікувати та поширювати його. Це також означає, що ви можете допомогти у вдосконаленні SourceAFIS, вносячи внески у код.

- 2) Багатоплатформеність: SourceAFIS доступний для різних мов програмування і платформ, включаючи .NET, Java та інші.
- 3) Висока точність та швидкість: SourceAFIS надає високу точність ідентифікації відбитків пальців, використовуючи сучасні алгоритми та техніки. Він також оптимізований для швидкості, що робить його підходящим для використання в реальному часі.
- 4) Масштабованість: SourceAFIS може працювати з великими базами даних відбитків пальців, що робить його підходящим для використання в масштабних системах ідентифікації.

SourceAFIS використовує алгоритми обробки зображень та комп'ютерного зору для вилучення мінуцій, або точок інтересу, з відбитків пальців. Відбитки пальців є унікальними для кожної особи завдяки паттернам гребінців шкіри, які включають закінчення гребінців та біфуркації, відомі як мінуції. Для розуміння алгоритму роботи цієї бібліотеки, я наведу загальний принцип її роботи. Спочатку проходить зчитування зображення, SourceAFIS зчитує зображення відбитка пальця та конвертує його у відтінки сірого, що спрощує подальшу обробку. Після цього зображення проходить попередню обробку. Зображення проходить через кілька етапів попередньої обробки, що включає згладжування шуму, вирівнювання контрасту та інші методи покращення якості. Далі програма займається вилученням мінуцій. Після попередньої обробки, SourceAFIS використовує алгоритми виявлення краю для вилучення мінуцій. Мінуції можуть бути різних видів, детальніше ми розглядали у підрозділі 2.4.1 - «Мінуції». Останнім етапом є створення та збереження мінуцій. Інформація про мінуції, що включає їх положення та тип, зберігається для подальшого використання, наприклад, для порівняння відбитків пальців.

3.2 Програмна реалізація

Написана мною програма має на меті можливість вилучення мінуцій для ідентифікації відбитку пальців за цими мінуціями. Після того як

відбиток пальців буде збережено у систему, за цим відбитком встановлюється певний ідентифікатор (index 0,1,2... і т.д.), що буде закріплено за людиною, якої належить цей відбиток пальця. Також, програма має можливість знаходити ідентифікатор після його збереження у буфер системи, за відбитком пальця.

Програма була створена з використанням технології «In memory», завдяки чому програма не має необхідності в створенні окремої бази даних, де усі відбитки пальців будуть зберігатися разом з ідентифікаторами. Це допомагає підвищити швидкодію та універсальність використання програми. Дане рішення було прийнято для зручності використання програми в рамках тестового продукту, що має дослідницькі цілі, а саме – реалізацію практичної частини дипломної роботи. За необхідності, до програми можливо буде створити та додати базу даних, що дає можливість використовувати програму в реальних умовах промисловості для створення безпеки ідентифікації особистості. Також, до цієї системи за необхідності можливо підключити фізичний сканер відбитків пальців, тому що бібліотека SourceAFIS та моя реалізація ідентифікуючої системи дозволяють використання технології у реальному часі.

Важливим елементом програми є те, що за одним відбитком пальців можливо закріпити лише один ідентифікатор. Через це людина, чию особу необхідно буде ідентифікувати при використанні програми, може бути ідентифікована лише за відбитком одного пальця. Більшість промислових систем безпеки використовують лише один палець для ідентифікації особи, через те що навіть наявність двох відбитків пальців збільшить рівень навантаження на систему та необхідного розміру її оперативної пам'яті вдвічі. Саме тому, за одним ідентифікатором буде встановлено лише один відбиток пальців та набір мінуцій.

Для коректного відображення та використання програми, повинен використовуватись фреймворк для автоматизації збирання проєктів Apache

Maven 3 (третьої версії). У якості мови програмування була обрана Java, а для того що запустити програму потрібна Java версії 11 або пізніша.

Наразі програмна реалізація не має графічного інтерфейсу, тож використання можливе через консоль за допомогою команд «save <path>», «saveAll <path>» та «find <path>». Наявність графічного інтерфейсу програми може бути виправдано при необхідності реалізувати її для публічного використання, чого наразі програма не передбачає.

Програмною реалізацією також передбачено функцію «help», яка може бути викликана для опису усіх можливих функцій керування системою. Функція «Exit» завершує роботу програми.

Програмний код основної програми поданий у повному виді у Додатку А.

3.3 Алгоритм роботи програми

3.3.1 Відбитки пальців

Для створення системи та перевірки її реалізації нам потрібно знайти базу даних, з якою ми будемо працювати. Для прикладу перевірки алгоритмів, я буду використовувати базу даних FVC Competition за 2002 рік, що знаходиться на офіційному сайті міжнародного конкурсу. Після завантаження ми будемо мати 4 різні директорії з відбитками пальців

DB1_V	10.05.2023 18:27	Папка с файлами
DB2_V	10.05.2023 18:25	Папка с файлами
DB3_V	10.05.2023 18:25	Папка с файлами
DB4_V	10.05.2023 18:25	Папка с файлами

Рисунок 3.1 База даних відбитків пальців FVC Competition

Через те, що я можу наразі використовувати лише бази даних анонімних осіб, в мене немає можливості задати ідентифікатори (ім'я, фамілія) до кожного з цих відбитків пальців. Саме тому я буду робити це

власноруч, використовуючи властивості та функціонал свого програмного забезпечення.

Важливо наголосити, що у базі даних надано декілька варіантів відбитків одного й того самого пальця. Без попередніх модифікацій у базі даних вони мають спільний ідентифікаційний номер, наприклад – «101_...». Проте порядковий номер в кожного зі сканувань одного й того ж самого відбитку пальця буде різний, тому два різних сканування одного й того ж самого пальця будуть виглядати як «101_1» та «101_2». Проте «102_1» - це буде вже відбиток іншого пальця.

Це допоможе мені дослідити корисність використання бібліотеки SourceAfis при створенні систем ідентифікації за відбитком пальця. Тому що я зможу завантажити до системи одне будь-яке сканування відбитку пальця і якщо система при виконанні пошуку інших прикладів сканувань цього ж самого пальця з інших ракурсів буде показувати спільний ідентифікатор, це значить що система працює вірно, тому що при скануванні одного й того ж самого пальця проте під різними кутами або з різною площиною сканування, система усе одно повинна ідентифікувати цей відбиток. Виключенням може бути лише ситуація, коли після сканування палець був фізично пошкоджений, та цілісність папілярних ліній було зруйновано. Саме через це при повторному скануванні відбитку пальця він може бути ідентифікований як інший палець та користувачу не буде надано доступ до системи.

Проте у рамках використання бази даних відбитків пальців FVC Competition це буде неможливо через те що кожне сканування було проведено у приблизно один й той самий час з попереднім, та палець не міг зазнати шкоди.



Рисунок 3.2 Відбитки пальців

Також, дуже важливо пам'ятати що у кожній системі ідентифікації особистості повинен бути певний процент збігу даних (мінуцій у випадку з відбитками пальців) у відбитках пальців, при якому система буде надавати доступ та ідентифікувати особистість. Такий процент називається FMR (з англ. False Meter Rate). За допомогою команди «set treshold N» даний параметр у системі можна змінити, проте у мануалі до використання бібліотеки SourceAfis рекомендується використовувати значення 40, при якому FMR буде дорівнювати 0.01%. На мою думку, змінювати цей параметр для проведення практичної частини не потрібно, тому у програмній реалізації я залишив параметр зі значенням 40.

3.3.2 Створення програми

Через те що програма повинна працювати з певним масивом даних, що можуть бути представлені як у вигляді одного файлу, так й у вигляді бази даних, я вирішив створити програму що працює на Java, та використовує бібліотеки що допомагають працювати з відбитками пальців.

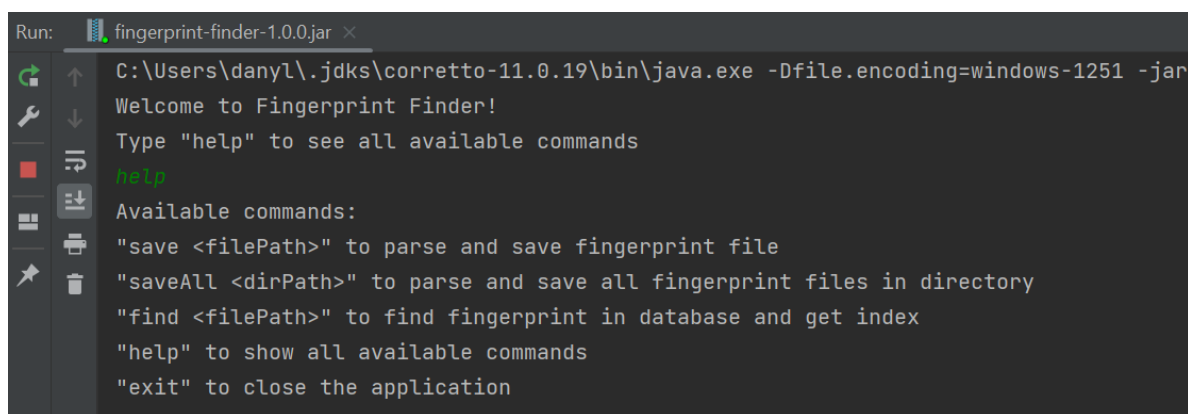
Головними елементами моєї реалізації системи ідентифікації за відбитками пальців є клас «App» та сама програма, що має таку ж назву

для зручності. Спочатку, детальніше опишу процес створення класу «App» та основні аспекти його роботи. У цьому класі визначено такі компоненти:

- 1) Finder: Примірник класу FingerPrintFinder. Цей об'єкт використовується для операцій з відбитками пальців, таких як збереження та пошук.
- 2) main(): У цьому методі починається виконання програми. Програма вітає користувача і потім входить у цикл, який очікує на введення команд від користувача. Команди обробляються та обробляються, повертаються повідомлення про помилки у разі виключень, і користувач надає відповідь на команду. Цей цикл триває доти, доки користувач не введе команду "exit".
- 3) answer(): Метод, який обробляє введення користувача. Спочатку введення розбирається на складові за допомогою методу `parseInput()`. Потім визначається яка команда була введена і виконуються відповідні дії. Результат виконання команди повертається у вигляді рядка.
- 4) `parseInput()`: Цей метод приймає введений користувачем рядок і розбирає його на окремі слова або рядки в лапках. Це робиться за допомогою регулярного виразу, який шукає або послідовності символів без пробілів (`\S+`), або послідовності символів у лапках (`"[^"]+"`).
- 5) Клас FingerPrintFinder: FingerPrintFinder може "зберігати" і "шукати" відбитки пальців, хоча неясно, що ці операції мають на увазі без додаткового контексту. Для можливості перевірки та подальшого використання системи ідентифікації, вона була завантажена на платформу GitHub, де її можна завантажити та використовувати. Посилання на готовий репозиторій буде подано у переліку посилань та літературних джерел. Програмна реалізація класу наведена у Додатку Б.

3.3.3 Тестування та експлуатація програмного забезпечення

Для початку роботи програми, нам необхідно відкрити її репозиторій за допомогою середовища програмної розробки. У моєму випадку, я використовував IntelliJ IDEA Community Edition. Для того щоб очистити буфер програми та створити виконавчий файл для реалізації та огляду моєї програми, використовується команда «`mvn clean package`», яку ми повинні прописати на початку роботи в рутовій (головній) папці репозиторію. Після цього, ми можемо переходити до використання програмного забезпечення. Для цього, нам потрібно запустити файл «`fingerprint-finder-1.0.0.jar`», що утворився у результаті команди, що ми виконали раніше. У консолі ми побачимо те, що програма була запущена та ми можемо викликати меню «`help`» з переліком усіх команд, для того щоб зрозуміти як саме можна працювати з програмою.



```
Run: fingerprint-finder-1.0.0.jar x
C:\Users\danyl\.jdk\corretto-11.0.19\bin\java.exe -Dfile.encoding=windows-1251 -jar
Welcome to Fingerprint Finder!
Type "help" to see all available commands
help
Available commands:
"save <filePath>" to parse and save fingerprint file
"saveAll <dirPath>" to parse and save all fingerprint files in directory
"find <filePath>" to find fingerprint in database and get index
"help" to show all available commands
"exit" to close the application
```

Рисунок 3.3 Програмний інтерфейс у консолі

Спочатку, я продемонструю використання опції «`save`», що має на меті зберігання у базі даних одного відбитку пальців з вилученими мінуціями для подальшої ідентифікації та запису у базу даних. Програма надає можливість використовувати відбитки пальців різних форматів, таких як .PNG, .JPEG або .TUF. Якщо спробувати зберегти у системі файл,

що буде представлений іншим форматом, ми зможемо побачити повідомлення про помилку у зберіганні

```
save "C:\Users\danyl\Desktop\Анкета_випусника_Золотоверхий_Данило_КБ-41_2023.pdf"
Unsupported image format [ImageIO = 'java.lang.IllegalArgumentException: Unsupported image format.'
```

Рисунок 3.4 Помилка при використанні файлу іншого формату

База даних FVC Competition складається з відбитків пальців формату .TUF, тому я буду тестувати саме їх. Для того щоб зберегти відбиток пальців у системі, я використаю команду «save <path>», де <path> - це буде шлях до відбитка пальця на моєму комп'ютері, який я хочу зберегти у базі даних. Після виконання цієї команди, ми можемо побачити повідомлення про вдалу спробу зберегти відбиток пальця у системі.

```
save "C:\Users\danyl\Desktop\FVC Competition\001_8\101_1.tif"
Saved
```

Рисунок 3.5 Зберігання відбитку пальця у базі даних

Палець було ідентифіковано в системі та за ним було наведено ідентифікаційний номер. Тепер ми можемо використати інше сканування того ж самого відбитку пальців для того щоб перевірити чи працює програма правильно. У програмі для цього процесу передбачено команду «find <path>», що може знайти індекс відбитку пальця.

```

save "C:\Users\danyl\Desktop\FVC Competition\DB1_B\101_1.tif"
Saved
find "C:\Users\danyl\Desktop\FVC Competition\DB1_B\101_8.tif"
Match found in record with index 0
find "C:\Users\danyl\Desktop\FVC Competition\DB1_B\101_3.tif"
Match found in record with index 0
find "C:\Users\danyl\Desktop\FVC Competition\DB1_B\101_6.tif"
Match found in record with index 0

```

Рисунок 3.6 Пошук ідентифікатора відбитку пальця

Як ми бачимо, програма видає коректний результат, що свідчить про те, що ідентифікатор було привласнено потрібним відбитком. Тепер для того щоб перевірити працездатність програми у випадку невірних наведених даних, спробуємо виконати пошук індексу відбитку пальця, що не був раніше збережений у програмі.

```

find "C:\Users\danyl\Desktop\FVC Competition\DB1_B\102_5.tif"
Index not found!

```

Рисунок 3.7 Помилка при пошуку незбереженого відбитку пальця

Отже, якщо спробувати знайти індекс відбитку пальця, що не був заданий раніше, система не зможе виконати запит та виведе на екран повідомлення.

Для зручного керування базою даних у моїй системі ідентифікації було також наведено можливість зберігати відбитки пальців групами (репозиторіями). Для цього процесу використовується команда «saveAll <path>». Процес реалізації та перевірки коректності ідентифікації буде представлено на рисунку 3.7.


```

saveAll "C:\Users\danyl\Desktop\FVC Competition\DB3_B"
Saved
find "C:\Users\danyl\Desktop\FVC Competition\DB3_B\102_5.tif"
Match found in record with index 13

```

Рисунок 3.8 Використання та перевірка групового зберігання

Проте важливо пам'ятати що при збереженні цілого репозиторія у програмі, кожному відбитку пальців у цій системі буде надано певний індекс, тому різні сканування одного й того ж самого відбитку пальців будуть ідентифікуватись системою як різний набір мінуцій, через те що при зміні ракурсу, площі поверхні сканування відбитка пальця, кута нахилу пальця до поверхні сканера, набір мінуцій буде змінюватись і програма не буде намагатись знайти процент збігу між ними.

Тому ця команда може бути корисна, коли потрібно додати до бази даних велику кількість відбитків різних пальців, що містяться в одній директорії. Для кожного з цих відбитків буде встановлено власний ідентифікаційний номер та його можна буде знайти у базі даних.

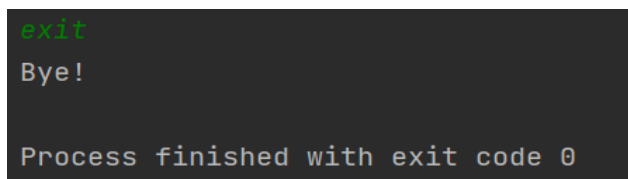
```

Save <filePath> to parse and save fingerprint file
"saveAll <dirPath>" to parse and save all fingerprint files in directory
"find <filePath>" to find fingerprint in database and get index
"help" to show all available commands
"exit" to close the application
save "C:\Users\danyl\Desktop\FVC Competition\DB1_B\101_1.tif"
Saved
find "C:\Users\danyl\Desktop\FVC Competition\DB1_B\101_1.tif"
Unknown command use "help" to see available commands
find "C:\Users\danyl\Desktop\FVC Competition\DB1_B\101_1.tif"
Match found in record with index 0
save "C:\Users\danyl\Desktop\FVC Competition\DB1_B\101_2.tif"
Saved
find "C:\Users\danyl\Desktop\FVC Competition\DB1_B\101_2.tif"
Match found in record with index 1
find "C:\Users\danyl\Desktop\FVC Competition\DB1_B\101_3.tif"
Match found in record with index 0
find "C:\Users\danyl\Desktop\FVC Competition\DB1_B\101_4.tif"
Match found in record with index 0

```

Рисунок 3.9 Демонстрація робочого процесу програми

Для того щоб завершити життєвий цикл програми ми можемо використати команду «exit».



```
exit
Bye!

Process finished with exit code 0
```

Рисунок 3.10 Завершення роботи програми з використанням команди «exit»

3.4 Результати та перспективи використання мого програмного забезпечення

Після проведення власних досліджень та процесу розробки програмного забезпечення я можу сформулювати оцінку актуальності та корисності бібліотеки SourceAfis та систем ідентифікації за відбитками пальців взагалі.

Бібліотека SourceAfis є одним з найбільш доступних та якісних засобів для створення систем ідентифікації за відбитками пальців у 2023 році. Такого висновку я дійшов через те що бібліотека знаходиться у вільному доступі, не потребує використання великої кількості фреймворків, окрім Apache Maven версії 3, та надає великий функціонал та простір для реалізації власних програмних рішень.

Також, одною з переваг я можу зазначити гнучкість у використанні бібліотеки через те що вона не потребує наявності фізичного сканера під час роботи. SourceAfis дає можливість використовувати програму для ідентифікації заздалегідь сканованих відбитків пальців та сканування їх у режимі реального часу при потребі. Це відкриває простір для подальшого розвитку моєї програми. Вже наразі систему можна використовувати у пасивному режимі.

Наприклад, створивши базу даних з відбитків пальців співробітників компанії, можна створити ID-картки, що будуть містити на собі

зображений відбиток пальця певного співробітника, який буде повинен використовувати цю картку при необхідності отримати доступ до певного сектора робочого простору або до отримання певної інформації. Через те що у компанії може працювати безліч людей, що будуть мати різні рівні робочих задач та привілеїв, кожен з відбитків пальців можна додати до бази даних рівнів перепусток, що будуть надавати або відмовляти у доступі співробітнику при спробі ідентифікації на різних секторах робочого простору. Завдяки цьому, ми можемо змінити параметр «threshold» у програмі таким чином, щоб необхідний рівень збігу був близький то максимального. Якщо в нас буде зображено фіксований відбиток пальця на ID-картці, похибки коректності ідентифікації у вигляді фізичних пошкодження відбитку пальця, іншого кута сканування можна запобігти.

Проте, програму можна використовувати й зі сканерами відбитку пальців у режимі реального часу, без необхідності створення ID-карток, зменшивши процент необхідного збігу під час проведення сканування. Це може мати мізерний негативний ефект для безпеки та зручності системи через можливу похибку, проте не буде потреби створювати фізичні носії ідентифікаційних даних, які можуть бути загублені, знищені або вкрадені.

Крім того, моє програмне забезпечення має здебільшого дослідницький характер та є гарним прикладом реалізації лише структури програми, яку можна модифікувати та покращувати безліччю різних засобів.

Якщо додати до програми постійну базу даних, що буде зберігатись в оперативній пам'яті системи, моє програмне забезпечення можна буде використовувати у будь-якій промисловій системі, що потребує створення процесів забезпечення безпеки інформації, без необхідності додаткових модифікацій. Також, для зручності використання до програми можна додати Графічний Інтерфейс (з англ. GUI), що дозволить використовувати програму у більш зручному для користувача форматі.

З цього я можу дійти висновку, що мій процес дослідження біометричних систем ідентифікації за відбитками пальців, а зокрема бібліотеки SourceAfis був виконаний вдало, та результатом цих досліджень можна вважати створення власної системи ідентифікації за відбитками пальців з можливістю подальшого використання. Програмне забезпечення виконує основну задачу ідентифікації особистості без критичних помилок та не перевантажує систему, тому проблем з технічною складовою програми виявлено під час роботи не було.

ВИСНОВКИ

Під час виконання дипломної роботи бакалавра на тему «Система ідентифікації за відбитками пальців» я виконав дослідницьку роботу у сфері сучасних методів Біометричної ідентифікації. Мною було окреслено основні методи сучасної Біометричної ідентифікації, їх переваги та недоліки у використанні. Зокрема, я дослідив методологію створення систем ідентифікації за відбитком пальців від етапу планування системи до її програмної реалізації. Основним об'єктом дослідження стали мінуції, їх типи та сучасні процеси вилучення.

Окрім цього, було проведено програмну реалізацію системи ідентифікації за відбитками пальців на основі бібліотеки SourceAfis, та мови програмування Java. Готове програмне забезпечення має функціонал для аналізу, збереження та керування відбитками пальців у системі. Також, програмне забезпечення ідентифікує відбитки пальців за допомогою вилучення мінуцій з керованим рівнем можливої похибки, що дає можливість використовувати систему для забезпечення безпеки інформації вже на даному етапі.

Результатом виконання дипломної бакалаврської роботи я можу вважати те, що я набув навичок у створенні та керуванні системами ідентифікації за відбитками пальців, та здобуті знання у сфері біометрії, що можуть допомогти при моделюванні та проектуванні КСЗІ (комп'ютерних систем захисту інформації) у майбутньому. Готове програмне забезпечення можна використовувати у якості прототипу для створення системи ідентифікації особистості за відбитками пальців, або створення програмного забезпечення, що може виконувати це процес у вигляді процесу, що проходить у реальному часі.

ПЕРЕЛІК ПОСИЛАНЬ НА ЛІТЕРАТУРНІ ДЖЕРЕЛА

- 1) Царьов Р.Ю., Лемеха Т. М. Біометричні технології: навчальний посібник [для вищих навчальних закладів] : Одеса : ОНАЗ ім. Попова О.С., 2016. 140 с.
- 2) Rassomakhin S. G., Melkozerova O. M., Nariezhnii O.P. The method of vicinity minutiae decomposition with higher level graphs for fingerprint verification : V. N. Karazin Kharkiv National University, Ukraine, 2021.
- 3) Biometric Systems: Technology, Design and Performance Evaluation / James W. and others. : 2005. 374 p.
- 4) ISO/IEC 19794-2:2005. Information technology – biometric data interchange formats – Part 2: Finger minutiae data. 2005, International organization for standardization ISO Central Secretariat. (дата звернення: 29.03.2023).
- 5) Cappelli R., Ferrara M., Maltoni D. Minutia Cylinder-Code: A New Representation and Matching Technique for Fingerprint Recognition : IEEE Transactions on Pattern Analysis and Machine Intelligence : 2005. P. 2128-2141.
- 6) Jain A., Patrick F., Arun A. Handbook of Biometrics : Springer Science+Business Media, LLC, 1st edition : 2008. P. 1-42.
- 7) Nallaperumall K., Fred A., Padmapriya S. A Novel Technique for Fingerprint Feature Extraction Using Fixed Size Templates : IEEE 2005 Conference : 2005. P. 371-374.
- 8) Fronthaler H., Kollreider K. and Bigun J. Pyramid-based Image Enhancement of Fingerprints : IEEE Xplore : 2007.
- 9) Бази даних FVC Competition 2002 та FVC Competition 2004. URL: <http://bias.csr.unibo.it/fvc2002/download.asp> ,

<http://bias.csr.unibo.it/fvc2004/download.asp> (дата звернення: 18.04.2023).

- 10) Створений репозиторій програми на GitHub. URL:
<https://github.com/dan1984-bit/FIngerprint-finder-v1.0.0>.

ДОДАТОК А

Лістинг основного коду програми ідентифікації за відбитками пальців

```
package com.zolotoverchy.daniel.finder;

import java.util.Scanner;
import java.util.regex.MatchResult;
import java.util.regex.Pattern;

import static com.zolotoverchy.daniel.finder.Constants.COMMANDS;
import static com.zolotoverchy.daniel.finder.Constants.GREETING;

public class App {
    public static FingerPrintFinder finder = new FingerPrintFinder();

    public static void main(String[] args) {
        System.out.println(GREETING);

        Scanner scanner = new Scanner(System.in);

        while (scanner.hasNext()) {
            String input = scanner.nextLine();
            input = input.trim();
            if (input.isEmpty()) continue;
            String answer = "Something went wrong";

            try {
```



```

        answer = answer(input);
    } catch (ArrayIndexOutOfBoundsException e) {
        answer = "Missing arguments to execute command";
    } catch (RuntimeException e) {
        answer = e.getMessage();
    }

    System.out.printf(answer + "%n");
    if (answer.equals("Bye!")) return;

}
scanner.close();
}

private static String answer(String input) {

    String [] values = parseInput(input);
    Command command = null;
    String answer = null;
    try {
        command = Command.valueOf(values[0].toUpperCase());
    } catch (IllegalArgumentException e) {
        throw new RuntimeException("Unknown command use \"help\" to see
available commands");
    }

    switch (command) {
        case HELP: answer = COMMANDS;
            break;

```

```

    case SAVE: finder.save(values[1].replaceAll("\\\"", ""));
        answer = "Saved";
        break;
    case SAVEALL: finder.saveAll(values[1].replaceAll("\\\"", ""));
        answer = "Saved";
        break;
    case FIND: answer = String.format("Match found in record with index
%d", finder.find(values[1].replaceAll("\\\"", "")));
        break;
    case EXIT: answer = "Bye!";
        break;
}
return answer;
}

private static String[] parseInput(String input) {
    Pattern ARG_PAT = Pattern.compile("\"[^\"]+\"|\\S+");

    return ARG_PAT.matcher(input)
        .results()
        .map(MatchResult::group)
        .toArray(String[]::new);
}
}

```

ДОДАТОК Б

Програмна реалізація класу

```
package com.zolotoverchy.daniel.finder;

import java.util.Scanner;
import java.util.regex.MatchResult;
import java.util.regex.Pattern;

public class App {
    public static FingerPrintFinder finder = new FingerPrintFinder();

    public App() {
    }

    public static void main(String[] args) {
        System.out.println("Welcome to Fingerprint Finder! \nType \"help\" to see
all available commands");
        Scanner scanner = new Scanner(System.in);

        while(scanner.hasNext()) {
            String input = scanner.nextLine();
            input = input.trim();
            if (!input.isEmpty()) {
                String answer = "Something went wrong";

                try {
```

```

        answer = answer(input);
    } catch (ArrayIndexOutOfBoundsException var5) {
        answer = "Missing arguments to execute command";
    } catch (RuntimeException var6) {
        answer = var6.getMessage();
    }

    System.out.printf(answer + "%n");
    if (answer.equals("Bye!")) {
        return;
    }
}

scanner.close();
}

private static String answer(String input) {
    String[] values = parseInput(input);
    Command command = null;
    String answer = null;

    try {
        command = Command.valueOf(values[0].toUpperCase());
    } catch (IllegalArgumentException var5) {
        throw new RuntimeException("Unknown command use \"help\" to see
available commands");
    }

    switch (command) {
        case HELP:

```

```

        answer = "Available commands:\n\"save <filePath>\n" to parse and
save fingerprint file\n\"saveAll <dirPath>\n" to parse and save all fingerprint files
in directory\n\"find <filePath>\n" to find fingerprint in database and get
index\n\"help\n" to show all available commands\n\"exit\n" to close the
application";

```

```

        break;

```

```

    case SAVE:

```

```

        finder.save(values[1].replaceAll("\\\"", ""));

```

```

        answer = "Saved";

```

```

        break;

```

```

    case SAVEALL:

```

```

        finder.saveAll(values[1].replaceAll("\\\"", ""));

```

```

        answer = "Saved";

```

```

        break;

```

```

    case FIND:

```

```

        answer = String.format("Match found in record with index %d",

```

```
finder.find(values[1].replaceAll("\\\"", "")));

```

```

        break;

```

```

    case EXIT:

```

```

        answer = "Bye!";

```

```

    }

```

```

    return answer;

```

```

}

```

```

private static String[] parseInput(String input) {

```

```

    Pattern ARG_PAT = Pattern.compile("\\\"([^\"])+\\\"|\\S+");

```

```

    return

```

```

    (String[])ARG_PAT.matcher(input).results().map(MatchResult::group).toArray(
(x$0) -> {

```

```
        return new String[x$0];  
    });  
}  
}
```