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

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 2021р.

На правах рукопису
УДК 004.056.5:510.22(043.3)

ДИПЛОМНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «БАКАЛАВР»

Тема: «Система керування доступом на основі технології SSO, з використанням біометричної автентифікації»

Виконавець: А.О.Маланчук
Керівник: к.т.н. О.О.Висоцька
Нормоконтролер: к.т.н. О.О.Висоцька

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки, комп'ютерної та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Бакалавр

Спеціальність: 125 «Кібербезпека»

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

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ С.В. Казмірчук

«__» _____ 2021 р.

ЗАВДАННЯ

на виконання дипломної роботи

здобувача вищої освіти Маланчука Артема Олеговича

1. Тема*: Система керування доступом на основі технології SSO, з використанням біометричної автентифікації.*

затверджена наказом ректора від «26» квітня 2021 р. № 652/ст.

2. Термін виконання: з 10.05.2021 р. по 20.06.2021 р.

3. Вихідні дані: проаналізувати існуючі технології управління доступом та технолгії автентифікації, описати SSO, агрументувати вибір теми SSO, проаналізувати та аргументувати вибір біометричних технологій автентифікації, а також метод розпізнавання, виконати моделювання персональних даних в біометричних системах (вказати метод, технології, алгоритм програми), а також результат тестування.

4. Зміст пояснювальної записки: аналіз технології SSO, сучасні методи та засоби оцінки біометричних технологій автентифікації, принципи розробки та дослідження експеременту з алгоритмом порівняння відбитків, користуючись фреймворком.

КАЛЕНДАРНИЙ ПЛАН

виконання дипломної роботи

№ п/п	Етапи виконання дипломної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	19.04.2021	*Виконано*
2.	Аналіз літературних джерел	25.04.2021	*Виконано*
3.	Обґрунтування вибору рішення	28.04.2021	*Виконано*
4.	Збір інформації	30.04.2021	*Виконано*
5.	Аналіз понять авторизації та автентифікації	05.05.2021	*Виконано*
6.	Аналіз біометричних систем та технології SSO	10.05.2021	*Виконано*
7.	Розробка алгоритму порівняння відбитків пальців , користуючись фреймворком.	14.05.2021	*Виконано*
8.	Демонстрування роботи фреймворка в C# для розпізнавання відбитків пальця та показ кодів алгоритму.	17.05.2021	*Виконано*
9.	Оформлення і друк пояснювальної записки	22.05.2021	*Виконано*
10.	Перевірка на антиплагіат	24.05.2021	*Виконано*
11.	Оформлення презентації	28.05.2021	*Виконано*
12.	Отримання рецензій від рецензента	02.06.2021	*Виконано*

Здобувач вищої освіти А.О.Маланчук

(підпис, дата)

Керівник дипломної роботи О.О.Висоцька

(підпис, дата)

РЕФЕРАТ

Дипломна робота складається зі вступу, трьох розділів, загальних висновків до кожного розділу, списку використаних джерел, додатків і має 66 сторінки основного тексту, 26 рисунків, однієї таблиці, 4 сторінок додатків. Список використаних джерел містить 14 найменування і займає 2 сторінки. Загальний обсяг роботи 79 сторінки.

Метою роботи є розробка системи керування доступом на основі технології SSO з використанням біометричної автентифікації.

Для посягнення поставленої мети необхідно розв'язати наступні задачі:

- Проаналізувати методи біометричної автентифікації та визначити можливість застосування їх в системах керування доступом на основі технології SSO;
- Розробити систему керування доступом на основі технології SSO з використанням біометричної автентифікації;
- Провести тестування розробленної системи керування доступом на основі технології SSO з використанням біометричної автентифікації.

Об'єктами дослідження дипломної роботи є: процеси біометричної автентифікації, процеси керування доступом на основі технології SSO.

Предметами дослідження дипломної роботи є: методи біометричної автентифікації, системи керування доступом на основі технології SSO.

Актуальність роботи полягає в проведеному аналізі технології SSO, розбіру її перевагів та недоліків, а також написанні фреймворку на основі C # для аутентифцкації по розпізнаванню відбитків пальців.

Практична цінність роботи: Розроблено система керування доступом на основі технології SSO з використанням біометричної автентифікації за відбитком пальця, яка дає змогу забезпечити санкціонований доступ користувачів одночасно до декількох ресурсів системи за технологією єдиного входу.

Методами дослідження є: створення бази на основі фреймворку C # з використанням бібліотек .Net Framework для успішної автентифіцкаії за допомогою відпитку пальця.

Ключові слова: Єдиний вхід (SSO - *Single Sign-On*), інтелектуально атоматизована система, автоматизовані системи, біометрія, біометричні системи, автентифікація, безпека, поведінка, ризик, державні інформаційні ресурси.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПЗ – програмне забезпечення

ГВЧ – генератор випадкових чисел;

ГПВП – генератор псевдовипадкових послідовностей;

ГПВЧ – генератор псевдовипадкових чисел;

ДПФ – дискретне перетворення Фур’є;

ЕОМ – електронна обчислювальна машина;

ЗІ – захист інформації;

КС – комп'ютерна система;

БД – база даних;

ПВ – псевдовипадковість;

ПВП – псевдовипадкова послідовність;

СЗІ – системи захисту інформації;

3DES – Triple Data Encryption Standard – стандарт шифрування даних;

ANSI – American National Standards Institute – Американський національний інститут стандартів;

BBS – Blum Blum Shub – генератор псевдовипадкових чисел;

RSA – Rivest-Shamir-Adleman – стандарт шифрування даних;

CDMA – Code Division Multiple Access – технологія зв’язку;

GPS – Global Positioning System – супутникова система навігації;

IDEA – International Data Encryption Algorithm – міжнародний алгоритм шифрування даних;

ISO – Міжнародна Організаця зі Стандартизації

СУБД – стема управління базами даних

СЕДО – система електронного документообігу

АС – автоматизована система

ЕД – електронний документ

ДСТУ – державні стандарти України

VPN – (Virtual Private Network) віртуальна приватна мережа

ЕЦП – електронний цифровий підпис

ACL – (Access Control List) список прав доступу до об’єкта.

PKL – Інфраструктура відкритих ключів

ВСТУП

• *Метою* роботи є розробка системи керування доступом на основі технології SSO з використанням біометричної автентифікації.

• Для посягнення поставленої мети необхідно розв’язати наступні задачі*:*

– Проаналізувати методи біометричної автентифікації та визначити можливість застосування їх в системах керування доступом на основі технології SSO;
– Розробити систему керування доступом на основі технології SSO з використанням біометричної автентифікації;
– Провести тестування розробленної системи керування доступом на основі технології SSO з використанням біометричної автентифікації.

• *Об’єктами дослідження дипломної роботи є*: процеси біометричної автентифікації, процеси керування доступом на основі технології SSO.

• *Предметами дослідження дипломної роботи є*: методи біометричної автентифікації, системи керування доступом на основі технології SSO.

• *Актуальність роботи полягає в* проведеному аналізі технології SSO, розбіру її перевагів та недоліків, а також написанні фреймворку на основі C # для аутентифцкації по розпізнаванню відбитків пальців.

• *Практична цінність роботи:* Розроблено система керування доступом на основі технології SSO з використанням біометричної автентифікації за відбитком пальця, яка дає змогу забезпечити санкціонований доступ користувачів одночасно до декількох ресурсів системи за технологією єдиного входу.

• *Методами дослідження є:* створення бази на основі фреймворку C # з використанням бібліотек .Net Framework для успішної автентифіцкаії за допомогою відпитку пальця.

Показано, що поєднання паролів із біометричними характеристиками людини підвищує надійність системи доступу в сотні і тисячі разів.

В даний час перспективним засобом захисту даних від несанкціонованого доступу (НСД) є *автентифікація користувачів за рахунок біометричних параметрів людини*, що об'єднують біометричні характеристики самого користувача.

Засоби автентифікації на основі паролів, що видаються авторизованим користувачам, які прості в реалізації і мають низьку вартість. Головним недоліком таких засобів, при захисті даних від несанкціонованого доступу, є можлива втрата конфіденцальності даних користувачів. Людині важко запам'ятати довгі паролі. Тому такі паролі зберігають в блокноті або в незахищеному файлі на комп'ютері. Короткі смислові паролі легко підбираються зловмисником. Це робить автентифікацію за паролем слабозахищенною.

Одним з видів безпечного засобу автентифікації вважається персональні пристрої зберігання ключової інформації: пластикові карти, смарт-карти, токени. При наявності такого пристрою, користувачеві немає необхідності запам'ятовувати довгі паролі. Щоб зламати захист зловмисникові необхідно вкрасти пристрій користувачеві. Помітивши крадіжку, власник пристрою може відразу ж повідомити про факт викрадення службі безпеки. Вартість засобів автентифіцкаціі з використанням носіїв ключової інформації вище в порівнянні із засобами автентифікації з використанням звичайних паролів.

Засоби біометричної автентіфцікаціі використовують фізіологічні і поведінкові особливості, якими володіє користувач і нерозривно пов'язані з ним. До засобів біометричної автентифікації відносяться: геометрія особи, геометрія рук, малюнок відбитка пальця, малюнок райдужної оболонки ока, рукописний почерк, особливості голосу. Біометричні характеристики неможливо забути, втратити, вкрасти, передати іншій людині. За допомогою біометрії не тільки перевіряється відповідність користувача, але і підтверджується його особистість. Система біометричної автентифікації повинна гарантувати високу надійність, щоб підтверджувати авторизованого користувача, але і відкидати зловмисника зі схожими біометричними параметрами, а також забезпечувати конфіденційність біометрії як персональних даних користувачів.

Тому надійна ідентифікація користувачів системою може бути гарантована лише тоді, коли одним з факторів звірки є його унікальна біометрична характеристика. Ціни на біометричні пристрої стали більш прийнятними для покупців. Таким чином, біометричні технології досягли стадії практичного використання, і їх застосування в засобах захисту інформації цілком доцільно.

Однак все ж залишаються деякі важливі питання застосування біометричних даних в засобах захисту. Справа в тому, що використання унікальних біометричних характеристик людини вимагає їх надійного захисту від викрадання шахраями , яке може привести до серйозних наслідків.

Фізіологічні та поведінкові особливості людини дозволяють несанкціоновано встановити його особистість, організувати за ним приховане стеження. З цієї причини деякі користувачі відмовляються від зберігання своїх біометричних даних, наприклад, дані малюнка відбитка пальця в будь-яких базах даних інформаційних систем, побоюючись погроз, пов'язаних з порушенням приватного життя та конфіденційності особистостей.

Актуальним завданням є безпечне зберігання неоднозначно відтворюваних біометричних даних. Саме ця проблема унеможливлює використання крпітографіческіх хеш-функцій для безпечного зберігання біометричної інформації. З плином часу з'явилося два напрямки щодо вирішення проблеми безпеки. Один напрямок, створений і розвивається за кордоном, характеризується використанням нечітких екстракторів на основі кодів з виявленням і виправленням помилок.

Одним з ефективних способів захисту персональних даних є знеособлення. Знеособлення дозволяє знизити ризики несанкціонованого використання і заподіяних шкод в разі витоку. Біометричні дані також відносяться до персональної інформації, яку необхідно захищати від несанкціонованого використання. Однак традиційні способи знеособлення вкрай неефективні для інфмаціоннних систем, що обробляють біометричні дані. Тому актуальним завданням є розробка способів знеособлення, що враховують особливості біометричних даних і систем які їх використовують.

Для вирішення одного з аспектів такої проблеми існує і широко застосовується досить довгий час Single Sign-On, спрямована на рішення. Технологія єдиного (одноразового) входу (англ. «Single Sign-On», «SSO») - технологія доступу до різних програм за допомогою одноразової процедури автентифікації.

Вирішення такої проблеми дає компанії-постачальнику послуг в сфері інформаційних технологій незаперечну перевагу, дозволяючи залучати більше клієнтів в кілька існуючих систем одночасно.

Одним з ефективних способів захисту персональних даних є знеособлення. Знеособлення дозволяє знизити ризики несанкціонованого використання і заподіяних шкод в разі витоку. Біометричні дані також відносяться до персональної інформації, яку необхідно захищати від несанкціонованого використання. Однак традиційні способи знеособлення вкрай неефективні для інфмаціоннних систем, що обробляють біометричні дані. Тому актуальним завданням є розробка способів знеособлення, що враховують особливості біометричних даних і систем які їх використовують.

Для вирішення одного з аспектів такої проблеми існує і широко застосовується досить довгий час Single Sign-On.

Технологія єдиного (одноразового) входу (англ. «Single Sign-On», «SSO») - технологія доступу до різних програм за допомогою одноразової процедури автентифікації.

Вирішення такої проблеми дає компанії-постачальнику послуг в сфері інформаційних технологій незаперечну перевагу, дозволяючи залучати більше клієнтів в кілька існуючих систем одночасно.

РОЗДІЛ 1.
АВТОРИЗАЦІЯ ТА АВТЕНТИФІКАЦІЯ В АТОМАТИЗОВАНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

1.1. Поняття авторизації

Поняття авторизація та автентифікація – різні, але вони супроводжують одна одну і використовуються разом, через що більшість користувачів не знає про різницю між ними.

Авторизація стала актуальною у зв'язку з посиленням впливу людського чиннику на роботу автоматизованих систем та популяризацію надання послуг віддалено, через інтернет мережу, що вимагає ідентифікації користувача, який має намір скористатися відповідними послугами .

Авторизація – це процес підтвердження прав на виконання певних операцій – зміни даних. Це необхідно для забезпечення безпеки при виконанні різних дій, для розмежування прав користувачів та для захисту від зловмисників. Використовується на сайтах, в банкоматах, інтернет магазинах, державних установах. Зазвичай користувач повинен ввести свій логін та пароль. Якщо данні введено правильно, дозволяється вхід в систему і виконання дозволених маніпуляцій. Якщо допущена помилка, вхід в систему не виконується.

Помилка авторизації – неправильне введення логіну, паролю та інших даних. При наборі кодового слова, користувач повинен звернути увагу на правильний порядок символів, регістр, встановлену розкладку клавіатури. При помилковій авторизації система блокує доступ користувача та може виконувати такі дії:

- фіксація факту несанцкіонованого доступу;
- подання звукового або світлового сигналу , повідомлень на екрані;
- обмеження доступу на конкретний час;
- пропозиція повторного набору коду;
- відновлення паролю;
- блокування облікового запису.

Код авторизації являє собою набір символів, які зберігаються в пам'яті системи і дозволяють ідентифікувати права користувача. У якості коду

зазвичай представлені комбінації 3-12 букв, цифр, знаків, набраних у визначеній послідовності. Код авторизації генерується в процесі реєстрації користувача і може змінюватись за бажанням власників облікового запису або за необхідністю служби безпеки. Часто встановлюється певне обмеження на кількість зміни комбінацій в період часу. Для безпечного користування сервісом користувач повинен зберігати набір символів в таємниці.

Авторизація в особистому кабінеті дозволяє користувачеві отримати доступ для зміни налаштувань облікового запису, інтерфейс взаємодії з системою, паролем, типовими операціями, керування рахунком, внесення змін в систему. Для виконання авторизації, відвідувач веб-сайту може використовувати обмежений набір функцій: переглядати загальнодоступну інформацію, виконувати транзакції, не вимагаючи підтвердження правдивих дій. Часто при авторизації в особистому кабінеті використовують додаткові засоби безпеки – введення “капчі”, підтвердження через SMS або електронну пошту.

Онлайн авторизація дозволяє користувачеві використовувати сервіси без особистого відвідування закладів. Для цього необхідно перейти на відповідний сайт, переглянути відповідні посилання або натиснути на певну кнопку, ввести дані у форму. Онлайн авторизація допомагає відвідувачам економити час, а організація – робити всі доступні послуги масовими, залучати більше число клієнтів, покращувати якість обслуговування, підвищувати ступінь безпеки виконання операцій, проводити статистичні дослідження, проводити статистичні дослідження, перевіряти права доступу до користувачів.

Якщо увійти до системи, користувачу може бути видано повідомлення про те, що авторизація недоступна. У цьому випадку користувачу потрібно заново авторизуватися, з виконанням всіх вимог безпеки, відновлення запасного паролю або логіну, або звернення до служби технічної підтримки за телефоном або електронною поштою. Повідомлення “Авторизація недоступна”, видається відвідувачу сайту або користувачеві сервісу у наступних випадках:

- неправильне введення логіну або паролю;
- анулювання прав доступу до системи, блокування користувача;

– несправності в роботі ПЗ;

– спроба отримати доступ в неробочий час.

Данні авторизації – відомості, які повинен ввести користувач системи для підтвердження права доступу до виконання операції. Зазвичай це логін та пароль, або рідше прізвище, ім’я, по батькові, посада, додаткові кодові комбінації, “капча”, слова перевірки. Данні авторизації зберігаються в системі і можуть бути змінені користувачем або службою безпеки. При втраті інформації, відвідувач сайту або сервісу повинен пройти процедуру її відновлення, що включає повторну ідентифікації різноманітними способами, наприклад за допомогою SMS або e–mail, шляхом звернення в службу технічної підтримки.

Для зручності користувачів , для використання апаратури яка є в наявності і для забезпечення дотримання заходів безпеки, створені різні види режимів авторизації. Часто використовується комбінація декількох таких режимів.

За способом доступу авторизація буває:

– онлайн – підключення можливе тільки за наявності онлайн підключення до інтернету;

– офлайн – дозволяє авторизуватися без доступу до інтернету.

Існують різні види авторизації, які поділяються на три класи:

Дискреційне керування доступом – доступ до об’єктів, даних чи фукнцій, надається явно вказаним суб’єктам, користувачам або групам користувачів. Наприклад користувачу user_1 дозволено читати файл file_1, але заборонено його змінювати. Кожен об’єкт має прив’язаного до нього суб’єкта – власника, який встановлює права доступу до об’єкта. Також система має одного виділеного суб’єкта – супер користувача, який має право встановлювати права доступу для всіх суб’єктів, а будь який суб’єкт може передати права які він має, іншим користувачам. Такий доступ використовується в сучасних операційних системах, де для авторизації використовується права і списки контролю доступу (ACL).

Мандатне керування доступом – полягає в розділі інформації за ступенем секретності, а користувачів по рівнях допуску до цієї інформації. Головною перевагою мандатного доступу є обмеження прав користувача об’єкту. Права суб’єктів на об’єкти що ними створюються, будуть залежати від їх рівня

допуску. Відповідно вони не зможуть випадково або спеціально видати їх неавторизованим користувачам.

Керування доступом на основі ролей – є розвитком політики вибіркового доступу, де доступ до об’єктів системи формується з врахуванням специфіки їх застосування на основі ролі суб’єктів в кожен момент часу. Ролі дозволяють визначити зрозумілі поняття для користувачів правила розмежування доступу. Роль поєднує властивості вибіркового керування доступом, встановлюючи у відповідності суб’єктам об’єкти. При зміні ролей міняється доступ до групи файлів. Цей тип доступу більш гнучкий, в порівнянні з попередніми і може їх моделювати.

1.2. Поняття автентифікації

Автентифікацією – називається процедура верифікації належності ідентифікатора суб'єкту.

Автентифікація здійснюється на основі того чи іншого секретного елемента (автентифікатора), який є у розпорядженні як суб'єкта, так і інформаційної системи. Звичайно, система має в розпорядженні не сам секретний елемент, а деяку інформацію про нього, на основі якої приймається рішення про адекватність суб'єкта ідентифікатору. Наприклад, перед початком інтерактивного сеансу роботи більшість операційних систем запитують у користувача його ім'я та пароль. Введене ім'я є ідентифікатором користувача, а його пароль – автентифікатором. Операційна система зазвичай зберігає не сам пароль, а його хеш–суму, що забезпечує складність відновлення пароля.

Існують такі методи автентифікації:

– однобічна автентифікація, коли клієнт системи для доступу до інформації доводить свою автентичність;
– двобічна автентифікація, коли, крім клієнта, свою автентичність повинна підтверджувати і система (наприклад, банк);
– трибічна автентифікація, коли використовується так звана нотаріальна служба автентифікації для підтвердження достовірності кожного з партнерів в обміні інформацією.

Методи автентифікації також умовно можна поділити на однофакторні та двофакторні.

Однофакторні методи діляться на:

– логічні (паролі, ключові фрази, які вводяться з клавіатури комп'ютера чи клавіатури спеціалізованого пристрою);
– ідентифікаційні (носієм ключової інформації є фізичні об'єкти: дискета, магнітна карта, штрих–кодова карта тощо. Недоліки: для зчитування інформації з фізичного об'єкта (носія) необхідний спеціальний зчитувальний пристрій; носій можна загубити, випадково пошкодити, його можуть викрасти або зробити копію);

– біометричні (в їх основі – аналіз унікальних характеристик людини, наприклад: відбитки пальців, малюнок райдужної оболонки ока, голос, обличчя. Недоліки: біометричні методи дорогі і складні в обслуговуванні; чутливі до зміни параметрів носія інформації; володіють низькою достовірністю; призначені тільки для автентифікації людей, а не програм або інших ресурсів).

Автентифікація за відбитками пальців. Ця біометрична технологія, цілком імовірно, в майбутньому використовуватиметься найширше. Переваги засобів доступу по відбитку пальця – простота використання, зручність і надійність. Весь процес ідентифікації здійснюється досить швидко і не вимагає особливих зусиль від користувачів. Вірогідність помилки при ідентифікації користувача набагато менша порівняно з іншими біометричними методами.

Використання геометрії руки. Цей метод сьогодні застосовується в більш ніж 8000 організацій, включаючи Колумбійський законодавчий орган, Міжнародний Аеропорт Сан-Франциско, лікарні і імміграційні служби. Переваги ідентифікації по геометрії долоні порівнянні з автентифікацією по відбитку пальця в питаннях надійності, хоча пристрій для читання відбитків долонь займає більше місця. Найбільш досконалий пристрій “Handkey”, сканує як внутрішню, так і бічну сторону руки.

Автентифікація за райдужною оболонкою ока. Перевага сканування райдужної оболонки полягає в тому, що зразок плям на оболонці знаходиться на поверхні ока, і від користувача не вимагається спеціальних зусиль. Фактично зображення ока може бути відскановане на відстані метра, що робить можливим використання таких сканерів в банкоматах. Ідентифікуючі параметри можуть скануватися і кодуватися, зокрема, і у людей з ослабленим зором, але непошкодженою райдужною оболонкою.

Автентифікація за сітківкою ока. Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, направленого через зіницю до кровоносних судин на задній стінці ока. Сканери для сітківки ока набули великого поширення в надсекретних системах контролю доступу, оскільки ці засоби автентифікації характеризуються одним з найнижчих

відсотків відмови в доступі зареєстрованим користувачам і майже нульовим відсотком помилкового доступу.

Автентифікація за рисами особи (за геометрією особи) – один з напрямів, що швидко розвиваються, в біометричній індустрії. Розвиток цього напряму пов’язаний з швидким зростанням мультимедійних відео-технологій. Проте більшість розробників поки зазнають труднощі в досягненні високого рівня виконання таких пристроїв. Проте можна чекати появу в найближчому майбутньому спеціальних пристроїв ідентифікації особи за рисами обличчя в залах аеропортів для захисту від терористів і т. ін.

Двофакторні методи автентифікації отримують в результаті комбінації двох різних однофакторних методів, частіше всього ідентифікаційного та логічного. Наприклад: “пароль + дискета”, “магнітна карта + PIN”.

Кожен клас методів має свої переваги і недоліки. Майже всі методи автентифікації мають один недолік – вони, насправді, автентифікують не конкретного суб’єкта, а лише фіксують той факт, що автентифікатор суб’єкта відповідає його ідентифікатору. Тобто всі відомі методи не захищені від компрометації автентифікатора.

Найпопулярніший метод автентифікації – парольна автентифікація, головна її перевага – простота й звичність. Паролі вбудовані в операційні системи й інші сервіси. При правильному використанні паролі можуть забезпечити прийнятний для багатьох організацій рівень безпеки. Проте, по сукупності характеристик їх варто визнати найслабшим засобом перевірки дійсності.

Щоб пароль був запам’ятовуваним, його найчастіше роблять простим (ім'я подруги, назва спортивної команди й т.п.). Однак простий пароль неважко вгадати, особливо якщо знати пристрасті даного користувача. Іноді паролі із самого початку не зберігаються в таємниці, тому що мають стандартні значення, зазначені в документації, і далеко не завжди після установки системи виробляється їхня зміна.

Введення паролю можна підглянути. Іноді для підглядання використовуються навіть оптичні прилади.

Паролі нерідко повідомляють колегам, щоб ті могли, наприклад, підмінити на якийсь час власника пароля. Теоретично в подібних випадках більш правильно залучити засоби керувань доступом, але на практиці так ніхто не робить: а таємниця, яку знають двоє, це вже не таємниця

Пароль можна вгадати “методом грубої сили”, використовуючи словник. Якщо файл паролів зашифрований, але доступний для читання, його можна скачати собі на комп'ютер і спробувати підібрати пароль, запрограмувавши повний перебір (передбачається, що алгоритм шифрування відомий).

Проте, важливі заходи дозволяють значно підвищити надійність парольного захисту:

- накладення технічних обмежень (пароль повинен бути не занадто коротким, він повинен містити букви, цифри);
- керування терміном дії паролів: їхня періодична зміна;
- обмеження доступу до файлу паролів;
- обмеження числа невдалих спроб входу в систему, це ускладнить застосування "методу грубої сили";
- навчання користувачів;
- використання програмних генераторів паролів (така програма, ґрунтуючись на нескладних правилах, може породжувати тільки благозвучні й, отже, запам'ятовувані паролі).

Перераховані заходи доцільно застосовувати завжди, навіть якщо поряд з паролями використовуються інші методи автентифікації.

Розглянуті вище паролі можна назвати багаторазовими: їхнє розкриття дозволяє зловмисникові діяти від імені легального користувача.

1.3. Поняття ідентифікації

Ідентифікація – процедура розпізнавання користувача в системі як правило за допомогою наперед визначеного імені (ідентифікатора) або іншої апріорної інформації про нього, яка сприймається системою .

Ідентифікація об'єкта – це його впізнання, ототожнення із чим–небудь. Якщо ж говорити про області інформаційних технологій, то даний термін звичайно означає встановлення особистості користувача. Цей процес необхідний для того, щоб система надалі змогла ухвалити рішення щодо видачі людині дозволу для роботи на комп'ютері, доступу до закритої інформації тощо. Таким чином, ідентифікація є одним з основних понять в інформаційній безпеці.

У кожного способу ідентифікації є свої переваги і недоліки, завдяки чому деякі технології підходять для використання в одних системах, інші – в інших. Однак у багатьох випадках немає строго певного рішення. А тому як розроблювачам програмного забезпечення, так і користувачам приходиться самостійно думати, який спосіб ідентифікації реалізовувати в продуктах.

1.3.1. Апаратна ідентифікація

Цей принцип ідентифікації ґрунтується на визначенні особистості користувача за певним предметом, ключем, що перебуває в його ексклюзивному користуванні. Прикладом є спеціальні електронні ключі, вказані на *рисунку 1.1*. На даний момент найбільше поширення одержали два типи пристроїв. До першого ставляться всілякі карти. Їх досить багато, і працюють вони за різними принципами. Так, наприклад, досить зручні у використанні безконтактні карти, які дозволяють користувачам проходити ідентифікацію як у комп'ютерних системах, так й у системах доступу в приміщення. Найбільш надійними вважаються смарт-карти – аналоги звичних банківських карт. Крім того, є й більш дешеві, але менш стійкі до злому карти: магнітні, зі штрих-кодом та інші.

Рисунок 1.1 – Карта ідентифікації користувача

Іншим типом ключів, які можуть використатися для апаратної ідентифікації, є токени. Ці пристрої мають власну захищену пам’ять і підключаються безпосередньо до одного з портів комп’ютера (USB, LPT), зображені на *рисунках 1.2 – 4.4.*

Рисунок 1.2 – Токен “RSA SecurID”

Рисунок 1.3 – USB-токен “eToken”

Рисунок 1.4 – Токен “VeriSing”

Головною перевагою застосування апаратної ідентифікації є досить висока надійність. У пам’яті токенів можуть зберігатися ключі, підібрати які хакерам не вдасться. Крім того, у них реалізовано чимало різних захисних механізмів. А вбудований мікропроцесор дозволяє електронному ключу не тільки брати участь у процесі ідентифікації користувача, але й виконувати деякі інші корисні функції.

Недоліком апаратної ідентифікації є висока ціна. Взагалі ж останнім часом вартість як самих електронних ключів, так і програмного забезпечення, що може працювати з ними, помітно знизилася. Проте для введення в експлуатацію системи ідентифікації однаково будуть потрібні деякі вкладення. Все-таки кожного зареєстрованого користувача потрібно забезпечити персональними токенами. Крім того, згодом деякі типи ключів можуть зношуватися або можуть бути загублені користувачами.

1.3.2. Багатофакторна ідентифікація

В наведених вище прикладах, йшлося про однофакторну ідентифікацію. Тобто в розглянутих системах для визначення особистості користувача використовувався тільки один фактор. Однак подібні процеси сьогодні не можна назвати надійними. Наприклад, зловмисник може вкрасти токен у зареєстрованого користувача й легко скористатися ним для несанкціонованого доступу до інформації. Тому все більшого поширення одержує багатофакторна ідентифікація, коли для визначення особистості застосовується відразу кілька параметрів, як зображено на *рисунку 1.5*.

Рисунок 1.5 – Двофакторна ідентифікація (картка + PIN-код)

Комбінуватися ці фактори можуть у довільному порядку. Втім, сьогодні в переважній більшості випадків використається тільки одна пара: парольний захист і токен. У цьому випадку користувач може не боятися підбору його паролю зловмисником (без електронного ключа вона працювати не буде), а також крадіжки токену (він не буде працювати без паролю). Втім, у деяких системах застосовуються максимально надійні, можна навіть сказати перебільшено надійні процедури ідентифікації. У них одночасно використаються паролі, токени й біометричні характеристики людини.

1.3.3. Біометрична ідентифікація.

Біометрія – це ідентифікація людини за унікальними, властивими тільки їй біологічними ознаками. Сьогодні експлуатується вже більше десятка різних біометричних ознак. Причому для найпоширеніших з них (відбитки пальців (рисунок 1.6) і райдужна оболонка ока) існує безліч різних за принципом дії сканерів.

Головною перевагою біометричних технологій є найвища надійність. І дійсно, усі знають, що двох людей з однаковими відбитками пальців у природі просто не існує.

Рисунок 1.6 – Пальцевий дактилоскопічний сканер.

Але , сьогодні вже відомо кілька способів обману дактилоскопічних сканерів, що зображено на рисунку 1.7. Наприклад, потрібні відбитки пальців можуть бути перенесені на плівку або до пристрою може бути прикладена велика фотографія пальця зареєстрованого користувача. Втім, треба зізнатися, що сучасні пристрої вже не попадаються на такі прості виверти. Так що зловмисникам доводиться видумувати все нові й нові способи обману біометричних сканерів.

Рисунок 1.7 – Сканер долонний дактилоскопічний

Основним недоліком біометричної ідентифікації є вартість устаткування. Адже для кожного комп’ютера, що входять до цієї системи, необхідно придбати власний сканер. Варто також відзначити, що подібні дешеві сканери недовговічні. Крім того, у них досить високий відсоток помилок другого роду (відмова в доступі зареєстрованому користувачеві). Тому користувачеві доводиться вибирати, який пристрій придбати – дорожчий й кращий або дешевший й гірший.

У стадії розробки знаходяться нові біометричні технології, пов'язані з іншими фізіологічними характеристиками.

Порівняння ДНК – це найдосконаліша на сьогодні біометрична технологія, що дає прямий доказ ідентичності особи, – окрім близнюків, в яких однаковий генотип. Цей метод інколи називається дактилоскопією ДНК, що збиває з пантелику і вводить в оману, оскільки відбитки пальців не «проникають до рівня геному». Біометричні системи, засновані на порівнянні ДНК, можуть бути введені в дію лише згодом

Судинні рисунки – розташування вен в різних частинах тіла людини, включаючи зап'ястя і тильну сторону долоні.

Сигнали, що виробляються серцем (мозком, легенями), – в цій системі користувач торкається датчика «біодинамічного підпису» («Biodynamic signature» sensor) і залишається з ним в контакті деякий час (залежно від точності вимірів – до 8 секунд). За цей час датчик ідентифікує індивідуальні параметри людини.

Методи ідентифікації особи за райдужною оболонкою ока побудовані за одним і тим же принципом – виділення частотної або будь-якої іншої інформації про текстуру райдужної оболонки із зображенням і збереженням цієї інформації у вигляді спеціальних кодів. Існує можливість порівнювати коди райдужних оболонок і зберігати в базі даних.

Побудова коду здійснюється в три етапи:

- виділення зобаження райджуної оболонки із загального зображення;
- обробка отриманого зображення, наприклад, усунення шуму (denoising), поліпшення зображення (enhansing), у тому числі вирівнювання гістограми, усунення відблиску; деякі методи "розгортають" круглу зіницю в прямокутне зображення – відбувається перехід від полярних координат в декартові; інколи після такої "розгортки" частина зображення відсікається, щоб накопичена на даному етапі помилка не вплинула на якість розпізнавання;
- складання коду : перетворене зоображення фільтрується способом , залежним від конкретного методу ; за результатами фільтрації складається представляення у вигляді коду. Більшість методів працють із зоображенням в градаціяї сірого або картами яскравості зображень , тобто кольорова складова є надлшишковою.

При розпізнаванні за портретом, будується двовимірний або тривимірний образ обличчя людини. За допомогою камери і спеціалізованого програмного забезпечення на зображенні або наборі зображень особи виділяються контури брів, очей, носа, губ і обчислюються відстані між ними й інші параметри, залежно від алгоритму, що використовується. За цими даними будується образ, що перетворюється в цифрову форму для порівняння. Причому кількість, якість і різноманітність образів (різні кути повороту голови, зміни нижньої частини обличчя при вимові ключового слова) може варіюватися залежно від алгоритмів в функцій системи, що реалізує даний метод.

Ідентифікація особи за особливостями голосу має ряд привабливих сторін. По-перше, існує високорозвинена телефонна мережа; по-друге, звукові карти стали стандартним устаткуванням сучасних персональних комп'ютерів. Як недолік біометричних систем ідентифікації особи за голосом необхідно відзначати, перш

за все, те, що парольну фразу важко зберегти в таємниці. Сучасні засоби акустичного прослуховування дозволяють досить успішно здійснювати несанкціоноване копіювання парольної фрази. Очікується, що виключення небезпеки використання злочинцями прослуховування відбудеться при переході до ідентифікації особи за довільними фразами. Як потенційна протидія прослуховуванню – використовується комбінування з іншими методами біометричної автентифікації. Ймовірність помилки для голосових систем складає від 1% до 2%. Для того, щоб ідентифікувати абонента за голосом, необхідно мати мовний шаблон, з яким порівнюватиметься голосовий ключ , що вводиться в систему. Порівняння ключа і шаблону може проводитися в цілому або за декількома характеристиками мовного сигналу (тут, ми говоримо про цифровий мовний сигнал, що пройшов обробку і адаптований до поставленого завдання): амплітуда і потужність (гучність), часові, частотні (тембр), енергетичні, фазові характеристики. Для забезпечення простоти аналізу мовний сигнал, його попередньо піддають дискретизації з використанням частотного або Вейвлет перетворення. Ідентифікація абонента може виконуватися за такими показниками:

- короткочасна енергія сигналу (визначається функцією короткочасної енергії з використанням вікон Хеммінга);
- автокореляційна функція (дозволяє визначити енергію і періодичні властивості сигналу);
- число переходів сигналу через нуль (оскільки високі частоти приводять до великого числа переходів через нуль, а низькі – до малого, то існує жорсткий зв'язок між числом нульових переходів і розподілом енергії по частотах);
- спектр сигналу;
- коефіцієнти лінійного передбачення ;
- кепстральні коефіцієнти;
- кепстральні коефіцієнти, обчислені на основі лінійного передбачення.

Існуючі дослідження моніторингу маніпулятора(мишки) при роботі користувача в системі показують високу надійність розпізнавання. При цьому екран розбивається на зони, в яких курсор миші знаходиться найчастіше і кожні

дві хвилини аналізуються характеристики руху миші між зонами. Пропонується моніторинг всього процесу еволюції системи «користувач-миша» впродовж тривалого (потенційно необмеженого) інтервалу часу спостереження за користувачем. При використанні ідентифікації за динамічними характеристиками насамперед необхідно визначити спосіб представлення набору числових значень. При аналізі підпису можна виділити координати характерних точок та інші параметри траєкторії. Після вибору ключових значень можна розпочати накопичення бази зразків характеристик користувачів, на підставі порівняння з якими здійснюватиметься ідентифікація (еталонні зразки). Також необхідно зробити важливе обмеження: всі траєкторії будемо вважати осмисленими, тобто користувач їх продукує в процесі повсякденної діяльності і з певною метою – маніпулювання певними елементами управління програмного забезпечення. В такому випадку генеровані траєкторії зумовлені такими факторами: антропологічними,фізіологічними та психологічними.

Антропологічні дані людини (довжина ліктьового суглоба і розміри зап’ястя) впливають на таку характеристику, як радіус кривизни траєкторії. Фізіологічні дані людини, такі як структура м’язів ліктьового і плечового суглобів, впливають на швидкість і прискорення руху курсору, тобто динаміку руху. З іншого боку, психологічні фактори також впливають на зазначені характеристики, вводячи додатково елементи звички при виконанні робочих операцій. Таким чином, наведені фактори вступають у взаємозв’язок між собою і постійно впливають на процес генерування траєкторії. Загалом, задача аналізу вказаних траєкторій має аналоги із задачею аналізу рукописного тексту або рукописних підписів. Проте комп’ютерна система дає змогу розглянути цей процес в динаміці і скористатися додатковою інформацією про динаміку руху курсору. Для аналізу отриманих на попередньому етапі характеристик нині вироблено декілька підходів:

- статистичний аналіз: обчислюється середнє кожного з ключових значень, його середньоквадратичне відхилення і здійснюється перевірка належності ключових значень зразка, що пред'являється, довірчим інтервалам, отриманим з аналізу еталонних зразків;
- застосування байєсівських мереж;

– застосування прихованих моделей Маркова. Аналіз почерку миші може здійснюватись повністю, або виконується попередня сегментація почерку з подальшим аналізом сегментів.

Також існує **система єдиного входу (SSO, Single Sign-On)** - це як окремий тип продуктів або вбудована технологія, що дозволяє не використовувати повторні аутентифікації користувачів перед його переходами за різними розробками та сервісом одного порталу, таким як форум, блог та інші, або при роботі з кількома додатками.

Іншими словами, користувач проходить процедуру аутентифікації в одному місці, після чого отримує доступ до всіх пов’язанних розділів розробленню.

У відповідь від стандартних методів аутентифікації при спробі користувачів отримати доступ до сервісу, запрошення аутентифікації даних зроблено не для користувача, а в SSO-додатку. Існує кілька варіантів застосування технологій єдиного входу, а саме: Клієнтський; Серверний; Комбінований; Веб-єдиний запит (Web SSO) .

Детальніше про систему SSO , про її переваги , недоліки та загальне призначення можна знайти у Розділі 2.

1.3.4. Парольна ідентифікація.

Ще не дуже давно парольна ідентифікація була чи ледве не єдиним способом визначення особистості користувача. Справа в тому, що парольна ідентифікація найбільш проста як у реалізації, так й у використанні. Суть її зводиться до наступного. Кожен зареєстрований користувач системи одержує набір персональних реквізитів (звичайно використаються пари: логін-пароль). Далі при кожній спробі входу людина повинна вказати свою інформацію. Оскільки вона унікальна для кожного користувача, то на підставі її система й робить висновок про особистість та ідентифікує.

Недоліком парольної ідентифікації є значна залежність надійності ідентифікації від користувачів, точніше від обраних ними паролів. Справа в тому, що більшість людей використовують ненадійні ключові слова, які легко підбираються. Фахівці в області інформаційної безпеки радять використати довгі паролі, що складаються з безладного сполучення букв, цифр і різних символів.

Висновки до першого розділу

Проаналізувавши різні види автентифікації, ідентифікації та авторизації, стає зрозумілим, що краще всього для використання підходить двофакторний метод ідентифікації з використанням біометрії користувача та трибічний метод автентифікації, який використовує третю, довірену сторону для підтвердження особи. Авторизація повинна відбуватися з використанням мандатної системи, так як це дозволить обмежити доступ користувачам, якщо потрібно це зробити масово, з наданням повноважень групі користувачів. Обов'язково повинна бути система розмежування доступу, щоб користувач мав рівно стільки можливостей, скільки йому потрібно.

Оцінивши матеріальні можливості та потреби програми, яку потрібно захистити від несанкціонованого доступу, доцільно краще за все для її захисту необхідно підібрати програму з двофакторною автентифікацію, використовуючи токен, а в якості ідентифікатора вказати гешований серійний номер флешки, а також логін користувача та пароль, реалізувавши метод мандатного керування доступом.

РОЗДІЛ 2.
ОСНОВНІ ПОНЯТТЯ ПРО ТЕХНОЛОГІЮ ЄДИНОГО ВХОДУ (SSO TECHNOLOGY) ТА АНАЛІЗ БІОМЕТРИЧНИХ СИСТЕМ

2.1 Технологія SSO , переваги та недоліки.

Сьогодні користувачі стикаються з проблемою частого жонглювання паролями та комбінаціями імен користувачів. При роботі з різними платформами та додатками їм пропонується увійти в систему .

Технологія єдиного входу (SSO) - це спосіб усунення цієї проблеми. SSO постійно розвивається для вирішення проблем, з якими стикаються працівники інформаційних технологій та їх застосування. У цій дипломній роботі представлено деякі з методів єдиного входу, що використовуються сьогодні, та досліджено потенціал механізмів після автентифікації, які можуть використовувати знання про поведінкові атрибути зареєстрованого користувача, щоб зменшити навантаження на користувача від явної необхідності входити знову і знову.

Єдиний вхід (SSO) – це механізм перевірки сеансу , який дозволяє клієнтові використовувати поєднання пароля та імені для доступу до декількох програм . Механізм перевіряє клієнта для всіх програм і усуває необхідність запитів автентифікації , коли користувач перемикається між програмами в рамках сеансу.

Механізм єдиного входу можна класифікувати як:

- програмний – орієнтований на потреби замовника проти домовленностей на стороні сервера. На сьогоднішній день є п'ять найбільш часто використовуванних механізмів Єдиного входу :

- Єдиний вхід в систему підприємства , Kerberos (або автентифікація квитків / токенів) , відкритий ідентифікатор чи об'єднана інформація.

SSO - це не єдине поняття, а скоріше загальний термін, що використовується для всіх тих методів та пристроїв або комбінацій, які мають на

меті зменшити навантаження на декілька екземплярів входу протягом сеансу. Це домовленість, яка допомагає кінцевим споживачам систем отримувати безперешкодний доступ до їх роботи з додатковими перевагами для підприємств, що забезпечують безпеку та послідовність. Забезпечення цілого ряду заходів, починаючи від перегляду Інтернету та навігації через різні платформи та застарілі програми, є складним завданням. Кожен із цих видів діяльності має власний набір питань, вимог та параметрів безпеки, які можуть сильно відрізнятися від одного до іншого.

Основною перевагою технології SSO – є дозвіл користувачеві отримати доступ до багатьох різних систем без необхідності входити в кожну з них окремо.

Основними недолікоами технології SSO є:

- спроба первісної реалізації може бути складною , в залежності від кількості існуючих непорівнянних систем;
- скомпрометовані Вхідні Дані (credentials) користувача можуть призвести доступ до великої кількості додатків;
- виробник або не використовує існуючий відкритий стандарт , або використовує стандарти , несумісні з іншими додатками

ОДНАК SSO ПРЕДСТАВЛЯЄ РИЗИК ДЛЯ БЕЗПЕКИ , ОСКІЛЬКИ ЯК ТІЛЬКИ ЗЛОВМИСНИК ОТРИМУЄ ДОСТУП ДО ЄДИНОЇ СИСТЕМИ , ТОДІ ЗЛОВМИСНИК МАЄ ДОСТУП ДО ВСІХ СИСТЕМ ОДНОЧАСНО.

2.2. SSO та архітектура безпеки.

SSO спрощує складність різнорідної архітектури безпеки. Система, що використовує єдиний вхід, повинна керувати управлінням ресурсами, інформаційними послугами та управлінням даними. Більше того, безпека повинна забезпечуватися наскрізно в архітектурі безпеки.

Асоціації безпеки (SA) використовують різні методи та підходи для вирішення цієї вимоги. Кожен SA визначає протоколи, ключі та алгоритми шифрування, які повинні бути використані для забезпечення цієї наскрізної безпеки. Якщо є порушення у створенні SA, це спричиняє порушення в роботі цієї частини системи організації. Порушення можуть бути спричинені невідповідністю ключів та протоколів.

Ефективність SA буде залежати від використовуваного алгоритму шифрування та алгоритму хешування. Деякі алгоритми, такі як алгоритми шифрування відкритих ключів, обчислювально дорогі через великі розміри криптографічних ключів, необхідність використання двох криптографічних ключів замість одного, а також із введенням органу сертифікації додаткових пошукових систем доменних імен та перевірки сертифікатів . З усіх цих причин використання інфраструктури відкритих ключів (PKI) підвищує рівень безпеки за рахунок збільшення часу відгуку сервера.

Веб-система SSO представляє веб-архітектуру, в якій клієнтам може знадобитися входити в різні веб-системи, але їм потрібно це зробити лише один раз. Така система єдиного входу може бути інтрамережею, але основна мета полягає в тому, що кожен користувач входить лише один раз (за сеанс).

Для забезпечення безпеки SSO використовують маркери / файли cookie та розгортання мови розмітки мови твердження (SAML). Маркер перевірки передається через захищений канал, як правило, рівень захищеного сокета (SSL). SSL використовує сертифікати сервера. Криптографічні функції SSL надаються клієнтам через браузери. Ці маркери надсилаються через захищені канали до інших систем безпеки з метою забезпечення перевірки ідентичності користувача . Після успішної автентифікації такі маркери видаляються, а ідентифікаційні

підписи передаються системі, яка ініціювала транзакцію, щоб забезпечити клієнтській системі доступ до даних або інших ресурсів.

Навіщо необхідно використовувати SSO (single sign-on)?

Сьогодні програми розгортаються в центрах обробки даних та хмарах і поставляються як SaaS (одна з форм хмарних обчислень, модель обслуговування, при якій передплатникам надається готове прикладне програмне забезпечення, яке повністю обслуговується провайдером) . Кожна комерційна програма вимагає автентифікації користувачів, перш ніж вони отримають доступ до ресурсу. Ще до відсутносі технології SSO кожен раз, коли користувачеві необхідно було переходити між програмами, йому доводилося авторизовуватися з набором облікових даних. Здебільшого кожна програма мала окремий набір облікових даних, і це призводило до поганого користувацького досвіду, невдалих входів в результаті забутих облікових даних, непослідовних політик контролю доступу та високих витрат на підтримку цих програм.

SSO спростив спосіб взаємодії та доступу користувачів до своїх програм. Завдяки SSO користувачі можуть економити час, отримуючи доступ до всіх своїх корпоративних, веб-додатків, а також до інших корпоративних ресурсів, таких як спільні мережеві файли, лише з одним набором облікових даних.

2.3. Аналіз біометричних систем та способів їх захисту.

Біометричні системи мають абсолютну надійність, однак дослідники активно рухаються вперед по шляху виявлення вразливостей біометрії та розробки заходів протидії їм.

Біометричні системи розпізнають людей на основі їх анатомічних особливостей (відбитків пальців, образу обличчя, малюнка ліній долоні, райдужної оболонки ока , голосу) або поведінкових рис (підписи). Оскільки ці риси фізично пов'язані з користувачем, біометричне розпізнавання надійно в ролі механізму, що стежить, щоб тільки ті, у кого є необхідні повноваження, могли потрапити в будівлю, отримати доступ до комп'ютерної системи або перетнути кордон держави. Біометричні системи також мають унікальні переваги - вони дають можливість визначити, коли індивідуум користується декількома посвідченнями (наприклад, паспортами) на різні імена. Таким чином, при грамотній реалізації у відповідних додатках біометричні системи забезпечують високий рівень захищеності.

Правоохоронні органи вже більше століття в своїх розслідуваннях користуються біометричною автентифікацією з використанням відбитка пальця, а в останні десятиліття відбувається швидке зростання впровадження систем біометричного розпізнавання в урядових і комерційних організаціях у всьому світі. На рис. 2.1 показані деякі приклади. Хоча багато з цих впроваджень дуже успішні, існують побоювання з приводу незахищеності біометричних систем і потенційних порушень приватності через несанкціоновані публікації збережених біометричних даних користувачів. Як і будь-який інший автентифікаційний механізм, біометричну систему може обійти досвідчений шахрай, який володіє достатнім часом і ресурсами. Важливо розвіювати ці побоювання, щоб завоювати довіру суспільства до біометричних технологій.

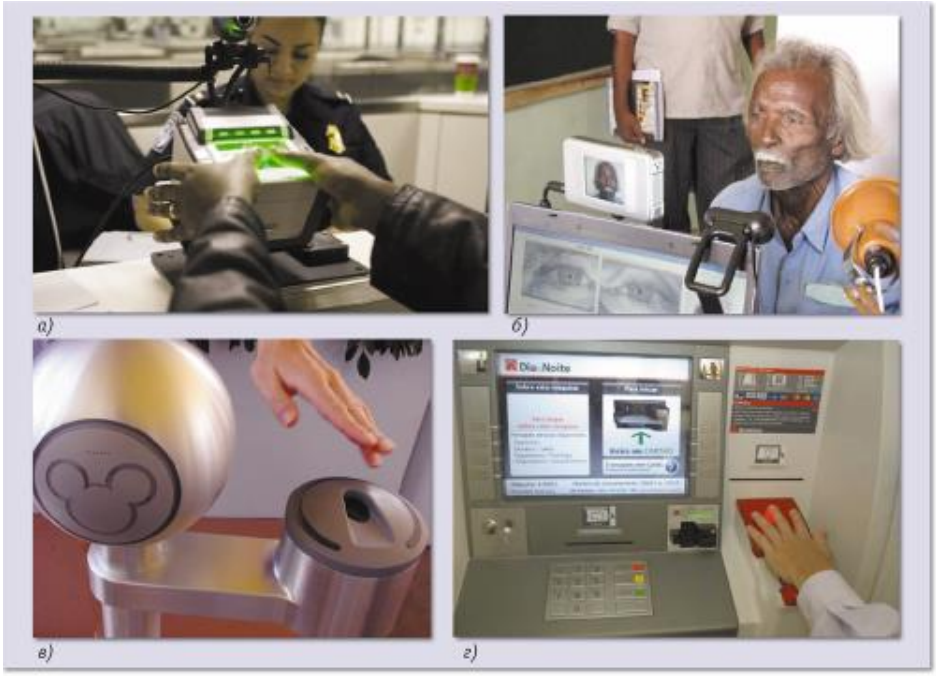


Рисунок. 2. Приклади систем біометричної автентифікації, що застосовуються в урядових і комерційних організаціях:

- а) програма US-VISIT, яка фіксує факт перетину державних кордонів, записує відбитки всіх десяти пальців подавача заяви на отримання візи;
- б) система реєстрації цивільних станів Aadhaar (Індія), крім відбитків 10 пальців, зберігає знімки райдужної оболонки ока і особи;
- в) в центрі відпочинку Disney World в Орландо (штат Флорида) для запобігання підробки квитків використовується система контролю доступу на основі відбитків пальців;
- г) у багатьох банках Японіх і Бразилії застосовуються банкомати , які реєструють малюнок вен.

2.3.1. Біометричні характеристики людини.

Всі біометричні характеристики людини можна розділити на два класи: статичні і динамічні характеристики . Статичні біометричні характеристики є фізіологічними особливостями, які не змінюються протягом життя людини. До фізіологічних особливостей відносяться:

- геометрія обличчя ;
- малюнок відбитків пальців;
- райдужна оболонка ока;
- геометрія рук

Фізіологічні особливості можуть бути втрачені в результаті хвороби людини, при фізичному (хірургічному) впливі на його органи.

До динамічних біометричних характеристик відносяться:

- динаміка рукописного почерку;
- голос;
- серцевий ритм;
- хода.

Не існує єдиної біометричної характеристики, яка підійшла б для всіх потреб. Кожна біометрична характеристика має свої переваги і недоліки. Процес отримання біометричної характеристики повинен бути по можливості швидким і простим, без заподіяння будь-яких незручностей людині.

Сьогодні біометричні дані осіб широко використовуються в інформаційних системах для органолептичної ідентифікації громадян. Але з розвитком засобів обчислювальної техніки біометричні дані осіб стали успішно застосовуватися автоматичними засобами розпізнавання людини для встановлення і підтвердження його особистості. У загальному випадку можна виділити два класи засобів біометричної ідентифікації людини по обличчю. Перший клас засобів аналізує плоскі зображення обличчя людини (2D портрети). Двомірний аналіз плоского зображення полягає у виділенні на ньому характерних точок і обчисленні геометрії, а саме відстаней між центрами очей, між лінією очей і кінчиком носа і т.п.

Двомірний аналіз плоского зображення обличчя людини дозволяє отримати зовсім не багато біометричної інформації. Перехід до більш складного

тривимірному аналізу геометрії особи людини дозволяє значно збільшити обсяг одержуваної біометричної інформації.

Особливості папілярного малюнка відбитка пальця широко використовуються в дактилоскопії, яка сьогодні є невід'ємною і важливою частиною криміналістики, оперативно-розшукової діяльності. Поява малогабаритних сканерів зчитування папілярного малюнка відбитка пальця дозволило успішно використовувати дані біометричні характеристики для підтвердження особи людини в системах контролю і управління доступом. Варто відзначити, що виникла гостра необхідність застосування відбитків пальців паспортно-візовими службами і міграційної політики різних держав світу.

Райдужна оболонка ока є унікальною фізіологічної характеристикою людини. Сканування засноване на поглинанні інфрачервоного випромінювання меланіном, що відповідає за пігментацію райдужної оболонки. Параметри вимірюються по одержуваному зображенню.

В даний час існує два основних підходи до ідентифікації геометрії руки людини. Перший підхід ґрунтується на геометричних характеристиках кисті людини. Другий відноситься до сучасних підходів, оскільки крім геометричних параметрів використовують ще такі характеристики руки як розташування кровоносних судин.

Рукописний почерк - це динамічна характеристика, яка пов'язана з особливістю поведінки людини. Вимірюваними параметрами є залежності координат кінця пера від часу, одержувані, як правило, за допомогою графічного планшета.

Певну ступінь унікальності також мають біометричні характеристики голосу людини. Встановлення належності різних мовних фраз однієї і тієї ж людини, ідентифікація особистості по голосу застосовуються в криміналістиці. Існують автоматичні засоби розпізнавання здатні визначати параметри на основі характерних для звуків мови сигналів, що мають свою форму коливань тиску. Відомо, що частина звуків мови є періодичними, а інша частина звуків є шиплячими (НЕ періодичними).

Серцевий ритм і хода людини не мають високого ступеня унікальності біометричних параметрів, тому не отримали застосування.

Ідентифікація по райдужній оболонці ока.

Малюнок райдужної оболонки ока - унікальний для кожної людини. В цьому методі важлива не тільки спеціальна камера, але і надійне програмне забезпечення. Адже саме за допомогою програмного забезпечення із зображення виділяється малюнок потрібної нам райдужної оболонки. Цей метод є одним з найбільш точних серед біометричних методів.

Ідентифікація за формою кисті руки.

Цей метод ґрунтується на розпізнаванні геометричних особливостей кисті руки. Спеціальний сканер формує тривимірний малюнок кисті. При аналізі цього малюнка виконуються вимірювання, за допомогою яких формується відповідний цифровий код.

Таким чином, можна виділити позитивні властивості біометричних характеристик людини. Біометрію неможливо втратити, забути, передати іншій людині, як наприклад інші ідентифікатори: пароль, PIN-код, смарт-карту, токен. Дані властивості особливо важливі для забезпечення безпеки таких систем, які вимагають надійну автентифікацію користувачів.

2.3.2. Таємні та відкриті біометричні образи.

Серед біометричних характеристик людини можна виділити ті характеристики, які можуть залишатися людиною в таємниці або невідомим чином, яким не розкривається ніяким іншим особам. Дані на *рисунку 2.1* відображають сучасну практику використання відкритих біометричних образів при ідентифікації людини.

Найбільш зручними біометричними технологіями з точки зору забезпечення таємниці образів є біометричні технології аналізу голосу і рукописного почерку людини. Забезпечити таємницю таких біометричних образів найпростіше, досить голосом або своїм почерком відтворювати парольне слово (парольний фразу). Для того, щоб забезпечити таємницю статичних образів, які не змінюються з волі людини. Необхідно користуватися системою організаційно-технічних заходів, що забезпечують знеособлення людини. Як тільки сторонній спостерігач дізнається ім'я людини - знайти людину і скомпрометувати дані його статичного біометричного образу не складно. Можна зробити висновок, що таємниця біометричного способу набагато сильніше, ніж біометричні технології.

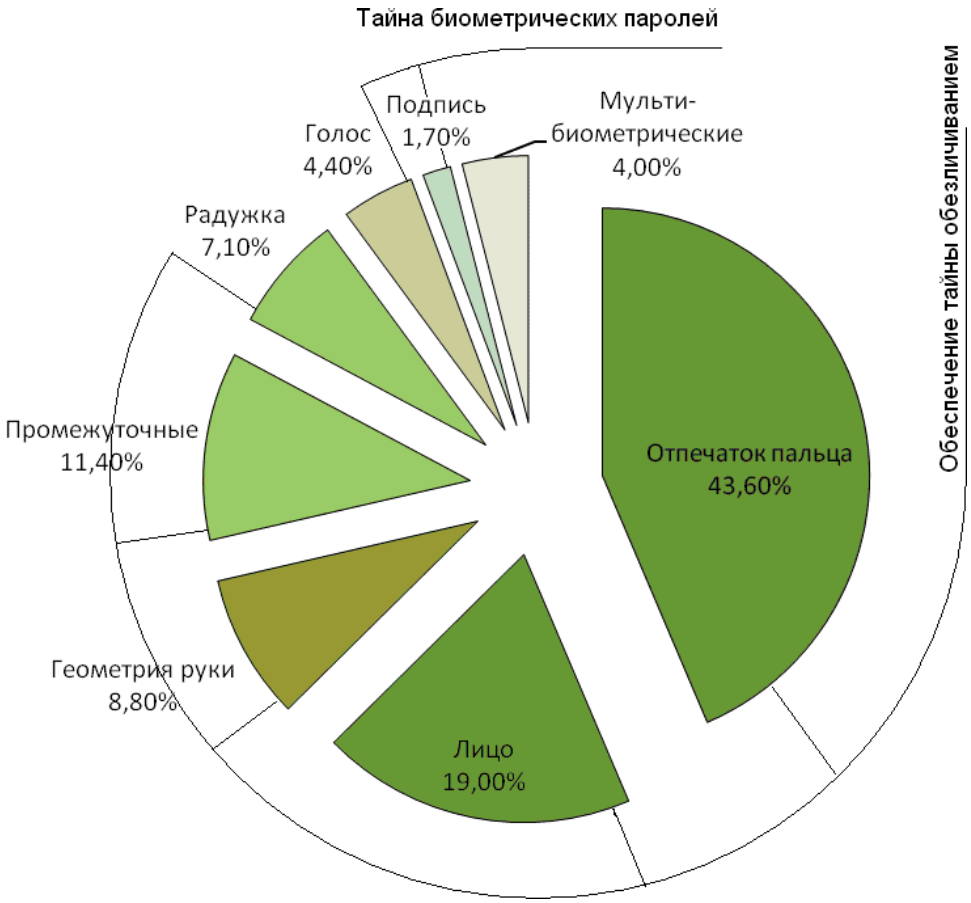


Рисунок 2.1 - Розподіл затребуваності біометричних технологій

На сьогоднішній день спостерігається дві виражені тенденції в розвитку засобів захисту інформації:

- масове використання асиметричної криптографії (пари з відкритого і закритого ключа);
- посилення процедур ідентифікаціх та автентифікаії за допомогою біометричніх технологій.

За експертними оцінками вітчизняних і зарубіжних дослідників безпеку використання коштів асиметричної криптографії може бути посилена за рахунок зв'язування відкритих і закритих ключів з біометрією їх власника. При авторизації прав особистості на управління закритим криптографічним ключем необхідно забезпечувати збереження в таємниці закритого біометричного образу. Відкритий ключ може бути пов'язаний з відкритим (загальнодоступним) біометричним чином людини, наприклад, з 3D-маскою обличчя людини. Закритий ключ обов'язково повинен бути пов'язаний з таємним (закритим) образом людини, наприклад, з його рукописним паролем.

2.3.3. Характеристика біометричних систем

Біометричні системи проектуються і розробляються для здійснення контролю доступу в приміщення, що охороняються, на військові об'єкти. Таким чином створюються системи автоматичної ідентифікація особистості, які використовуються в оперативно-розшукової діяльності правоохоронних органів. У світі набувають поширення системи біометричної ідентифікації громадян при доступі до соціальних послуг, надання медичної допомоги, голосуванні, перепису населення, обліку тривалості робочого часу, купівлі товарів і т.д.

У якості нормативної бази з розробки біометричних систем виступають як міжнародні, так і вітчизняні стандарти .

Гілка біометричних стандартів, орієнтованих на створення біометричних систем на основі біометричних образів, що зберігаються в таємниці, поки активно створюється тільки в Америці.

Згідно з міжнародними стандартами найпростіша біометрична система - це автоматизована система, яка здійснює:

- реєстрацію біометричного способу користувача за допомогою біометричного сканера;
- обчислення біометричних параметрів і формування біометричного шаблону;
- порівняння біометричних параметрів з параметрами , що містяться в біометричному шаблоні;
- прийняття рішення і видачу результату ідентифікації і верифікації.

Біометрична система складається з підсистем реєстрації і верифікації (ідентифікації) користувачів. **Підсистема реєстрації** (навчання) здійснює збір біометричних даних та інших відомостей про користувача (суб'єкті доступу), дії якого регламентуються згідно певним правилам розмежування доступу. При цьому даних має бути достатньо для ідентифікації (присвоєння ідентифікатора) користувача і перевірки приналежності суб'єкту доступу пред'явленого їм ідентифікатора.

Типова структура біометричної системи представлена на *рисунку 2.2.*

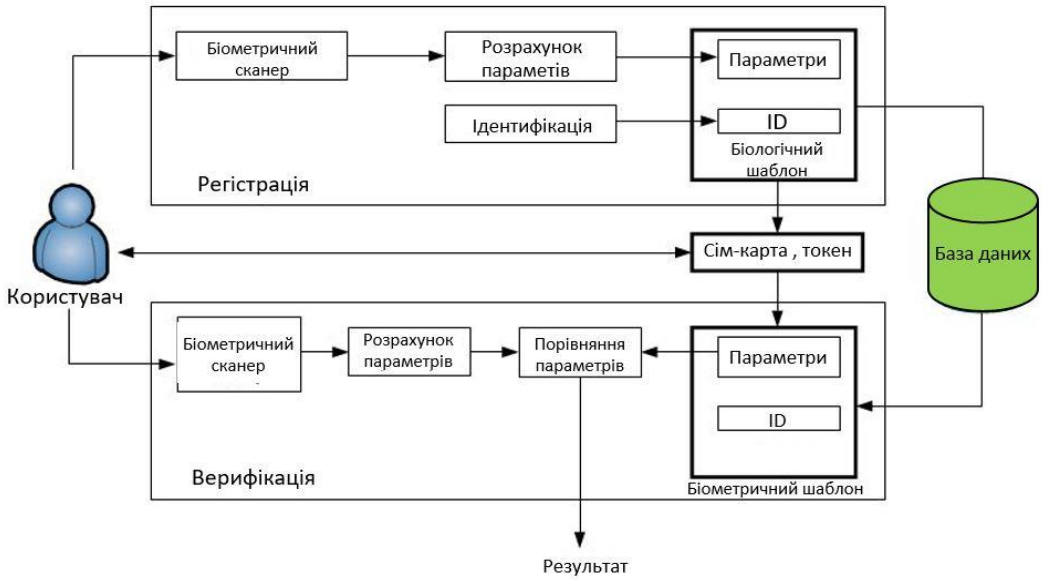


Рисунок 2.2. - Типова структура біометричної системи

У процесі реєстрації біометричний образ зчитується біометричним пристроєм введення, далі виділяються значущі параметри користувача, формується біометричний шаблон і зберігається в базі даних разом з будь-яким ідентифікатором, який має користувач або присвоюється йому в процесі реєстрації. Ідентифікатор користувача та біометричний шаблон можуть бути розміщені на смарт- карті, токені. При верифікації користувач пред'являє системі ідентифікатор і біометричні дані. Потім обчислюються значущі параметри користувача, які порівнюються з параметрами біометричного шаблону, отриманого з бази даних за пред'явленим ідентифікатором. Після чого приймається рішення і дається відповідь «Чи то той чоловік, за кого він себе видає» (відображається результат «Так» / «Ні»).

Також біометрична система може відповісти на питання, чи належать біометричні дані кому-небудь з користувачів системи, тобто ідентифікація особи.

При порівнянні біометричних параметрів обчислюється деяка міра подібності S, яка порівнюється з граничним значенням *T*. У тому випадку, якщо *S* більше, або дорівнює *T*, приймається рішення про те, що пред'являються біометричні параметри і параметри біометричного шаблону належать одній людині. Якщо *S* менше *T*, приймається рішення про те, що параметри належать різним людям.

Основними характеристиками біометричних систем є помилки першого і другого роду. Коли пред'являються біометричні параметри і параметри біометричного шаблону дійсно належать одній людині, а результат їх порівняння менше порогового значення, виникає помилка першого роду P_I.

Коли пред'являються біометричні параметри і параметри біометричного шаблону належать різним людям, а результат порівняння більше порогового значення, виникає помилка другого роду P_{II} . У таблиці 1.1 наведені середні показники P_I та $P_{II.}$ для різноманітних біометричних систем.

Таблиця 2.1 - Характеристики відомих біометричних систем

Хар.	Обличчя	Відбиток пальця	Вени долоні	Вени пальця	Радйужка	Підпис	Голос
P_I	$2{,}6 \cdot 10^{-2}$	10^{-2}	10^{-2}	10^{-2}	10^{-3}	10^{-2}	10^{-1}
P_{II}	$1{,}3 \cdot 10^{-2}$	10^{-5}	10^{-7}	10^{-5}	10^{-6}	10^{-6}	$3 \cdot 10^{-2}$

Біометричні системи, які відповідають виключно вимогам міжнародних стандартів прийнято називати класичними біометричними системами. Такі системи прості в реалізації, але в той же час мають такі значимі недоліки:

- біометричний шаблон , який зберігається і обробляється в біометричній системи – є незахищеним. Компрометація біометричного шаблону призводить до компрометації як таємного так і відкритого біометричного образу людини;
- однобітовий результат («Так / «Ні») робить кошти автентифцікації уразливими до атак , спрямованих на підміну результату автентифікації;
- зберігання секретного криптографічного ключа спільно з біометричним шаблоном також неприпустимо.

Перераховані уразливості класичних біометричних систем можуть бути усунені за рахунок способів захищеної біометричної автентифікації, які засновані на таких основних положеннях. По-перше, біометрію людини необхідно пов'язувати з деяким кодом доступу. По-друге, біометричні шаблони не повинні використовуватися для прийняття рішення і видачі результату ідентифікації і верифікації.

2.3.4. Історія формування та створення біометричних систем.

У 2001 році закордонними вченими вперше були запропоновані способи усунення загроз порушення конфіденційності біометричних шаблонів в системах біометричної автентифікації і ідентифікації. Зокрема запропоновані способи трансформації біометричного шаблону і його перетворення за допомогою поліноміальних необоротних функцій.

Синтез біометричних технологій і криптографії привів до утворення біометричних криптографічних систем . У таких системах біометричні дані користувача перетворюються в його особистий криптографічний ключ, містяться механізми захисту біометричного шаблону. Даний напрямок отримало назву «біометричний шифрування» («biometric encryption»).

В даний час технологія розвивається за кількома напрямками і номінується кілька видів біометричних криптографічних систем:

- система зі звільненням ключа (key release cryptosystem);
- системи зі св'язуванням ключа (key binding cryptosystem);
- системи з генерацією ключа.

Розглянута кожна система більш детально, зокрема принципи і способи виконуваних перетворень.

В системі зі звільненням ключа зберігається як криптографічний ключ так і біометричний шаблон. Звільнення ключа (надання доступу до ключа) відбувається при успішній біометричної автентифікації. У процесі автентифікації потрібен доступ до біометричного шаблоном, тому він зберігається відкрито, що є недоліком. Таким чином, можлива модифікація ключової інформації і даних шаблону. Перевагою систем із звільненням ключа є простота їх реалізації.

В системі зі зв'язуванням ключа криптографічний ключ зв'язується з біометричним шаблоном шляхом заміщення його значущих даних даними витягується ключа. Стійкість такої системи залежить від конфіденційності алгоритму зв'язування. Проте, даний вид систем може бути застосовний для захисту біометричних шаблонів.

В системі з генерацією ключа криптографічний ключ не зберігається, а витягується безпосередньо з біометричних даних користувача, що є незаперечною перевагою системи. Однак реалізація системи з генерацією ключа набагато складніше розглянутих систем. Складність полягає в необхідності створення

алгоритмів обчислення якісних біометричних параметрів і генерації двійкового вектора фіксованої довжини, що дає точне значення криптографічного ключа легітимного користувача при пред'явленні системі одного і того ж біометричного образу «Свій» та ймовірний розподіл нулів і одиниць при пред'явленні випадкових значень біометричних даних.

На сьогоднішній день відомі такі підходи до перетворення біометричних даних в криптографічний ключ і застосовні для різних біометричних технологій:

- нечіткі екстрактори («fuzzy extractors»);
- нечіткі сховища («fuzzy valt»);
- Біометрика – нейромережеве перетворення.

В нечітких екстракторах і нечітких сховищах застосовуються коди з виявленням і виправленням помилок, що виникають у довічному векторі через неточне відтворення біометричних даних . Якість перетворення біометричних даних в ключ багато в чому визначається якістю застосовуваних кодів, що виявляють і виправляють помилки. При обчисленні криптографічного ключа обидва методи перетворення вимагають зберігання додаткових відкритих даних (відкритий хелпер від англ. Public helper).

Шляхом створення нечітких екстракторів йдуть в основному зарубіжні дослідники. Нейромережеві перетворювачі біометрія-код запропоновані вітчизняними дослідниками . У нейромережевих перетворювачах біометрія-код використовується штучна нейронна мережа (ІНС), яка автоматично навчається на етапі реєстрації користувача формувати його особистий ключ при пред'явленні біометричного образу «Свій». При цьому для випадкових біометричних даних, прикладів образів «Чужий» ІНС формує випадкову кодову комбінацію.

Таким чином, в даний час існує два основних підходи до перетворення неоднозначного біометричного способу в криптографічний ключ користувача, в подальшому використовується в класичних механізмах автентифікації: нечіткий екстрактор та нейромережовий перетворювач біометрія-код. Нечіткий екстрактор, вдає із себе аналог кодів, що виявляють і виправляють помилки в векторі довічних біометричних параметрів. Нейромережевий перетворювач біометрія-код використовує навчену ІНС для формування точного значення ключа. Розглянемо дані підходи більш докладно.

2.3.5 Нечіткі екстрактори

Біометрічна система автентіфікації на основі нечіткіх екстракторів потребує виконання етапу реєстрації користувача. На етапі біометрічної реєстрації користувача створюється ключ *key*, який потім перетворюється в двійковий вектор *KEY* з використанням завадостійких кодів таких, як Боуза- Чоудхурі-хоквінгема (БЧХ) і Ріда-Соломона:

$$KEY = Encode(key), \qquad (2.1)$$

Більшість нечітких екстракторів будується на гамуванні . Двійковий вектор *KEY* шифрується гаммуванням, а в якості гами використовується який вираховується відповідно до отриманої вибірки на етапі реєстрації двійковий вектор біометричних параметрів B:

$$T = B \oplus KEY, \qquad (2.2)$$

де:

- знак $\oplus$ означає операцію побітового виключающого АБО;
- T – двійковий вектор , результат виконання операції гамування;

У відкритому хелперів зберігаються T та Hash(key) - хеш-сумма ключа *key*.

Сам відкритий хелпер поміщається в базу даних відкритих хелперів зареєстрованих користувачів.

В процесі біометричної автентифікації при пред'явленні користувачем біометричних даних знову обчислюється двійковий вектор біометричних параметрів B'. Відновлення ключа *key* відбувається з використанням відкритого хелпера:

$$KEY' = T \oplus B' = KEY \oplus err, \qquad (2.3)$$

де:

- err – помилка , яка виникає через різницю між двома двійковими векторами біометричних параметрів B та B', обумовлюється неточністю відтворення біометричних даних. Таким чином, ключ *key*' необхідно назад декодувати:

$$\text{key}' = \text{Decode}(\text{KEY}'), \qquad (2.4)$$

Процедура автентифікація вважається пройденою при виконанні рівності:

$$Hash(key') = Hash(key), \qquad (2.5)$$

У разі нерівності хеш-сум користувач не проходить перевірку його справжності. На рисунку 1.4 і рисунку 1.5 показаний принцип роботи нечіткого екстрактора, що використовує коди БЧХ для виправлення помилок err.

Для того щоб вважати перетворення з використанням нечіткого екстрактора надійним має виконуватися кілька умов. По-перше, вхідний вектор довічних біометричних параметрів B повинен мати рівно-ймовірний розподіл бітів.

По-друге, вхідний вектор довічних біометричних параметрів повинен містити незалежні (некорельовані) дані. По-третє, дані T, які розміщуються у відкритому хелперів, не повинні приводити до витоку криптографічного ключа. По-четверте, при пред'явленні образів «Чужий» перетворювач повинен формувати випадкову кодову комбінацію.

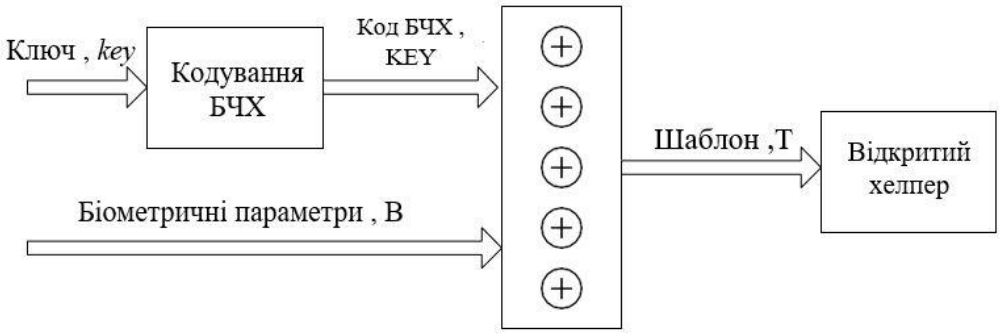


Рисунок 2.3. - Формування відкритого хелпера (реєстрація біометрії)

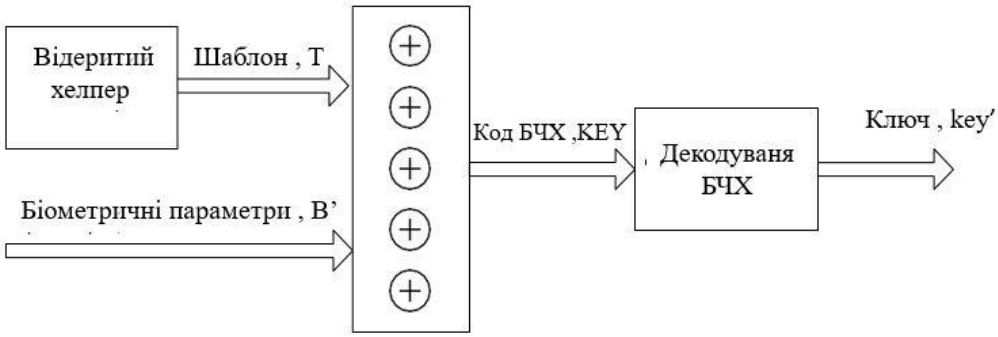


Рисунок 2.4. - Формування ключа нечітким екстрактором з використанням біометричних даних і відкритого хелпера

Імовірність помилок першого роду P_I , , тобто здатність системи формувати ключ користувача при пред'явленні біометричного образу «Свій» істотно залежить від помилки err . В одних з останніх роботах американсксьих дослідників показано, що відновлення 25% помилок виявляється недостатнім для повного відновлення ключа з вектора довічних біометричних параметрів. Для забезпечення рівня P_I менше 0.1 дослідниками вводиться надмірність коригуючого коду, отже, його

позиції стають більш залежними. Багато в чому завищені оцінки ймовірності помилок другого роду P_{II} розробниками систем біометричної автентифікації обумовлені тим, що не беруться до уваги кореляційні зв'язки біометричних параметрів.

Спроби використання кодів з виявленням і виправленням помилок призводять до багаторазової надмірності довічного вектора біометричних параметрів B.

Доводиться застосовувати коди з 90% надмірністю, втрачаючи більшу частину низькоякісних параметрів (використовується не більше 10% вхідних параметрів, що мають достатню якість).

Існує декілька робіт, в яких досить детально описується принцип побудови нечітких екстракторів, що зв'язують біометрію та криптографію, тобто що перетворюють біометрію в особистий ключ користувача.

Таким чином, структура нечіткого екстрактора є коригувальним кодом (БЧХ, Ріда-Соломона), який прагне виправити помилки, що виникають в біометричних параметрах, з метою дешифрування точного значення ключа з використанням відкритого хелпера. Основна складність, яка виникає при побудові нечіткого екстрактора, полягає в створенні алгоритму обчислення більш стійких до шумів біометричних параметрів рисунка відбитка пальця. В даний час загальноприйнятого підходу до створення такого алгоритму не існує.

Висновки до другому розділу

У розділі були показано та описано основні переваги та недоліки технології SSO , а також була розглянута архітектура безпеки Single Sign-On техології.

З розділу стало зрозуміло , що SSO – це як окремий тип продуктів або вбудована технологія, що дозволяює не вдаватися до повторної автентифікації користувача при його переході з різних розділів і сервісів одного порталу, таким як форум, блог та інші, а користувач проходить процедуру автентифікації в одному місці, після чого отримує доступ до всіх пов'язаних з ним розділів, таким чином йому не доводиться вводити свої облікові дані в кількох формах.

Також було проведено огляд основних видів біометричних систем, який показав, що їх можна розділити на системи в яких обробляються біометричні шаблони, і системи, в яких обробляються біометричні контейнери.

Проведено аналіз зарубіжних і вітчизняних технологій перетворення біометричних даних в код автентифікації (біометрія- код), який показав, що існує два основних напрямки вирішення завдання. Перший напрямок характеризується використанням нечітких екстракторів на основі кодів з виявленням і виправленням помилок. Другий напрямок характеризується застосуванням великих штучних нейронних мереж. Аналіз літератури показав, що дослідження нечітких екстракторів проходять переважно за кордоном. В Україні створено і активно розвивається напрямок нейросетевого перетворення біометричних даних людини в код доступу.

На основі нейромережевого перетворювача і нечіткого екстрактора можуть бути розроблені способи знеособлення біометричних даних, які дозволили б зробити неможливим визначення приналежності біометричного контейнера конкретного суб'єкта. Тому актуальними завданнями є розробка способів знеособлення біометричних даних та їх моделювання.

РОЗДІЛ 3.
РОЗРОБКА СИСТЕМИ FRAMEWORK В C#
ДЛЯ ПЕРЕВІРКИ ВІДБИТКІВ ПАЛЬЦЯ

3.1. Мета, алгоритм роботи, цілі розробки фреймворка та реазлізування.

У наш час розпізнавання відбитків пальців є активним напрямком досліджень. Важливим компонентом в системі розпізнавання відбитків є дотримання алгоритмів. У зв'язку з проблемою даної сфери алгоритми розпізнавання відбитків пальців діляться на дві категорії:

- алгоритм перевірки;
- алгоритм ідентифікації.

Мета алгоритмів перевірки відбитків пальців є - визначити, який з двох відбитків зроблений одним пальцем, а який ні. З іншого боку, алгоритми ідентифікації роблять пошук запиту відбитка пальця в базі даних, шукаючи відбиток, зроблений одним і тим же пальцем.

Алгоритм розробки проекту :

- проведення експеременту над розпізнанням відбитка пальця;
- показ шаблона відбитка пальця після виконання алгоритму;
- розрахунок та виведення на дисплей відбитку пальця;
- інтегрування алгоритмів у фреймворк.

Основна з цілей при розробці даного фреймворка була розробка класів інтерфейса простими і доступними. Таким чином процес додавання нових алгоритмів дуже простий.

У роботі були використані:

- інструменти, бібліотеки та класи, доступні в .Net Framework, які економлять багато часу для написання коду.
- Одна з найвідоміший мов програмування C#;

Фреймворк реалізований на C # з використанням .Net Framework .

Наш фреймворк дозволяє експериментувати в базах даних типу B від FVC2000, FVC2002 і FVC2004, і в базах даних типу A від FVC2002 і FVC2004. У цих експериментах ми виконуємо індикатори the Fingerprint Verification Competitions (EER (%), FMR100 (%), FMR1000 (%), ZeroFMR (%), Time (ms) і ROC curves). Крім того, ми можемо робити досліди навіть зі звичайним протоколом і різними базами даних.

Ми реалізували алгоритми розпізнавання відбитків пальців, запропонований Tico і Kuosmanen, Jiang і Yau, Medina-Pérez. Важливо звернути увагу на те, що всупереч алгоритму Qi - це набір шаблонів відбитків пальців, який базується на алгоритмах, ми реалізували тільки алгоритми, зіставні протоколами введення відбитка пальця. Також ми проаналізували та використали алгоритми виділення ознак, запропонований Ratha, і орієнтацію на отримання зображення. Даний фреймворк дозволяє нам додавати, як нові алгоритми розпізнавання відбитків, так і нові алгоритми виділення ознак з мінімальними зусиллями і без перекомпіляції фреймворка.

Наша робота складається з файлів:

- Вхідний код документації;
- Вихідні файли нашого фреймворка.
- Ссилка для самого розширення з метою його дослідження.

3.2. Загальна інформація , та недоліки веб-системи *FVC-onGoing.*

У даній роботі ми будемо використовувати сисетму FVC-onGoing , тому що вона є найбільш відповідною для роботи з нашим фреймворком.

• *FVC-onGoing* - це автоматизована веб-система оцінки алгоритмів розпізнавання відбитків пальців. Тести проводяться на наборі ізольованих наборів даних, а результати повідомляються в режимі онлайн з використанням добре відомих індикаторів продуктивності та показників.

•**Мета** полягає в тому, щоб відстежувати досягнення в технологіях розпізнавання відбитків пальців за допомогою постійно оновлюваного незалежного тестування і звітності про продуктивність по заданим тестам. Алгоритми оцінюється з використанням суворо контрольованих підходів для забезпечення максимальної надійності.

•*FVC-onGoing* - це еволюція FVC: міжнародних змагань з перевірки відбитків пальців, організованих в 2000, 2002, 2004 і 2006 роках.

•Ця система має наступні **недоліки**:

- у нас немає доступу до інших алгоритмів , крім своїх власних;
- це не фраємворк , тому ми не можему використовувати інші компоненти програмного забезпечення;
- система не може бути використана з метою навчання , так як учень не може подивитися , як працють алгоритми;
- після виконання досліду використовується база даних (стандартна або жорстка) нам необхідно чекати 30 днів для того , щоб зробити наступний експеремент , використовуючи ту ж базу даних.
- ми не можемо керувати базою даних. Таким чином , ми не можемо використовувати власну базу даних або редагувати існуючу.
- відустутність доступу до тих відбитків , для яких наш алгоритм не виконувався. Отже , ми не зможемо проаналізувати , чому саме наш алгоритм не виконався для того , щоб виправити код
- ми не зможемо створити експеремент за допомогою звичайного протоколу для оцінки виконання.

3.3. Запуск дослідження для розпізнавання відбитків пальців.

• Спочатку виймаємо з архіву файл "FingerprintRecognition.zip" і будуємо рішення. Далі можете налагоджувати проект "FR.FVCExperimenter" або можемо запустити "FR.FVCExperimenter.exe" в директорію, яка містить згенерований вузол. Яке відкриє вікно вибору бази даних (Рисунок 3.1):

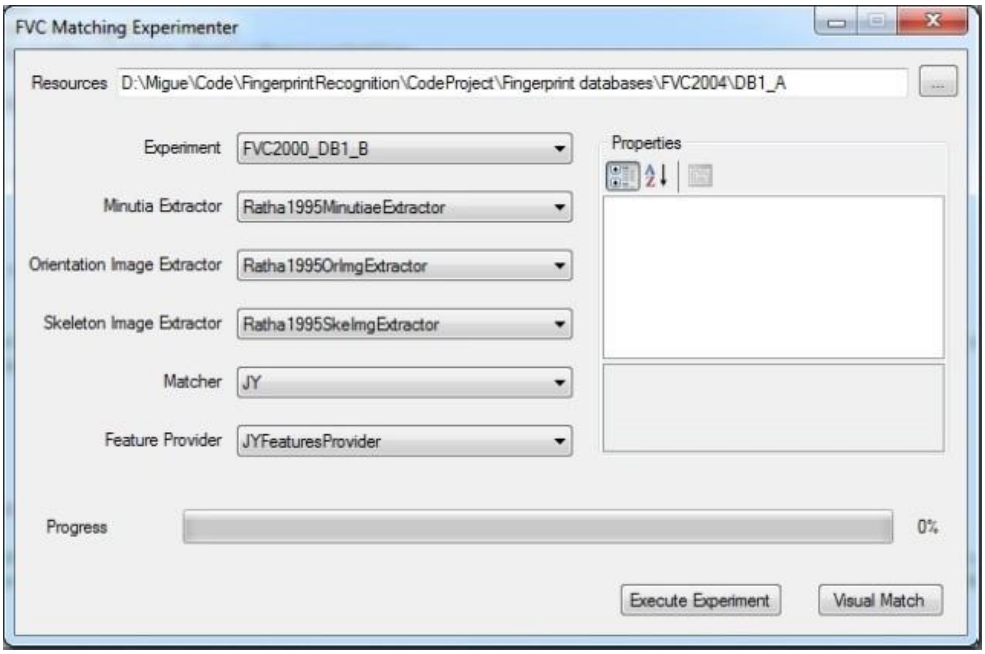


Рисунок 3.1 – Вікно вибору бази даних

• У рядку "Resources" записаний шлях до бази даних, яку ви збираєтеся використовувати, наприклад: "D: MALANCHUK_NAU\ PR Databases \ Fingerprints \ FVC2004 \ DB1_B".

•Вибераємо відповідний нам тип досвіду в спливаючому меню з назвою "Experiment".

•Використовуємо меню з назвами "Minutia Extractor", "Orientation Image Extractor" і "Skeleton Image Extractor" для вибору алгоритму, який буде використовуватися для знаходження основних особливостей (відбиток, орієнтоване зображення і його образ).

• Використовуємо поле "Matcher" для вибору алгоритму розпізнавання відбитків пальців і поле "Feature Provider" для вибору алгоритму, який буде зберігати та видавати риси обраних збігів. Незважаючи на те, що ми реалізували тільки одну рису розпізнавання для кожного збігу, існують сценарії, де ми можемо використовувати кілька ознак для одного збігу.

•Поле з назвою "Properties" дозволяє змінювати параметри обраного алгоритму.

•Натисніть на кнопку "Execute Experiment" для запуску дослідження. Даний досвід використовує протокол оцінки від *the Fingerprint Verification Competitions.*

У цьому досвіді ми вирахували такі індикатори: EER (%), FMR100 (%), FMR1000 (%), ZeroFMR (%), Час (мс) і ROC-крива.

Ці індикатори збережені в файлі з ім'ям, сформованим в залежності від обраного нами алгоритму із закінченням ".Summary.csv".

Цей файл зберігається в папці з назвою "Results" в тій же папці, де зберігаються відбитки пальців.

Також збережені ще два файли, один зберігає в собі неправдиві відповідності відбитків пальців, інший - помилкові невідповідності відбитків.

•Якщо ми хочемо порівняти 2 відбитка і перевірити їх збіг, клікаємо на кнопку "Visual Match", після якої відкриється форма "Visual Fingerprint Matching".

Вона завантажує відбитки, які ми хочемо порівняти і натискаємо кнопку "Match". Екстрактор ознак і обраний в "FVC Experimenter" режим також тут використовуються для того, щоб виконати порівняння відбитків пальців. Нижче приклад порівняння двох відбитків. (рисунок 3.2)

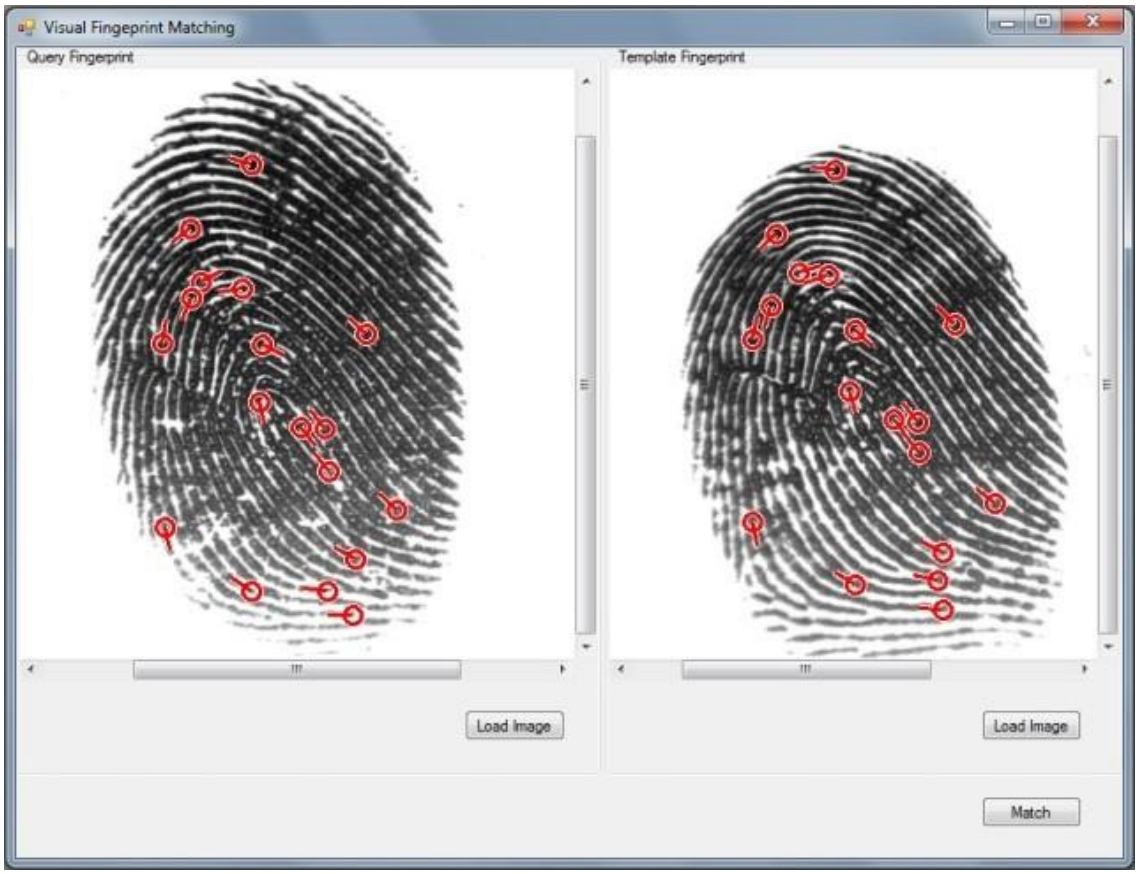


Рисунок 3.2 - Приклад порівняння двох відбитків

3.4. Візуалізація обрисів відбитка пальця.

• Якщо ми хочемо вивести картинку обрисів відбитка, тоді нам потрібно використовувати проект "FR.FeatureDisplay".

У графі "Fingerprint Feature Display" ми можемо змінювати екстрактор ознак і їх зображення. У фреймворку ми використовуємо класи для візуалізації відбитка, орієнтоване зображення і скелет картинки.

У наступному прикладі ми можемо побачити візуалізацію приблизного зображення відбитка (Рисунок 3.3).

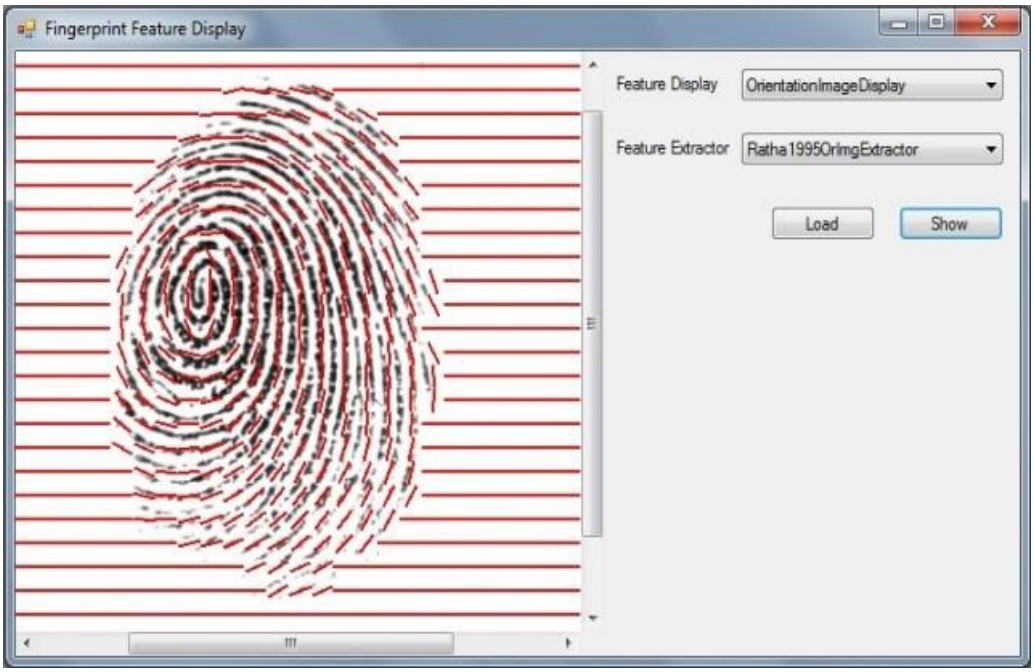


Рисунок 3.3 – Візуалізація приблизного зоображення відбитка.

3.5. Відповідність відбитків поза фреймворка.

В даному пункті представлений приклад використання фреймворка для порівняння двох зображень відбитків в звичайному призначеному для користувача додатку. Він складається з 3х кроків для порівняння 2х зображень відбитків: завантажити картинку, витяг ознак і їх порівняння.

В цьому випадку користувачам потрібно додати посилання з їх застосування до збірки FR.Core і FR.Medina2012.

Збірки *SHullDelaunayTriangulation* і *ImageProcessingTools* повинні бути додані в папку виведення, де з'явиться бінарний файл. (див. ДОДАТОК А.БІНАРНИЙ ФАЙЛ У ПАПЦІ ВИВОДУ).

Приклад використання *M3gl* показує, як легко використовувати фреймворк, і як добре він складний та не вимагає пояснень сам код.

3.6. Додавання нових алгоритмів в фреймворк.

Перше, що ми повинні знати - це те, що нам не потрібно модифікувати додаток фреймворка для розпізнавання власних алгоритмів, тому що ми використовуємо Рефлекцію , для того щоб завантажити всі динамічні алгоритми під час виконання.

Ви можете створити стільки додатків, скільки хочете в директорії, яка містить фреймворк. Для кожного нового додатка зайдіть в налаштування та вкажіть шлях виведення зі значенням ".. \ bin \ Release \".

• Для додавання нової функції визначення нам потрібно наслідувати з базового класу *FeatureExtractor* і реалізувати метод *ExtractFeatures (Bitmap image).*

Наприклад, припустимо, що ми хочемо створити функцію визначення типу *MyFeature*, далі ми можете реалізувати клас за прикладом (Рисунок 3.4).

```
public class MyFeatureExtractor : FeatureExtractor
{
  public override MyFeature ExtractFeatures(Bitmap image)
    {
   // Place here your code to extract features
    }
}
```

Рисунок 3.4 –Реалізація класа за прикладом

У разі, якщо нова функція була побудована на деяких існуючих, ми можемо поступити таким чином: (див ДОДАТОК Б-РЕДАГУВАННЯ КОДУ).

Для кожної функції визначення ми повинні створити постачальник ресурсу. Постачальник ресурсу дозволяє зберігати (отриманий) в (вихідний) файловий ресурс, пов'язаний з відбитком. Фреймворк включає в себе постачальник ресурсу для вилучення відбитків (MinutiaListProvider), орієнтоване зображення (OrientationImageProvider) і скелет картинки (SkeletonImageProvider).

У наступному прикладі постачальника ресурсів для функції вилучення. (див ДОДАТОК В – ФУНКЦІЇ ВИЛУЧЕННЯ ДЛЯ ПОСТАЧАЛЬНИКА РЕСУРСІВ).

Прийшов час створити новий алгоритм збігу відбитків пальців. Припустимо, що ми хочему порівняти функції типу *MyFeature*, для цього нам необхідно створити «зрівнювач» (Рисунок 3.5).

```
public class MyMatcher : Matcher
{
  public override double Match(MyFeature query, MyFeature template)
    {
   // Place here your code to match fingerprints
    }
}
```

Рисунок 3.5 – Створення «Зрівнювача»

У разі, якщо ми реалізували алгоритм порівняння відбитків, далі нам необхідно змінити в коді нижче наступне: (Рисунок 3.6)

```
public class MyMatcher : Matcher, IMinutiaMatcher
{
  public override double Match(MyFeature query, MyFeature template)
    {
   List matchingMtiae;
   return Match(query, template, out matchingMtiae);
    }
  public double Match(object query, object template, out List matchingMtiae)
    {
   // Place here your code to match fingerprints
    }
}
```

Рисунок 3.6 – Змінення у кодуванні

3.7. Інтегровані вбудовані алгоритми в фреймворку.

Користувачам не потрібно змінювати фреймворк для інтеграції звичайних алгоритмів, так як рефлекції завантажуються динамічно, під час виконання програми. У цьому випадку користувачі повинні додати нові алгоритми до їх власних звичайних збірок.

Для того, щоб використовувати існуючі алгоритми порівняння в фреймворку, перше, що необхідно зробити, це створити постачальник ресурсів. Постачальник ресурсів дозволяє зберігати (отриманий) в (вихідний) файл ресурси, пов'язані з відбитками пальців. Наприклад, припустимо, що користувачі хочуть інтегрувати *SourceAFIS SDK (http://www.sourceafis.org/)* в фреймворк, наступна функція забезпечення може використовуватися як (див. ДОДАТОК Г – ФУНКЦІЇ ЗАБЕЗПЕЧЕННЯ).

А зараз алгоритм порівняння відбитків може бути записаний в наступні класи (Рисунок 3.7)

```
public class SourceAFISMatcher : Matcher

{

  public override double Match(Person query, Person template)

    {

    return Afis.Verify(query, template);

    }

  private static AfisEngine Afis = new AfisEngine();

}
```

3.8. Методи, які були використані для виконання роботи.

МЕТОД TICO І KUOSMANEN

Метод Tico і Kuosmanen (або алгоритм постобробки зображення відбитка пальця).

Метод заключається у постобробці яка спрямована на відсіювання помилкових структур кусочно-лінійному уявленні відбитка. Деякі конфігурації ліній свідомо не властиві лініям відбитку пальців, і якщо вони все-таки зустрічаються, то вони є результатом недоробки попередніх етапів.

МЕТОД JIANG І YAU

Метод Jiang I , Yau (або розпізнавання відбитків пальців: на основі глобальних ознак і по локальним (місцевим) ознакам.

Глобальні ознаки - це зовнішній вигляд відбитка, орієнтація зображення, кривизна і поле напрямків, що описує загальний стан формування папілярних ліній відбитків пальців.

Локальні ознаки або Мінуції (від англ. Minutia) – це місцеві особливості папілярних ліній, унікальні для кожного відбитку точки по площі всього зображення. Всього існує 155 різновидів Мінуцій, однак найбільш відомими вважаються два види Мінуцій, в яких обриваються або роздвоюються папілярні лінії.

МЕТОД MEDINA-PÉREZ

Метод Medina-Perez (або удосконалення стратегії декількох вирівнювань для перевірки відбитків пальців)

Важливою складовою цього алгоритма є стратегія вирівнювання. Стратегія єдиного вирівнювання з часовою складністю використовує місцеву пару відповідних дрібниць, яка максимізує значення подібності для вирівнювання дрібниць.

Стратегія багаторазового вирівнювання полегшує обмеження, виконуючи багаторазові вирівнювання дрібниць.

3.9. Автентифікація на базі сертифікатів та технології SSO.

Автентифікація з алгоритмами порівнянням вібитків пальців – це сучасно, надійно та безпечано але в якихось випадках зручніше використовувати аутентифікацію на базі сертифікатів, в якихось - одноразові паролі. Важливо, що автоматизована система, за допомогою якої забезпечується аутентифікація користувачів в ІС і на базі якої ми будуємо технологію SSO (Single Sign On), дозволяє нам застосовувати практично будь-які види аутентифікації користувачів в системах.

Якщо ми задумалися про перехід на сувору аутентифікацію, варто підходити до вирішення проблеми комплексно. Необхідно опрацювати єдину технологію аутентифікації в усіх основних додатках, в якихось випадках зробивши її наскрізно - прозорою для користувача. Перведення користувачів просто на якусь із технологій суворої аутентифікації, наприклад, в домені організації, звичайно, підвищить рівень ІБ, але може упустити безліч інших можливостей, які роблять технологію привабливою для користувача і для бізнесу.

Недоліки, пов'язані з використанням паролів, послужило поштовхом для прийняття рішення про перехід на інший спосіб аутентифікації, які вже багато разів обговорювалися. До середини 2000-х рр. явно проявилися ще два негативних аспекти, пов'язаних з використанням паролів.

Перший - з'явилося безліч інтернет-сервісів з парольною аутентифікацією - різні соціальні мережі, месенджери, інтернет-магазини і безліч інших. Для кожної треба придумати мінімум по одній можливості складання унікального паролю.

Практика підказує, що відсоток користувачів, у яких паролі від банківських систем і паролі від інтернет-сервісів збігаються, буде близький до 90%. Заразивши комп'ютер користувача і зібравши його паролі від інтернет-сервісів, можна бути впевненим, що якийсь із них підійде і до банківських ІС.

Інший аспект, який почав викликати тривогу, - це збільшення частки мобільних користувачів, яким необхідний віддалений доступ до ІС банку. І для організації такого доступу звичайної парольної аутентифікації явно недостатньо.

Спочатку ми розглядали аутентифікацію за сертифікатами, що зберігаються на токенах, але є досить багато тонкощів, які можуть звести нанівець всі її переваги.

3.10. Результати тестування та реалізація аутентифікації за вібдитком.

Судячи з результатів написання нашого алгоритму ми можем смофмувати таблицю-порівння готових нам зображень для порівння справжнього відбитку користувача та відбитку так званного фейку , який видає себе за справжнього користувача (Рис 3.8 – Порівняння користувачів).

Зразок	Оригінальне зооб.	Порівняльне зооб
1		
2		
3		
4		

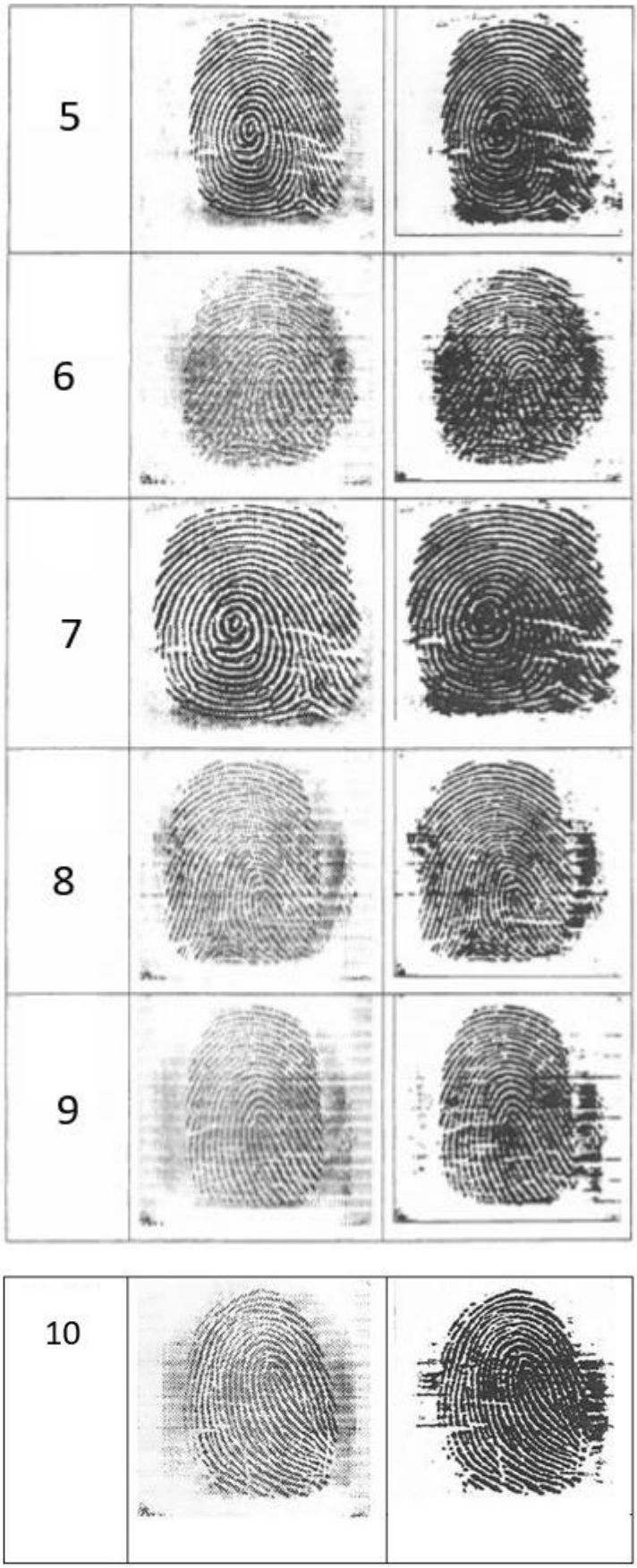
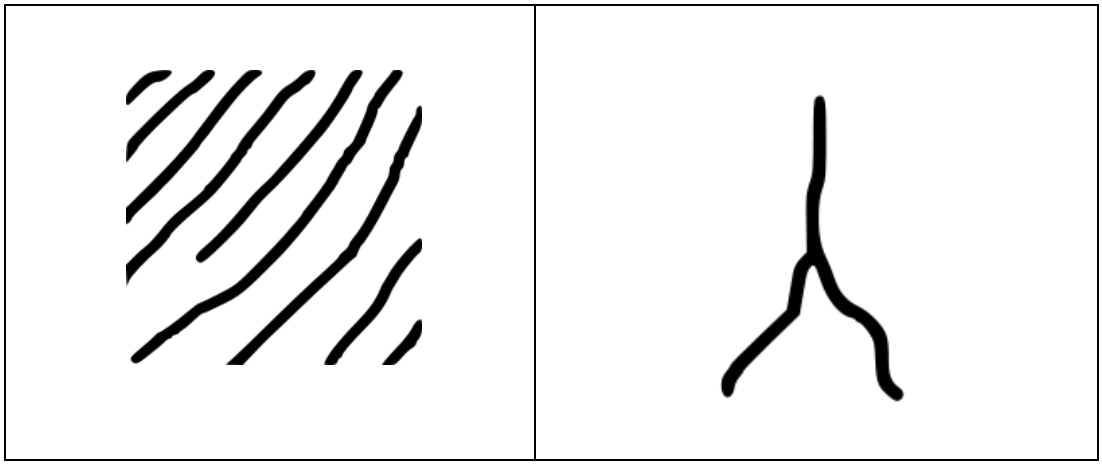


Рис 3.8 – Порівняння користувачів

Завдяки готовому порівнянню ми з легкістю можемо порівняти типі взорів користуючись наукою під назвою Мінуція (Рисунок 3.9- Мінуція відибитків) та зрозуміти де – справжній користувач, а де – зловмисник.

Мінуція - унікальні для кожного відбитку ознаки, що визначають пункти зміни структури папілярних ліній (закінчення, роздвоєння, розрив і т. д.), орієнтацію папілярних ліній і координати в цих пунктах. Кожен відбиток містить до 70 Мінуцій.



Біофункція:

Рисунок 3.9- Мінуція відибитків

Реалізація аутентифікації за відбитком:

Реалізація аутентифікації має проводитись за двома варінтами. Перший реалізовує реєстрацію на основі JWT-token, за відсутності сканера відбитків пальців.

JSON Web Token (JWT) — JSON-об’єкт, який містить в зашифрованому вигляді всю мінімально необхідну інформацію для аутентифікації і авторизації. Аутентифікація користувача за допомогою JWTтокенів відбувається наступним чином:

– користувач запитує доступ до сервера (Authorization Server) висилаючи логін і пароль.
– Authorization Server перевіряє валідність користувача і висилає йому access token, який містить термін 2 тижні (expriation date);
– користувач використовує цей access token для доступу до ресурсів (Рисунок 3.10 – Реєстрація на основі JWT-токену).

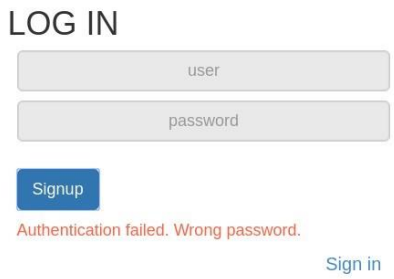


Рисунок 3.10 – Реєстрація на основі JWT-токену

Другий спосіб реалізування аветинтифікації – це FlexCode SDK - безкоштовний SDK для розробки програмного забезпечення для відстеження відбитків пальців, призначений для додавання функцій перевірки відбитків пальців. Даний SDK є найбільш придатним для розробки біометричних додатків для входу в систему, зчитує більше 10 відбитків пальців.

SDK працює під Linux, OS X та Windows. Не потребує ніякої інсталяції чи налаштувань на сервері. Функція SDK для перевірки відбитків пальців дозволяє відсканувати відбитки від сканерів та здійснювати перевірку відбитків пальців (відповідність 1: 1). Контроль якості може бути застосований для прийняття лише хороших якісних відбитків пальців від сканерів відбитків пальців.

JavaScript відповідає за клієнтську частину, реакцію на дії користувача та забезпечення інтерактивності.

Замість традиційної моделі паралелізму на основі потоків в Node.js використовуються принципи подієво-орієнтованих систем - в порівнянні з підходом «один потік на кожне з'єднання» код виходить простіше і швидше. Node.js став популярний завдяки великому обсягові NPM, а також великій

спільноті розробників і можливості використовувати JavaScript на клієнті, на сервері і для розробки інструментів.

Алгоритм автентицікації завдяки відбитку пальця та логіну користувача.

Головне вікно входа у програму, де ми можемо авторизуватися завдяки логіну та відбитку пальця (Рисунок 3.11 – Головне вікно входу)

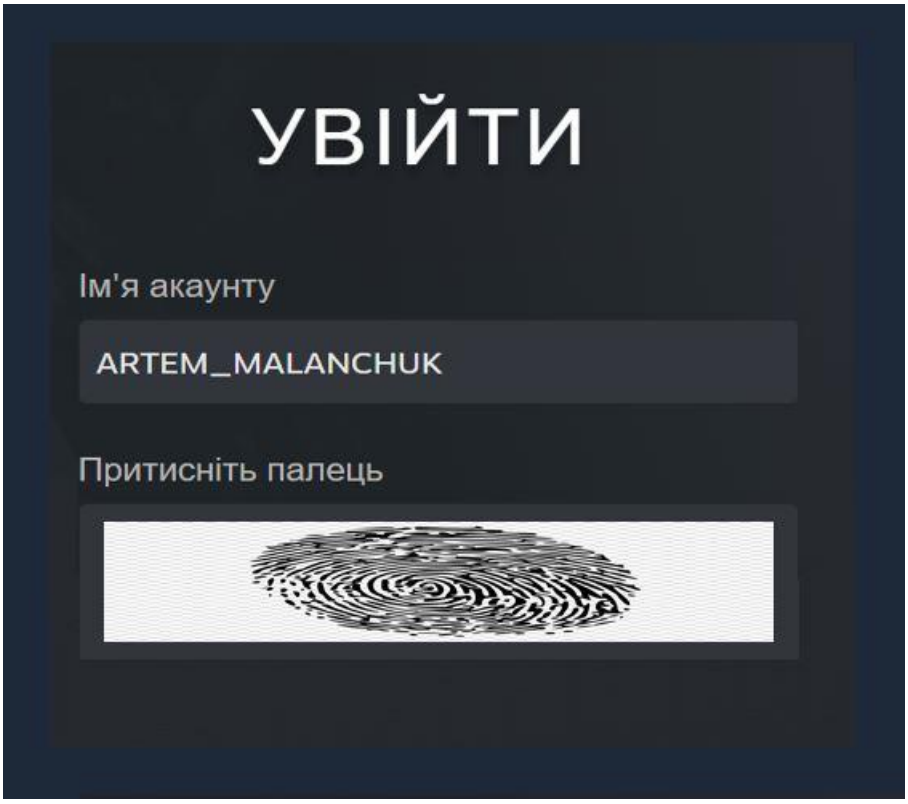


Рисунок 3.11 – Головне вікно входу

Автентифікаця після вдалого входу:

Якщо користувач вдало пройшов автентифікацю він потрапляє до основного меню програми де користувач має можливість вільно користуватися ресурсами.(Рисунок 3.12)

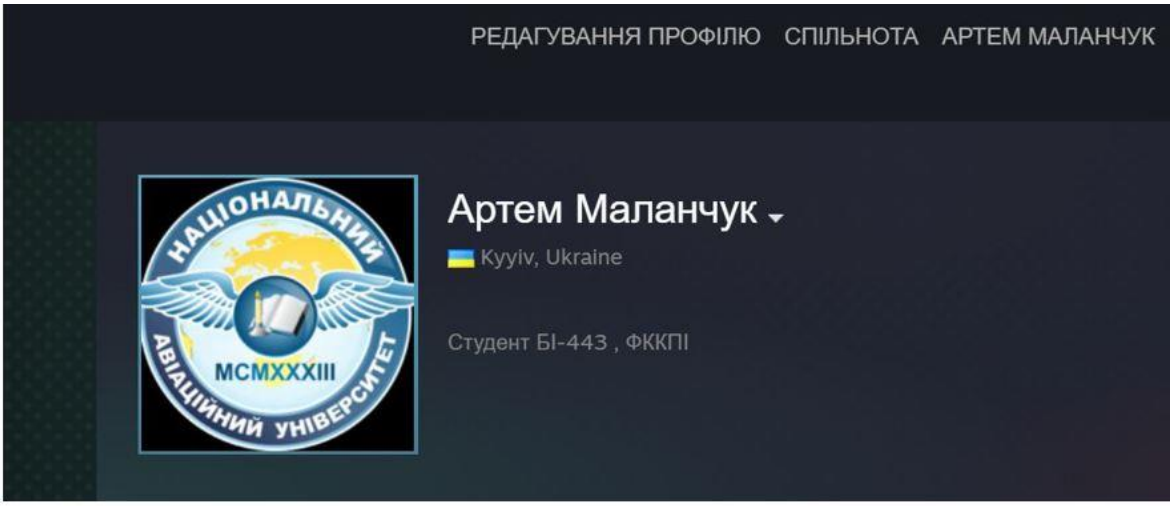


Рисунок 3.12 – Вдалий вхід у програму.

Автентифікаця після невдалого входу:

У разі якщо зловмисник видав Ваше ім’я та недійсний відбиток пальця для акаунту, у нього з’явиться помилка , яка повідомить про невірний відбиток пальця або невірне ім’я користувача (Рисунок 3.13 – Невдалий вхід)

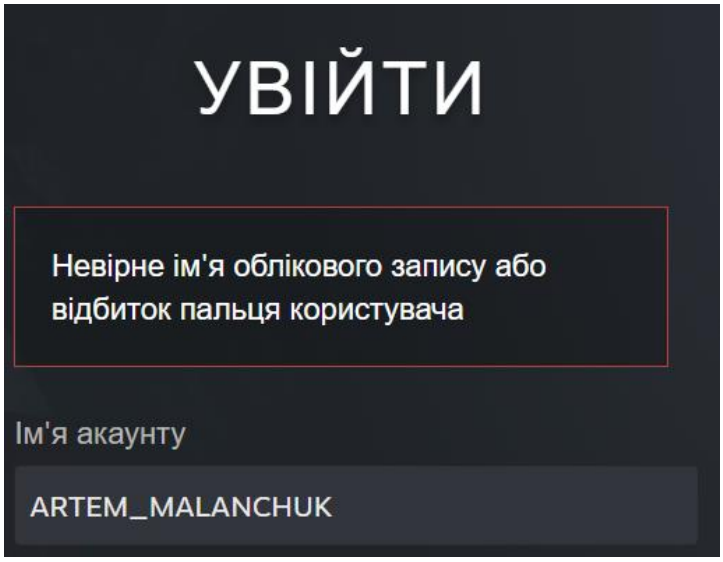


Рисунок 3.13 – Невдалий вхід

Завдяки технології SSO ми можемо отримати доступ до інших привілегій (таких, як доступ до Обговорення на форумі , Публікації користувача, Приватні повідомлення і т.д) і це все під одним єдиним входом у облікову мережу (Рисунок 3.14 – Привілегії Єдиного входу).

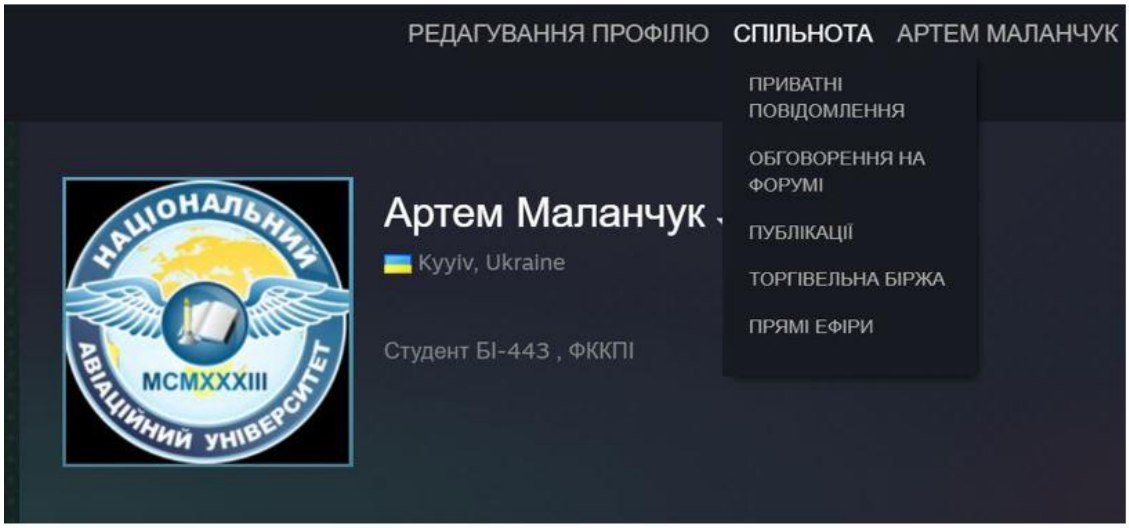


Рисунок 3.14 – Привілегії Єдиного входу

Як приклад при успішній авторизації та доступу до інших підсистем при вдалій аветнтифікації ми можемо перейти до різних так званих «топіків», у яких користувачі можуть створювати та обговорювати різноманітні цікаві їм теми (Рисунок 3.15)

Рисунок 3.15 – Доступ до інших підсистем при автентифікації.

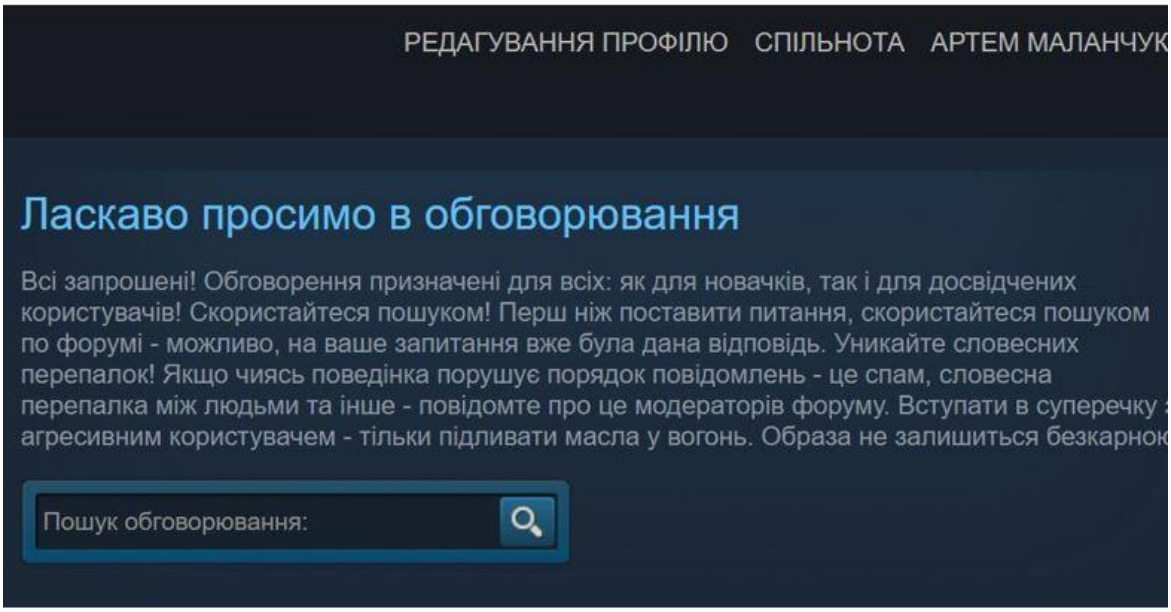


Рисунок 3.15 – Доступ до інших підсистем при автентифікації

Висновки до третього розділу та Результати експеременту.

- У результаті третього розділу ми виконали великий експеримент з алгоритмами порівняння відбитків пальців, користуючись фреймворком.
- За допомогою роботи було продемонстровано фреймворк в C # для розпізнавання відбитків пальців. Завдяки роботі було коротко поясненно , як можно виконати досліди з розпізнавання відбитків та як інтегрувати власні алгоритми в фреймворк. Також було надано кілька алгоритмів порівняння відбитків пальців і алгоритмів вилучення ознак, за допомогою яких ми можемо не тільки робити експерименти, а й створити власні програми.
- Було показано вихідні коди всіх алгоритмів, тому користувач може використовувати будь-яку частину коду так само, як і будь-який компонент програмного забезпечення.
- Було показане порівняння двох відбитків (справжнього користувача та зловмисника), а також за рахунок відбитків була зроблена автентифікація завдяки JSON Web Token та FlexCode SDK.

ВИСНОВКИ:

В результаті виконання дипломної роботи,отримані наступні результати:

1)Проаналізовані методи біометричної автентифікації та визначена можливість їх застосування в системах керування доступом на основі технології SSO, що стало основою при розробці відповідної системи.

2)Розроблено систему керування доступом на основі технології SSO з використанням біометричної автентифікації за відбитком пальця, що дає змогу

забезпечити санкціонований доступ користувачів одночасно до декількох ресурсів системи за технологією єдиного входу.

3)Проведено тестування розробленної системи керування доступом на основі технології SSO з використанням біометричної автентифікації, що дало змогу перевірити можливість її використання для вирішення поставленої задачі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1) Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 16 січня 2014 р. № 30. URL: https://zakon.rada.gov.ua /laws/show/3475-15 (дата звернення: 15.05.2021).

2) Про основні засади забезпечення кібербезпеки України : Закон України від 21 червня 2018 р. № 2469-VIII URL: https://zakon.rada.gov.ua /laws/show/2163-19 (дата звернення: 15.05.2021).

3) Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України": Указ Президента України від 27 січня 2016 р. URL: https://www.rnbo.gov.ua/ua/Ukazy/417.html. (дата звернення: 15.05.2021).

4) Команда CERT-UA Держспецзв’язку з 18 по 24 квітня зареєструвала 2882 кіберінциденти : Офіційний сайт ДССЗЗІ. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=320629&cat_id=317163 (дата звернення: 15.05.2021).

5) Applying Cyber Kill Chain® Methodology to Network Defense : GAINING THE ADVANTAGE Lockheed Martin. URL: https://www. lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.

6) Про управління інформаційною безпекою : Закон Сполучених Штатів Америки. Від 17 грудня 2002 р. Режим доступу до ресурсу: https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-07publ347.pdf (дата звернення: 15.05.2021).

7) Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу : Директива Європейського Парламенту і Ради (ЄС) 2016/1148. URL: https://zakon.rada.gov.ua/laws/show/984_013-16 (дата звернення: 15.05.2021).

8) Про затвердження Порядку доступу до мережі Інтернет : Аналіз регуляторного впливу проекту постанови Кабінету Міністрів України від 01

січня 2019 р. URL: http://195.78.68.84/dsszzi/control/uk/publish/article?showHid den =1&art_id=299628&cat_id=38837 (дата звернення: 15.05.2021)

9) Носенко К. М., Півторак О. І., Ліхоузова Т. А. Огляд систем виявлення атак в мережевому трафіку : Міжвідомчий науково-технічний збірник “Адаптивні системи автоматичного управління”, 2014. 67–75с.

10) K. K. Security Management Process in Distributed, Large Scale High Performance Systems : Online Journal on Power and Energy Engineering.2015. – URL : https://www.researchgate.net/publication/268356955_Security_Manage ment_Process_in_Distributed_Large_Scale_High_Performance_Systems.

11) Про рішення Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України" : УКАЗ ПРЕЗИДЕНТА УКРАЇНИ від 27 січня 2016 р. URL: https://zakon.rada.gov.ua/laws/show/96/2016.

12) Конвенція про кіберзлочинність : веб-сайт Верховної Ради України : від 07 вересня 2005р. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 15.05.2021).

13) Оперативна інформація Держспецзв’язку щодо захисту державних інформаційних ресурсів : від 16 червня 2020 URL: http://www.dsszzi.gov.ua/ dsszzi/control/uk/publish/article;jsessionid=07515BBA5DC8FCDE53AF420BD4C 0 5FB8.app1?art_id=321621&cat_id=317163 (дата звернення: 15.05.2021).

14) Про електронні довірчі послуги : Закон України № 440-IX від 14 січня 2020р. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення: 15.05.2021).

ДОДАТОК А
БІНАРНИЙ ФАЙЛ У ПАПЦІ ВИВОДУ

```
// Loading fingerprints

var fingerprintImg1 = ImageLoader.LoadImage(fileName1);

var fingerprintImg2 = ImageLoader.LoadImage(fileName2);

// Building feature extractor and extracting features

var featExtractor = new MTripletsExtractor() { MtiaExtractor = new Ratha1995MinutiaeExtractor() };

var features1 = featExtractor.ExtractFeatures(fingerprintImg1);

var features2 = featExtractor.ExtractFeatures(fingerprintImg2);

// Building matcher and matching

var matcher = new M3gl();

double similarity = matcher.Match(features1, features2);
```

ДОДАТОК Б

РЕДАГУВАННЯ КОДУ

```
public class MyFeatureExtractor : FeatureExtractor

{

  public FeatureExtractor<List> MtiaExtractor { set; get; }

  public FeatureExtractor OrImgExtractor { set; get; }

  public override MyFeature ExtractFeatures(Bitmap image)

    {

   try

        {

     var mtiae = MtiaExtractor.ExtractFeatures(image);

     var orImg = OrImgExtractor.ExtractFeatures(image);

     return ExtractFeatures(mtiae, orImg);

        }

   catch (Exception e)

        {

     if (MtiaExtractor == null)

       throw new InvalidOperationException("Cannot extract MyFeature: Unassigned minutia list extractor!",
e);

     if (OrImgExtractor == null)

            throw new InvalidOperationException("Cannot extract MyFeature: Unassigned orientation image
extractor!", e);

     throw;

        }

    }

  public MyFeature ExtractFeatures(List mtiae, OrientationImage orImg)

    {

   // Place here your code to extract features

    }

}
```

ДОДАТОК В

ФУНКЦІЯ ВИЛУЧЕННЯ ДЛЯ ПОСТАЧАЛЬНИКА РЕСУРСІВ

```
public class MyFeatureProvider : ResourceProvider
{
  public MinutiaListProvider MtiaListProvider { get; set; }
  public OrientationImageProvider OrImgProvider { get; set; }
  public override string GetSignature()
    {
    return "myf";
    }
  public override bool IsResourcePersistent()
    {
    return true;
    }
  protected override MyFeature Extract(string fingerprint, ResourceRepository repository)
    {
    try
        {
      var mtiae = MtiaListProvider.GetResource(fingerprint, repository);
      var orImg = OrImgProvider.GetResource(fingerprint, repository);
      return featureExtractor.ExtractFeatures(mtiae, orImg);
        }
    catch (Exception e)
        {
      if (MtiaListProvider == null)
            throw new InvalidOperationException("Unable to extract MyFeature: Unassigned minutia list
provider!", e);
      if (OrImgProvider == null)
          throw new InvalidOperationException("Unable to extract MyFeature: Unassigned orientation image
provider!", e);
      throw;
        }
    }
  private MyFeatureExtractor featureExtractor = new MyFeatureExtractor();
```

ДОДАТОК Г.
ФУНКЦІЇ ЗАБЕЗПЕЧЕННЯ.

```
public class SourceAFISFeatureProvider : ResourceProvider

{

  protected override Person Extract(string fingerprint, ResourceRepository repository)

    {

        Fingerprint fp = new Fingerprint();

        fp.AsBitmap = imageProvider.GetResource(fingerprint, repository);

        Person person = new Person();

        person.Fingerprints.Add(fp);

        Afis.Extract(person);

    return person;

    }

  public override string GetSignature()

    {

    return string.Format("sAFIS");

    }

  public override bool IsResourcePersistent()

    {

    return true;

    }

  private static AfisEngine Afis = new AfisEngine();

}
```