Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління _____
(повна назва)

Кафедра _____Безпеки інформаційних технологій _____
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____

Біометрична аутентифікація користувачів для захисту веб-додатків

Виконав:

студент __2_ курсу, групи _БІКСм-20-1___

Морозов О.Ю._____

(прізвище, ініціали)

Спеціальність _____125 Кібербезпека _____

(код і повна назва спеціальності)

Освітня програма «Безпека інформаційних і комунікаційних систем»

(повна назва освітньої програми)

Керівник доцент Олешко І.В.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ _____Халімов Г.З.__
(підпис) (прізвище, ініціали)

2021 р.

Харківський національний університет радіоелектроніки

Факультет_____Комп'ютерної інженерії та управління _____

Кафедра_____Безпеки інформаційних технологій_____

Рівень вищої освіти_____другий (магістерський)_____

Спеціальність_____125 Кібербезпека _____
(код і повна назва)

Освітня програма_____«Безпека інформаційних і комунікаційних систем»___
(повна назва)

ЗАТВЕРДЖУЮ:

Зав. кафедри _____
(підпис)

«____»_____ 20 ___ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студентові_____Морозову Олексію Юрійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи: Біометрична аутентифікація користувачів для захисту веб-додатків

_____

затверджена наказом по університету від «08»_листопада___2021 р. № 1685Ст

2. Термін подання студентом роботи до екзаменаційної комісії 13 грудня_____2021 р.

3. Вихідні дані до роботи Системи ідентифікації та автентифікації на основі біометричних даних людини та їх застосування у веб додатках; методології тестування вразливостей веб-додатків (OWASP, PCI DSS, ISO/IEC 27002, OSSTMM); статистичні дані щодо характеристик основних методів біометричної автентифікації; нормативна документація: ISO/IEC 19989-2:2020 – Criteria and methodology for security evaluation of biometric systems; ISO/IEC 19792:2009 – Specifies the subjects to be addressed during a security evaluation of a biometric system; ISO/IEC 15408-3:2008 –Security techniques –Evaluation criteria for IT security.

_____

_____

_____

_____

4. Перелік питань, що потрібно опрацювати в роботі:

Загрози безпеці веб-додатків; методологія аналізу загроз безпеки; оцінка ризиків безпеки для веб-додатків; аналіз наслідків та способів експлуатації загроз безпеки; аналіз можливостей використання різних методів біометричної автентифікації у веб-додатках; методи біометричної автентифікації за геометрією обличчя; переваги та недоліки застосування біометрії у веб- додатках; розробка веб-додатку з авторизацією за геометрією обличчя.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _презентаційний матеріал у вигляді слайдів _____

_____

_____

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання	02.09.2021	Виконано
2	Затвердження плану і завдання кваліфікаційної роботи	02.09.2021	Виконано
3	Аналіз джерел за тематикою роботи	17.09.2021-18.10.2021	Виконано
4	Аналіз наслідків та способів експлуатації загроз безпеки	19.10.2021-01.11.2021	Виконано
5	Аналіз можливостей використання різних методів біометричної автентифікації у веб-додатках	01.112.2021-30.11.2021	Виконано
6	Розробка веб-додатку з авторизацією за геометрією обличчя	01.12.2021-12.12.2021	Виконано
6	Здача на перевірку та підпис кваліфікаційної роботи керівнику	13.12.2021	Виконано
7	Проходження перевірки на плагіат та нормоконтроль кваліфікаційної роботи	15.12.2021	Виконано
8	Допуск завідувачем кафедри до захисту кваліфікаційної роботи	15.12.2021	Виконано
9	Захист кваліфікаційної роботи	17.12.2021	Виконано

Дата видачі завдання 08 листопада 2021 р.

Студент _____
(підпис)

Керівник роботи _____ _____доцент Олешко І.В.___
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка до атестаційної роботи магістра: 74 с., 20 рис., 2 таблиці, 21 джерела, 1 додатку.

БІОМЕТРИЧНА АВТЕНТИФІКАЦІЯ, ГЕОМЕТРІЯ ОБЛИЧЧЯ, МЕТОД БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ, ВЕБ ДОДАТОК, СЕРВЕР, АТАКИ НА ВЕБ ДОДАТКИ.

Об’єкт дослідження – біометрична автентифікація у веб-додатках.

Предмет дослідження – методи біометричної автентифікації для захисту веб-додатків.

Мета роботи – підвищити захист веб-додатків шляхом авторизації користувачів за допомогою біометричних особливостей людини, розробити веб-додаток з біометричною авторизацією.

Методи дослідження – аналіз літературних джерел щодо захищеності веб-додатків та методів біометричної автентифікації; методи тестування та обробки результатів експерименту.

На основні даних про вразливості веб-додатків запропонований аналіз можливості використання різних методів біометричної автентифікації користувачів з метою підвищення стійкості веб-додатків до можливих атак. Створені рекомендації щодо використання та зберігання біометричних даних користувачів, проаналізовані переваги та недоліки застосування біометрії у веб- додатках. Розроблений веб-додаток з авторизацією за біометричними характеристиками людини, а саме геометрією обличчя.

ABSTRACT

Explanatory note to the certification work of the master: 74 pages, 20 figures, 2 tables, 21 sources, 1 appendix.

BIOMETRIC AUTHENTICATION, FACE GEOMETRY, BIOMETRIC AUTHENTICATION METHOD, WEB APPLICATION, SERVER, ATTACKS ON WEB APPLICATIONS.

The object of research is biometric authentication in web applications.

The subject of research - methods of biometric authentication to protect web applications.

The purpose of the work is to increase the protection of web applications by authorizing users with the help of human biometric features, to develop a web application with biometric authorization.

Research methods - analysis of literature sources on the security of web applications and methods of biometric authentication; methods of testing and processing the results of the experiment.

Based on the basic data on web application vulnerabilities, an analysis of the possibility of using different methods of biometric authentication of users in order to increase the resilience of web applications to possible attacks is proposed. Recommendations for the use and storage of biometric data of users are created, the advantages and disadvantages of using biometrics in web applications are analyzed. Developed a web application with authorization for human biometric characteristics, namely facial geometry.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

CA - Certificate Authority

EDL - Enclave Definition Language

EER - Equal Error Rate

FRR - False Rejection Rate

HTML – Hypertext markup language

HTTP – Hypertext transfer protocol

OWASP - Open Web Application Security Project

LEM - Line Edge Map

SPA - Single page application

SQL - Structured Query Language

SVM - Support Vector Machine

TLS - Transport Layer Security

URL - Uniform Resource Locator

АЦСК – Акредитований центр сертифікації ключів

НСД - несанкціоновані дії

ВСТУП

На сьогоднішній день цінність інформації зростає разом з попитом на неї. Багато людей мають власні сторінки в соціальних мережах та публікують інформацію про себе тощо. Вони вкладають в цей процес вельми широкий смисл і можуть пояснити його, як правило, на інтуїтивному рівні.

Інформація надходить телефоном, комп'ютерними мережами, через радіо і телебачення, газети і журнали, зберігається у бібліотеках, архівах, базах даних тощо.

Будь-хто може дізнатися про іншу людину з її профілів в соціальних мережах. Така інформація вважається загальнодоступною та незахищеною. Технічна інформація напроти – повинна бути захищеною від НСД (несанкціонованих дій) та доступу людей, яким вона не призначена.

Існують такі види захисту інформації:

– Криптографічний — попереджує доступ доінформації за допомогою математичних перетворень повідомлення;

– Організаційний — попередження доступу на об'єкт інформаційної діяльності сторонніх осіб за допомогою організаційних заходів (правила розмежування доступу);

– Інженерний – попереджує руйнування носія внаслідок навмисних дій або природного впливу інженерно технічними засобами (сюди входять обмежуючі конструкції);

– Технічний – забезпечує обмеження доступу до носія повідомлення апаратно-технічними засобами (антивіруси, брандмауери, маршрутизатори, токени, смарт-карти тощо).

До технічних також відносяться й паролі – унікальні послідовності символів, які знає тільки власник носія інформації або ресурсу даних. Але паролі не дуже надійні, бо їх можливо скомпрометувати, забути, бо для захисту багатьох своїх ресурсів даних потрібно використовувати різні паролі, щоб

зловмисник не отримав доступ до всіх, якщо отримає пароль. На заміну складним паролям прийшла біометрія.

В запропонованій кваліфікаційній роботі проаналізована можливість підвищення захисту веб-додатків шляхом авторизації користувачів за допомогою біометричних особливостей людини.

У першому розділі буде розглянуто, як працюють веб-додатки. Розглянемо архітектуру клієнт-сервер — це обчислювальна модель, в якій сервер розміщує, доставляє та керує більшістю ресурсів і послуг, які споживає клієнт.

Буде розглянуто роботу HTTP та його недоліки перед захищеним HTTPS. Атаки на веб-додатки та методи захисту від найпоширеніших атак. Як за допомогою сертифікату запобігти витоку інформації до зловмисника.

У розділі 2 розглянуті біометричні методи автентифікації, зроблений висновок, та поради щодо використання біометричних характеристик людини у веб-додатках.

У 3 розділі буде розглянуто, як захистити веб-додаток за допомогою біометричних даних людини. Детально розглянутий метод біометричної автентифікації за геометрією обличчя.

Розпізнавання обличчя має перевагу бути пасивною, ненав'язливою системою, яка перевіряє особистість. Загалом, біометричні пристрої можна визначити за допомогою трьох етапної процедури:

1. Коли датчик проводить спостереження. Тип датчика і його спостереження залежать від типу біометричного використовувані пристрої

2. Комп'ютерний алгоритм «нормалізує» біометричну сигнатуру, щоб він був у тому самому форматі як сигнатура в базі даних системи.

3. Система порівнює нормалізовану сигнатуру з набором нормалізованих підписів у базі даних системи і надає «оцінку подібності», яка порівнює індивідуальну нормовану сигнатуру.

Будуть розглянуті недоліки біометричної автентифікації саме для веб-додатків та надані поради, щодо використання біометрії у веб додатку, наприклад, для біометричної авторизації використовується нечіткий пошук, який

буде розглянуто в главі 3.2. Це такий пошук, при якому ми шукаємо елементи, що не повністю збігаються, а сутності найбільш схожі одна на одну.

В 4-му розділі представлений веб-додаток, який побудовано для демонстрації підвищення надійності автентифікації за рахунок додавання двофакторної автентифікації.

1 ВЕБ ДОДАТКИ

1.1 Як працюють веб технології

Веб-додатки можна розділити на кілька типів, залежно від різних поєднань його основних складових:

– Backend (бекенд або серверна частина програми) працює на віддаленому комп'ютері, який може знаходитися будь-де. Вона може бути написана різними мовами програмування: PHP, Python, Ruby, C# та інші. Якщо створювати програму використовуючи лише серверну частину, то в результаті будь-яких переходів між розділами, відправок форм, оновлення даних, сервером буде генеруватися новий HTML-файл і сторінка в браузері перезавантажуватиметься;

– Frontend (фронтенд або клієнтська частина програми) виконується у браузері користувача. Ця частина написана мовою програмування Javascript. Програма може складатися тільки з клієнтської частини, якщо не потрібно зберігати дані користувача довше за одну сесію. Це можуть бути, наприклад, фоторедактори чи прості іграшки.

– Single page application (SPA або односторінковий додаток). Цікавіший варіант, коли використовуються і бекенд і фронтенд. За допомогою їх взаємодії можна створити програму, яка працюватиме зовсім без перезавантаження сторінки в браузері. Або у спрощеному варіанті, коли переходи між розділами викликають перезавантаження, але будь-які дії розділу обходяться без них [1].

Архітектура клієнт-сервер — це обчислювальна модель, в якій сервер розміщує, доставляє та керує більшістю ресурсів і послуг, які споживає клієнт. Цей тип архітектури має один або кілька клієнтських комп’ютерів, під’єднаних до центрального сервера через мережу або підключення до Інтернету. Архітектура клієнт-сервер також відома як модель мережевих обчислень або

мережа клієнт-сервер, оскільки всі запити та послуги доставляються через мережу На рисунку 1.1 показана клієнт-серверна архітектура.

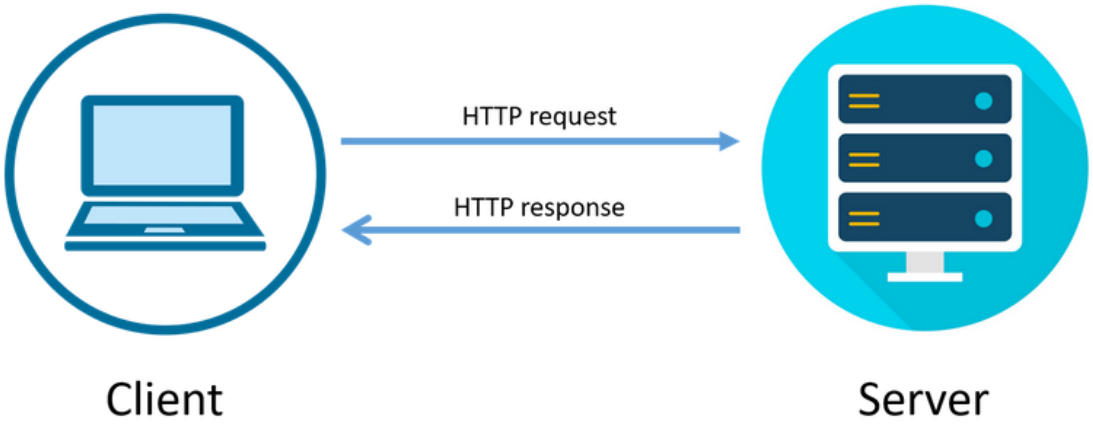

Рисунок 1.1 – Клієнт-серверна архітектура

HTTP — це клієнт-серверний протокол, для якого є запити відправляються якою-то однією стороною — учасником обміну (користувачем). Частіше за все в якості учасника виступає веб-браузер. Кожен запит повертається серверу, який обробляє його і повертає відповідь. Між цими запитами і відповідями, як правило, існують багаточисельні посередники, які називаються проксі, які виконують різні операції і працюють як шлюзи або кеш, наприклад.

Зазвичай між браузером і сервером набагато більше різних пристроїв-посередників, які відтворюють будь-яку роль в роботі запиту: маршрутизатори, модеми і так далі. Завдяки тому, що мережа побудована на основі системи рівнів взаємодії, ці посередники знаходяться на мережевому та транспортному рівнях. На цій системі рівня HTTP займає самий верхній рівень, який називається прикладним. Знання про рівні мережі, такі як представницький, сеансовий, транспортний, мережевий, канальний та фізичний, мають важливе значення для пошуку роботи мережі та діагностики можливих проблем [2].

Рисунок 1.2 – Модель TCP/IP та OSI

HTTP/1.0 відкриває TCP-з'єднання для кожного обміну запитом/відповіддю, має два важливих недоліки: відкриття з'єднання вимагає кількох обмінів повідомленнями, і тому повільно, хоча стає більш ефективним при відправленні кількох повідомлень, або при регулярному відправленні повідомлення.

Для вирішення цих недоліків HTTP/1.1 забезпечив конвеєрну обробку і стійкі з’єднання, що розташоване в основі TCP з’єднання можна частково контролювати через заголовок Connection, що зображено на рисунку 1.3. HTTP/2 зробив наступний крок, додавши мультиплексування повідомлень через просто з'єднання, допомагаючи тримати з'єднання відкритими і більш ефективним.

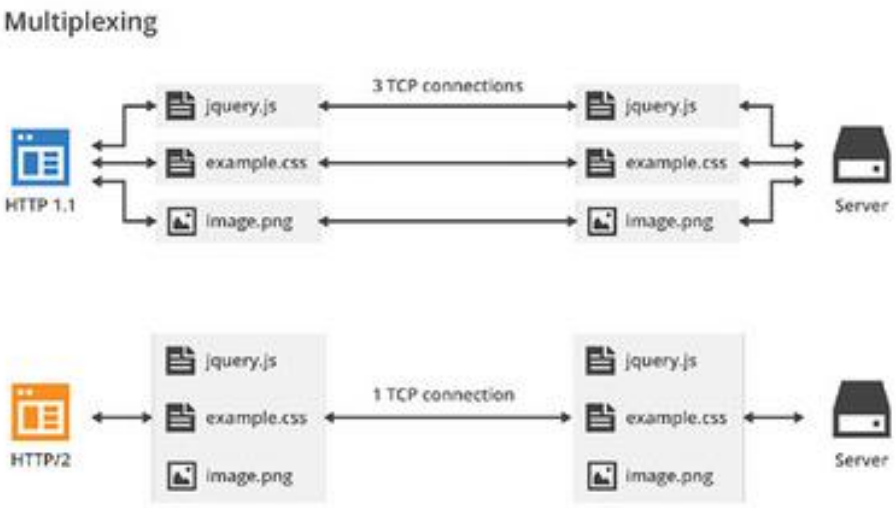

Рисунок 1.3 – Різниця з’єднання між HTTP 1.1 та HTTP 2

Нижче включені загальні функції, керовані за допомогою HTTP:

– Кеш. Сервер може інструктувати проксі та клієнти, вказуючи, що і як довго гешувати. Користувач може інструктувати проксі проміжного кешу і ігнорувати сховані документи.

– Ослаблення обмеженого джерела. Для попередження порушень приватності вторгнень веб-браузер забезпечує суворе розділення між веб-сайтами. Тільки сторінки з цього джерела можуть отримати доступ до інформації на веб-сторінці. Хоча такі обмеження дають більше навантаження на сервер, заголовки HTTP можуть послабити суворе розділення стороннього сервера, дозволяючи документу стати частиною інформації з різних доменів.

– Автентифікація. Деякі сторінки доступні лише спеціальним користувачам. Базова аутентифікація може надаватися через HTTP, або через використання заголовка WWW-Authenticate (en-US) і подібних йому, або за допомогою спецсесії, використовуючи куки.

– Проксі і тунелювання. Сервери або клієнти часто знаходяться в Інтернеті і скривають свої істинні IP-адреси від інших. HTTP-запити проходять через проксі для уникнення цього мережевого бар'єру

– Сесія. Використання HTTP-кука дозволяє зв'язати запит із станом сервера. Це створює сесію, хоча ядро HTTP — протокол без стану.

HTTP/1.1 і раніше HTTP повідомлення були зрозумілі для читання людині. У версії HTTP/2 ці повідомлення вбудовані в нову бінарну структуру, кадр, що дозволяє оптимізації, такі як компресія заголовків та мультиплексування.

Навіть якщо частину оригінального повідомлення HTTP надіслано в цій версії HTTP, семантика кожного повідомлення не змінюється і клієнт відтворює (віртуально) оригінальний HTTP-запит [2].

Запити містять такі елементи:

– HTTP-метод, зазвичай дієслово подібно до GET, POST або іменник, як OPTIONS або HEAD, що визначає операцію, яку клієнт хоче виконати. Зазвичай клієнт хоче отримати ресурс (використовуючи GET) або передати значення HTML-форми (використовуючи POST), хоча інші операції можуть бути необхідні в інших випадках;

– Шлях до ресурсу: URL ресурси позбавлені елементів, які є очевидними з контексту, наприклад без protocol (http://), domain (developer.mozilla.org), або TCP port (80);

– Версію HTTP-протоколу;

– Заголовки, які надають додаткову інформацію для сервера, або тіло для деяких методів, таких як POST, що містить відправлений ресурс.

Відповіді містять такі елементи:

– Версію HTTP-протоколу;

– HTTP код стану, що повідомляє про успішність запиту або причину невдачі;

– Повідомлення стану — короткий опис коду стану;

– HTTP заголовки, подібно до заголовків у запитах;

– Тіло, що містить ресурс, що пересилається.

1.2 Атаки на веб додатки

1. Ін'єкції. Усі дані, зазвичай, зберігаються у спеціальних базах, звернення до яких будуються як запитів, найчастіше написаних спеціальною мовою запитів SQL (Structured Query Language – структурований мову запитів). Програми використовують SQL-запити для того, щоб отримувати, додавати, змінювати або видаляти дані, наприклад, під час редагування користувачем своїх особистих даних або заповнення анкети на сайті. При недостатній перевірці даних від користувача, зловмисник може впровадити у форму Web-інтерфейсу програми спеціальний код, що містить шматок SQL-запиту. Приклад виконання такої ін’єкції можна побачити на Рисунку 1.4, де за допомогою утиліти Burpsuite був доданий '+UNION+SELECT+username, +password+FROM+users — такий рядок для того, щоб отримати дані користувачів.

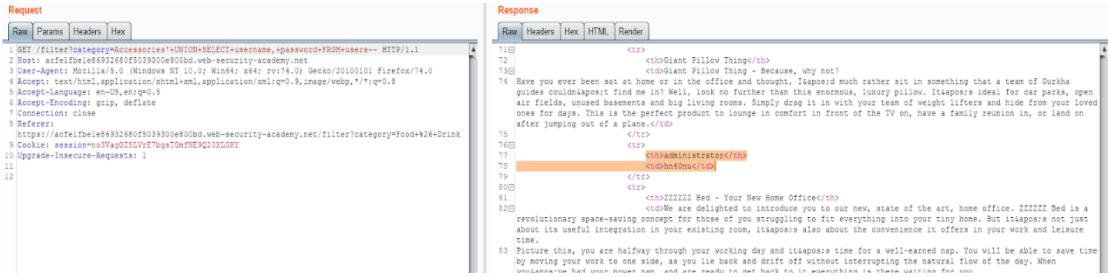

Рисунок 1.4 – Приклад виконання ін’єкції

Це найнебезпечніша вразливість, що дозволяє зловмиснику отримати доступ до бази даних та можливість читати/змінювати/видаляти інформацію, яка для нього не призначена [3].

2. Недоліки системи аутентифікації та зберігання сесій (Broken Authentication and Session Management) Для того, щоб відрізняти одного користувача від іншого, web-додаток використовує так звані сесійні куки. Після того, як ви ввели логін і пароль та програму вас авторизувало, у сховищі браузера зберігається спеціальний ідентифікатор, який браузер надалі пред'являє

серверу при кожному запиті сторінки вашого web-додатку. Саме так web-додаток розуміє, що ви це саме ви [3].

3. Міжсайтовий скриптинг - XSS (Cross Site Scripting) Міжсайтовий скриптинг – ще одна помилка валідації даних користувача, яка дозволяє передати JavaScript код на виконання в браузер користувача. Атаки такого роду часто називають HTML-ін'єкціями, адже механізм їх впровадження дуже схожий з SQL-ін'єкціями, але на відміну від останніх, впроваджуваний код виконується в браузері користувача.

По-перше, зловмисник може вкрасти вашу сесійну cookie. По-друге, можуть бути викрадені дані, що вводяться у форми на зараженій сторінці. По-третє, через JavaScript можна змінювати дані на сторінці, наприклад, там можуть бути реквізити для банківського переказу, які зловмисник із задоволенням підробить і замінить підставними [3]. Приклад виконання такої атаки можно побачити на Рисунку 1.5, де в поле вводу був доданий такий рядок: <script>alert(1)</script>.

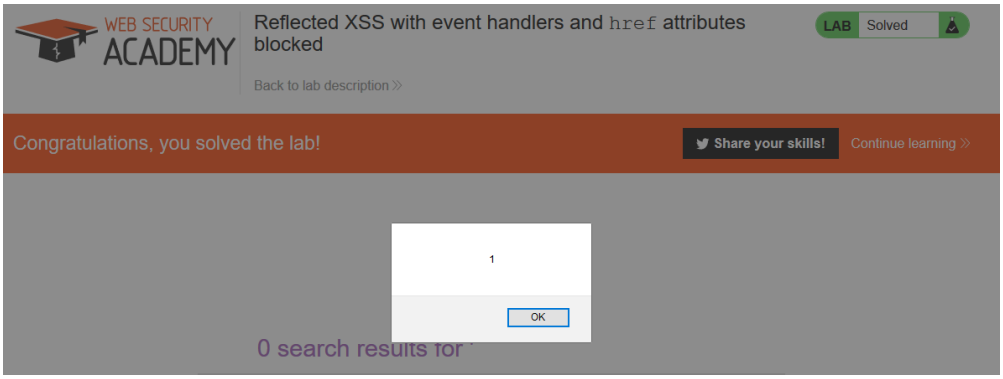

Рисунок 1.5 – Приклад виконання XSS атаки

4. Небезпечна конфігурація (Security Misconfiguration) Безпека Web-програми вимагає наявності безпечної конфігурації всіх компонентів інфраструктури: компонентів програми (таких як фреймворки – frameworks), веб-сервера, сервера баз даних та самої платформи.

Налаштування компонентів сервера зазвичай небезпечні і відкривають можливості до атак. Наприклад, крадіжка сесійної cookie через JavaScript при XSS-атаці стає можлива завдяки вимкненому за замовчуванням налаштуванню cookie_http only. При правильному налаштуванні сервера та увімкненому опції cookie_httponly, отримати сесійну cookie через JavaScript неможливо, але найчастіше це просте і важливе налаштування не було в таких критично важливих місцях, як особисті кабінети платіжних систем [3].

5. Незахищеність критичних даних (Sensitive Data Exposure) Багато веб-програм не захищають конфіденційні дані, такі як кредитні картки та облікові дані для автентифікації. Зловмисники можуть вкрасти або модифікувати такі слабко захищені дані для використання у своїх корисливих цілях. Найпростіший приклад – передача даних за протоколом HTTP.

Справа в тому, що дані, що передаються за протоколом HTTP, ніяк не шифруються, а при проходженні даних від комп'ютера користувача до Web-сервера, дані пройдуть досить багато різних вузлів: маршрутизатор офісу або домашній роутер, маршрутизатор провайдера, маршрутизатор на каналі, маршрутизатор в дата- центр хостинг-провайдера сервера і так далі. На кожному з цих вузлів може зачаїтися зловред, так званий сніффер, програма, яка зчитує весь трафік і передає зловмиснику [3].

6. Міжсайтова підробка запиту (Cross-Site Request Forgery, CSRF/XSRF) Вектор атаки CSRF, також відомий як XSRF, дозволяє зловмиснику виконувати від імені жертви дії на сервері, де не реалізовано додаткових перевірок [3].

1.3 Захист веб-додатків

Коли браузер робить запит до будь-якого веб-сайту, цей запит повинен пройти через безліч різних мереж, будь-яка з яких може бути потенційно використана для прослуховування або втручання у встановлене з'єднання. З вашого власного комп'ютера на інші комп'ютери вашої локальної мережі, через

роутери та хаби, через вашого провайдера та через безліч інших проміжних провайдерів – безліч організацій ретранслює ваші дані.

Якщо зловмисник виявиться хоча б в одній із них, він має можливість подивитися, які дані передаються. Як правило, запити передаються за допомогою звичайного HTTP, в якому запит клієнта, і відповідь сервера передаються у відкритому вигляді. І є безліч вагомих аргументів, чому HTTP не використовує стандартне шифрування: для цього потрібно більше обчислювальних потужностей, передається більше даних, не можна використовувати кешування Але в деяких випадках, коли по каналу зв'язку передається виключно важлива інформація (така як паролі або дані кредитних карток), необхідно забезпечити додаткові заходи, що запобігають прослуховування таких з'єднань. Transport Layer Security (TLS).

Отже, криптографія дозволяє захистити з'єднання від потенційних зловмисників, які хочуть впливати на з'єднання або просто прослуховувати його. TLS — спадкоємець SSL — це протокол, який найчастіше використовується для забезпечення безпечного HTTP з'єднання (так званого HTTPS). TLS розташований на рівні нижче протоколу HTTP моделі OSI. Для більш детального пояснення, це означає, що в процесі виконання запиту спочатку відбувається все , що пов'язане з TLS-з'єднанням і вже потім, що пов'язано з HTTP-з'єднанням. TLS – гібридна криптографічна система. Це означає, що вона використовує кілька криптографічних підходів.

Наприклад:

1)Асиметричне шифрування (криптосистема з відкритим ключем) для генерації загального секретного ключа та автентифікації (тобто посвідчення в тому, що ви – той, за кого себе видаєте).

2) Симетричне шифрування, що використовує секретний ключ для подальшого шифрування запитів та відповідей.

Криптосистема з відкритим ключем – це різновид криптографічної системи, коли кожна сторона має і відкритий, і закритий ключ, математично пов'язані між собою. Відкритий ключ використовується для шифрування тексту

повідомлення, тоді як закритий ключ використовується для дешифрування та отримання вихідного тексту. З того часу, як повідомлення було зашифровано за допомогою відкритого ключа, воно може бути розшифроване лише відповідним закритим ключем. Жоден із ключів не може виконувати обидві функції.

Відкритий ключ публікується у відкритому доступі без ризику розкриття загального секрету, але закритий ключ не повинен потрапити до будь-кого, який не має прав на дешифрування даних.

Одним з найбільш вражаючих переваг асиметричного шифрування є те, що дві сторони, які раніше зовсім не знають один одного, можуть встановити захищене з'єднання, спочатку обмінюючись даними по відкритому, незахищеному з'єднанню. Клієнт і сервер використовують власні закриті ключі і опублікований відкритий ключ для створення спільного секретного ключа на сесію. Це означає, що якщо хтось знаходиться між клієнтом та сервером і спостерігає за з'єднанням – він все одно не зможе дізнатися ні закритий ключ клієнта, ні закритий ключ сервера, ні секретний ключ сесії.

Цифровий сертифікат – електронний документ, що містить відкритий ключ, інформацію про власника ключа, область застосування ключа, підписаний акредитованим центром сертифікації ключів, що його видав, і що підтверджує належність відкритого ключа власнику.

Цифровий підпис на сертифікаті означає, що хтось засвідчує той факт, що цей відкритий ключ належить певній особі чи організації. Насправді сертифікати пов'язують доменні імена з певним публічним ключем. Це запобігає можливості того, що зловмисник надасть свій публічний ключ, видаючи себе за сервер, до якого звертається клієнт.

Щоб сертифікату довіряв будь-який веб-браузер, він має бути підписаний акредитованим центром сертифікації (центром сертифікації, Certificate Authority, CA). CA – це компанії, які виконують ручну перевірку, що особа, яка намагається отримати сертифікат, задовольняє наступним двом умовам:

– є реально існуючим;
– має доступ до домену, сертифікат якого він намагається отримати.

Сертифікати зазвичай використовуються для обміну зашифрованими даними у великих мережах. Криптосистема з відкритим ключем вирішує проблему обміну секретними ключами між учасниками безпечного обміну, однак не вирішує проблему довіри до відкритих ключів. Припустимо, що Аліса, бажаючи отримувати зашифровані повідомлення, генерує кілька ключів, один з яких (відкритий) вона публікує будь-яким чином.

Будь-хто, хто бажає надіслати їй конфіденційне повідомлення, має можливість зашифрувати його цим ключем, і бути впевненим, що тільки вона (оскільки вона має відповідний секретний ключ) зможе це повідомлення прочитати. Однак описана схема нічим не може завадити зловмисникові Еві створити пару ключів і опублікувати свій відкритий ключ, видавши його за ключ Аліси. У такому разі Ева зможе розшифровувати і читати принаймні ту частину повідомлень, призначених Алісі, які були помилково зашифровані його відкритим ключем.

Ідея сертифікату — це наявність третьої сторони, якій довіряють дві інші сторони інформаційного обміну. Передбачається, що таких третіх сторін небагато, і їх відкриті ключі всім відомі у будь-який спосіб, наприклад, зберігаються в операційній системі або публікуються в журналах. Таким чином, підроблення відкритого ключа третьої сторони легко виявляється [4].

Сертифікат відкритого ключа видається центром сертифікації та складається з таких полів як: сам відкритий ключ власника сертифіката, термін дії, ім'я емітента (центру сертифікації), ім'я власника сертифіката і, найважливішої частини, цифровий підпис.

Цифровий підпис гарантує неможливість підробки сертифіката. Вона є результатом криптографічної хеш-функції даних сертифіката, зашифрованим закритим ключем центру сертифікації. Відкритий ключ центру сертифікації є загальновідомим, тому будь-який може розшифрувати ним цифровий підпис сертифіката, потім обчислити хеш самостійно і порівняти, чи хеші збігаються. Якщо хеші збігаються — значить дійсний сертифікат і можна не сумніватися,

що відкритий ключ належить саме тому, з ким ми збираємося встановлювати з'єднання [4].

Як тільки CA засвідчується в тому, що заявник є реальним і він реально контролює домен, CA підписує сертифікат для цього сайту, по суті, встановлюючи штамп підтвердження на тому факті, що публічний ключ сайту дійсно належить йому і йому можна довіряти. У кожен браузер вже спочатку завантажено список акредитованих CA. Інакше кожен міг би підписувати фіктивні сертифікати.

Так що навіть якщо хакер узяв відкритий ключ свого сервера і згенерував цифровий сертифікат, що підтверджує, що цей публічний ключ, асоційований з сайтом facebook.com, браузер не повірить у це, оскільки сертифікат не підписаний акредитованим CA.

Інші речі, які потрібно знати про сертифікати - це розширена валідація. На додаток до звичайних сертифікатів X.509, існують Extended validation сертифікати, що забезпечують більш високий рівень довіри. Видаючи такий сертифікат, CA здійснює ще більше перевірок щодо особи, яка отримує сертифікат (зазвичай використовуючи паспортні дані або рахунки). При отриманні такого сертифіката, браузер відображає в адресному рядку зелену плашку, крім звичайної іконки із замочком.

Оскільки обмін даними за протоколом TLS відбувається ще до початку HTTP з'єднання, можуть виникати проблеми у випадку, якщо кілька веб-сайтів розташовані на тому самому веб-сервері, за тією ж IP-адресою. Роутінг віртуальних хостів здійснюється веб-сервером, але TLS з'єднання виникає ще раніше. Єдиний сертифікат на весь сервер буде використовуватися при запиті до будь-якого сайту, розташованого на сервері, що може викликати проблеми на серверах з безліччю хостів. Якщо власник веб сайту користується послугами веб-хостингу, то швидше за все йому потрібно придбати виділену IP-адресу, щоб він мав можливість використовувати у себе HTTPS. А якщо ні, то власнику доведеться постійно отримувати нові сертифікати (і верифікувати їх) при кожному оновленні сайту.

1.4 Модель порушника та модель загроз для веб-додатків

Модель порушника представляє собою опис можливих дій порушника, який складається на основі аналізу типу зловмисника, рівня його повноважень, знань, теоретичних та практичних можливостей. Порушників прийнято поділяти на зовнішніх і внутрішніх. До внутрішніх належать співробітники, користувачі інформаційної системи, які можуть наносити шкоду інформаційним ресурсам як ненавмисно, так і навмисно; технічний персонал, який обслуговує будівлі і приміщення; персонал, який обслуговує технічні засоби. Зовнішні порушники - це сторонні особи, які знаходяться поза контрольованою зоною організації або не авторизовані особи.

Для веб-додатку порушники можуть бути тільки зовнішні, які за допомогою додатків, що прослухують мережу, перехоплюють запити клієнта та відповіді сервера можуть отримати доступ до будь-якої інформації користувача веб додатком, тощо.

Порушник, скориставшись атаками, які описані в розділі 1.2, або іншими вразливостями веб-додатків та незахищеною мережею передачі даних, може отримати дані власника, які в такому випадку призведуть до втрати грошей, отримання персонального ключу доступу та біометричних даних, які відсилаються для автентифікації. Таким чином порушник має змогу отримати дані автентифікації іншого користувача та видавати себе за нього в своїх цілях. Таким способом зловмисник може перевести собі гроші іншої людини.

Модель загроз представляє собою можливі атаки або помилкові дії направлені на канал передачі інформації, або сам веб додаток та дані що отримає порушник. За допомогою соціальної інженерії можна отримати конфіденційні дані. За допомогою крадіжки можна отримати логіни та паролі аккаунтів пошти, соцмереж, номери мобільних телефонів, дані банківських карт.

Отже можна підвести висновки щодо розділу. Веб технології розвиваються дуже стрімко та мають доволі гарний захист. Як було сказано вище пакети у мережі захищаються за допомогою шифрування даних. Шифрування

забезпечується за рахунок HTTPS з’єднання та використанню TLS та сертифікатів. Сертифікати видані АЦСК – акредитованим центром, який перевіряє дані власника сертифікату та може гарантувати, що сертифікат дійсний. Тому клієнту веб додатку можна не хвилюватися за свої дані, бо вони відправляються мережею у захищеному вигляді та тільки сервер до якого йде запит може розшифрувати дані. У наступному розділі буде розглянуті біометричні методи автентифікації, та їх застосування у веб-додатках.

2 БІОМЕТРІЯ В ВЕБ ДОДАТКАХ

2.1 Загальні відомості про біометрію

З появою стандартів для оцінки ефективності роботи біометричних систем, створених в National Institute of Standards and Technology Standards розробка систем дуже змінилася. Приклади таких стандартів:

– ISO/IEC 19989-2:2020 –Criteria and methodology for security evaluation of biometric systems;

– ISO/IEC 19792:2009 –specifies the subjects to be addressed during a security evaluation of a biometric system;

– ISO/IEC 15408-3:2008 –Security techniques –Evaluation criteria for IT security.

Оскільки для таких систем перевірка ефективності повинна виконуватися на великій кількості тестових зображень, то до алгоритмів, які виконують порівняння біометричних характеристик висунуто такі вимоги:

– робастність – стійкість до викривлень зображень;

– точність – збереження структури інформації, що знаходиться в зображеннях;

– обчислювальна реалізація алгоритмів для роботи в реальному часі.

Структура системи повинна враховувати обсяг та структуру бази даних зображень, сценарій вирішуваної задачі, часові обмеження та фізичну реалізованість.

Задоволення даних вимог дозволить забезпечити вирішення прикладної задачі обробки зображень; адаптацію системи до постійно змінюваних умов отримання вихідних зображень; необхідну пропускну здатність системи; безвідмовну роботу системи в заданому режимі; простоту експлуатації і супроводу системи [5].

Ефективність біометричних систем обробки зображення визначається використовуваними в ній методами та моделями представлення зображення, алгоритмами реалізації, структурою даних та обчислювальною технікою.

Після того як система спроектована, перед розробниками постає завдання її тестування для отримання кількісних характеристик, зокрема, визначення швидкості роботи та ймовірності появи помилок. Для оцінки якості роботи алгоритму порівняння відбитків пальців існують характеристики, за якими легко можна отримати кількісні показники, що визначають надійність систем.

Ці характеристики супроводжуються наявністю помилок першого і другого роду. Помилка першого роду з'являється при порівнянні "свій" до "свого", коли "свій" визнається системою "чужим". Позначається як FRR (False Rejection Rate) - ймовірність помилки першого роду, тобто ймовірність відмови "своєму". При цьому існує і зворотня характеристика помилки першого роду: GAR (Genuine Acceptance Rate) = 1 - FRR, ймовірність пропуску "свого". Помилка другого роду з'являється при порівнянні "чужий" до "чужого", коли "чужий" визнається "своїм". Позначається як FAR (False Acceptance Rate) - ймовірність помилки другого роду, тобто ймовірність пропуску "чужого". Для комплексної оцінки алгоритму існує параметр EER (Equal Error Rate) - рівень помилок біометричної системи доступу, при якому FAR і FRR рівні [6].

Біометричну ідентифікацію часто називають чистою або реальною автентифікацією, тому що використовується не віртуальна, а біометрична ознака (ідентифікатор), що реально має відношення до людини. Специфічною особливістю біометричної ідентифікації буде великий розмір біометричної бази даних: кожен із біометричних зразків має бути зіставлений з усіма наявними записами в базі даних (порівняння 1:N або «один до багатьох»). Для використання в реальному житті така система потребує високої швидкості зіставлення біометричних ознак. Приклад: звичайний веб сайт, яким користуються кожен день має велику кількість користувачів, від кількох сотень до кількох тисяч осіб.

Візьмемо для прикладу кількість 10 000 чоловік. Значить розмір бази даних (виходимо, що для однієї людини використовується один відбиток пальця) становитиме 10 000 відбитків пальців. При прикладанні пальця до зчитувача відбитків система вироблятиме зіставлення 1:10 0000. Що дуже небагато для сучасних систем. Саме тому всі системи контролю доступу чи обліку робочого дня працюють у режимі біометричної ідентифікації. З іншого боку полюса — верифікаційні системи, вони роблять зазвичай лише одне зіставлень як 1:1. Тобто пред'явлена біометрична ознака порівнюється з однією біометричною ознакою з бази даних. Тобто система відповідає на запитання, чи ти за кого себе видаєш.

Автентифікація – процедура перевірки належності суб'єкту доступу пред'явленого ним ідентифікатора. Простий приклад автентифікації - підтвердження особи користувача шляхом порівняння введеного ним логіну з паролем у базі даних, ідентифікованих раніше користувачів.

У цьому прикладі аутентифікацією є процес порівняння паролів, і наступне або надання доступу або відмова, а ідентифікатором буде саме логін. Способи автентифікації можуть бути згруповані в три основні категорії, засновані на так званих факторах автентифікації: те, що людина знає, що користувач володіє або щось таке, що є ознакою людини [6].

У біометрії розрізняють два автентифікаційні методи: верифікація, заснована на біометричному параметрі та на унікальному ідентифікаторі, який виділяє конкретну людину, тобто цей метод заснований на комбінації автентифікаційних прийомів. Ідентифікація, на відміну від верифікації, заснована лише на біометричних вимірах. При цьому виміряні параметри порівнюються з усіма записами з бази зареєстрованих користувачів, а не з одним із них, вибраним на підставі якогось ідентифікатора.

Кожен чинник аутентифікації охоплює ряд елементів, що використовуються для автентифікації чи перевірки особи до надання доступу, затвердження запиту транзакції, підписання документа, надання повноважень іншим тощо. Фактори знання - це те, що користувач знає і пам'ятає, наприклад,

пароль, PIN-код, відповідь на секретне питання. Фактори ознаки - це те, що є частиною нас, наприклад, відбиток пальця, підпис, голос. Фактори володіння - це те, що користувач має, наприклад, безконтактну ідентифікаційну карту, стільниковий телефон, фізичний ключ.

При порівнянні біометричної автентифікації з іншими видами автентифікації необхідно звернути увагу на їх сильні та слабкі сторони. Автентифікація на основі факторів знання, наприклад, використання пароля або графічного ключа. Використання пароля технічно просто реалізується як у програмному забезпеченні, так і в будь-яких спеціалізованих пристроях. Але з такою ж легкістю пароль може бути скомпрометований наприклад шпигунської програми або комп'ютерним вірусом, які можуть бути завантажені на пристрої користувача з інтернету [6].

2.2 Біометрична автентифікація за геометрією обличчя

Розпізнавання обличчя має перевагу бути пасивною, ненав'язливою системою, яка перевіряє особистість. Загалом, біометричні пристрої можна визначити за допомогою трьох етапної процедури:

1. Коли датчик проводить спостереження. Тип датчика і його спостереження залежать від типу біометричного використовувані пристрої. Це спостереження дає біометричну сигнатуру фізичної особи [10].

2. Комп'ютерний алгоритм «нормалізує» біометричну сигнатуру, щоб він був у тому самому форматі (розмір, роздільна здатність, вид тощо) як сигнатуру в базі даних системи. Нормалізація біометричних даних сигнатури дає нам «нормалізовану сигнатуру» особи [10].

3. Система порівнює нормалізовану сигнатуру з набором нормалізованих підписів у базі даних системи і надає «оцінку подібності», яка порівнює індивідуальну нормовану сигнатуру [10].

Розпізнавання обличчя починається з виявлення візерунків обличчя іноді захаращені сцени, протікає шляхом нормалізації обличчя зображення для

врахування геометричних змін і зміни освітлення, можливо, використовуючи інформацію про місце розташування та зовнішній вигляд орієнтирів обличчя, ідентифікує обличчя за допомогою відповідних алгоритмів класифікації та постобробки результатів за допомогою схеми на основі моделі та логістичний зворотний зв'язок [3]. Застосування техніки розпізнавання обличчя може бути поділяються на дві основні частини: застосування правоохоронних органів і комерційне застосування. На рисунку 2.1 зображена схема розпізнавання обличчя.

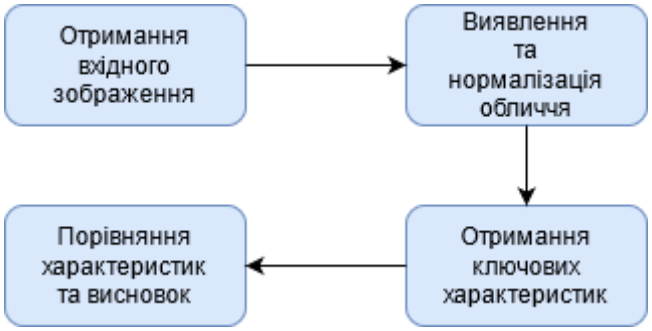

Рисунок 2.1 - Схема розпізнання зображень обличчя

Усі алгоритми розпізнавання обличь узгоджуються з двома основними частини: (1) виявлення та нормалізація обличчя та (2) ідентифікація обличчя. Алгоритми, які складаються з обох частин називають повністю автоматичними алгоритмами і тими, які складаються з лише другої частини називаються частково автоматичними алгоритми.

Частково автоматичним алгоритмам дається обличчя зображення і координати центру очей. Повністю автоматичним алгоритмам надаються лише зображення обличчя. З іншого боку, розвиток розпізнавання обличь за останні роки дозволяє організації поділити на три типи алгоритми розпізнавання, а саме фронтальне та профільне розпізнавання, залежно від типу зображень та алгоритми розпізнавання.

Профільні схеми дуже практичні як для швидкої та грубої обробки попередній пошук у великій базі даних обличчя, щоб зменшити обчислювальне

навантаження для подальшого складного алгоритму, або як частина гібридної схеми розпізнавання. Такий гібридний підхід має особливий статус систем розпізнавання обличь, оскільки вони поєднують різні підходи до розпізнавання для подолання недоліку з окремих компонентів. Ці моделі фіксують інформацію про клас і надають надійну інформацію обмеження при роботі зі зміною зовнішнього вигляду.

Методи узгодження геометричних об’єктів. Засновані на обчислення набору геометричних об’єктів з малюнка обличчя. Справа в тому, що розпізнавання обличчя можливо навіть при грубій роздільній здатності до 8x6 пікселів [11], коли одиночні риси обличчя майже не розкриваються в деталях, має на увазі, що загальний геометричний контур риси обличчя є достатньо для визначення. Загальна конфігурація може бути описана вектором, що представляє положення та розмір основних рис обличчя, такі як очі та брови, ніс, рот, і форму контуру обличчя.

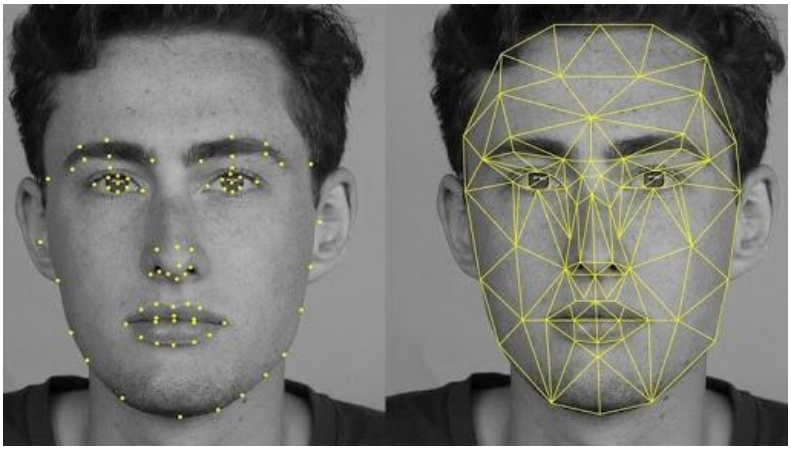

Рисунок 2.2 – ображення геометрії обличчя

У роботі [12] використано декомпозицію Габора для виявлення характерних точок для кожного зображення обличчя, що значно зменшило вимоги до зберігання бази даних. Як правило, на кожне обличчя було 35-45 ознак згенеровано. У процесі зіставлення використовувалася інформація представлений у топологічному графічному зображенні об’єкта точки. Після компенсації

різного розташування центроїдів два значення вартості, топологічна вартість і вартість подібності, були оцінено. Точність розпізнавання з точки зору найкращого збігу до правильної людини було 86% і 94% від правильної людини.

Підсумовуючи, на основі відповідності геометричних об’єктів точно виміряні відстані між об’єктами можуть бути найбільшими корисно для пошуку можливих збігів у великій базі даних. Однак це буде залежати від точність алгоритмів розташування об’єктів. Даний автоматизований алгоритм розташування ознак обличчя не забезпечує високий ступінь точність і вимагає значного обчислювального часу.

Зіставлення графіків. Це ще один підхід до розпізнавання обличчя. У статті [12] представлена динамічна структура зв'язку для спотворення інваріантного розпізнавання об'єкта, який використовується еластичним зіставлення графіка, щоб знайти найближчий збережений графік. Динамічне посилання архітектури є розширенням класичної штучної нейронної системи мереж.

Об’єкти, що запам’ятовуються, зображуються розрідженими графи, вершини яких позначені роздільністю ребер з точки зору локального спектру потужності, такі ребра позначаються геометричними векторами відстані. Об'єкт розпізнавання можна сформулювати як еластичний графік, що відповідає якому виконується шляхом стохастичної оптимізації відповідної вартості функції.

Загалом, архітектура динамічного посилання є кращою до інших методів розпізнавання обличь з точки зору обертання інваріантність; однак процес узгодження є дуже затратним при обчисленні та порівнянні зображень.

Інформація про контур. Це корисна функція представлення об’єктів які до певної міри нечутливі до змін освітлення. Хоча карта контурів широко використовується в різних візерунках поля розпізнавання, наприклад відбитків пальців. Зображення контурів об’єктів можна використовувати для розпізнавання об’єктів і для досягнення такої ж точності, як і зображення сірого кольору.

Процес розпізнавання обличчя може початися у набагато більш ранні етапи до отримання зображення контуру, який можна використовувати для розпізнавання обличь без залучення високого рівня когнітивної функції. Підхід до лінії контурів, запропонований [10], витяги лінії з карти контурів граней як особливості. Такий підхід може бути розглядається як комбінація відповідності шаблону і відповідність геометричних об’єктів Приклад зазначений на рисунку 2.1.

Підхід (Line Edge Map) LEM не тільки володіє перевагами підходів на основі функцій, таких як незмінність до освітлення та низькі вимоги до пам'яті, але також має перевагу високої продуктивності розпізнавання відповідність шаблону. Line Edge Map інтегрує структурну інформацію з просторова інформація зображення обличчя шляхом групування пікселів обличчя відображення країв у відрізки.

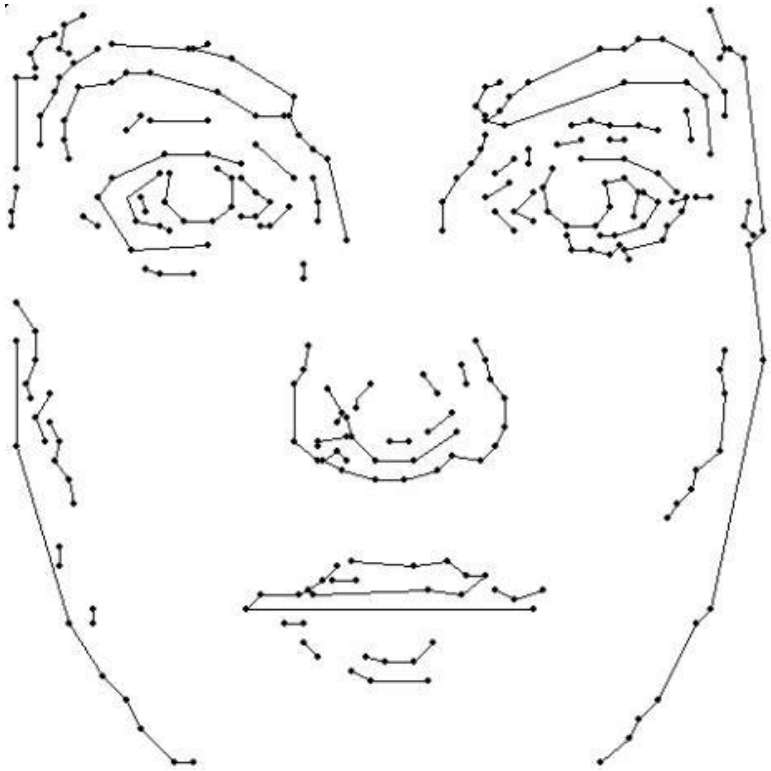

Рисунок 2.3 - Підхід Line Edge Map

Після стоншення карти контуру процес підгонки полігональної лінії [10] використовується для створення LEM обличчя. Прикладом людського лобового обличчя LEM є показано на рисунку. 2.3. Подання LEM зменшує вимоги до зберігання, оскільки він записує лише кінцеві точки лінії відрізків на кривих.

Також очікується, що LEM буде менше чутливий до змін освітлення через те, що він є зображенням середнього рівня, отримане від низького рівня подання карти контурів.

Основною одиницею LEM є сегмент лінії, згрупований з пікселів карти країв. Запропоновано алгоритм попередньої фіксації обличчя, який можна використовувати як попередній процес узгодження LEM в ідентифікації обличчя додаток. Операція попередньої фіксації може прискорити пошук за рахунок зменшення кількості кандидатів і фактичного обличчя.

Експерименти на лобових обличчях під контрольованим /ідеальним умови вказують на те, що запропонований LEM перевершує карту контурів. LEM правильно ідентифікує 100% і 96,43% вхідних фронтальних граней у базах даних осіб. У порівнянні з методом власних граней, LEM виконується так само, як і метод власних граней для граней під ідеальні умови і значно перевершує власне обличчя метод для обличчя з незначними змінами зовнішнього вигляду.

Крім того, підхід LEM набагато надійніший за розміром варіації, ніж метод власних граней і підхід до карти контурів. У джерелі [10] показано, що підхід LEM суттєво перевершує підхід власних граней для ідентифікації обличь під різні умови освітлення. Підхід LEM також менший чутливі до змін пози, ніж метод власних граней, але більш чутливий до великих змін виразу обличчя.

Support Vector Machine (SVM) – це методика визначення, яка вважається ефективною методикою загального розпізнавання образів через її високу продуктивність, узагальнення без необхідності додавати інших відомостей [13]. Інтуїтивно, заданий набір точок, що належать до двох класів, SVM знаходить

гіперплощину, яка розділяє найбільшу можливу частку очок одного класу з тієї ж сторони, максимізуючи відстань від будь-якого класу до площини. Відповідно до [13] ця площина називається - оптимальна розділювальна гіперплощина (OSH), яка зводить до мінімуму ризик неправильної класифікації не лише прикладів у навчальному наборі. Використані методи навчання засновані на принципі мінімізації структурного ризику (SRM), який стверджує, що кращі можливості узагальнення досягаються за допомогою мінімізації межі похибки узагальнення.

Ця методика навчання просто еквівалентна розв'язуванню лінійного завдання проблема квадратичного програмування з обмеженими можливостями. SVM підходить для систем розпізнавання обличчя середнього розміру, тому що зазвичай ці системи мають лише невелику кількість навчання зразки.

Підсумовуючи, основні характеристики SVM:

– мінімізація формально доведеної верхньої межі для узагальнених помилок;

– працюють на високовимірних характеристиках просторів за допомогою подвійного формулювання в термінах ядра;

– передбачення базується на гіперплощинах, де простори характеристик відповідають задіяним критеріям класифікації вхідних даних;

– виділяється навчальний набір даних, що можна обробляти за допомогою відступів.

Таблиця 2.1 - Показник розпізнавання різних методів [14]

Метод	Зіставлення графіків	Інформація про контур	Line Edge Map
Відсотковий показник розпізнавання	97.7%	92%	100%

2.3 Інші види біометричної автентифікації

Метод автентифікації за райдужкою ока. Процес розпізнавання складається з послідовного виконання наступних етапів: пошук, нормалізація, вибір ключових точок, порівняння цих точок.

Локалізація райдужної оболонки. Межа між райдужною оболонкою і склерою є плавним переходом за кольором, у зв'язку з цим завдання виявлення межі переходу стає більш складним, але межа зіниці і райдужки досить чітка.

Його пошук набагато простіше. З цієї причини пошук райдужної оболонки починається з пошуку зіниці. Процес визначення місця розташування райдужної оболонки складається з двох кроків: знаходження зіниці та знаходження райдужної оболонки біля зіниці. Детектор використовує інформацію про контури, що отримує в результаті обчислення градієнта зображення, для уточнення цих контурів за допомогою подвійної порогової фільтрації та відстеження.

Нормалізація райдужної оболонки. Під час запису зображення в різних умовах око може мати різну форму, наприклад, при збільшенні або звуженні зіниці змінюється кількість пікселів, призначених для зображення райдужної оболонки. Розмір очей на знімку також може бути різним через фізичний стан людини по відношенню до камери. Для врахування таких факторів необхідно привести кільцеподібний малюнок райдужної оболонки до стандартизованої форми, інакше обчислення подібності двох райдужок буде неможливим або близьким до нього.

Виділення характерних ознак. Для того щоб виділити відмінні риси райдужної оболонки, необхідно підвищити контрастність зображення, що зробить текстуру райдужної оболонки більш чіткою. Це означає, що дискретне перетворення зможе отримувати детальну інформацію набагато ефективніше. Посилення контрасту досягається шляхом застосування операції вирівнювання гістограми до нормованого зображення райдужної оболонки [7].

Метод автентифікації за геометрією обличчя. Процеси розпізнавання обличчя на основі відео використовують зображення обличчя або серію зображень, знятих відеокамерою. Точність розташування та освітлення об'єкта може вплинути на роботу системи. Зазвичай повністю фіксується зображення обличчя, на яке можна прикріпити ключові точки обличчя людини. Наприклад, розташування очей, рота і ніздрів може бути таким, що створюється унікальний візерунок. Тривимірні моделі обличчя можна створювати різними способами, наприклад, шляхом проектування ІЧ-сітки («структурованого світла»), об'єднання кількох зображень.

Тепловізорне зображення обличчя показує кількість тепла, що створюється припливом крові в обличчя. Тепловізорна камера фіксує невидимий тепловий малюнок кровоносних судин під шкірою. Оскільки під час зйомки обличчя за допомогою ІЧ-камери освітлення не потрібно, системи можуть робити зображення в темряві. Однак ІЧ-камери дорожчі за інші типи відеокамер.

За допомогою спеціальних алгоритмів або нейтронної мережі в ядрі розпізнавання біометричної системи зображення обличчя перетворюється в шаблон, а потім в унікальний математичний код. Цей код зберігається як шаблон для певної особи.

Голосовий метод автентифікації. Обробка мовного сигналу розділяється на кілька основних кроків: попередня обробка сигналу, вибір критеріїв, розпізнавання мовця. Основні характеристики голосу формуються трьома основними властивостями: механікою коливань голосових складок, анатомією мовного тракту та системою управління артикуляцією.

Перевагами є низька вартість цього методу, оскільки потрібні лише мікрофон і звукова карта, які зараз є в кожному комп'ютері. Під час розпізнавання голосу аналізуються висота, модуляція, інтонація тощо.

Основні ознаки, за якими приймається рішення про особу, голос якої перевіряється, формуються з урахуванням усіх факторів процесу формування мовлення: джерела голосу, резонансних частот мовленнєвого тракту та їх загасання, а також динаміки артикуляції. контроль. Крім того, враховується

тріада слова, ритм (розподіл наголосу), рівень сигналу, частота та тривалість перерв. Однак надійність і точність цього методу невисокі, оскільки голос може залежати від здоров'я та поведінкових факторів [7].

Метод автентифікації підпису. Пристрої ідентифікації динаміки підпису використовують геометричні або динамічні функції почерку підпису в реальному часі. Підпис робиться користувачем на спеціальній сенсорній панелі, за допомогою якої змінюється тиск ручки (швидкість, прискорення) перетворюється в електричний аналоговий сигнал. Електронна схема перетворює цей сигнал у цифрову форму, придатну для машинної обробки.

При створенні «еталону» необхідно враховувати, що для однієї і тієї ж особи характерне певне розходження ознак почерку від одного акту до іншого. Тому для створення підпису шаблону потрібно зробити кілька спроб. Ідентифікація підпису не може бути використана скрізь, зокрема цей метод не підходить для обміну доступом до приміщень або доступу до комп'ютерних мереж. Однак у деяких сферах, таких як банківська справа, а також при обробці важливих документів перевірка підпису може бути найефективнішим способом.

Метод автентифікації за відбитком пальця.

Є два типи ємнісних сенсорів: пасивні (кожен осередок сенсора має лише одну з пластин конденсатора) і активні (комірка сенсора містить обидві пластини конденсатора).

Це найбільш широко поширений тип напівпровідникових сканерів, в яких для отримання зображення відбитка пальця використовується ефект зміни ємності pn-переходу напівпровідникового приладу при зіткненні гребеня папілярного візерунка з елементом напівпровідникової матриці. Існують модифікації описаного сканера, в яких кожен напівпровідниковий елемент в матриці сканера виступає в ролі однієї пластини конденсатора, а палець - в ролі іншої.

При додатку пальця до сенсора між кожним чутливим елементом і виступом або впадиною папілярного візерунка утворюється якась ємність,

величина якої визначається відстанню між поверхнею пальця і елементом. Матриця цих ємностей перетворюється в зображення відбитка пальця, рисунок 2.4.

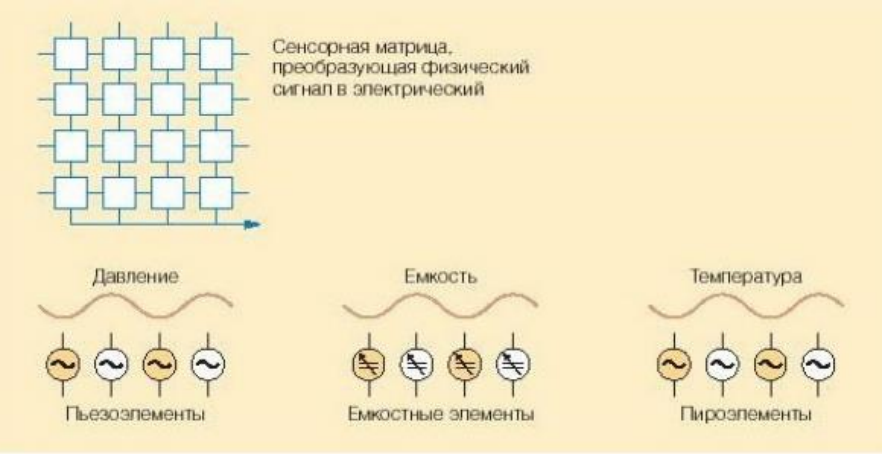

Рисунок 2.4 – Ємнісний сканер

Ємнісні сенсори неможливо обдурити, просто надрукувавши зображення папіломного малюнка на папері. Більш значуща перевага ємнісних сканерів полягає в тому, що вони компактніші і тому легко інтегруються в портат ивні пристрої. Саме за рахунок цієї їх особливості вони й набули на даний момент найширшого поширення у смартфонах.

Порівняння вище розглянутих методів можна побачити в таблиці 2.2. Дані методи були порівняні за характеристиками універсальності застосування, стійкості до муляжів, унікальності, та продуктивності сканерів.

Можна зробити висновки для даної роботи, щодо подальшого дослідження. На даний момент біометрична автентифікація у мобільному пристрої набула дуже високих показників в надійності, захисті та зручності використання. Це зв’язано з тим, що мобільний пристрій має безпечне сховище для таких даних, що називається Enclave, до якого має доступ лише сам процесор.

Тепер всі секрети зберігаються на одному рівні з одними додатками, як і код, який цими секретами управляє за однієї умови: ніхто, абсолютно ніхто, крім процесора, не може отримати туди доступ. Програма та дані як би упаковані в сховище, ключ від якого є тільки у процесора [9].

Таблиця 2.2 – Порівняння біометричних методів автентифікації [8].

Метод	Універсальність	Унікальність	Постійність	Продуктивність	Стійкість
Обличчя	Висока	Середня	Середня	Висока	Висока
Палець	Середня	Середня	Висока	Висока	Середня
Геометрія руки	Середня	Середня	Середня	Середня	Середня
Райдужка	Висока	Висока	Висока	Висока	Низька
Сітківка	Висока	Висока	Середня	Висока	Низька
Підпис	Низька	Низька	Низька	Низька	Висока
Голос	Середня	Низька	Низька	Низька	Висока

Довірена частина являє собою набір функцій і процедур, які називаються ECALL (Enclave Call). Сигнатура таких функцій повинна бути прописана в спеціальному header-файлі, а їх реалізація в файлі з вихідним кодом.

В цілому, підхід схожий з тим, що використовується при звичайному прописуванні хедерів, однак, в даному контексті використовується спеціальний C-подібна мова EDL (Enclave Definition Language). Також необхідно прописати прототипи тих функцій, які можна буде викликати зсередини анклаву, такі функції називаються OCALL (Outside Call). Прототипи прописуються в тому ж хедері, де і ECALL-функції, а реалізація, на відміну від ECALL, прописується відповідно в недовірених частини програми. Рисунок 2.5 ілюструє анклав.

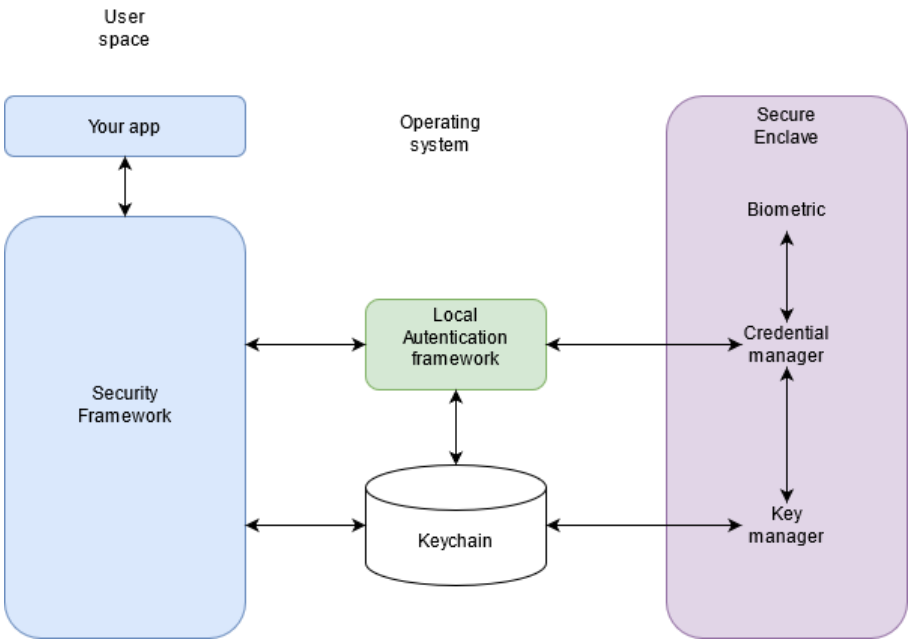

Рисунок 2.5 – Enclave мобільного пристрою

Довірений і недовірений код жорстко зв'язуються між собою сертифікацією з використанням протоколу Діффі-Хеллмана. За процедуру підпису відповідає процесор, де і зберігається ключ обміну інформацією, оновлюється кожного разу при перезавантаженні системи. Вміст анклавів спільну пам'ять, що використовується для користувача додатками, проте зберігання відбувається в зашифрованому вигляді. Розшифрувати вміст може тільки процесор. Подивитися приклад створення додатку CGX Enclave можна за посиланням [9].

В даному випадку мобільний пристрій може бути надійним для зберігання біометричних даних. Щодо веб додатків, то надійність буде розглянута в розділі 3.3. Також веб додатки додають складності та обмеження у виборі методу біометричної автентифікації.

Наприклад дуже мала кількість сучасних комп’ютерів та ноутбуків мають сканери відбитків пальців. Але 95% ноутбуків мають вбудовану камеру. Тому в цьому розділі буде розглянуто більш детально метод біометричної автентифікації за геометрією обличчя. В подальшому в цій роботі буде зосереджена вся увага саме на цьому методі та буде розроблений веб додаток з автентифікацією по геометрії обличчя.

2.4 Атаки на біометричні системи розпізнавання людини

Якщо перед вами стоїть завдання довести, що ви саме той, за кого себе видаєте, якщо ви хочете, щоб доступ до будь-якої інформації або системи управління мали тільки ви, то для цієї мети є зручним використовувати біометричні технології.

У зв'язку з цим останніми роками відбувається їх впровадження в інформаційно-телекомунікаційні системи як засіб ідентифікації (зокрема, віддаленої), а часто й аутентифікації користувачів. Якщо користувач є доброчесною людиною, він зацікавлений у коректному результаті роботи таких систем. Якщо ж ні, то залежно від цілей зловмисник намагається або використовувати випадковий, або цілеспрямовано ініційований збій роботи системи.

Незважаючи на значне підвищення точності, існуючі методи розпізнавання зображень є імовірнісними і припускаються помилок розпізнавання, викликаних різними факторами: зовнішнім освітленням, характеристиками пристроїв реєстрації (оцифрування) біометричних ознак.

З іншого боку, зловмисник може намагатися цілеспрямовано вносити помилки у процес розпізнавання, намагаючись змусити систему некоректно розпізнати образ, що обробляється. Здебільшого алгоритми біометричних систем складаються з послідовності елементарних перетворень вхідних даних, причому більшість таких перетворень є дуже чутливими до найменших змін вхідних даних. Використання цієї властивості дозволяє порушнику часом впливати на результат розпізнавання біометричної системи за допомогою модифікацій біометричних образів і є важливою проблемою в забезпеченні безпеки системи.

Атаки на біометричні образи бувають двох типів:

– нецільова атака (загальний тип атаки, коли основною метою є неправильний результат класифікації);

– цільова атака (складніша атака, метою якої є отримання певного класу при даному вхідному зображенні).

Атаки на біометричні характеристики можуть виконувати такі зловмисники:

– Самозванець може здійснювати атаки двома різними способами. У першому випадку суб’єкт-порушник має намір бути розпізнаним як певний індивід, відомий біометричній системі. У другому випадку суб'єкт-порушник намагається бути розпізнаний як будь-який індивід, відомий біометричній системі.

– Суб’єкт, який приховує свою особистість, навпаки, намагається приховати свої власні біометричні характеристики шляхом підробки біометричних параметрів (Concealer), відомих біометричній системі, наприклад з використанням артефакту (артефакт – штучний об'єкт або зіставлення з копією біометричних характеристик або синтезованими біометричними даними), за допомогою маскування або зміни власних біометричних характеристик.

Найпростіший, і в той же час ефективний алгоритм атаки відомий як швидкий метод градієнта знака (FGSM – Fast Gradient Sign Method), запропонований Гудфеллоу.

Він може використовуватись при обох типах атак. Основна ідея цього ітеративного методу полягає в тому, щоб додавати деякий слабкий шум до зображення на кожній ітерації, переходячи у напрямку до необхідного зображення даних (змінювати кожен піксель зображення). Це можливо, коли порушник має обмежений доступ до системи, так як часто вхідні дані алгоритм розпізнавання отримує, наприклад, з камер відеоспостереження, до яких супротивник не має прямого доступу, що робить багато спуфінга атак практично нереалізованими. Щоб подолати розрив між теоретичними результатами та реальними умовами, останнім часом створюється багато тестових пристроїв. Одним із яскравих прикладів є окуляри, розроблені із зображенням на оправі, що дозволяє ідентифікувати власника як іншу людину, рисунок 2.6.

Рисунок 2.6 – Додавання окулярів на обличчя для зміни біометричних характеристик

2.5 Методи протидії атакам на біометричні системи розпізнавання

Спуфінг - це технічний прийом видачі себе за іншу особу, щоб обдурити мережу або конкретного користувача з метою викликати довіру до надійності джерела інформації. Наприклад, хакери за допомогою email спуфінгу можуть ввести користувача в оману щодо справжності відправника та отримати доступ до конфіденційних даних.

Заходи антиспуфінгу в біометричних системах включають наступні методи:

– Рандомізація даних верифікації. Система може рандомізувати відбитки пальців або вирази осіб, що посилають запит для верифікації. Це зменшує ймовірність запобігання фальшивих біометричних зразків для верифікації.

– Використання кількох біометричних зразків. У процесі реєстрації в системі кожного користувача реєструється, наприклад, кілька відбитків пальців. Після цього в процесі автентифікації у користувача запитують для перевірки кілька знімків у будь-якій послідовності, що значно ускладнює вхід до системи з фальсифікованими знімками.

– Мулитимодальна біометрія. Для виявлення живучості можна використовувати кілька біометричних характеристик від тимчасових, наприклад відбиток пальця та форма особи або райдужна оболонка ока і т.д. створює для зловмисника проблеми с фальсифікуванням декількох біометричних характеристик одночасно, ніж одну характеристику.

– Мультифакторна автентифікація. Мультифакторна автентифікація потрібна для того, щоб забезпечити більшу надійність у той час, коли токени або паролі, можуть зменшити ймовірність обману біометричних систем. В цьому випадку для обману зловмиснику разом із фальшивими біометричними даними потрібні додаткові ідентифікатори. Але мультифакторна автентифікація також зменшує зручність використання біометричних систем.

– Контроль за процесом ідентифікації. Контроль над операціями біометричних систем у свою чергу може підвищити рівень безпеки системи. Очевидно, що розпочати атаку спуфінгу проти контрольованої біометричної системи в цьому у разі складніше. Супервізор допоможе користуватись та правильно представити свої біометричні характеристики та мінімізувати помилки.

– Виявлення живучості. Мета виявлення живучості у біометричних системах полягає в тому, щоб переконатися, що для реєстрації, верифікації та ідентифікації використовуються тільки "справжні" біометричні характеристики. В принципі виявлення живучості ґрунтується на збігу одного або кількох ознак біометричного зразка з ознаками, що пов'язуються з дійсним зразком. Підходи щодо виявлення живучості можна розділити: на виявлення живучості та неживучості. На практиці біометричні системи частіше розробляються на виявлення живучості, ніж на неживучості. У методах виявлення живучості як ознак життя використовується фізіологічна або поведінкова інформація або інформація, що міститься в біометричному зразку.

В системах розпізнавання відбитків пальців для виявлення живучості використовуються вимір температури, пульсу, діелектричного опору, виявлення підшкірних ознак, порівняння послідовно прийнятих біометричних зразків і

т.д. Інших біометричні методи виявлення живучості, як правило, використовують аналізи довільної поведінки.

Системи розпізнавання особи можуть вимагати від користувача руху голови, губ, очей або зміни виразу обличчя. Системи розпізнавання голосу можуть вимагати користувача вимовити випадково генеровану фразу або буквено-цифрову послідовність, щоб запобігти відтворенню записаних звуків.

Методи виявлення живучості обличчя. У системах розпізнавання облич спуфінг атаки можна використовувати фотографію особи, записане відео, 3D моделі обличчя з рухом губ, 3D моделі з різними виразами обличчя тощо. У роботі [18] застосовується метод оптичного потоку для оцінки структури послідовність зображень.

У методі оптичного потоку сегментується карта оптичного потоку та групуються пікселі, що належать окремим об'єктам. Після обчислення потоку кожного пікселя можна оцінити 3D координати точок поверхні. Алгоритм, запропонований у роботі [18], базується на аналізі руху очей у послідовність зображень.

В загальному варіації у формі компонентів осіб послідовності зображень дуже незначні, але варіації у формі ока можуть бути великими, наше миготіння ока і рух зіниці очі завжди є мимовільними.

Також в роботі [18] для виявлення живучості розроблено метод стеження за особами реальний час. Характеристики особи витягуються за допомогою фільтрів Габора та класифікуються SVM-експертами. Для продуктивності в реальному часі вибрані точки були використані для формування регіональних моделей особи

Модель руху очей навчається з використанням численних зразки позиції очей. У цьому методі виявлення живучості щоб пройти тест користувач повинен блимати очима. Фальшиві зображення особи, які не вміють блимати, не вступають у стадію розпізнавання та зупиняються.

Система дає вказівку користувачеві посміхнутися або мигнути, щоб переконатися за короткий період часу, що зображення особи належить даному

людині, обидва рухи не можна здійснити одночасно. Ця технологія виявлення живучості вимагає зазвичай 2 - 3 знімки і не вимагає спеціального обладнання.

Для визначення того, що пред'являється живий відбиток пальця, застосовуються апаратні або програмні методи, а також їх комбінації.

3 ЗАХИСТ ВЕБ ДОДАТКІВ

3.1 Способи вбудовування біометричної автентифікації до веб-додатку

Не зважаючи на те, що інформаційні технології розвиваються дуже швидко, для відправки біометричних даних на backend service потребується набагато більше ресурсів, ніж для простого логіну та паролю. Найпростіша річ – об’єм даних, який значно більший. Справа в тому, що звичайна пара логіну та паролю займає приблизно до 60 символів. Це дуже малий розмір для передачі мережею.

У той час, як для передачі якісного знімку біометричних даних мережею знадобиться відправляти повністю зображення, приблизно 1024 x 1024 пікселя. Для передачі мережею такого об’єму інформації можна виконати гешування, або стискання даних. Геш-функція — функція однозначного зображення строки будь-якої довжини на кінцевій множині до строки заданої довжини. Але в такому випадку при авторизації по паролю ми повинні в точності відтворити пароль. Дані при цьому будуть передаватися і зберігатися у вигляді гешу цього пароля. У зв'язку з тим, що одне з ключових правил хеша — складність дешифровки, навіть дуже схожі паролі будуть видавати зовсім різні геші. Наприклад, ось кілька гешей для дуже схожих комбінацій символів (алгоритм SHA512):

password
b109f3bbbc244eb82441917ed06d618b9008dd09b3befd1b5e07394c706a8bb980b1d7785e5976ec049b46df5f1326af5a2ea6d103fd07c95385ffab0cacbc86

password
cc28edf8bd1e768a03fd79cb48230dd13e082da4ff260526ad7a00b28f5f82a8624a05997040bb6ae501cbfeb7e089778de36f1fd4e56efb9356b02b675a9db8

Password
e6c83b282aeb2e022844595721cc00bbda47cb24537c1779f9bb84f04039e1676e6b
a8573e588da1052510e3aa0a32a9e55879ae22b0c2d62136fc0a3e85f8bb

Password
4846ee019bb2f83122c6aeaf92e61e9b5dcab8f4be0ffcaaa024cc1f992b7543b0dc1cc
32bb68d29fca86753667b3a0cf7c712255907b1b8aeba2085dca74d6b

В останніх двох парах в слові Password латинська буква P замінена на російську Р. Як ми бачимо, рядки виходять абсолютно різні, і при введенні пароля ми не зможемо порівняти навіть символосполучення, що практично не відрізняються [15].

Наступна складність в тому, що людина не може декілька разів зробити абсолютно ідентичний знімок обличчя та сканер обличчя не може однозначно точно отримати 100% такий самий набір ключових точок, як і в попередні рази.

Справа в тому, що для біометричної авторизації використовується нечіткий пошук, який буде розглянуто в главі 3.2. Це такий пошук, при якому ми шукаємо не повністю збігаються елементи, а сутності найбільш схожі один на одного. Скажімо, для авторизації за відбитком пальця, точність у повторенні малюнка в 90 відсотків — дуже хороший показник, і він означає, що маємо і є справжній власник відбитка. Проте його відбиток на 10 відсотків складається з абсолютно інших даних, у зв'язку з чим ми отримуємо абсолютно інший хеш і втрачаємо можливість безпечного зберігання даних.

Більше того, дані доведеться зберігати повністю - геш функція, що видає близькі значення для схожих символьних поєднань не відповідає правилам безпеки і не може вважатися хорошою геш функцією. Але навіть якщо ми зможемо якимось чином описати дані за допомогою нечіткого геша, у нас виникає інша, ще більш нетривіальна проблема. Існують люди, що дуже схожі один на одного, тому вірогідність збігу посилюється. Або ціла нація людей, що дуже схожі один на одного, бо типажів дуже мало і ймовірність збігу ще більше посилюється[15].

Проаналізувавши всі вище перераховані плюси та мінуси можна зробити висновок, що біометрична автентифікація у веб додатках не показує себе, як кращий спосіб автентифікації, бо має ряд недоліків у порівняні з мобільним пристроєм:

- великий обсяг даних;
- нечітке порівняння;
- схожі показники у різних людей.

Але як додатковий метод автентифікації може покращити захист. Наприклад використання біометрії у якості двофакторної автентифікації має право на існування та підвищить ефективність захисту електронних ресурсів людини при компрометації паролю.

3.2 Нечіткий пошук

Алгоритми нечіткого пошуку (також відомого як подібний пошук або fuzzy string search) є основою систем перевірки орфографії і повноцінних пошукових систем на кшталт Google або Yandex. Наприклад, такі алгоритми використовуються для функцій на кшталт «Можливо ви мали на увазі…» у тих самих пошукових системах.

Нечіткий пошук є надзвичайно корисною функцією будь-якої пошукової системи. Разом з тим його ефективна реалізація набагато складніша, ніж реалізація простого пошуку за точним збігом.

Завдання нечіткого пошуку можна сформулювати так: "За заданим словом знайти в тексті або словнику розміру n всі слова, що збігаються з цим словом (або починаються з цього слова) з урахуванням k можливих відмінностей". Наприклад, при запиті "Машина" з урахуванням двох можливих помилок знайти слова "Машинка", "Махіна", "Малина", "Калина" і так далі.

Алгоритми нечіткого пошуку характеризуються метрикою - функцією відстані між двома словами, що дозволяє оцінити ступінь їхньої подібності в даному контексті.

Найчастіше застосовуваної метрикою є відстань Левенштейна, чи відстань редагування, алгоритми обчислення якого можна знайти кожному кроку. Проте варто зробити кілька зауважень щодо найбільш популярного алгоритму розрахунку — методу Вагнера-Фішера [16]. Вихідний варіант цього алгоритму має тимчасову складність O(mn) і споживає O(mn) пам'яті, де m і n — довжини рядків, що порівнюються. Весь процес можна представити наступною матрицею рисунок 3.1:

		m	e	i	l	e	n	s	t	e	i	n
	0	1	2	3	4	5	6	7	8	9	10	11
l	1	1	2	3	3	4	5	6	7	8	9	10
e	2	2	1	2	3	3	4	5	6	7	8	9
v	3	3	2	2	3	4	4	5	6	7	8	9
e	4	4	3	3	3	3	4	5	6	6	7	8
n	5	5	4	4	4	4	3	4	5	6	7	7
s	6	6	5	5	5	5	4	3	4	5	6	7
h	7	7	6	6	6	6	5	4	4	5	6	7
t	8	8	7	7	7	7	6	5	4	5	6	7
e	9	9	8	8	8	7	7	6	5	4	5	6
i	10	10	9	8	9	8	8	7	6	5	4	5
n	11	11	10	9	9	9	8	8	7	6	5	4

Рисунок 3.1 – Матриця відстані Левенштейна

Якщо подивитися на процес роботи алгоритму, неважко помітити, що на кожному кроці використовуються лише два останні рядки матриці, отже споживання пам'яті можна зменшити до O(min(m, n)). Але це ще не все - можна далі оптимізувати алгоритм, якщо стоїть завдання знаходження не більше відмінностей. У цьому випадку необхідно обчислювати в матриці лише діагональну смугу шириною 2k+1 (відсікання Укконена), що зводить тимчасову складність до O(k min(m, n)) [16].

Алгоритм розширення вибірки. Він заснований на зведенні задачі про нечіткий пошук до завдання точного пошуку. З вихідного запиту будується безліч «помилкових» слів, кожного з яких потім виробляється точний пошук у словнику. Час його роботи залежить від числа k помилок і зажадав від розміру алфавіту

Наприклад, при k = 1 і слова довжини 7 (наприклад, «Крокодил») в російському алфавіті безліч помилкових слів буде розміром близько 450, тобто необхідно зробити 450 запитів до словника, що цілком прийнятно. Але вже при k = 2 розмір такої множини становитиме понад 115 тисяч варіантів, що відповідає повному перебору невеликого словника, або ж 1/27 у нашому випадку, і, отже, час роботи буде досить великим.

При цьому не потрібно забувати ще й про те, що для кожного з таких слів необхідно здійснити пошук на точний збіг у словнику. особливості: Алгоритм може бути легко модифікований для генерації «помилкових» варіантів за довільними правилами, до того ж, не вимагає ніякої попередньої обробки словника, і, відповідно, додаткової пам'яті.

Можливі покращення: можна генерувати не всю множину «помилкових» слів, а лише ті з них, які найімовірніше можуть зустрітися в реальній ситуації. Приклад можна побачити на рисунку 3.2.

3.3 Біометрія з можливістю скасування

Один з способів захистити біометричні дані після отримання їх на сервері – є перемішування цих даних. Ми не можемо змінити свої біометричні дані, але можемо змінити алгоритм зберігання та роботи з ними. Для цього розробляються спеціальні рішення під загальною назвою «біометрія, що скасовується»[17].

Ця технологія заснована на навмисному перекручуванні біометричних даних, що повторюється, на основі попередньо обраного перетворення.

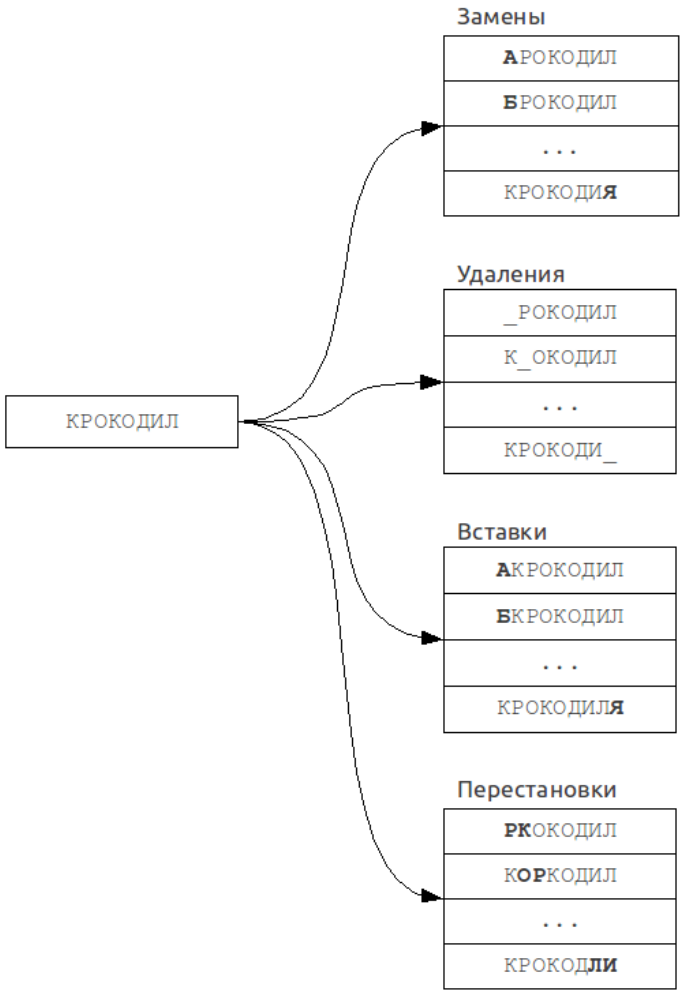

Рисунок 3.2 – Приклад алгоритму розширеної вибірки

Біометричний сигнал однаково спотворюється як із реєстрації, і за кожної ідентифікації.

Такий підхід дозволяє використовувати для кожного запису свій метод, що перешкоджає перехресному зіставленню. Крім того, якщо екземпляр перетвореної біометрії скомпрометовано, достатньо змінити алгоритм конвертації, щоб згенерувати новий варіант для повторної реєстрації. Для безпеки використовуються незворотні функції. Таким чином, навіть якщо алгоритм конвертування відомий і є перетвореними біометричними даними, відновити по них вихідну (не спотворену) біометрію не вийде.

Перетворення можуть застосовуватися як області сигналу, так і в області ознак. Тобто або біометричний сигнал перетворюється безпосередньо після отримання, або обробляється звичайним чином, після чого перетворюються вилучені ознаки.

Алгоритм перетворення дозволяє розширити шаблон, що дозволяє збільшити надійність системи. Приклади перетворень на рівні сигналу включають перестановку блоків сітки. Змінене зображення не може бути успішно порівняно з вихідним чином або з аналогічними зображеннями, отриманими з іншими параметрами перетворення [17].

Розгортання біометричних даних на масовому ринку, як авторизація картки або доступ до банкомату викликає додаткові занепокоєння, крім безпеки трансакцій. Однією з таких проблем є сприйняття громадськості про можливе вторгнення в приватне життя.

Окрім особистої інформації, такої як ім’я та дата народження, користувача просять надати зображення частин тіла, наприклад, пальці, обличчя та райдужка. Ці зображення чи інші такі біометричні сигнали зберігаються в цифровій формі в різноманітні бази даних. Це викликає занепокоєння щодо можливого обміну даними між правоохоронними органами чи комерційними підприємствами. Громадськість стурбована постійно зростаючим тілом інформації, яка збирається про окремих людей у нашому суспільстві. Зібрані дані охоплюють багато додатків і включають медичні записи та біометричні дані.

Ці занепокоєння посилюються тим, що біометричні дані особи надаються на все життя і не можуть бути змінені.

Одна з властивостей, яка робить біометрію настільки привабливими для цілей аутентифікації,— їх незмінність у часі — також є одним із його зобов’язань. Коли номер кредитної картки скомпрометовано, банк, який подає позов, може просто призначити клієнту новий кредит номер картки. Якщо біометричні дані скомпрометовані, заміна неможлива. Щоб усунути цю проблему, ми вводимо концепція «біометрії, яку можна скасувати».

Вона складається з навмисного повторювання та спотворення біометричного сигналу на основі обраного перетворення. Біометричний сигнал спотворюється однаково під час кожної перевірки, для реєстрації та для кожної автентифікації. Приклад такого спотворення можна побачити на рисунку 3.3.

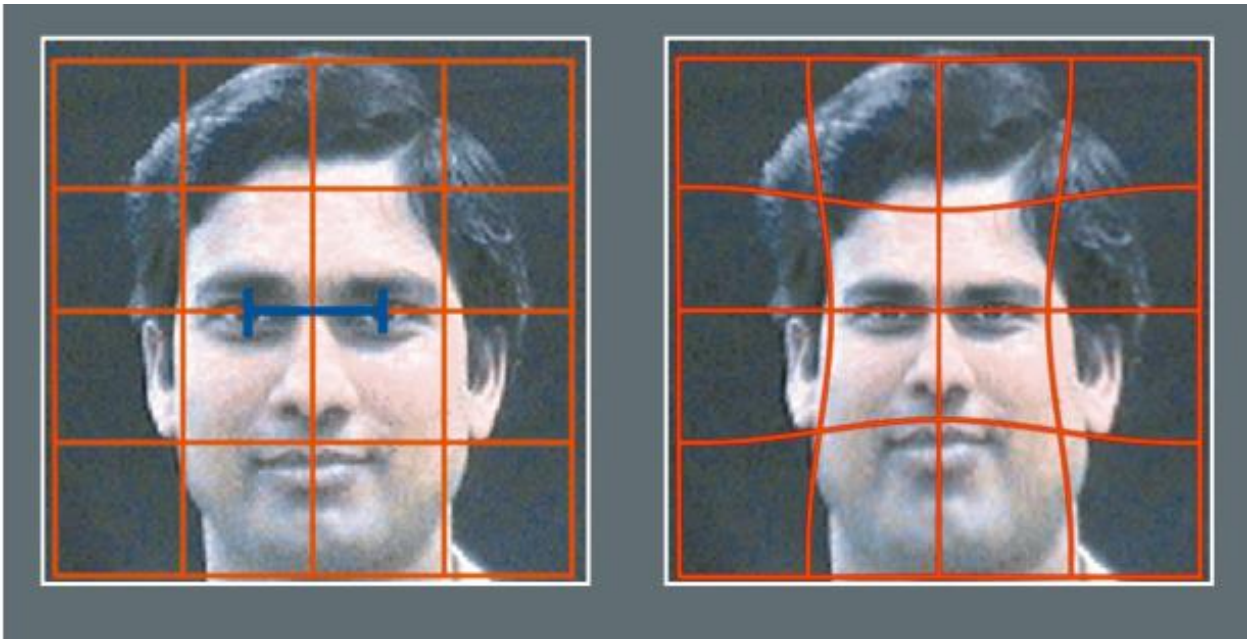

Рисунок 3.3 – Спотворення зображення

Завдяки такому підходу кожен екземпляр реєстрації може використовувати інше перетворення, що робить неможливим перехресне зіставлення. Крім того, якщо один варіант перетворення біометричних даних скомпрометований, то функцію трансформації можна просто змінити на створення нового варіанту для повторного зарахування, нової особи.

Загалом, перетворення спотворення вибираються незворотними. Отже, навіть якщо функція перетворення відома і отримані перетворені біометричних даних є відомо, оригінальна (неспотворена) біометрична інформація не може бути відновленою [17].

У запропонованому методі, перетворення спотворення можуть бути застосовані або в області сигналу, або в області ключових точок. Це або біометричний сигнал може бути трансформований безпосередньо після отримання,

або сигнал може бути оброблений як зазвичай, і вилучені ознаки можна потім трансформувати.

Крім того, розширення шаблону до більшого простору представлення за допомогою відповідного перетворення може додатково збільшити об’єм системи. В ідеалі перетворення має бути необоротним, щоб істинне біометричне зображення користувача не було відновлене з одного або більше спотворених версій, збережених зловмисниками.

Приклади перетворень на рівні сигналу включають морфінг сітки та перестановка блоків, рисунок 3.4.

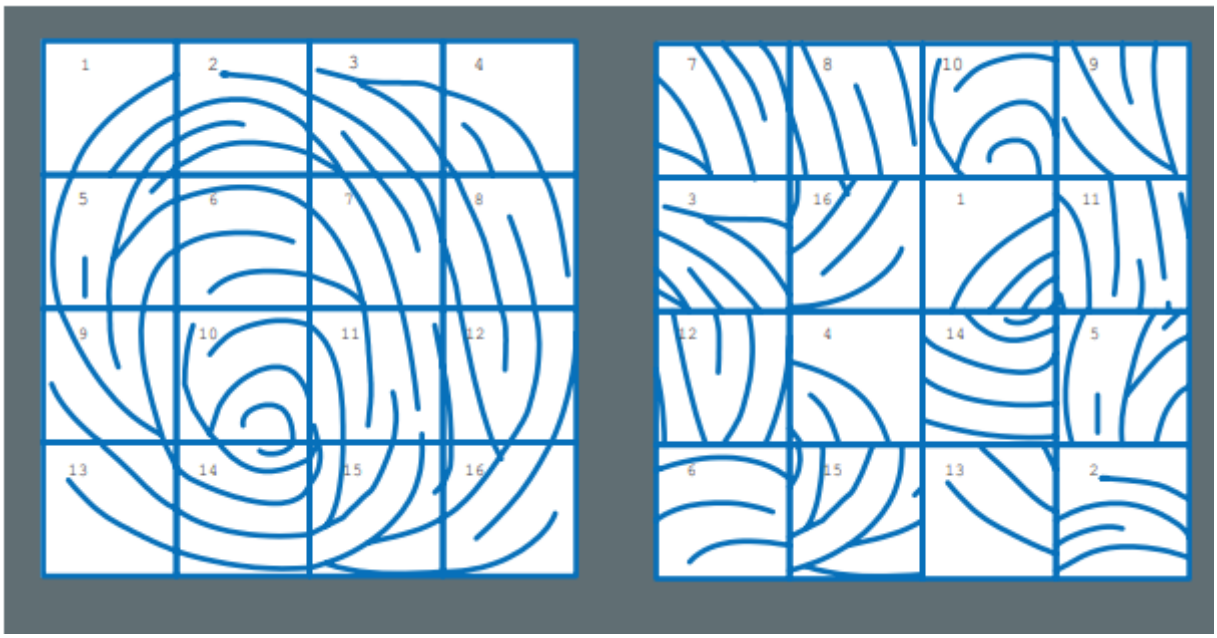

Рисунок 3.4 – переставлення блоків зображення

Трансформовані зображення неможливо успішно зіставити проти оригінальних зображень або проти подібних трансформацій того самого зображення з використанням різних параметрів. Хоча метод деформованого шаблону може бути в змозі щоб знайти такий збіг, залишкова енергія деформації, ймовірно, буде такою ж високою, як і відповідність шаблону до непов’язаного образу [17].

Блоки в оригінальному зображенні згодом зашифровуються випадковим чином, але повторно. Прикладом перетворення в області ознак є набір випадкових, повторюваних скуплень ключових точок. Це можна зробити в межах того самого фізичного простору, як оригінал, або, при збільшенні діапазону осей.

Другий випадок забезпечує більше грубої сили. Приклад такого перетворення показано на рисунку 3.5.

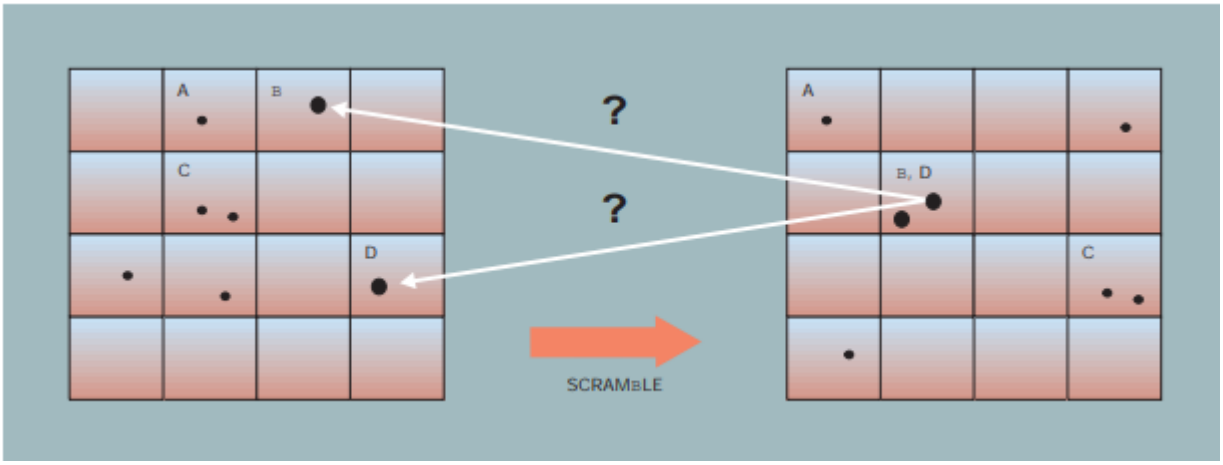

Рисунок 3.5 – Замішування блоків вхідного зображення

Тут блоки ліворуч випадковим чином зіставляються на блоки на праворуч, де кілька блоків можна відобразити на той самий блок. Таким чином, такі перетворення є незворотними вихідні набори функцій неможливо відновити спотворені версії. Наприклад, це неможливо щоб визначити, з якого з двох блоків спочатку походять точки в складеному блоці B, D. Отже, власника біометричних даних не можна ідентифікувати інакше як через інформацію, пов’язану з цим конкретним записом [17].

Для того, щоб перетворення було повторюваним, нам потрібно щоб біометричний сигнал був належним чином зареєстрований перед перетворенням. На щастя, ця проблема на нього частково відповіла низка методів, доступних

у літературі (наприклад, пошук точки «ядро» та «дельта» в відбитку пальця або ока і виявлення носа на обличчі).

3.4 Застосування біометрії в сфері банкінгу

Фінансова галузь розвивається зараз величезними темпами, на очах змінюючи фінансову інфраструктуру та навіть підходи до ведення бізнесу. При цьому ключових вимог до цієї галузі лише дві: підвищення ефективності фінансової системи або окремого бізнесу та безпека.

Біометричні технології забезпечують виконання обох перелічених вимог і добре поєднуються з новітніми досягненнями фінансової галузі. Найочевидніша область використання біометрії – це оперативна та надійна ідентифікація клієнта на різних кроках та у різних сценаріях фінансових взаємодій. Друга область – забезпечення безпеки під час роботи з персональною інформацією та фінансовими даними [19].

Це актуально і для всіляких систем платежів та переказів, банкінгу та персональних фінансів, кредитування, управління активами та інвестиціями та, нарешті, страхування. Найпростіша біометрія застосовується у сканерах відбитків пальців сучасних смартфонів та планшетів, з їх допомогою можна отримати доступ до систем Google Pay та Apple Pay. Багато великих банків вже використовують біометрію у своїх мобільних додатках як для входу в додаток, так і для підтвердження операцій.

Але це поки що теж складно назвати гідним захистом – виробники смартфонів наголошують на швидкості спрацьовування дактилоскопічного датчика, що не найкращим чином позначається на точності розпізнавання. Датчик зазвичай зчитує лише частину відбитка.

Існує і 3D Secure [20] - нова версія протоколу, що отримала змінену процедуру верифікації. Саме підтвердження платежів реалізується за допомогою різних біометричних параметрів - контури особи, відбитки пальців, малюнок вен долоні та інше. При цьому на відкуп внутрішньої системи оцінки ризиків

віддано до 95% загальних транзакцій, і тільки у випадку з 5% система буде запитувати код верифікації. Повсюдна мобільність стала одним із невід'ємних трендів для фінансів, і складно уявити якийсь новий фінансовий додаток без використання біометрії.

Належний рівень захисту при збереженні комфорту та швидкості використання може забезпечити лише мультимодальний підхід – автентифікація одразу за декількома біометричними показниками. Найслабша і найвразливіша модальність – це голос – сильно залежить від навколишнього шуму, легко перехоплюється сторонніми технічними засобами.

Аналогічні проблеми виникають і при виборі відеоідентифікації як єдиного способу - якість освітлення, погода, незначні зміни зовнішності ускладнюють процес і впливають на результат. Набагато краще йдуть справи з ідентифікацією по малюнку вен долоні, тривимірної моделі особи, по фото, зробленому в ІЧ-діапазоні, або райдужній оболонці, особливо при їх суперпозиції з метою контролю компрометації та управління ризиками [19].

Розглянемо, у яких сферах технології RecFaces можуть прискорити, оптимізувати та убезпечити використання фінансових сервісів. При скануванні паспорта біометричне правило перевірки зображення обличчя допоможе перевірити справжність документа, виключити зовні схожих людей і використання чужого документа. За будь-яких дистанційних фінансових операцій мультимодальна біометрична верифікація буде запорукою зручного та безпечного проведення транзакції.

З допомогою зовнішнього устаткування, встановленого різні клієнтські додатки, створюється біометрична характеристика (БХ) конкретної людини. Може бути використане різне обладнання (сканер сітківки ока, сканер відбитка пальця, фотоапарат, мікрофон тощо), у тому числі для створення мультимодального профілю клієнта. Клієнтський інтерфейс і клієнтські послуги зв'язуються з веб-сервером.

Характеристика міститься в ізольованому модулі зберігання із застосуванням механізмів деперсоніфікації. При надходженні запиту Модуль обробки біометричних зразків виконуються наступні кроки:

– отримання характеристик зі сховища;

– перевірка на якість характеристик (якість фото, відстань, освітленість, розмитість, кути повороту голови, інтегральні індекси якості, рівень сторонніх шумів тощо).

У разі поганої якості процес припиняється з відповідним повідомленням; У разі задовільної якості зображення перетворюється на біометричний шаблон; шаблон розміщується в модуль зберігання із застосуванням механізмів деперсонифікації [19].

Модуль контролю захисту від компрометації запускає конвеєр перевірки характеристик та шаблону щодо фальсифікації, підміни, невідповідності, заміни осіб тощо. До конвеєра можуть бути включені механізми, що працюють за різними ознаками (аналіз контексту, поведінки людини, оптичного спотворення тощо). У модуль розпізнавання та пошуку надходить запит на пошук шаблону в еталонній базі шаблонів профілів людей.

У модуль розпізнавання та пошуку надходить шаблон поточної операції. Реалізується функція біометричної верифікації. Повертається міра схожості та значення автентифікований/не автентифікований як результат. Завантаження результату ідентифікації користувача в клієнтський UI або апаратні виконавчі механізми.

Важливо відзначити, що цей багатоступінчастий процес забезпечує високу надійність результату, а займає всього 1,5-2 секунди.

Шляхом виконання таких операцій отримуємо такі переваги:

– зручна та безпечна біометрична автентифікація клієнтів у каналах дистанційного обслуговування;

– біометричні механізми перевірки клієнта у процесі кредитування;

– зручна та безпечна біометрична автентифікація персоналу, контроль та підтвердження окремих видів операцій та присутності співробітника;

– ефективні сучасні біометричні засоби боротьби з внутрішнім та зовнішнім фродом;

– способи управління пріоритизацією обслуговування клієнтів [19].

4. РЕАЛІЗАЦІЯ ВЕБ ДОДАТКУ З БІОМЕТРИЧНОЮ АВТЕНТИФІКАЦІЄЮ

4.1 Основні функції програми

Веб додаток призначений для демонстрації автентифікації за геометрією обличчя, як при двофакторній автентифікації. Додаток має сторінку реєстрації користувача, де потрібно ввести свою пошту, придумати пароль та зробити знімок з камери за допомогою додатку.

Наступна функція – вхід користувача в систему, де потрібно виконати ідентифікацію за допомогою пошти та паролю. Після чого, якщо запит пройшов успішно потрібно підтвердити особистість за допомогою знімку з камери обличчя користувача. Якщо перевірка зображення пройшла успішно – користувач потрапляє до веб-додатку.

4.2 Опис користувацького інтерфейсу

Даний користувацький додаток має чотири вікна, кожне з яких має свої особливості. Перша сторінка – реєстрація, зображена на рисунку 4.1, містить поля для вводу особистих даних користувача та робить еталонне фото, з яким потім буде порівнювати при спробі авторизуватися в додатку. Після вводу своїх даних потрібно натиснути кнопку «Registrate my account» для відправлення форми на сервер.

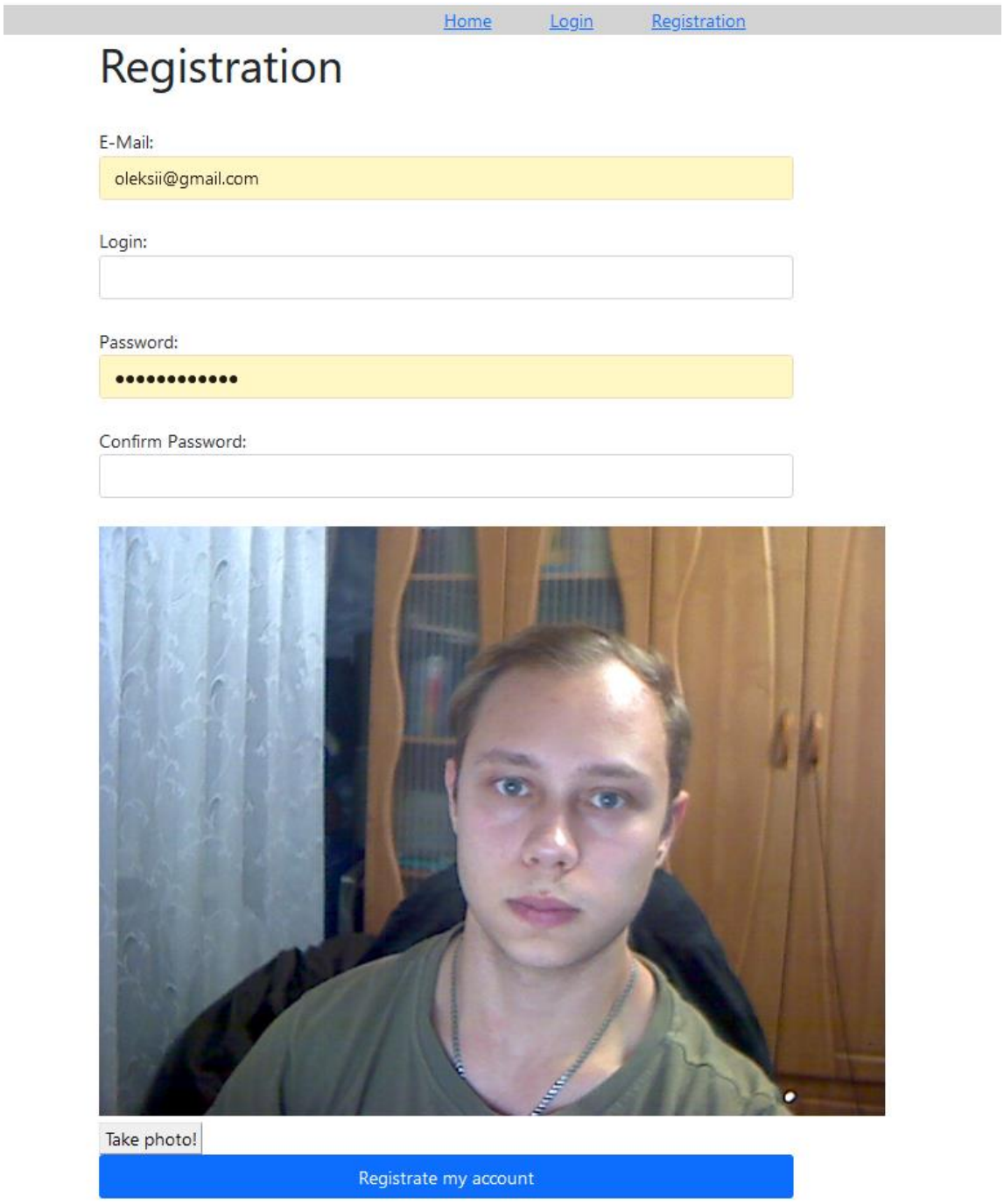

Рисунок 4.1 – Сторінка авторизації

Наступна сторінка – сторінка авторизації користувача. На цій сторінці потрібно ввести свої дані та натиснути кнопку «Login to my account» для того, щоб пройти ідентифікацію. Сторінка зображена на рисунку 4.2

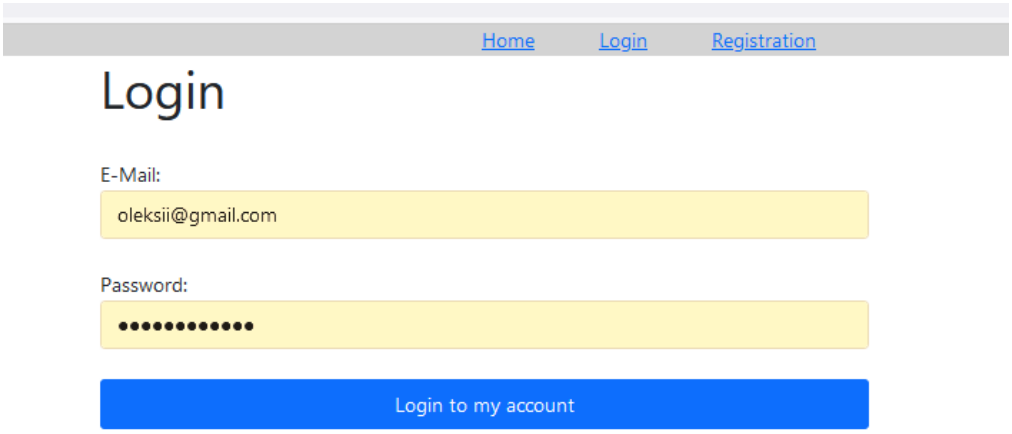

Рисунок 4.2 – Сторінка логіну

Після успішної ідентифікації потрібно пройти автентифікацію, де робиться знімок обличчя за допомогою камери. Це зображення відправляється на сервер для перевірки. Зображення сторінки автентифікації за обличчям зображене на рисунку 4.3

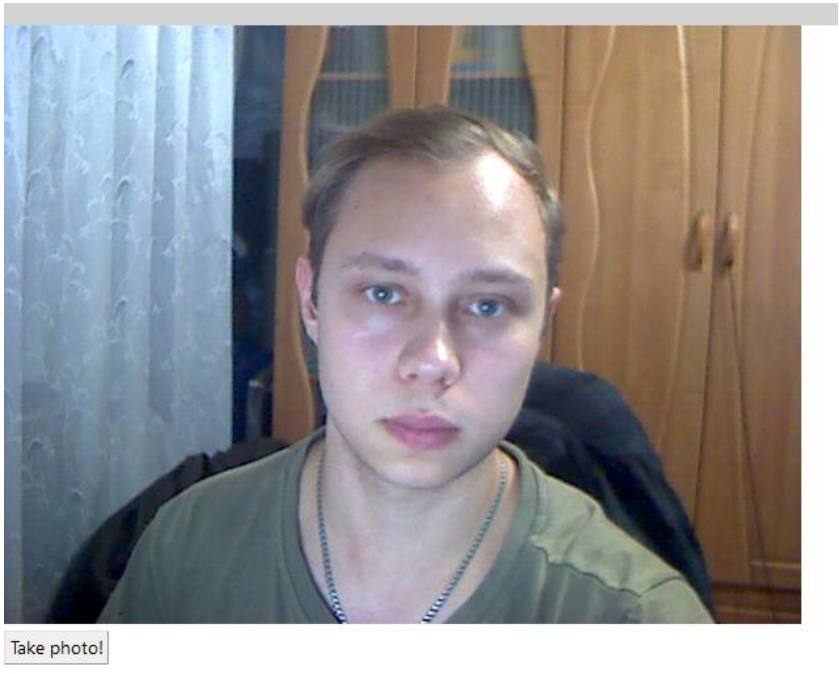

Рисунок 4.3 – Сторінка автентифікації за обличчям

Після успішної автентифікації користувача перенаправляє на головну сторінку. На цій сторінці перевіряється, чи пройшла успішно автентифікація. У випадку, коли автентифікація провалилася користувача не перенаправить до головної сторінки, у іншому випадку виводиться повідомлення, що користувач успішно авторизувався у веб додатку, рисунок 4.4.

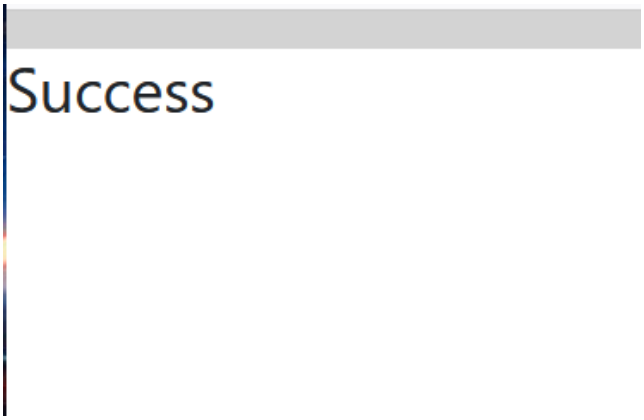

Рисунок 4.4 – Успішна авторизація

4.3 Опис проекту та бібліотеки для розпізнавання обличчя

Для написання програми була обрана мова програмування C# та платформа ASP.NET – це платформа розробки веб-додатків, до складу якої входять: веб-сервіси, програмна інфраструктура, модель програмування від компанії Майкрософт. ASP.NET входить до складу платформи .NET Framework і є розвитком старої технології Microsoft ASP.

Для розпізнавання обличчя була використана бібліотека Emgu CV, реалізована на мові програмування C#.

Emgu CV — це кросплатформна обгортка .Net для бібліотеки обробки зображень OpenCV. Дозволяє викликати функції OpenCV з .NET-сумісних мов. Обгортка може бути скомпільована Visual Studio та Unity, може працювати на Windows, Linux, Mac OS, iOS та Android.

Emgu CV повністю написано на C#. Його можна запускати на будь-якій платформі, яку підтримує .NET, включаючи iOS, Android, Mac OS X, Linux та Windows. Багато зусиль було витрачено, щоб мати чисту реалізацію C#, оскільки заголовки мають бути перенесені з керованою реалізацією, порівняно з C++, де можна просто включити файли заголовків.

OpenCV (Open Source Computer Vision Library: http://opencv.org) — це бібліотека з відкритим вихідним кодом, ліцензована BSD, яка включає кілька сотень алгоритмів комп'ютерного зору [21].

OpenCV має модульну структуру, що означає, що пакет включає кілька спільних або статичних бібліотек:

– Функціональність ядра (ядро) - компактний модуль, що визначає основні структури даних, включаючи щільний багатовимірний масив Mat і основні функції, які використовуються всіма іншими модулями.

– Обробка зображень (imgproc) — модуль обробки зображень, що включає лінійну та нелінійну фільтрацію зображень, геометричні перетворення зображення (зміна розміру, спотворення афінної та перспективи, загальне перемалювання на основі таблиці), перетворення колірного простору, гістограми тощо.

– Video Analysis (відео) - модуль аналізу відео, який включає в себе алгоритми оцінки руху, віднімання фону та відстеження об'єктів.

– Калібрування камери та 3D-реконструкція (calib3d) - основні алгоритми геометрії кількох переглядів, калібрування однієї та стереокамери, оцінка пози об'єкта, алгоритми стереовідповідності та елементи тривимірної реконструкції.

– 2D Features Framework (features2d) - визначні детектори ознак, дескриптори та відповідники дескрипторів.

– Виявлення об'єктів (objdetect) - виявлення об'єктів і екземплярів попередньо визначених класів (наприклад, облич, очей, людей, автомобілів і так далі).

– Високорівневий графічний інтерфейс (highgui) - простий у використанні інтерфейс для простих можливостей інтерфейсу користувача.

– Video I/O (videoio) - простий у використанні інтерфейс для запису відео та відеокодеків.

– Деякі інші допоміжні модулі, такі як тестові обгортки FLANN і Google, прив'язки Python та інші.

– Машинне навчання (модуль ml) використовує потужні класи машинного навчання для статистичної класифікації, регресії та кластеризації даних.

– Комп'ютерна фотографія (фотомодуль) використовує OpenCV для розширеної обробки фотографій.

– Зшивання зображень (модуль зшивання) створює красиві фотопанорами та багато іншого за допомогою конвеєра зшивання OpenCV.

– Комп'ютерний зір із прискореним графічним процесором (модуль cuda) [21].

OpenCV автоматично виділяє пам'ять для параметрів вихідної функції більшість часу. Отже, якщо функція має один або кілька вхідних масивів (екземплярів cv::Mat), то вихідні масиви автоматично розподіляються або перерозподіляються. Розмір і тип вихідних масивів визначаються з розміру і типу вхідних масивів. Якщо необхідно, функції приймають додаткові параметри, які допомагають визначити властивості вихідного масиву.

ВИСНОВОК

Біометрія - це наука, заснована на описі унікальних характеристик тіла людини. У застосуванні до систем автоматичної ідентифікації під біометричними розуміють ті системи і методи, які засновані на використанні для ідентифікації або автентифікації будь-яких унікальних характеристик людського організму.

У роботі було показано роботу веб-додатків, протоколу HTTP. Було порівняно цей протокол з захищеною версією такого протоколу. Продемонстровано, як саме захищає протокол HTTPS. Захист виконується при передачі за допомогою TLS — спадкоємець SSL — протоколу, який найчастіше використовується для забезпечення безпечного HTTP з'єднання (так званого HTTPS). TLS розташований на рівні нижче протоколу HTTP моделі OSI.

Для гарантування особистості серверу використовуються сертифікати, які були надані та засвідчені (CA). Як тільки CA засвідчується в тому, що заявник є реальним і він реально контролює домен, CA підписує сертифікат для цього сайту, по суті, встановлюючи штамп підтвердження на тому факті, що публічний ключ сайту дійсно належить йому і йому можна довіряти. У кожен браузер вже спочатку завантажено список акредитованих CA. Інакше кожен міг би підписувати фіктивні сертифікати.

У розділі 2 були розглянуті біометричні методи автентифікації, зроблений висновок, та поради щодо використання біометричних характеристик людини у веб-додатках.

Проаналізувавши всі вище перераховані плюси та мінуси можна зробити висновок, що біометрична автентифікація у веб-додатках не показує себе, як кращий спосіб автентифікації, бо має ряд недоліків у порівняні з мобільним пристроєм:

- великий обсяг даних;
- нечітке порівняння;

– схожі показники у різних людей.

Але як додатковий метод автентифікації може покращити захист. Наприклад використання біометрії у якості двофакторної автентифікації має право на існування та підвищить ефективність захисту електронних ресурсів людини при компрометації паролю.

У розділі 3 розповідається про «біометрію з можливістю скасування». Ця технологія заснована на навмисному перекручуванні біометричних даних на основі попередньо обраного перетворення. Біометричний сигнал однаково спотворюється як із реєстрації, і за кожної ідентифікації. Такий підхід дозволяє використовувати для кожного запису свій метод, що перешкоджає перехресному зіставленню.

В 4-му розділі представлений веб-додаток, який побудовано для демонстрації підвищення надійності автентифікації за рахунок додавання двофакторної автентифікації. Додаток використовує сертифікат для демонстрації відкритості та гарантії надійності. Додаток шифрує дані, що передаються та для підвищення надійності використовується біометрична автентифікація за геометрією обличчя. Такий спосіб підвищує надійність захисту персональних даних.

ПЕРЕЛІК ПОСИЛАНЬ

1. https://habr.com/ru/post/450282/
2. https://developer.mozilla.org/ru/docs/Web/HTTP/Overview
3. OWASP top 10, 2017. – 70 с.
4. https://en.wikipedia.org/wiki/Public_key_certificate
5. Aparecido Nilceu Marana, Juan Rogelio Falguera. Biometrics for Human Identification. - 2006, 28 с.
6. Біометрична ідентифікація [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: https://securityrussia.com/blog/biometriya.html.
7. Степаненко М.А., Дмитриев Д.В. Методы распознавания радужной оболочки глаза в задачах аутентификации. 2014. – № 6.
8. Aparecido Nilceu Marana, Juan Rogelio Falguera. Biometrics for Human Identification. - 2006, 28 с.
9. Trusted Execution Environment на примере Intel SGX. [Електронний ресурс] – Режим доступу до ресурсу: https://habr.com/ru/post/518004/.
10. G.j. Edwards, T.f. Cootes and C.J. Taylor, “Face recognition using active appearance models,” In ECCV, 1998.
11. S. Tamura, H. Kawa, and H. Mitsumoto, “Male/Female identification from 8_6 very low resolution face images by neural network,” Pattern Recognition, vol. 29, pp. 331-335, 1996.
12. B.S. Manjunath, R. Chellappa, and C. von der Malsburg, “A Feature based approach to face recognition,” Proc. IEEE CS Conf. Computer Vision and Pattern Recognition, pp. 373-378, 1992.
13. V.N. Vapnik, “The nature of statistical learning theory,” New York: Springverlag, 1995.
14. Y. Gao and K.H. Leung, “Face recognition using line edge map,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 6, June 2002.
15. https://habr.com/ru/post/415517/ [Електронний ресурс]

16. https://habr.com/ru/post/114997/ [Електронний ресурс]
17. Enhancing Security and Privacy in Biometrics-Based Authentication Systems" by N. K. Ratha, J. H. Connell, R. M. Bolle - 22 c, 2001.
18. Aggarwal J. K., Nandhakumar N. On the Computation of Motion from Sequences of Images — A Review//Proc. IEEE, 1998. V. 76. P. 917-935.
19. https://habr.com/ru/company/recfaces/blog/328674/
20. https://www.emvco.com/emv-technologies/3d-secure/
21. https://docs.opencv.org/3.4/d1/dfb/intro.html