Дипломна робота
на здобуття ступеня бакалавра
на тему:

Аналіз засобів для реалізації технологій багатофакторної біометричної аутентифікації користувачів у мобільних додатках

Виконав:

Студент групи ДА-62

ВАСИЛЕВИЧ Б.С.

Науковий керівник: Капшук О. О.

МЕТА РОБОТИ

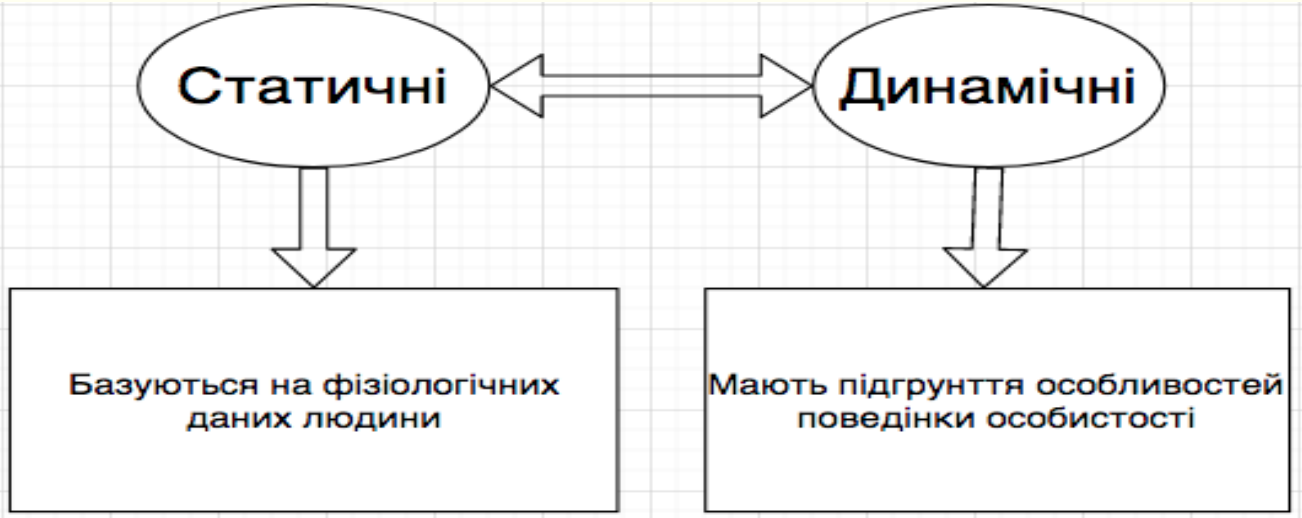
Основною метою і змістом даної роботи є проведення аналізу та дослідження для реалізації технологій багатофакторної біометричної аутентифікації користувачів у мобільних додатках.

Актуальність

Надійним захистом інформації в сучасному медійному просторі є розвиток технологій біометричної аутентифікації.

На сьогодення пріоритетним й не вирішеним питанням захисту інформації є аутентифікація користувача, що отримує доступ до конфіденційної інформації.

Види біометричної аутентифікації



В сучасному інформаційному світі розрізняють такі методи біометричної аутентифікації:

- статичні, що базуються на фізіологічних даних людини;
- динамічні, що мають підгрунтття особливостей поведінки особистості.

Ці дві великі групи методів біометричної аутентифікації - це взаємодоповнюючі та взаємопов’язані між собою методи.

Аутентифікація користувачів за відбитком пальців

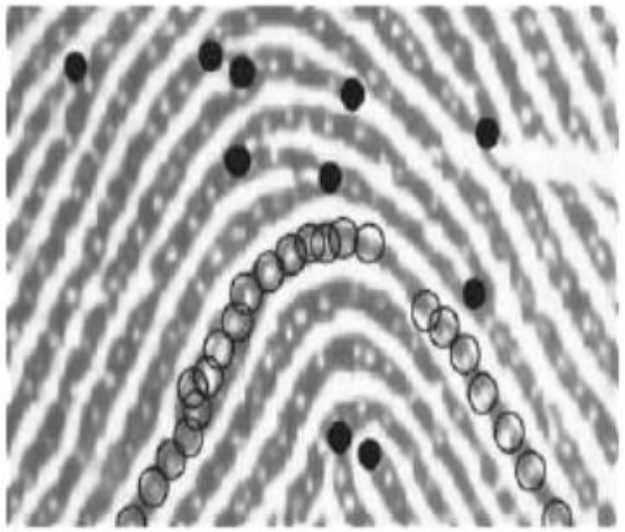
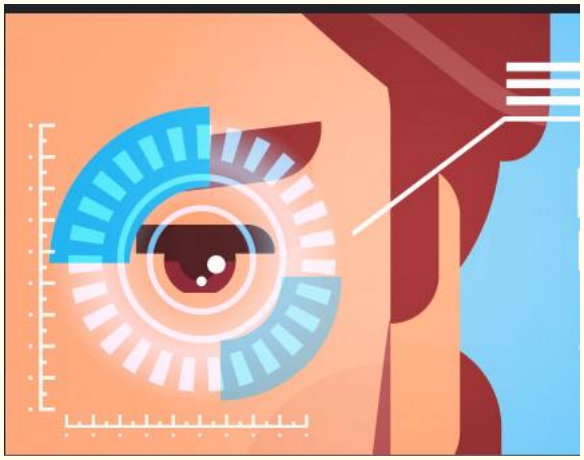


Рисунок 2 – Зображення відбитків пальців з відміченими порами, точками розгалуження і кінцевими точками

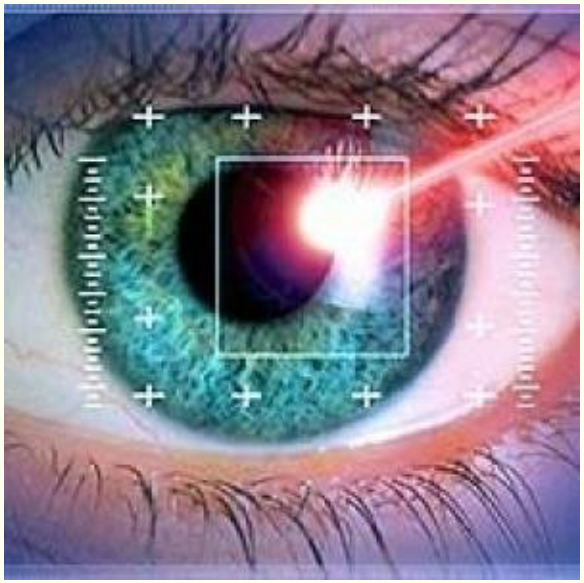
На поверхні зображення пальця можна виділити досить велику кількість дрібних деталей, за допомогою яких можна їх класифікувати, але, як правило, в системах аутентифікації використовують всього два типи деталей візерунку (особливих точок): кінцеві точки – точки, в яких "виразно" закінчуються папілярні лінії; точки розгалуження – точки в яких папілярні лінії роздвоюються. На зображенні відбитку пальця з роздільною здатністю близько 1000 dpi можна виявити деталі внутрішньої будови самих папілярних ліній. Їх розташування можна використовувати для біометричної аутентифікаї. При автоматизованому розпізнаванні відбитків пальців, на відміну від традиційної дактилоскопії, виникає значно менше проблем, пов'язаних із різними зовнішніми чинниками, що впливають на процес розпізнавання.

Аутентифікація за сітківкою ока



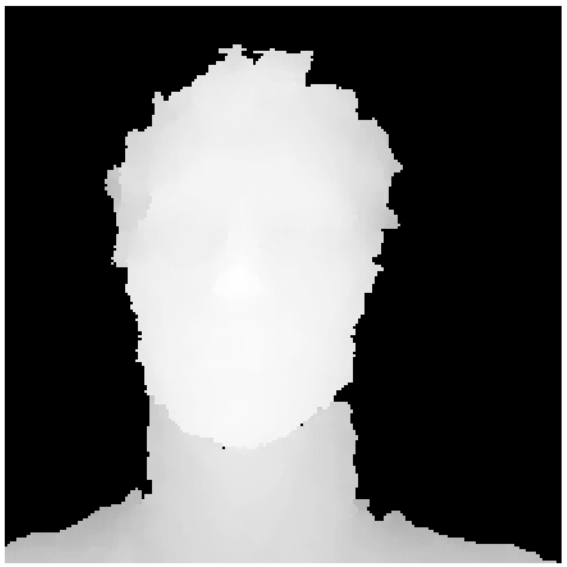
Сканування сітківки відбувається з використанням інфрачервоного світла низької інтенсивності, направленого через зіницю до кровоносних судин на задній стінці ока. Ймовірність пропуску незареєстрованого користувача при скануванні сітківки ока складає 0,0001%. При цьому передбачається, що користувачі можуть повторити процедуру аутентифікації декілька разів.

Аутентифікація за райдужною оболонкою ока



Методи ідентифікації особи за райдужною оболонкою ока побудовані за одним і тим же принципом – виділення частотної або будь-якої іншої інформації про текстуру райдужної оболонки із зображенням і збереженням цієї інформації у вигляді спеціальних кодів (для системи Дагмана (Daugman) цей код отримав спеціальну назву райдужний код (Iriscode)). Можна порівнювати коди райдужних оболонок і зберігати в базі даних. Побудова коду здійснюється в три етапи: виділення зображення райдужної оболонки із загального зображення; обробка отриманого зображення, наприклад, усунення шуму (denoising), поліпшення зображення (enhansing), у тому числі вирівнювання гістограми, усунення відблиску;

Аутентифікація за зображенням



У даному статичному методі аутентифікації будується двовимірний або тривимірний образ обличчя людини. За допомогою камери і спеціалізованого програмного забезпечення на зображенні або наборі зображень особи виділяються контури брів, очей, носа, губ і т. д., обчислюються відстані між ними й інші параметри, залежно від алгоритму, що використовується. За цими даними будується образ, що перетворюється в цифрову форму для порівняння.

Аутентифікація особи за особливостями голосу

Для того, щоб ідентифікувати абонента за голосом, необхідно мати мовний шаблон, з яким порівнюватиметься голосовий ключ, що вводиться в систему. Порівняння ключа і шаблону може проводитися в цілому або за декількома характеристиками мовного сигналу (тут, ми говоримо про цифровий мовний сигнал, що пройшов обробку і адаптований до поставленого завдання): амплітуда і потужність (гучність), часові, частотні (тембр), енергетичні, фазові характеристики. Для забезпечення простоти аналізу мовного сигналу, його попередньо піддають дискретизації з використанням частотного або Вейвлет перетворення.

Аутентифікація за динамікою рукописного підпису

Проблему аутентифікації користувача за його факсимільним підписом доцільно розглядати як дві незалежні задачі: ідентифікацію користувача лише за слідом пера автографа або за "мертвим" статичним підписом, вже наявним на документі, що перевіряється; ідентифікація автора за динамікою відтворення користувачем "живого" підпису, що вводиться ним у комп'ютер у момент ідентифікації. В першій постановці задачі мова йде про порівняння зображень, відтворених раніше в невідомій послідовності. В другій постановці – аналізуються дані про параметри коливань пера автора при відтворенні ним підпису в тривимірному просторі. Для користувача декартової системи координат (X, Y, Z) дані про динаміку відтворення підпису отримують у вигляді двох функцій часу коливань пера в площині графічного планшету X(t), Y(t) і ще одну функцію – варіації тиску пера на графічний планшет Z(t).

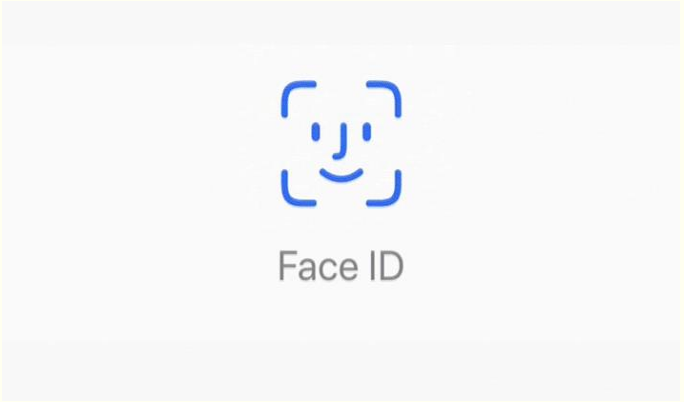
Технологія TouchID

Touch ID вбудований в кнопку «Home», покриту сапфіровим склом, яке має хороший захист від подряпин. Крім цього, дане скло виконує функцію лінзи. Навколо датчика розташоване металеве кільце, яке дозволяє визначити і активувати Touch ID без безпосереднього натиснення кнопки.

Принцип роботи TouchID

Вбудований в гаджет ємнісний КМОП -датчик сканує подушечки пальця, використовуючи розширення в 500 ppi (розмір одного пікселя складає 50 мкм), після чого розпізнає малюнок, навіть якщо палець знаходиться під різними кутами. Зашифрована біометрична інформація Touch ID зберігається тільки в так званому Secure Enclave («Безпечний анклав»). Таким чином, пристрій зберігає не зображення відбитку пальців, а його математичний образ. При цьому, відновити з цього образу відбиток неможливо. Він розташовується прямо на процесорі, що ускладнює завдання шкоди умовних зловмисників, які спробують здобути дані про відбиток пальця. Secure Enclave - це оптимізована під потреби Touch ID версія технології ARM TrustZone. Більш того, кожен окремий сканер Touch ID прив'язаний до конкретного процесора. Це означає, що при перестановці датчика від одного iPhone на інший сканер втратить свою працездатність.

Технологія FaceID



Face ID - сканер об'ємно-просторової форми обличчя людини, з встановленим сенсором (True Depth Camera або Time-of-Flight камера), що дозволяє розблокувати пристрій.

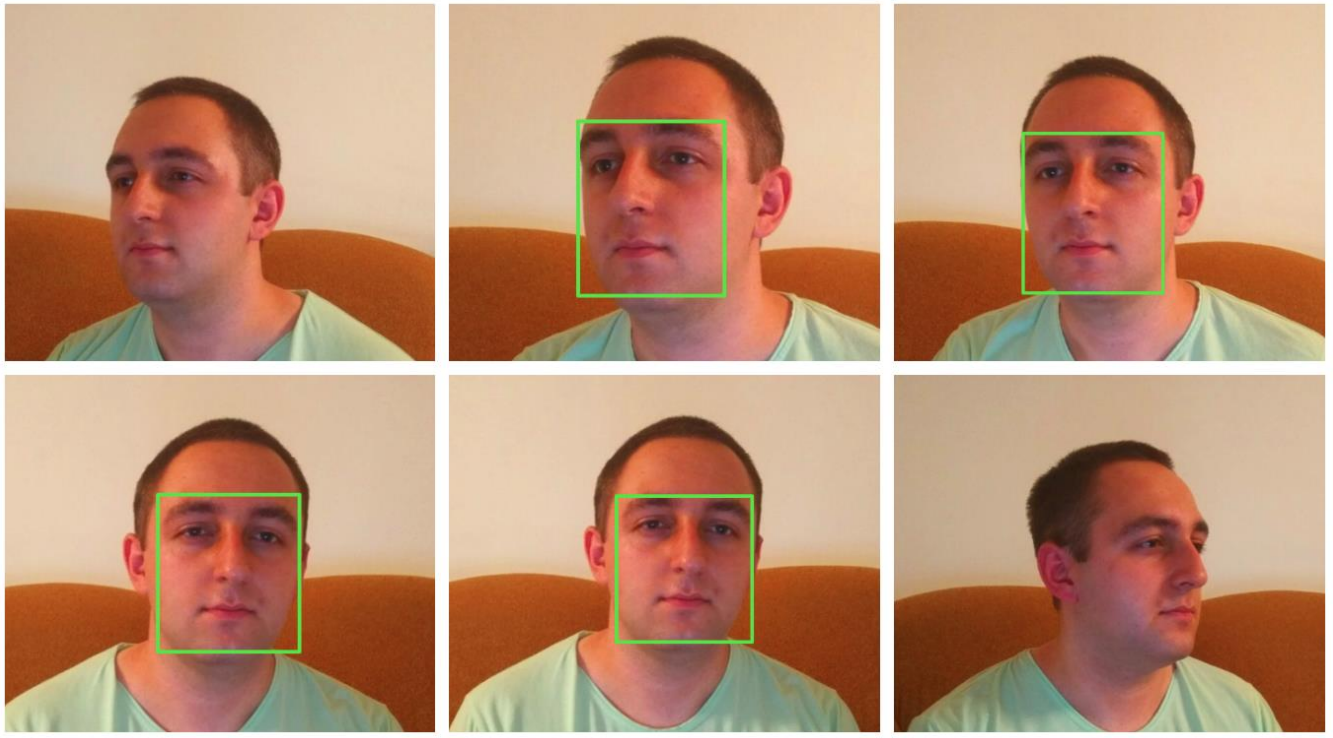
Принцип роботи FaceID

Технологія Face ID запам'ятовує зміни в обличчі за допомогою нейронних мереж в процесорі смартфона. Зображення особи користувача знімається за допомогою інфрачервоної камери, яка більш стійка до змін світла і кольору навколишнього середовища. Використовуючи deep learning, смартфон здатний розпізнати обличчя у найдрібніших деталях, тим самим "дізнаючись" власника кожен раз, коли той підхоплює свій телефон. Частота помилок надзвичайно низька 1 : 1 000 000. Перед використанням технології потрібно зареєструвати своє обличчя. Процес досить простий: користувач просто дивиться на телефон так, як робить це щодня, а потім повільно повертає голову по колу, тим самим реєструючи особа в різних позах. На цьому реєстрація закінчується, і телефон готовий до розблокування. Ця неймовірно швидка процедура реєстрації може розповісти багато про основні алгоритмах навчання.

Реалізація технології розпізнавання обличчя в мобільних додатках

Для реалізації методу розпізнавання обличчя на мобільній платформі була використана бібліотека OpenCV, у якій реалізовані такі методи як EigenFaces, FisherFaces та LBPH. Вибір OpenCV зумовлений тим, що вона реалізована на мові C++ і методи, реалізовані на базі цієї бібліотеки можуть бути скомпільовані у динамічну бібліотеку і використані при розробці додатків для самих поширених операційних систем (Android, iOS). Також цей підхід дозволить використовувати реалізацію алгоритмів і на комп'ютерах, обладнаних веб-камерою.

Демонстрація знаходження обличчя



Для початку роботи з програмою, необхідно зареєструвати своє обличчя, сфотографувавши його під різними кутами на свою веб-камеру. Розпізнати обличчя програмі дозволяє метод каскадів Хаара. Згідно нього, обличчя здатне бути розпізнаним при нахилі обличчя відносно камери не більше ніж на 30 градусів. Далі програма розпочинає аналіз фотографій та вчиться розпізнавати обличчя.

Демонстрація розпізнавання обличчя

Коли модель навчилась розпізнавати обличчя за фотографіями, можемо приступити до тестування. Тепер програма може розпізнати обличчя в живому режимі при включеній веб-камері. Зразок даної програми представлений з використанням алгоритму Local Binary Patterns Histograms (LBPH).

Успіх

Помилка

Помилка

Алгоритм Local Binary Patterns Histograms (LBPH)

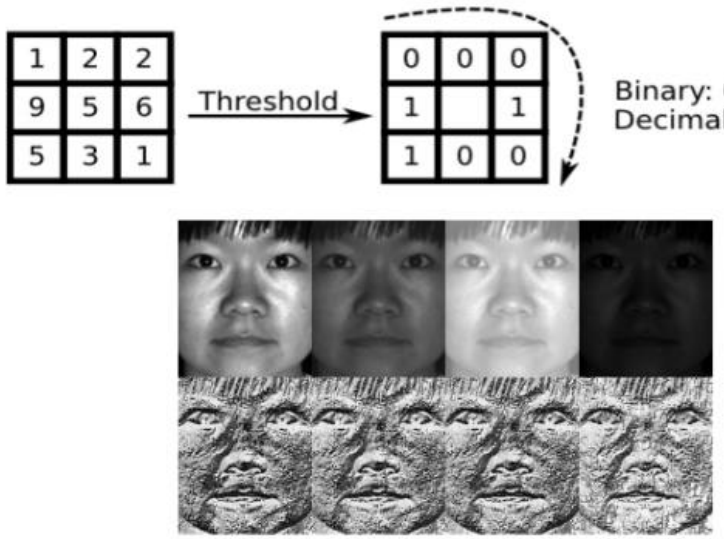
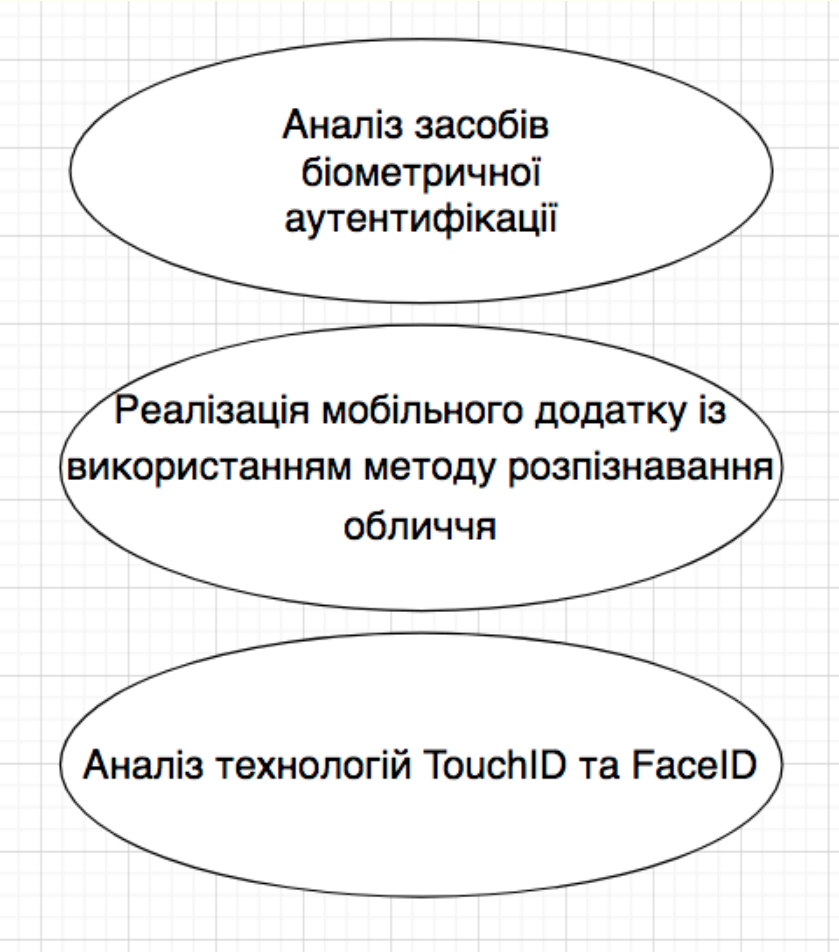


Рис – 4.3.3.1 приклад роботи LBPH

Основна ідея алгоритму - узагальнення локальної структури зображення шляхом порівняння кожного пікселя з його сусіднімі пікселями. Обираємо деякий центральний піксель. Якщо значення центрального пікселя більше від сусіднього, то записуємо "0" на місці сусіднього. Якщо ж менше - то "1". В кінцевому підсумку для кожного пікселя буде в результаті отримано восьмизначне двійкове число. Таким чином, з 8 оточуючих пікселів можно отримати 2 ^ 8 можливих комбінацій. Ці комбінації і є LBP кодами.

Висновки



Під час виконання даної роботи була проаналізовані засоби біометричної аутентифікація користувача та був обраний для реалізації і використання один із них – розпізнавання обличчя.

Також проаналізовані принципи роботи популярних засобів біометричної аутентифікації в мобільних пристроях - TouchID та FaceID.

Дякую за увагу