

**ВИСШЕ ВОЕННОМОРСКО УЧИЛИЩЕ „Н. Й. ВАПЧАРОВ“ ФАКУЛТЕТ
„ИНЖЕНЕРЕН“ - КАТЕДРА „ИНФОРМАЦИОННИ ТЕХНОЛОГИИ“**

КУРСОВ ПРОЕКТ

на тема „ПРОУЧВАНЕ И ВНЕДРЯВАНЕ НА БИОМЕТРИЧНА
АВТЕНТИКАЦИЯ ЧРЕЗ ЛИЦЕВО РАЗПОЗНАВАНЕ“

ДИСЦИПЛИНА:

„Методи и средства за автентикация“

Студент: Антон Евгениев Атанасов

Специалност: Киберсигурност

Фак. № 12621101

Дата: 10.12.2024 г.

гр. Варна

1. Въведение

Настиящият проект има за цел да подобри съществуващата технология за лицево разпознаване на мобилни устройства, като повиши сигурността дори на устройства от среден и нисък клас, които не са снабдени с необходимото оборудване за анализ на дълбочина в пространствот от или инфрачевени скенери за ефикасно и сигурно следене на човешко лице и изпълняване на проверка за жизненост. Тези устройства лесно могат да бъдат заблудени чрез снимка или видео на легитимен потребител, поставени пред камерата. Липсата на изискване за действие от страна на потребителя улеснява експлоатацията на такива системи без знанието или съгласието на легалния субект. Тъй като снимка или видео на човек могат лесно да бъдат получени в обществени пространства, подобни системи не могат да се считат за сигурни, освен ако не се въведат адекватни мерки срещу фалшификация.

Техниката, предложена в този проект, се основава на използването на предна и задна камера, налични дори при бюджетни смартфони. Те могат да се използват за едновременно извлечане на пулсовата вълна от лицето и пръста на потребителя. За извлечането на пулсовата вълна от лицето от разстояние ще бъде използвана техника за Ойлерово увеличаване на движение във видео записи, която усилва цветови промени, предизвикани от разширяването на капилярите, както и от леки движения на тялото, причинени от сърденния ритъм. Тъй като пулсовата вълна е силно индивидуална и зависима от времето и обстановката, тя може дори да служи като втори биометричен фактор (CHEN 2017). Това я прави трудна за фалшификация както за конкретен собект, така и за конкретен момент във времето, тя предоставя допълниителен фактор за сигурност по време на автентикацията.

В допълнение, биометричните системи обикновено разчитат на неизменността на физиологичните характеристики на потребителя и използват числови репрезентации, които ги представят в цифров формат. Дори ако тези кодирания са криптирани в покой, тяхното изтичане и декриптиране

компрометира сигурността на системата за целия живот на потребителя. Това се поражда от факта, че те могат да се използват за възстановяване на оригиналната характеристика, от която са били извлечени. Проектът цели да противодейства на този риск чрез използването на заменими биометрични шаблони за лицево разпознаване, които могат да бъдат използвани като временни или ротационни. Тези шаблони са модифицирани така, че да не разкриват истинска информация за лицето, от което са извлечени. В случай че бъдат компрометирани, потребителят може лесно да ги анулира и замени с нови.

Допълнително обезопасяване на шаблоните в облачна база данни или в съхранението на устройството и гарантиране на сигурността им е необходимо за сигурност дори при използване на слабо защитени, отарели или виртуализирани системи, такива с режим за отстраняване на грешки, или при декомпилация на изходния код на изпълняващата програма. С такава цел ще бъдат приложени хомоморфни криптографски алгоритми за шифриране на шаблоните - те позволяват извършване на математически операции върху данни, дори докато те са в криптиран вид, като никога не разкриват оригиналния шаблон и декриптират само резултата от съпоставянето на лицето с шаблона.

Методиката на настоящият проект предстои да бъде описана в права последователност в следващите секции на този документ.

2. Откриване и класификация на обекти в изображение и видео

За да се гарантира наличието на цели за наблюдение с растерна камера е необходим метод, който да посочи наличието на обекти в нейното полезрение, тяхната позиция и обхват в кадъра, както и увереността при класификация на целта. Тази функция се изпълнява с помощта на стандартната библиотека за компютърно зрение OpenCV. Предварително подгответи модели за визуална класификация, като “haarcascade_frontalface_alt.xml” (PISAREVSKY 2022) се

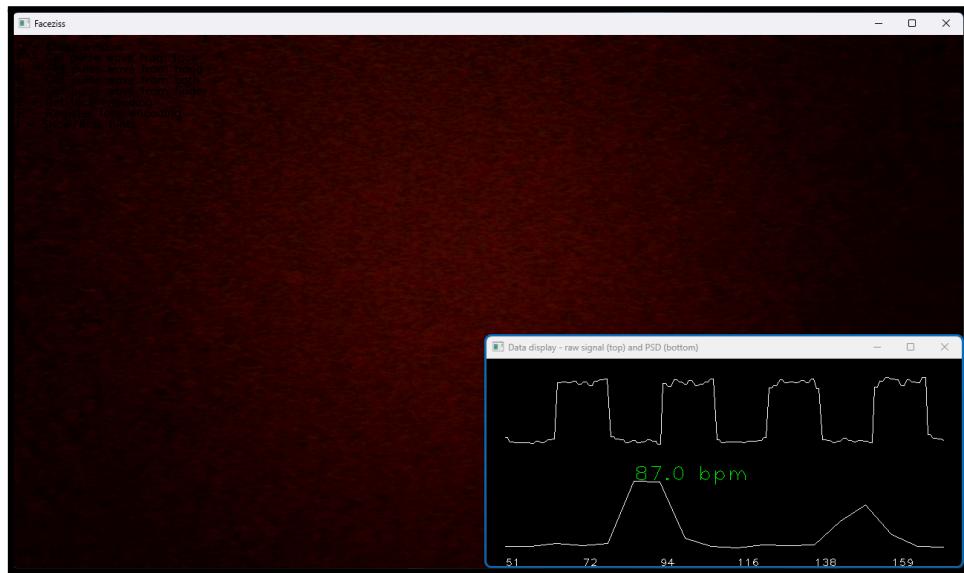
използват за засичане на човешко лице и човешка ръка във всеки кадър на камерата.

При успешно засичане на цел, се определя рамката, която съдържа изцяло обекта и се подава на програмен инструмент за анализ при нужда. В общия случай, рамката се преоразмерява до стандартен размер за да се уеднакви качеството на анализа и за да се намали изискването на ресурси по време на цифрова обработка - най-вече под формата на процесорно време, и оперативна памет.

3. Извличане на пулсова вълна

Технологията за извлечане на пулсовата вълна чрез камера на смартфон е добре установена и широко използвана в мобилни приложения за спорт и здраве. Процедурата се основава на прост, но ефективен механизъм. При лек натиск на пръста върху обектива на камерата, оптичните сензори на устройството се настройват за дълга експозиция, което позволява улавянето на достатъчно светлина, преминаваща през тъканите на пръста.

Този метод се възползва от разликите в оптичните свойства на окислената и неокислената кръв, както и от промените в обема на капилярите по време на сърдечния цикъл (Фиг. 1.). Тези промени се отразяват като вариации в интензитета на измерената светлина, което позволява директно изчисляване на относителните промени в кръвното налягане.

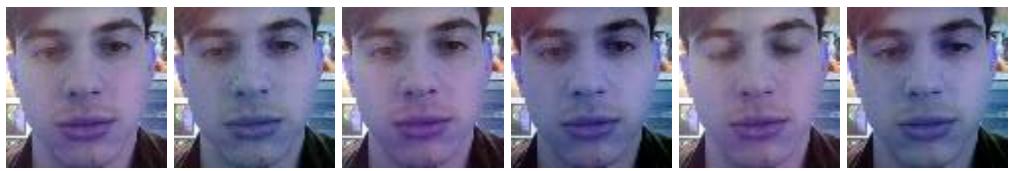


Фиг. 1. Измерване на пулсова вълна с трансформация на Фурье фърху интензитета на светлината с допрян пръст към мобилна камера

При условия на недостатъчно осветление, задната камера на смартфона може да използва вградената светкавица, ако такава е налична, за да осигури необходимото количество светлина за надеждно извлечане на пулсовата вълна.

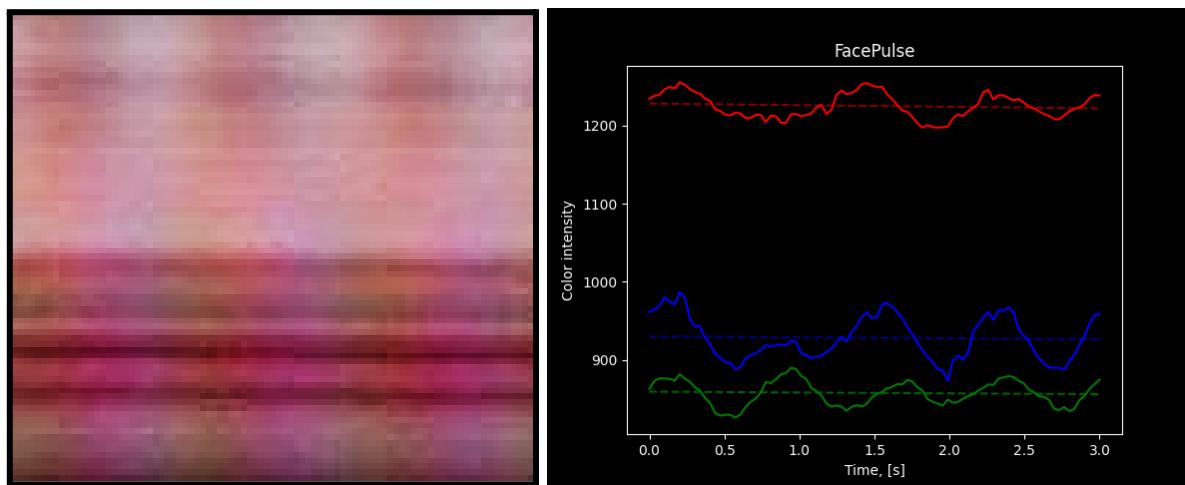
При измерване на пулсовата вълна във видео на лицето, същият подход е неефикасен поради разстоянието от сензора до кръвоснабдената тъкан, отблясъците в повърхностите както на оптиката на камерата, така и от кожата, и наличните шум и движения в кадъра. За да бъде възможен такъв анализ, се използва техника за Ойлерово усиливане на цвет и движения във видео, което може да увеличи леката промяна в оцветяването на кожата и ритмичното трептене на главата от врата, породени от сърдечните удари (DURAND 2012), (BELGACEM 2023).

Тази техника позволява селективно усиливане на определен диапазон от честоти и елиминирането на трептения, несвързани с целта на изследването (от 0.833 Hz до 2Hz, отговарящи на 50 до 120 сърдечни удъра в минута) (Фиг. 2.). Усилените честоти могат да бъдат наслагани на сумарен сигнал, който да приближи пулсовата вълна на потребителя. За целта в тази разработка се изчисляват споменатия спектър от честоти на осем поддиапазона.



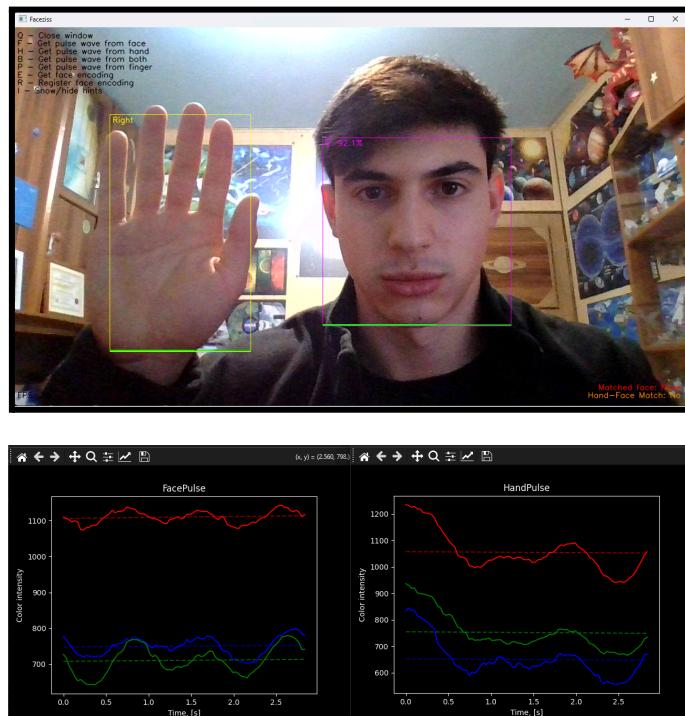
Фиг. 2. Усиливане на промяна в цветовете във видео кадри

Тъй като обработката произвежда видео, от входните кадри от камерата, за да се намали натоварването на устройството, кадрите се умалват до стандартна резолюция. След това се извлича вертикална лента от всеки кадър на изображението, който да се ползва за представителна извадка на интензитета на усилените цветове (Фиг. 3.). Поредицата от ленти образуват единствено изображение, което се сумира по редове и се разделя на цветни канали, репрезентиращи измената на всеки цвят във времето. На графиките, представящи сигнала от пулса на лицето се забелязва и ритмичната промяна на кръвното налягане (Фиг. 3.).



Фиг. 3. б) Вертикална лента за всеки кадър от видеото формира изображение с времева серия; б) времевата серия е разделена на цветни канали с интензитет на пулса

По време на разработката на проекта, поради ограничения в капацитета на оборудването в настолна вместо мобилна среда, пулсовата вълна не може да бъде взета едновременно от двата посочени източника. При работата с една камера, анализът на лицето остава непроменен на избраната за “предна” камера, докато пулсът от пръста на избраната за неналична “задна” камера се заменя с пулс, извлечен от дланта на потребителя. Чрез предварително вграден модел в използваните инструменти, подобно на засичането на лице в кадъра на камерата, се засичат и човешки ръце. Рамката на кадъра, в която са открити се отделя за анализ и се обработва със същата процедура, използвана за лицето. Двете мишени за засичане - лицето и ръката се снимат едновременно на видео, за да се гарантира, че данните са получени в един и същ момент и в еднакви светлинни условия (Фиг. 4).



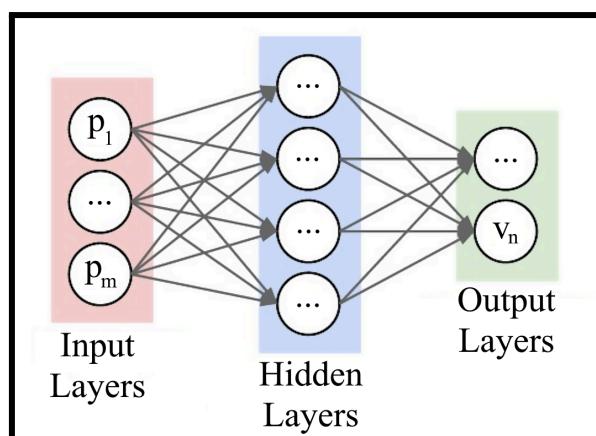
Фиг. 4. а) Засичане на лице и ръка във видео; б) извлечена пулсова вълна от лице и ръка във видео

След извличането на сигналите от видеото, се изпълнява функция за изчисляване на коефициент на корелация между съответните цветни канали в сигналите от двете камери. В съображение със изискванията за сигурност на системата и околната светлина, е необходима ръчна нагласа на праговете за съответствие между двета извлечени сигнала.

При достатъчно съответствие, проверката за жизненост и защита от фалшифициране се счита за приключена и системата навлиза в режим за разпознаване на лицето.

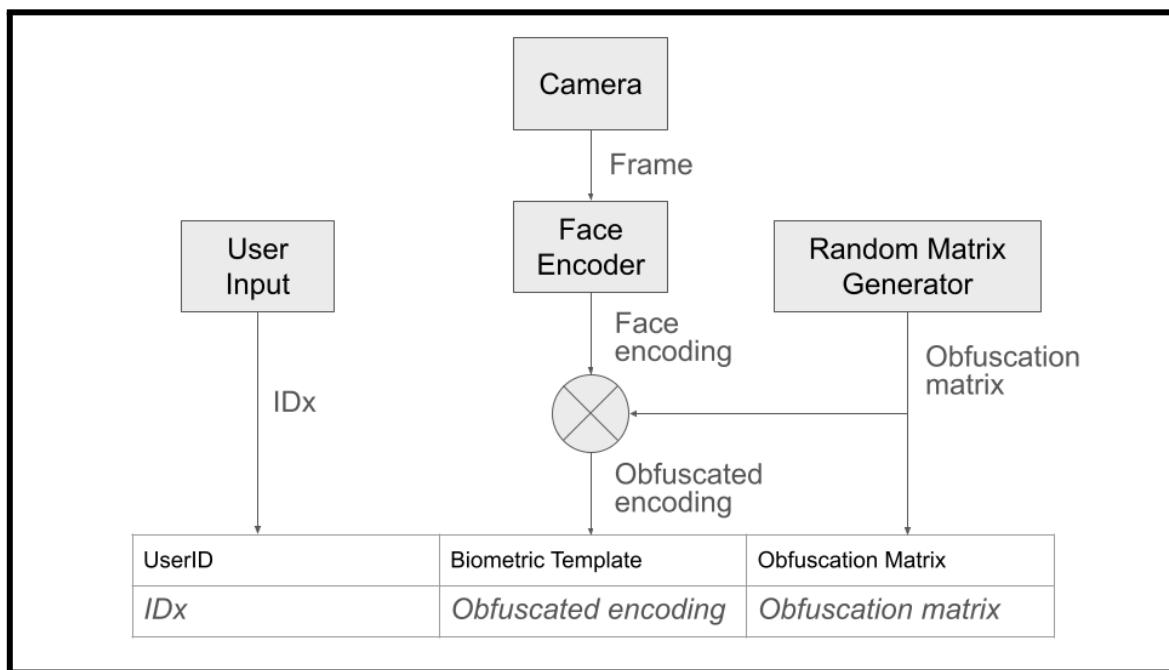
4. Лицево разпознаване

След успешно преминаване на анализа на пулсовата вълна, системата преминава към извличане на цифровата репрезентация на лицето на потребителя за целите на регистрация или автентикация. За тази задача се използва стандартната библиотека за компютърно зрение OpenCV и предварително обучен модел на невронна мрежа за извличане на характеристики на лица. Невронната мрежа генерира поредица от 128 стойности с плаваща запетая, които уникатно описват лицето на потребителя (Фиг. 5.).

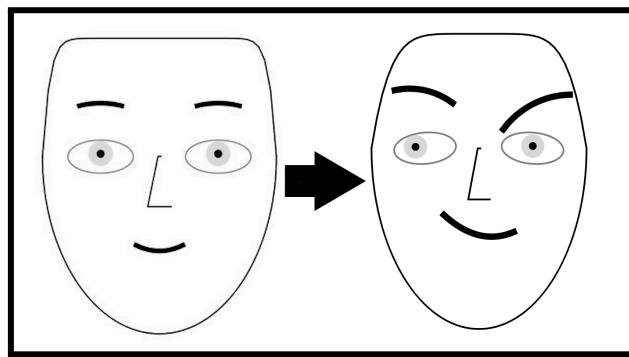


Фиг. 5. Невронна мрежа приема $m=$ брой пиксели от изображение и произвежда $n=128$ на брой параметъра, отговарящи на параметрите лицето

За повишаване на сигурността, вместо да се съхранява оригиналната цифрова репрезентация, системата генерира масив от произволни стойности за всеки нов потребител (Фиг. 6.). Тези стойности се наслагват върху оригиналната цифрова репрезентация, което обфускира характеристиките на лицето и предотвратява тяхното директно извлечане от съхранените данни (Фиг. 7.). Освен че добавя допълнителен слой сигурност, масивът от произволни стойности позволява заменяемост на шаблона в случай на компрометиране чрез замяна на стойностите и повторна регистрация на потребителя, като всеки нов шаблон ще е уникален и коренно различен от предходните.



Фиг. 6. Биометричният шаблон се обфускира с обфускационна матрица, която се прилага върху цифровата репрезентация на лицевите характеристики



Фиг. 7. Обфускираната матрица изменя образът, който може да се реконструира от биометричния шаблон

Съхранението на данните включва обфускираната цифрова репрезентация, произволния масив и идентификатор на потребителя (например име или друг уникален код). При всяка следваща заявка за достъп до системата, лицето на потребителя отново се анализира с помощта на невронната мрежа, като получената цифрова репрезентация се наслагва с уникалния масив от стойности на съответния потребител.

Проверка на съвпадението на лице в следващите употреби на системата се извършва чрез изчисляване на евклидовото разстояние между новоизвлечените параметри на лицето, наложено с всички възможни произволни масиви и записаните биометрични шаблони, репрезентирани като вектори в 128-мерно пространство. За подобряване на точността на системата може ръчно да се конфигурира праговата стойност за максимално допустимото разстояние, с цел балансиране между вероятността за фалшиво приемане и нежелан отказ от достъп.

5. Защита на данните

Цифровите данни, необходими за работата на системата за лицево разпознаване в този проект, могат да бъдат уязвими, ако се съхраняват в некриптиран вид (т.нар. открит текст). Въпреки че биометричният шаблон за автентикация е заменяем и не разкрива директно данните за лицето на

потребителя, неговото възстановяване е възможно, ако обфускационният масив и самият шаблон бъдат оznати. Това би довело до извлечане на оригиналната цифрова репрезентация на лицето и до компрометиране на системата.

Един от най-често използваните подходи за защита е съхранението на необходимите цифрови данни в криптиран вид, като те се декриптират само по време на употреба. Тази защита може да бъде реализирана чрез симетрични или асиметрични криптографски алгоритми. Въпреки това, и двата подхода изискват наличието на криптографски ключ (или двойка ключове за асиметричните алгоритми) на устройството, което създава допълнителни рискове. Ако тези ключове се съхраняват като отделен файл, те също трябва да бъдат защитени – например чрез парола на потребителя, чрез използване на вградени механизми за ограничаване на достъпа до локалните ресурси на ниво устройство или операционна система, или чрез допълнителни слоеве защита на файловата система.

Въпреки предприетите мерки, сигурността на криптографските ключове е толкова добра, колкото и сигурността на файловата система или базата данни, в която са съхранени. Рискове могат да възникнат от човешки фактори (като слаба парола), уязвимости в операционната система (например остатял софтуер), или наличие на задни вратички.

Алтернативен подход е интегрирането на уникален криптографски ключ директно в кода на програмата за автентикация. Тази техника обаче също е податлива на атаки, тъй като модерните технологии за анализ на изпълним код, включително декомпиляция и отстраняване на грешки в реално време, позволяват разкриването на такива вградени ключове. Това е особено приложимо за мобилни устройства с архитектура RISC, при която инструкциите са по-лесни за интерпретация.

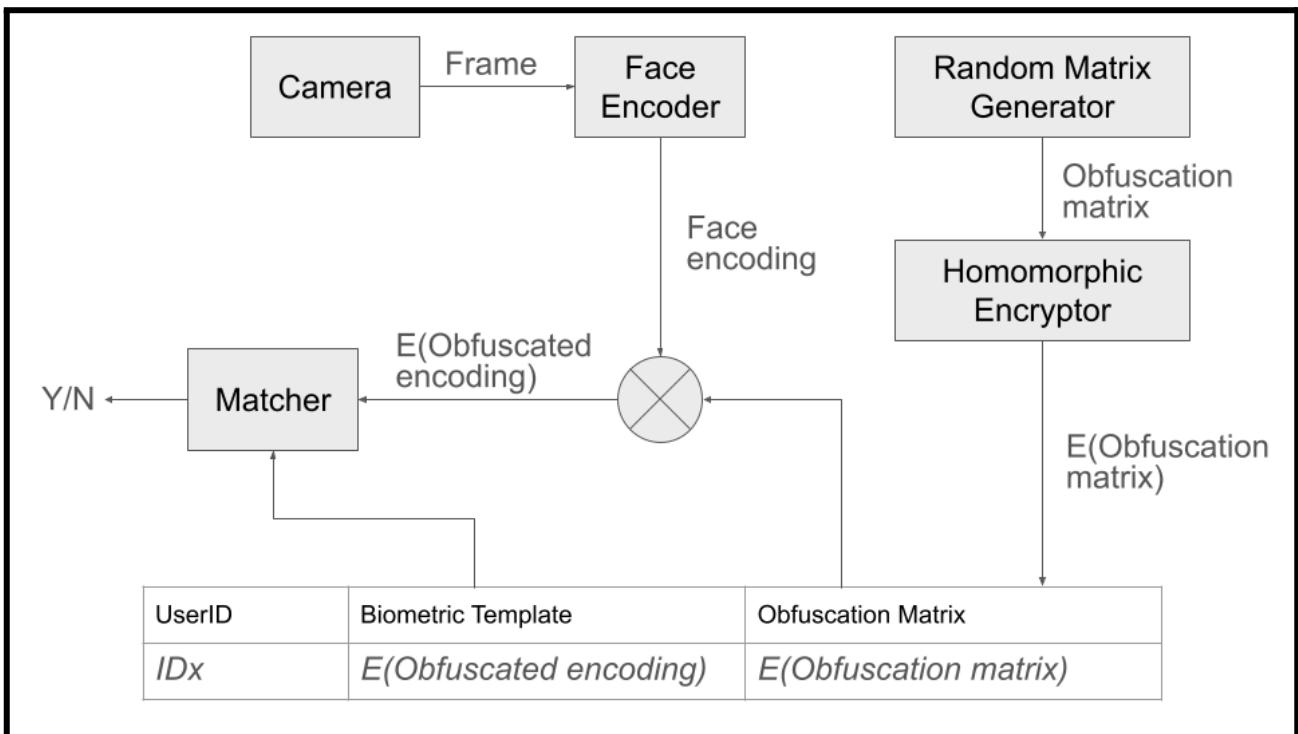
За да се минимизират рисковете, в проекта се обмисля използването на техники като хомоморфно криптиране, което позволява работа с данни в криптиран вид, елиминирайки нуждата от декриптиране по време на анализ

(BODDETI 2019). Този подход осигурява допълнителен слой защита срещу неоторизиран достъп и компрометиране на данните.

Хомоморфните криптографски алгоритми разширяват възможностите на традиционните асиметрични методи, като позволяват аритметични операции директно върху шифротекст без необходимост от дешифриране. Резултатът от тези операции е идентичен или приблизителен до този, който би се получил при работа с открит текст, преди или след декриптиране. Хомоморфните алгоритми се класифицират на два основни типа: частично хомоморфни, които поддържат ограничен набор от операции, и изцяло хомоморфни, които поддържат всички възможни аритметични операции.

Основните операции включват събиране, умножение, булеви операции между шифротекстове или между шифротекст и открит текст, както и извличане на статистически показатели от шифровани данни без тяхното разшифроване. В реални приложения най-често се използват частично хомоморфни алгоритми, тъй като изцяло хомоморфните алгоритми, макар и концептуално мощни, изискват значителни изчислителни ресурси и към момента са неефективни за работа в реално време на мобилни устройства.

При използването на подходящ хомоморфен криптографски алгоритъм в този проект е възможно биометричният шаблон за лицово разпознаване и обфускационният масив да бъдат трайно криптирани еднократно веднага след създаването им със секретен ключ. Този ключ не се съхранява локално в устройството, което допълнително подобрява сигурността. Всички операции, свързани с обфускиране на лицеви данни и сравнение с шаблона, се извършват изцяло върху шифротекст. Единствено крайният резултат от сравнението – дали потребителят е автентичен – се разкрива в открит вид (Фиг. 8.).



Фиг. 8. Схема на лицево разпознаване със заменими биометрични шаблони и хомоморфно шифриране

Този подход значително намалява риска от изтичане на чувствителна информация, включително частни криптографски ключове, които биха могли да компрометират цялата система. Така се осигурява високо ниво на защита за биометричните данни на потребителя, без това да влияе на ефективността на системата в реално време.

6. Следващи стъпки

Крайната цел на този проект е да подобри сигурността на системите за автентикация чрез лицево разпознаване, като ги направи приложими за мобилни устройства от среден и нисък клас. За постигането на тази цел е необходимо изчислителното натоварване да бъде съобразено с техните хардуерни ограничения, включително ARM-базирана архитектура, ограничен ресурс от оперативна памет и ниска енергийна консумация.

Текущият етап на развитие представлява демонстрация на разработените технологии върху настолен компютър с x86-базиран процесор, използващ множество нишки за обработка. В настоящата версия числовите операции не са оптимизирани за изпълнение в реално време, което ограничава тяхната ефективност в мобилна среда.

Първата стъпка към адаптиране на инструмента за мобилни устройства е оптимизацията на изчислителното натоварване чрез изместване на статичните операции за зареждане и изграждане на структури от данни извън основния работен процес на програмата. Следващата стъпка е имплементирането на паралелизация и разпределение на задачите между централния процесор и графичния ускорител на мобилната архитектура. Например, невронните мрежи и обработката на видео кадри могат да бъдат централизирани в графичния ускорител, докато криптографските операции и основната логика на програмата остават в централния процесор.

Въпреки че методиката за хомоморфно криптиране и изпълнение на аритметични операции върху шифротекст е описана в документацията, тази функционалност все още не е напълно имплементирана в текущата демонстрация. Това предстои да бъде интегрирано като допълнителна стъпка в развитието на системата.

Настоящото състояние на програмата представлява съвкупност от модули и библиотеки, написани на програмния език Python. Проектът е с отворен код и може да бъде изпълнен чрез локално инсталлиран Python интерпретатор чрез повикване на скрипта “faceziss.py” в основната директория – стандартен метод за разработка, но неефективен за използване на мобилно устройство. Освен това, графичният интерфейс е разработен за работа с настолна периферия, което го прави неподходящ за мобилни приложения.

Следващите стъпки включват рефакториране на потребителския интерфейс с интеграция на модерна система за дизайн, като например Android Material UI, както и компилиране на програмата в изпълним код за съответната

операционна система. Това ще позволи по-ефективно изпълнение, по-добро потребителско изживяване и възможност за внедряване на решението в реална мобилна среда.

7. Заключение

Разработеният проект демонстрира потенциала за прилагане на иновативни технологии за лицево разпознаване и криптографска защита в мобилни устройства с ограничени ресурси, като същевременно очертава конкретни стъпки за оптимизация и реализация в реална среда. Предстоящите етапи включват интеграция на хомоморфно криптиране, адаптация на графичния интерфейс и компилиране на кода за мобилни платформи, което ще гарантира сигурност, ефективност и потребителско удобство.

8. Литература

CHEN, Yimin, Jingchao SUN, Xiaocong JIN, Tao LI, Rui ZHANG, et al. Your face your heart: secure mobile face authentication with photoplethysmograms. Online. IEEE INFOCOM 2017 - IEEE Conference on Computer Communications, 2017, pp. 1–9. ISSN 978-1-5090-5336-0. Available from:

<https://doi.org/10.1109/INFOCOM.2017.8057220>.

PISAREVSKY, Vadim. opencv/data/haarcascades at master · opencv/opencv. Online. GitHub. 2022. Available from:

<https://github.com/opencv/opencv/tree/master/data/haarcascades>. [viewed 2024-12-10].

WU, Hao-Yu, Michael RUBINSTEIN, Eugene SHIH, John GUTTAG, Frédo DURAND, et al. Eulerian video magnification for revealing subtle changes in the world. Online. People | MIT CSAIL. 2012. Available from:

<https://people.csail.mit.edu/mrub/evm/>. [viewed 2024-12-10].

BELGACEM, Hussem. GitHub - hbenbel/Eulerian-Video-Magnification: Eulerian Video Magnification for colors and motions magnification. Online. GitHub. 2023.

Available from: <https://github.com/hbenbel/Eulerian-Video-Magnification>. [viewed 2024-12-10].

BODDETI, Vishnu. Secure face matching using fully homomorphic encryption. Online. 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), 2019. ISSN 2474-9699. Available from: <https://doi.org/10.1109/BTAS.2018.8698601>.

DUC, Nguyen, and Bui MINH. Your face is NOT your password: Face Authentication ByPassing. Online. Black Hat Briefings, vol. 4 (2009), no. 158. Available from:

<https://www.blackhat.com/presentations/bh-dc-09/Nguyen/BlackHat-DC-09-Nguyen-Face-not-your-password.pdf>.

M. A, Dabbah, Woo W. L, and Dlay S. S. Secure authentication for face recognition. Online. 2007 IEEE symposium on computational intelligence in image and signal processing, 2007, pp. 121–126. Available from:

<https://doi.org/10.1109/CIISP.2007.369304>.