МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра комп'ютерних наук

«До захисту допущено»
В.о. завідувача кафедри
Оксана ШОВКОПЛЯС
_____
(підпис)
грудня 2024 р.

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня магістр

зі спеціальності 122 «Комп'ютерні науки»

освітньо-професійної програми «Інформатика»

на тему: Інформаційна технологія підвищення надійності біометричної аутентифікації

здобувача групи ІН.м-32 Косюка Михайла Михайловича

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Михайло КОСЮК
(підпис)

Керівник Борис КУЗІКОВ
доцент,
кандидат технічних наук, доцент

_____
(підпис)

Суми – 2024

Сумський державний університет
Факультет електроніки та інформаційних технологій
Кафедра комп'ютерних наук

«Затверджую»
В.о. завідувача кафедри
_____ Оксана ШОВКОПЛЯС
(підпис)

ІНДИВІДУАЛЬНЕ ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістра

зі спеціальності 122 «Комп'ютерні науки», освітньо-професійної програми «Інформатика»
здобувача групи ІН.м-32 Косюка Михайла Михайловича

1. Тема роботи: Інформаційна технологія підвищення надійності біометричної аутентифікації затверджую наказом по СумДУ від *«03» грудня 2024 року № 1257-VI*
2. Термін здачі здобувачем кваліфікаційної роботи *до 06 грудня 2024 року*
3. Вхідні дані до кваліфікаційної роботи _____
4. Зміст розрахунково-пояснювальної записки (перелік питань, що їх належить розробити) *1) Аналіз проблеми предметної області, постановка й формування завдань дослідження. 2) Проектування технології для підвищення надійності біометричної аутентифікації 3) Вибір програмних засобів та реалізація прототипу технології. 4) Реалізація демонстраційного додатку 5) Валідація технології та аналіз результатів.*
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)_____
6. Консультанти до проекту (роботи), із зазначенням розділів проекту, що стосується їх

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв

7. Дата видачі завдання «____» _____ 20 ___ р.

Завдання прийняв до виконання _____ Керівник _____
(підпис) (підпис)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Назва етапів кваліфікаційної роботи	Термін виконання	Примітка
1	*Аналіз проблеми предметної області, постановка й формування завдань дослідження*	01.09.2024	
2	*Проектування технології для підвищення надійності біометричної аутентифікації*	11.10.2024	
3	*Вибір програмних засобів та реалізація прототипу технології*	07.11.2024	
4	*Реалізація демонстраційного додатку*	25.11.2024	
5	*Валідація технології та аналіз результатів*	29.11.2024	
6	*Оформлення пояснювальної записки до кваліфікаційної роботи*	06.12.2024	

Здобувач вищої освіти _____ Керівник _____
(підпис) (підпис)

АНОТАЦІЯ

Записка: 70 стр., 23 рис., 1 додаток, 52 використаних джерела.

Обґрунтування актуальності теми роботи – Тема кваліфікаційної роботи є актуальною, оскільки присвячена розв'язанню важливої практичної задачі посилення надійності біометричної аутентифікації, що є важливою у великій кількості сфер та сценаріїв використання.

Об'єкт дослідження – процес біометричної аутентифікації

Предмет дослідження – моделі та методи підвищення надійності біометричної аутентифікації

Мета роботи – розробка інформаційної технології підсилення надійності багатофакторної авторизації.

Методи дослідження — методи побудови моделей нейронних мереж, алгоритми виявлення аномалій, евристичні алгоритми.

Результати — розроблено інформаційну технологію для посилення біометричної аутентифікації та реалізовано прототипи основних функціональних компонентів технології, а саме введення біометричного пароля жестами обличчя та виявлення аномалій міміки, реалізовано демонстраційний додаток для взаємодії із ними. Створено датасет для задачі класифікації жестів обличчя. Проведено валідацію роботи функціональних компонентів на реальних даних.

БІОМЕТРИЧНА АУТЕНТИФІКАІЯ, ПОВЕДІНКОВА БІОМЕТРІЯ, НЕЙРОННІ МЕРЕЖІ, ВИЯВЛЕННЯ АНОМАЛІЙ, PYTHON

ЗМІСТ

ВСТУП

Задача аутентифікації особистості була і є актуальною протягом, щонайменше, декількох століть, починаючи із тривіальних методів, таких як сургучеві печатки та підпис на паперах у далекому минулому, закінчуючи найсучаснішими технологіями, як, наприклад, апаратні ключі безпеки [12] та біометрична аутентифікація, все це для досягнення однієї базової мети – переконатися в тому, що інформація, дія або намір надходить від конкретної очікуваної особи та може бути сприйнята із довірою. Одночасно із методами аутентифікації, закономірним чином, розвиваються і методи її підробки із метою імперсонувати довірену особу у власних інтересах, частіше за все – в злочинних цілях. Процес розвитку методів аутентифікації та її підробки неперервний та не має визначеного закінчення таким самим чином, як розвиток замків та способів їх зламу.

На сьогоднішній день одним із найпоширеніших методів аутентифікації, а у деяких сценаріях використання навіть найпоширенішим, є біометрична аутентифікація [1]. Розмір ринку технологій біометричної аутентифікації на 2021 рік сягав 18 мільярдів доларів та має прогнозоване стрімке зростання до 54 мільярдів до 2028 року (майже 300% за 7 років)[5]. За даними Cisco Duo’s Trusted Access Report [3] за 2022 рік частка мобільних телефонів із апаратними можливостями для біометричної аутентифікації сягала 81% на основі аутентифікацій, проведених із більш ніж 50 мільйонів пристроїв. Така популярність біометрії пояснюється її простотою використання, у більшості випадків користувачу не потрібно виконувати ніяких дій, а сам процес займає долю секунди, та високою безпекою, оскільки підробка біометрії є відносно складною задачею. Іншою стороною медалі цієї популярності є те, що цей метод аутентифікації використовується як основний і найчастіше єдиний, створюючи високу зацікавленість у пошуку та використанні його вразливостей.

Об’єктом дослідження даної роботи є процес біометричної аутентифікації. Предметом роботи є моделі та методи підвищення надійності

біометричної аутентифікації. За мету поставлено дослідити вразливі фактори біометрії загалом та визначити ті із них, що потребують додаткової уваги, в результаті розробивши технологічні методи для посилення надійності цих факторів; розуміючи дуже високу складність розробки та найголовніше тестування технологій біометричної аутентифікації у їх кінцевому вигляді, готовому до використання в реальному житті – ця робота сконцентрована на дослідженні та створенні концепції такої технології, більше, ніж створення готового продукту.

Для досягнення мети сформульовано наступні задачі роботи:

1. Збір, систематизація й узагальнення матеріалу для використання у кваліфікаційній роботі
2. Проведення досліджень та аналізу предмету, постановка технічних задач
3. Розроблення концепції рішення, підбір та дослідження технологій для реалізації
4. Розробка прототипу технології та створення демонстраційної програми

Дана робота складається зі вступу, аналітичного огляду, постановки задачі, вибір методу розв’язання поставленої задачі, опису програмного забезпечення інформаційної системи, висновків, списку використаних джерел та додатків.

1 АНАЛІТИЧНИЙ ОГЛЯД

1.1 Аналіз предметного середовища

Предметним середовищем даної роботи є аутентифікація, а точніше – аутентифікація користувача, тобто людини, що є важливим зауваженням, оскільки на сьогоднішній день термін аутентифікації також розповсюджується на аутентифікацію програмних додатків між собою та інші види, в яких використовуються нелюдські особистості. Розглядаючи предметне середовище аутентифікації важливо розуміти деякі ключові терміни та поняття, які будуть розглянуті далі.

Перш за все, необхідно встановити чітке розуміння терміну аутентифікації людини. Попереднім та невід'ємним кроком аутентифікації є поняття ідентифікації. Ідентифікація, достатньо очевидно, означає визначення конкретної особистості, яка намагається пройти аутентифікацію, в різних випадках крок ідентифікації користувача може відбуватися:

- явно, наприклад, при аутентифікації на веб-сайті користувач в першу чергу вводить свій юзернейм (електронну пошту), за якими система аутентифікації веб-сайту може їх ідентифікувати;
- неявно, наприклад, при спробі розблокувати стандартний мобільний телефон, що не передбачає існування кількох користувачів одночасно, особистість, яка проходить аутентифікацію, автоматично ідентифікується як єдиний власник телефона.

Сама аутентифікація людини (користувача) – це процес який підтверджує, що людина (користувач) насправді є тим, ким стверджує бути сама [6]. Іншими словами – це процес надання людиною (користувачем) певного доказу, який однозначно підтверджує, що ця людина (користувач) є тією особистістю, якою вона себе ідентифікує.

Наступною важливою частиною є доказ особистості, який згадується у визначенні аутентифікації, такі докази, зазвичай, називаються факторами аутентифікації. Більш чітко, фактор аутентифікації – це чітко визначена

окрема категорія доказів особистості, поєднана певною спільною природою. Традиційно, визначаються наступні три основні фактори аутентифікації користувача [10][11]:

- щось, що людина знає (SYK – Something You Know);
- щось, що людина має (SYP – Something You Possess);
- щось, чим людина є (SYA – Something You Are).

Додатково до цього, в деяких випадках часто визначаються ще два додаткових фактори аутентифікації [8][11]:

- де людина знаходиться (WAY – Where You Are);
- щось, що людина робить, знає як зробити (WYD – What You Do).

Далі розглянемо три основних та два додаткових фактори більш детально.

SYK із великим відривом є найпоширенішим фактором, оскільки також є найстаршим із усіх факторів аутентифікації. Фактори знання – це певна інформація, яку, теоретично, може знати тільки сам користувач. Абсолютною класикою SYK факторів є паролі, що завжди були в центрі уваги інформаційної безпеки. Паролі представляють собою комбінації символів із певних алфавітів, чим більший розмір алфавіту символів та чим більша довжина комбінації – тим більш надійним, традиційно вважається пароль. Іншими прикладами факторів знання є:

- PIN-коди – можна вважати підвидом швидких коротких паролів, традиційно – комбінації цифр довжиною в 4-8 символів;
- графічні ключі – традиційно є послідовністю ліній, якими поєднуються точки у матриці 3 на 3 точки, утворюючи певну фігуру;
- контрольні питання – певні тематичні питання, правильну відповідь на які може знати тільки сам користувач, часто використовується в ролі допоміжного фактору.

В той час, як SYK методи, а особливо паролі є найпоширенішим способом аутентифікації, в силу довгого часу існування та великої кількості застарілих систем, цей фактор є найпростішим для зламу або викрадення [6].

Обговорюючи саме тему паролів, доречно згадати організацію під назвою FIDO Alliance (“Fast Identity Online” Alliance), що є неприбутковою технологічною асоціацією із багатьох учасників із головною задачею – зменшити, або навіть повністю замінити глобальну залежність від паролів. Двома найголовнішими причинами через які FIDO вважає важливим зменшення залежності від паролів є:

- висока вразливість до атак соціальної інженерії, таких як фішинг, що у наш час робить паролі дуже вразливими;
- поганий user experience, пов’язаний із створенням та введенням надійних паролів. Іншими словами, більшості користувачів не подобається придумувати та запам’ятовувати складні паролі, слідуючи всім рекомендаціям надійності, що в більшості випадків призводить до критичних порушень безпеки на користь простоті, таких як використання однакового пароля всюди та спрощення пароля для легшого запам’ятовування.

Подібні причини призвели до зменшення популярності паролів в останні роки та збільшення використання різного роду PIN-кодів, що є простішими та швидшими для запам’ятовування та введення, проте вони є менш надійними ніж паролі у прямому порівнянні, тому ця зміна є більш складною, що буде розглянуто далі.

Другим базовим фактором аутентифікації є SYP. Фактор власності базується на ідеї використання певних предметів, які, теоретично, завжди фізично знаходяться разом із користувачем та можуть бути використані певним чином для підтвердження особистості. Розглядаючи предметну область аутентифікації ширше, можна сказати, що пред’явлення паспорту в державних установах також є прикладом аутентифікації за фактором власності. Втім, повертаючись до світу аутентифікації в програмному забезпечені, види цих факторів є трохи іншими, хоча, можна згадати певні приклади використання документів і тут – державний застосунок Дія, переніс традиційну концепцію пред’явлення паспорту в цифровий простір за

допомогою аутентифікації через сканування паспорту ID-картки за допомогою NFC мобільного телефона [13]. Цей приклад показує наскільки широким може бути використання фактору SYP, особливо для конкретних випадків, фактично необхідно визначати будь-який предмет, що фізично знаходиться із певною групою користувачів та розробити технологію підтвердження наявності цього предмета, наприклад, корпоративний сектор вводить у використання для працівників окремі корпоративні апаратні ключі, такі як YubiKey. Тим не менш, до найбільш поширених типів фактору власності, які можуть бути застосовані до більшості сучасних користувачів без додаткової підготовки, належать:

- мобільний телефон – безумовно є найпоширенішим типом, факт власності в даному випадку найчастіше підтверджується за допомогою одноразових кодів OTP, що генеруються спеціальним додатком, встановленим на конкретний телефон, або їх відправки за допомогою SMS;
- банківські картки – більшість я яких мають вбудований NFC.

Фактор власності в цілому є більш сучасним, в порівнянні із фактором знання, та такі його види як підтвердження власності мобільного пристрою за допомогою OTP, однозначно є менш вразливими до атак соціальної інженерії [8].

Останнім з основних факторів аутентифікації є фактор притаманності – SYA, іншими словами – біометричний фактор. Суть цього фактору полягає у підтвердженні особистості користувача за допомогою перевірки певної біометричної характеристики, яка, теоретично, може бути притаманна тільки конкретному користувачеві. В той час як використання цього фактору може здаватись дуже сучасною технологією, насправді, такий його вид як відбиток пальця почав систематично використовуватись не тільки для аутентифікації а й для ідентифікації особистості наприкінці XIX століття, коли були засновані точки Гальтона – набір специфічних точок на відбитку пальця, за якими можна однозначно ідентифікувати особистість [14]. В XX столітті Федеральне Бюро

Розслідувань в США розробило стандарти для технології розпізнавання відбитків пальця, що передбачає збирання приблизно 30 специфічних точок на відбитку. Іншими найпоширенішими типами фактору притаманності є такі біометиричні риси як:

- орієнтири обличчя – набір із багатьох точок на обличчі, що разом формують унікальну сітку, що може бути використана для задач аутентифікації;
- райдужка ока;
- голос.

Перевагою біометричних факторів є їх висока унікальність, звичайно, коли маються на увазі саме перераховані вище із них, що означає високу точність та надійність фактору в цілому, і хоча, наприклад, останні дослідження технології розпізнавання відбитку пальця [15] за допомогою штучного інтелекту показують, що унікальність саме оброблених даних (набір точок), не є абсолютною, шанси помилки біометричної аутентифікації на практиці є незначними. Головними ж перевагами біометрії є її:

- простота використання, в більшості випадків користувачеві не потрібно робити нічого, технологія розпізнавання та аутентифікації спрацьовує автоматично;
- незалежність від психічного, емоційного або фізіологічного стану користувача.

Втім, як і у випадку з іншими факторами, хоча підробка або викрадення біметричного фактору є досить складною задачею – вона не є неможливою, особливо із розвитком генеруючих нейронних мереж. Більше того, ризик такого викрадення, або підробки є непомірно вищим за інші фактори по одній простій причині – змінити притаманні біометричні фактори дуже складно або неможливо.

Як можна побачити, ні один із базових факторів аутентифікації не є достатньо надійним в сучасних реаліях. Для створення сильної системи

аутентифікації необхідне поєднання як мінімум двох базових факторів аутентифікації [11]. Саме тому протягом останніх років все більшу популярність набирає MFA. MFA (Multi Factor Authentication), мультифакторна аутентифікація – це тип аутентифікації, при якому послідовно перевіряються як мінімум два, або більше базових та додаткових факторів аутентифікації, в разі провалу хоча б одного з них, весь процес аутентифікації вважається проваленим. Популярним підвидом MFA є 2FA, що використовує конкретно два фактори.

Мультифакторна аутентифікація дозволяє використовувати кожний фактор як додатковий шар захисту для інших, як було розглянуто вище, кожний із факторів індивідуально має свої вразливості та недоліки, проте поєднання факторів разом дозволяє нейтралізувати багато із них. Напевно найпопулярнішим видом використання MFA є 2FA із використанням фактору знання та фактору власності (рідше – притаманності), саме таку аутентифікацію зараз можна побачити в багатьох корпоративних кейсах та у найбільших IDP (Identity Provider), таких як Google та Microsoft. Причиною для цього скоріше за все є те, що саме ця комбінація є найпростішою з точки зору всіх користувачів. Паролі, як найбільш традиційний спосіб аутентифікації продовжують існувати, не зважаючи на всі недоліки, з іншого боку, фактор власності, найчастіше мобільного телефона, може бути використаний у більшості випадків і робить увесь процес аутентифікації набагато надійнішим. Іншою популярною комбінацією, що більше використовується для локальної аутентифікації на пристроях для їх розблокування є фактор знання та біометричний фактор, при чому в даному випадку використання паролів переходить до використання більш простих у використанні PIN-кодів, це можливо за рахунок високої надійності біометрії, складності PIN-кодів достатньо для того, щоб забезпечити прийнятну загальну надійність.

Серед сучасних способів ще більшого посилення аутентифікації є такий її тип як адаптивна аутентифікація. Адаптивна аутентифікація, також відома

як ризико-орієнтована аутентифікація – це механізм, головною ідеєю якого є аналіз додаткових факторів поведінки користувача для вирахування певної оцінки ризику, цей механізм динамічно змінює вимоги до процесу аутентифікації, спираючись на оцінку ризику в конкретний момент часу [6]. Наприклад, якщо ризик мінімальний механізм може запросити тільки фактор знання при процесі аутентифікації, при вищому ризику, додати до процесу фактор власності, або навіть провести повну MFA. Саме тут до загальної картини входять додаткові фактори аутентифікації, що згадувалися вище. В залежності від сфери застосування та цільових користувачів, будь-які параметри, що можуть бути автоматично відстежені певним пристроєм, можуть використовуватись для оцінки ризику при процесі аутентифікації. Фактор поведінки WYD найчастіше відстежує такі параметри як IP адреса, з якої пристрій підключений до мережі, сам пристрій, що використовується для аутентифікації, час доби певної дії, траєкторія руху курсора та інші [6][8]. Єдиним додатковим фактором, що часто виділяється окремо є фактор місцезнаходження WYA, оскільки він є ключовим у таких випадках як викрадення або втрата пристрою, для визначення геолокації використовується приблизна локація за допомогою IP адреси, або більш точна, за допомогою GPS [8]. Всі ці фактори та параметри дозволяють утворювати інтегровані патерни поведінки користувача та використовувати відхилення від цих патернів для оцінки ризику при спробі аутентифікації.

Основною перевагою адаптивної аутентифікації є не стільки пряме збільшення надійності аутентифікації, хоча це теж має місце за рахунок використання додаткових вхідних даних, скільки підвищена зручність для користувача, при низькому ризику, процес мультифакторної аутентифікації може спрощуватись до використання єдиного фактору, що, очевидно, є більш комфортним для користувача, ніж постійне проходження повного процесу MFA.

Нарешті, беручи до уваги фокус цієї роботи на біометрії, розглянемо більш детально технології біометричної аутентифікації. Для розуміння

актуальності роботи, важливо розуміти поширеність та актуальність конкретних методів та технологій, для цього розглянемо чотири найсуттєвіших компанії в цій сфері – Google, Samsung, Apple та Microsoft. За наявною статистикою за 2023 рік по США, найпоширенішими сценаріями використання біометрії із відповідними долями є [16]:

- розблокування мобільних пристроїв – 43%;
- вхід до банківських облікових записів – 18%;
- онлайн покупки – 11%.

Зважаючи на те, що більшість онлайн-банкінгу реалізована за допомогою мобільних додатків, які для біометричної аутентифікації використовують вбудовані апаратні можливості пристроїв та величину долі сценарію використання для їх розблокування – очевидно, що саме апаратні технології мобільних пристроїв є найсуттєвішою сферою використання біометрії, що також підкреслює вибір технологічних компаній вибраних для аналізу вище.

Найпоширенішими модальностями біометричної аутентифікації по всьому світу є, безумовно, розпізнавання відбитку пальця, яким користуються, приблизно, 70% та розпізнавання обличчя, яким користуються відповідно, приблизно, 40% людей, що мають доступ до біометричних технологій [17], важливо відмітити, що відносно поширеним є випадок використання обох типів одним користувачем, наприклад, на різних пристроях. Менш поширеними технологіями є розпізнавання голосу та розпізнавання райдужки ока, приблизно 20% кожна.

Apple має найбільш чітку ситуацію із біометричними технологіями. Apple має свої власні технології для двох найбільш популярних типів біометрії, відбитку пальця та обличчя, що називаються Touch ID та Face ID відповідно. Touch ID є старшою біометричною технологією Apple, яка вперше була впроваджена в 2013 році в моделі iPhone 5s та подальших моделях [18]. В 2017 році в iPhone X вперше була представлена технологія Face ID і до теперішнього часу, уже 7 років, продовжує використовуватись у всіх моделях iPhone та iPad за виключенням двох бюджетних моделей iPhone SE та iPad Mini

[19]. Враховуючи загальне стабільне поступове зростання об’єму випущених телефонів, починаючи із 2013 року [20], співвідношення кількості моделей що використовують Touch ID та Face ID та той факт, що середнім значенням довжини циклу заміни телефонів за 2023 рік є 2.67 роки [21], можна вважати, що принаймні 70-80% сучасних користувачів Apple використовують телефони із Face ID. Тож у випадку Apple наявний дуже виражений тренд в сторону використання біометрії обличчя, за даними самої компанії ймовірність помилкового розпізнавання Face ID є в 20 разів нижчою за Touch ID [19].

Google є оригінальним розробником операційної системи Android і крім того має власну лінійку телефонів Google Pixel, які, хоча і мають дуже малу долю від загальних об’ємів Android смартфонів, однозначно створюють вплив на інших виробників, оскільки випускаються виробником самої ОС. На відміну від Apple, абсолютно всі моделі Google Pixel за виключенням одного минулого експерименту, використовують відбиток пальця для біометричної аутентифікації, більше того, абсолютна більшість користувачів Google віддають перевагу саме цій технології [22]. Такий же тренд можна побачити і у Samsung, який є найбільшим виробником Android смартфонів у світі [23]. Основною біометричною технологією, що використовується у телефонах Samsung є підекранний ульразвуковий сканер відбитку пальця, що також позиціонується компанією як найбіьлш надійна біометрична аутентифікація, в той же час в багатьох телефонах доступне і сканування обличчя, проте ця технологія є менш популярною та надійною, тому що в абсолютній більшості випадків, на відміну від Apple Face ID, не робить сканування обличчя у всіх трьох вимірах [24]. Ще менш поширеною технологією, яку можна зустріти тільки в флагманських моделях є сканування райдужки ока. Загалом можна стверджувати, що Android телефони, включно із найбільшими компаніями виробниками, покладаються на сканування відбитку пальця.

Останнім великим гравцем є Microsoft, що є розробником операційної системи Windows, в тому числі для ноутбуків, що є більш цікавими в рамках біометричної аутентифкації, як мобільні девайси. Windows є найпоширенішою

операційною системою для ноутбуків, займаючи 75% ринку [25]. Як і у випадку з Google, Microsoft має власну невелику лінійку ноутбуків, проте як розробник ОС має значний вплив на інших виробників. У 2015 році у версії Windows 10 Microsoft додали нову технологію мультифакторної аутентифікації Windows Hello [26], що вперше включала біометричні методи аутентифікації на системному рівні. Windows Hello, як і у випадку інших компаній, підтримує сканування відбитку пальця та обличчя для біометричної аутентифікації, варто відмітити, що в разі з розпізнавання обличчя технологія вимагає тримірного сканування із використанням інфра-червоного світла, що є більш надіним типом, на кшталт того, що використовується у Apple Face ID. Хоча у випадку ноутбуків вбудована біометрична аутентифікація є менш розвиненою, ніж у мобільних телефонів, вона поширюється достатньо активно. На даний момент не існує точної статистики, проте поверхнево проаналізувавши ринок ноутбуків, можна припускати, що приблизно 15% моделей сучасних ноутбуків мають апаратні можливості для сканування обличчя Windows Hello та приблизно 40% - для сканування відбитку пальця. Також варто підкреслити, що ця інформація є актуальною тільки для сучасних моделей та враховуючи те, що цикл заміни ноутбуків, зазвичай значно довший ніж у телефонів та може бути більшим за 4 роки [29], можна обґрунтовано припускати, що загальний відсоток пристроїв із підтримкою біометричних технологій є значно нижчим.

Підсумовуючи аналіз біометричних технологій в мобільних пристроях, може здатись, що відбиток пальця є найбільш актуальною технологією, оскільки вона стабільно присутня в усіх великих технологічних компаній, а 72% усіх мобільних телефонів світу використовують ОС Android [28], що в більшості покладається саме на відбиток пальця. В той час як це є правдою, слід звернути увагу на величезну різницю долей використання мобільних телефонів в конкретних групах країн – так, в Європі відсоток Android телефонів складає вже 65%, а Apple – 34%, в країнах Океанії (Австралія, Нова Зеландія та інші) Apple займає 52%, а в країнах Північної Америки – 62% [28].

Додатково до цього, можна бачити, що сектор Windows ноутбуків, в якому активно розвивається біометрична аутентифікація, робить певні ставки на використання технологій сканування обличчя, а після пандемії COVID-19, розпочався глобальний тренд безконтактної біометрії, якою не являється відбиток пальця [29]. Таким чином, хоча використання відбитку пальця в якості біометрії є найбільш масовим всесвітньо, що робить це актуальною технологією, враховуючи певні тренди та локалізовані регіональні сфери використання мобільних пристроїв в країнах «колективного Заходу», можна стверджувати, що сканування орієнтирів обличчя є не менш актуальною технологією в цих регіонах та має значні шанси стати найбільш поширеною глобально.

1.2 Огляд атак на біометрію

Для того, щоб розробити технологію, яка дозволить посилити біометричну аутентифікацію необхідно обов’язково розуміти існуючі типи та шляхи атак на неї.

Типова архітектура системи біометричної аутентифікації складається з шести основних компонентів, які можна побачити на рисунку 1.1, цими компонентами є [31]:

1. сенсор – задачею якого є зчитування фізичної біометричної проби, такої як відбиток пальця, або орієнтири обличчя;
2. екстрактор характеристик – витягує із необробленої біометричної проби певні ключові характеристики, які залежать від цільової біометричної, що використовуються для процесу аутентифікації;
3. вхідний зразок – що є проміжним представленням обробленої цифрової біометричної інформації, готової для перевірки;
4. модуль порівняння – задачею якого є виконання певного алгоритму порівняння вхідного зразку із оригінальним зразком;

5. модуль прийняття рішень – який може виконувати різноманітну логіку, використовуючи результат модуля порівняння та інші вхідні дані для видачі кінцевого рішення по результату аутентифікації;
6. додатково до цього виділяється база даних, що зберігає оригінальні зразки біометрії, що використовуються для порівняння.

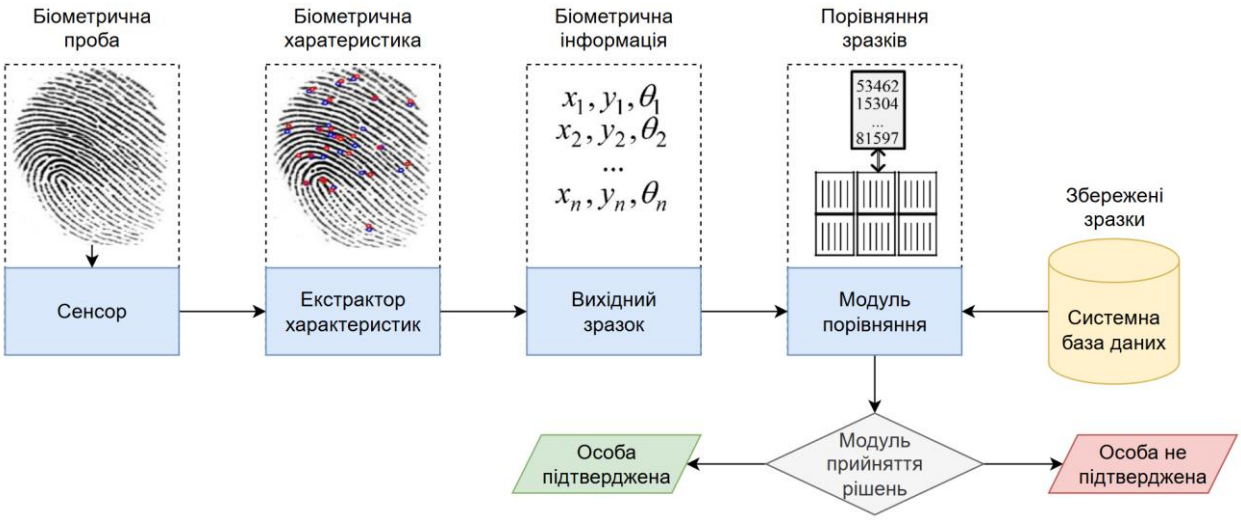


Рисунок 1.1 – Типова архітектура біометричної системи [31]

Шляхи та типи атак на біометричну аутентифікацію по своїй структурі відображають базову архітектуру системи аутентифікації. Загалом всі атаки поділяються на дві основних групи:

- презентаційні атаки;
- атаки програмного забезпечення.

Презентаційні атаки пов’язані виключно зі спробами зламати аутентифікацію напряму через сенсор, надаючи сфабриковані біометричні ознаки до нього, цей тип атак потребує здебільшого роботи із фізичними об’єктами для підробки ознак. Атаки програмного забезпечення, навпаки від презентаційних, використовують складні програмні інструменти та навички, для того щоб експлуатувати вразливості аутентифікаційної системи з метою її компрометації, теоретично ця група атак може бути застосована як до всіх архітектурних компонентів системи, так і на проміжках між ними [31]. Більш детально структуру атак можна побачити на рисунку 1.2.

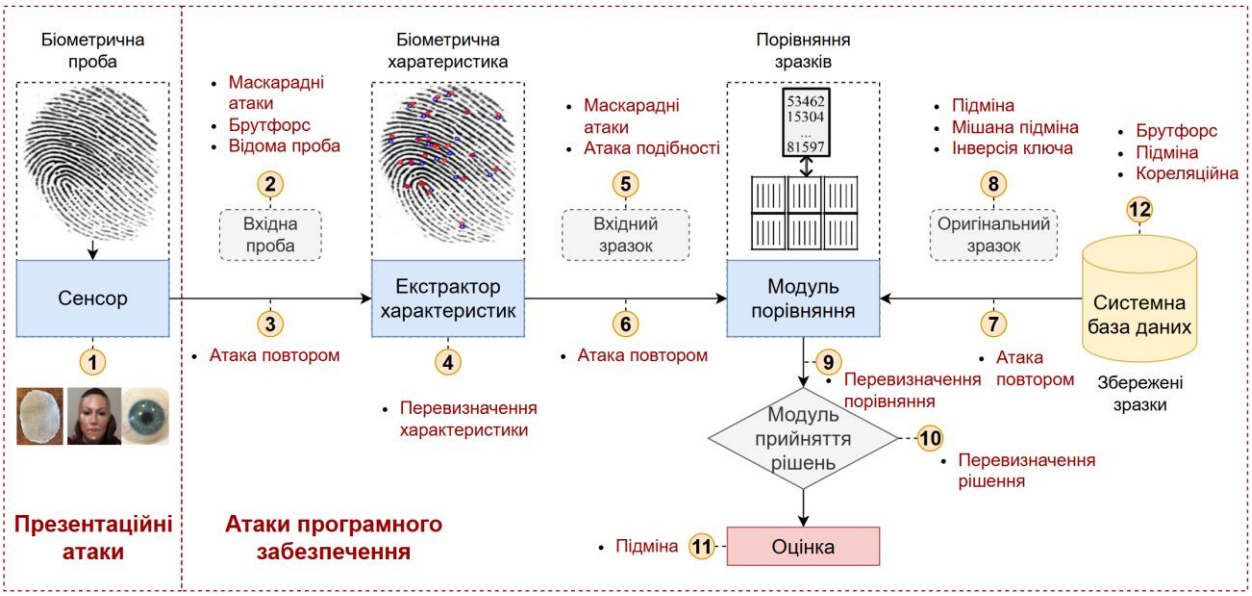


Рисунок 1.2 – Структура атак на системи біометричної аутентифікації [31]

Презентаційні атаки можуть бути націлені на різноманітні біометричні риси, проте найчастіше вони направлені на відбиток пальця, райдужку ока та обличчя [31]. В першу чергу, вони поділяються за вимірністю сфабрикованого фізичного об’єкту, який використовується для атаки – відповідно 2D та 3D атаки, що використовують відповідно двовимірні та тривимірні об’єкти. До 2D атаки можна далі поділити на використання зображення та відео, до яких відносяться наступні приклади [30]:

- друковане фото – цільове обличчя друкується на папері, варто відмітити, що папір може мати різноманітну фактуру, що може ефективно використовуватись для зламу аутентифікації;
- модифіковане друковане фото – має ту саму ідею, що і звичайний друк, але в цьому випадку фото може гнутися або вирізатися в певних місцях для досягнення кращого результату.
- цифрове фото – цільове обличчя показується на дисплеї телефона/планшета/ноутбука, що є дуже простим способом, проте має слабкості зі сторони фактури;
- відбиток на тонкій плівці – відбиток пальця наноситься на тонку плівку, що прикладається до сенсора, може бути віднесений до двомірних атак, оскільки є майже повністю пласким [32];

- відео – в даному випадку можуть бути присутні рухи обличчя, кліпання очима, які необхідні для обходу деяких захисних механізмів;
- відео діпфейк – може бути використаний подібно до звичайного відео, але в цьому випадку може бути цілenаправлено записано будь-яке відео для показу, наприклад, із конкретного ракурсу або із конкретною активністю обличчя.

До тривимірних презентаційних атак відносяться наступні приклади [30]:

- маска – є, напевно найпопулярнішим типом тривимірних атак, нападник одягає маску, яка відображає цільове обличчя, що може бути зробленою із різних матеріалів та залишати певні ділянки обличчя, такі як очі, рот непокритими для наявності активності обличчя;
- скульптура – є схожою на маску, але за рахунок більшого об’єму може в точності відповідати цільовому обличчю та використовувати більше різноманіття матеріалів та фактур;
- макіяж – ймовірно є найбільш небезпечною атакою, оскільки окрім майже точного зовнішнього співпадіння із цільовим обличчям, дозволяє зберегти більшу частину міміки, до макіяжу також відноситься використання контактних лінз, що можуть змінювати колір та форму райдужки ока;
- тривимірний друкований відбиток – в даному випадку двовимірне зображення відбитку пальця використовуються для створення тривимірної моделі, що в поєднанні з сучасними технологіями 3Д-друку, можуть створювати майже повні копії відбитків та обманювати найсучасніші сенсори [33].

Однакові типи атак програмного забезпечення, як можна бачити на рисунку 1.2, можуть бути націлені на різні компоненти, або проміжні дані. Серед найпоширеніших, можна виділити наступні їх приклади [31]:

- атака повтором – ключова ідея атаки повтором полягає в перевикористанні попередньо використаної успішної біометричної

проби або зразка, ця атака частіше застосовується на етапах передачі даних між компонентами;

- підміна – отримання доступу до різних компонентів для підміни результатів або вхідних даних на необхідні нападнику, наприклад, при підміні оцінки, що видає модуль прийняття рішень, можна досягти успішної аутентифікації;
- маскарадні атаки – включають у себе два основних типи – інверсія, ідея якої полягає у використанні знання про роботу екстрактора характеристик або іншої внутрішньої функціональності для створення синтетичних біометричних проб, та хибне прийняття, при якому створюються великі набори даних із певними відомими ключовими характеристики, які дозволяють успішно обманути систему;
- відома проба – при цій атаці нападнику відомі деякі оригінальні зразки із бази даних, що може бути використано для експлуатації процесу перетворення зразків;
- інверсія ключа – атака, що націлена на зворотне отримання криптографічних ключів, що використовуються для шифрування інформації в базі даних для подальшої атаки;
- кореляційна атака – використовує порівняння декількох сховищ зразків, або зразків із різних систем, що дозволяє знайти співпадіння між ними та розрахувати ключ, що використовуються для шифрування.

В той час як атаки програмного забезпечення є дуже небезпечними, оскільки вони можуть призводити до зламу цілих систем біометричної аутентифікації або бути націленими на організації або групи людей, презентаційні атаки складають не меншу небезпеку, особливо для типових користувачів. Причиною цього є той факт, що презентаційні атаки використовує єдиний публічно відкритий компонент систем аутентифікації – сенсор, а отже не потребують додаткових навичок та витрат на злам будь-яких програмних заходів безпеки, що є абсолютно необхідним для атак

програмного забезпечення, більше того, в багатьох випадках реальна ціна презентаційної атаки є доступної майже для кожної людини із достатньою мотивацією, а необхідні вхідні дані такі як обличчя, або навіть фото відбитків пальців можуть бути знайдені в інтернеті або отримані нескаладними способами. Тому хоч презентаційні атаки і мають набагато менший радіус ураження (найчастіше тільки одна особа) їх відносна простота та доступність робить їх максимально небезпечними. У підтвердження цього судження можна згадати найвідоміші випадки успішного зламу систем біометричної аутентифікації на мобільних пристроях. У 2017 році команда Bkav змогла зламати Apple Face ID на iPhone X за допомогою 3Д маски, створеної на основі двовимірних зображень цільового обличчя і ціною до 200$ [34]. Навіть після додавання Apple додаткових механізмів захисту, Face ID була зламана знов у 2019 році за допомогою додаткового використання темних окулярів [35]. Розпізнавання райдужки ока в Samsung Galaxy S8, було зламано в 2017 році, за допомогою використання макету ока із роздрукованими зображеннями райдужки, наклеєними на нього [32]. Навіть один із найсучасніших сканерів відбитку пальця в Samsung Galaxy S10, що використовує технологію ультразвукового сканування, був обманутий 3Д макетом пальця, створеним на основі фото відбитку пальця власника на скляному стакані [36]. Головний фактор, що поєднує всі ці випадки та багато інших – використання презентаційних атак.

Іншою важливою проблемою, що є непрямою вразливістю біометричної аутентифікації є психологічна довіра користувачів надійності цього фактора, в результаті чого додатковий фактор знання в багатьох випадках перетворюється на елементарний пін код, часто із очевидною комбінацією цифр, це означає, що загальний злам пристрою, не зважаючи на наявність надійної біометрії стає набагато простішим та піддається атакам соціальної інженерії [37].

1.3 Огляд існуючих рішень для посилення біометрії

Беручи до уваги попередній розділ, сконцентруємо увагу на рішеннях для захисту від презентаційних атак. Загалом, можна сказати, що ідеєю цих рішень є використання певної альтернативної або додаткової вхідної інформації, що дозволяє імплементувати більш складну логіку модуля прийняття рішень.

Найпоширенішою категорією механізмів для захисту від рукотворних презентаційних атак є аналіз текстури (texture analysis). Ці механізми засновані на отриманні текстурних характеристик обличчя за допомогою камери та подальшого аналізу, що визначає чи схожі ці текстурні характеристики на справжню шкіру, або більше схожі на папір чи інші штучні матеріали, з яких створюються маски. Найпопулярнішим методом текстурного аналізу є LBP (локальні бінарні патерни), який апроксимує малі локальні ділянки зображення до одного числа за допомогою попіксельного порівняння та використовує, далі всі локальні ділянки поєднується та віддаються до методу опорних векторів, що визначає чи є зображення реальним обличчям чи рукотворною презентаційною атакою [30].

Другим найпопулярнішим механізмом є виявлення руху (motion detection), основною ідеєю цих методів є відстеження певних рухів обличчя або фону. Одним із методів є оптичний потік (optical flow), він дозволяє відстежувати напрям та швидкість руху певних точок обличчя для виявлення презентаційних атак. Іншим методом є використання заднього фону, де, наприклад може відстежуватись різниця швидкості та напрямку руху обличчя та фону, або простим порівнянням фону до та після виявлення обличчя у кадрі, що може допомогти при презентаційних атаках за допомогою фото [30].

Виявлення ознак життя є іншою категорією методів, що основана на відстеженні конкретних ознак притаманних живому обличчю, до таких ознак відносяться моргання очей, або навіть пульсація чи потік крові в обличчі, що може бути поміченим через зміну кольорових каналів зображення, оскільки

при пульсації крові в обличчі, відбиття світла від нього періодично змінюється [30].

Для захисту від діпфейк та інших динамічних атак також використовується машинне навчання, ці методи використовують рекурентні та згорткові нейронні мережі для виявлення певних характеристик або поведінки. Найпоширенішим способом роботи цих механізмів є виявлення аномалій із узагальненим доменом, недоліком цих методів часто є вразливість до нових атак, в той час як вони добре справляються із відомими атаками.

Загалом важливо згадати два види біометричної аутентифікації – фізіологічна біометрія та поведінкова біометрія [32]. В близькому минулому та на даний момент, перша є найбільш поширеною, як було видно у попередніх розділах, більшість виробників персональних пристроїв інтегрували сенсори для сканування основних біометричних рис, таких як обличчя, відбиток пальця чи райдужка ока. Проте кількість, різноманітність та витонченість атак зростає як і випадки зламу тієї чи іншої біометричної аутентифікації. Фізіологічна біометрія, в першу чергу, призначена для використання в повноцінних процесах мультифакторної аутентифікації, але заради простоти користування, часто стає єдиним фактором аутентифікації, або, як було сказано вище в огляді атак, навіть спричиняє спрощення інших факторів аутентифікації, роблячи загальну систему аутентифікації слабшою. На основі всіх цих причин та проблем все більшої популярності може набрати поведінкова біометрія, що звертає увагу не на самі біометричні риси а їх динамічну поведінку або поведінку людини загалом, що в більшості випадків може надавати додаткову інформацію для прийняття рішень, а зчитування цієї біометрії може відбуватись непомітно для користувача одночасно із перевіркою фізіологічних рис.

1.4 Узагальнення аналізу

Беручи до уваги проведений аналіз предметної області, можна констатувати наступні висновки. Біометрична аутентифікація є найбільш

популярним типом аутентифікації у світі і стає все більш поширеним, при цьому, більш конкретно, використання розпізнавання орієнтирів обличчя є другою найпоширенішою всесвітньо біометричною характеристикою, вже зараз займає перше місце в певних регіонах, та має великі шанси стати найбільш поширеною у світі. Із наявних проблем, розпізнавання обличчя піддається великій кількості презентаційних атак, певна кількість з яких є успішними; використання мультифакторної аутентифікації в найпоширеніших сценаріях, як розблокування персональних пристроїв, спрощується на користь зручності користувача, одночасно перекладаючи велику відповідальність на біометрію та, іноді, послабляючи фактор знання в результаті дії людського фактору. В той час, як повна мультифакторна аутентифікація, безперечно, є найбільш надійним рішенням, актуальною задачею є посилення саме біометричного фактору.

В таблиці 1.1 нижче підсумовано всю статистику, знайдену під час аналізу, яка використовувалась в процесі судження та вибору направлення досліджень.

Таблиця 1.1 – Статистика

Статистична величина		**Значення**	**Регіон**
Мобільні телефони із апаратними можливостями для біометричної аутентифікації		81%	Глобально
Використання біометрії для	розблокування мобільних пристроїв	43%	США
	вхід до банківських акаунтів	18%	
	онлайн покупки	11%	
Поширеність модальностей біометричної аутентифікації	Відбиток пальця	70%	Глобально
	Орієнтири обличчя	40%	
Частка телефонів Apple з підтримкою Face ID		70-80%	Глобально
Частка ноутбуків Windows з біометрією обличчя		<=15%	Глобально

Продовження табл. 1.1

Статистична величина		**Значення**	**Регіон**
Частка мобільних пристроїв за ОС	Android	65%	Євпропа
		48%	Океанія
		37%	Північна Америка
	IOS (Apple)	34%	Євпропа
		52%	Океанія
		62%	Північна Америка

1.5 Постановка первинних задач

Метою цієї роботи є дослідження та розробка прототипу технології посилення біометричної аутентифікації. На основі проведеного аналізу, цільовою модальністю біометрії для посилення було обрано орієнтири обличчя, що має велику актуальність, зважаючи на тренди розвитку та певні регіони.

Беручи до уваги існуючі стандартні технології біометричної аутентифікації, що достатньо повно покривають базові задачі перевірки фізіологічної біометрії є сенс зосередитись на розробці технології, що зможе працювати на їх основі, додатково посилюючи та розширюючи їх.

Розуміючи високу складність реалізації та тестування повноцінних систем біометричної аутентифікації, практична частина цієї роботи зосереджуватиметься на двох основних частинах:

- Розробка прототипу додаткового механізму підвищення надійності біометричної аутентифікації орієнтирів обличчя
- Створення додатку для наочної демонстрації основних принципів роботи механізму

Оскільки прототип додаткового механізму біометричної аутентифікації не є готовим продуктом або додатком чи навіть інтеграцією до конкретного

сценарію використання, визначення детальних функціональних вимог для цієї частини роботи не є можливим на цьому етапі розвитку – заснування функціональних частин механізму для подальшого уточнення, інтеграції з конкретними базовими технологіями аутентифікації, конкретними сценаріями використання чи пристроями і є сенсом роботи. Виходячи з цього більш точні функціональні вимоги до механізму та відповідно до демонстраційного додатку для програмної реалізації будуть сформовані після розділу 2, що зосереджуватиметься на дизайні функціональних частин механізму.

Все ж, зважаючи на результати аналізу та базове розуміння механізмів аутентифікації орієнтирів обличчя, можна визначити наступні високорівневі вимоги:

1. механізм повинен зменшувати вразливість у випадку ігнорування користувачем фактору знання;
2. механізм повинен зменшувати вразливість до презентаційних атак;
3. механізм повинен інтегрувати поведінкову біометрію для надання додаткових даних для процесу аутентифікації та його загального посилення;
4. механізм повинен працювати з відео данними в реальному часі;
5. механізм не має зосереджуватись на конкретній ОС, пристрої або сценарії використання.

2 РОЗРОБКА ТЕОРЕТИЧНИХ ОСНОВ ТЕХНОЛОГІЇ

2.1 Загальна ідея та структура механізму аутентифікації

Оскільки основною метою цієї роботи є додаткове посилення біометричної аутентифікації, розробка повного механізму аутентифікації була б нераціональною. Як згадувалось у підсумках попереднього розділу, уже зараз вбудовані технології біометрії обличчя у персональних пристроях, як, наприклад Apple Face ID або Windows Hello, є досить просунутими та вже пройшли неабиякий шлях еволюції, тому створення цієї основи з нуля було б дуже складною та невиправданою задачею, хоча і мало б деякі переваги. З цих причин ця робота буде зосереджена на створенні додаткового plug-in механізму, який зможе посилювати уже існуючі базові системи біометричної аутентифікації. Більше того, такий форм-фактор, в теорії, дозволить застосовувати цей механізм для різних систем і задач.

Для задоволення первинних задач цієї роботи, механізм буде являти собою гібрид із двох факторів аутентифікації, що будуть посилювати базову систему із біометричним фактором орієнтирів обличчя, таким чином неявно реалізуючи мультифакторну аутентифікацію. По-перше, механізм буде розпізнавати та використовувати послідовності базових жестів обличчя в якості пароля, додаючи до системи фактор знання, одночасно вирішуючи задачі зменшення вразливості через ігнорування цього фактору та зменшення вразливості до презентаційних атак. По-друге, механізм виконуватиме виявлення аномалій міміки під час захоплення жестів обличчя, користуючись даними, отриманими під час початкового створення паролю. Ця логіка, фактично, є фактором поведінкової біометрії, який хоч і не підпадає під класичне визначення мультифакторної аутентифікації, але так само надає додатковий вимір для прийняття рішень.

Рисунок 2.1 показує високорівневу структуру технології. Загалом, додатковий механізм працює паралельно із базовою системою аутентифікації, отримуючи вхідні дані напряму із вбудованої камери пристрою і узгоджуючи свої рішення із базовою системою.

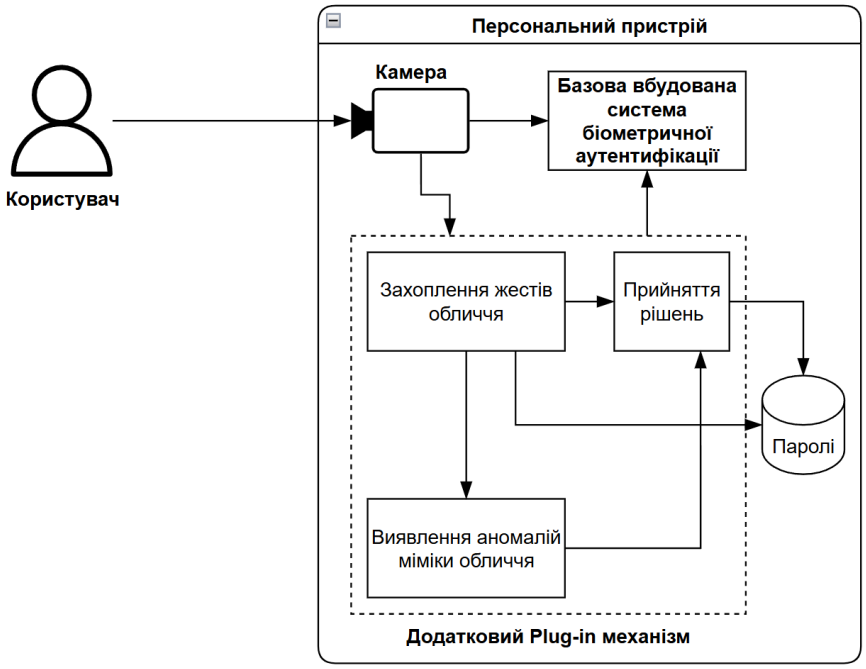


Рисунок 2.1 – Високорівнева структура технології

Сам додатковий механізм, логічно, складається із чотирьох основних компонентів:

- модуля захоплення жестів обличчя;
- сховища паролів;
- модуля виявлення аномалій міміки обличчя;
- модуля прийняття рішень.

Призначення та логіка роботи цих компонентів буде розкрита більш детально у наступних підрозділах. Слід зазначити, що рисунок показую високорівневу логічну структуру, це означає, що інтеграція механізму, що досліджується в цій роботі, до конкретних операційних систем та пристроїв може відрізнятися певним чином з точки зору реалізації логічної взаємодії між компонентами.

2.2 Задача введення фактору знання жестами обличчя

Як вже було описано вище, в наслідок зручності та відносної надійності біометрії в багатьох сценаріях використання весь процес аутентифікації почав зводитись до її ізольваного використання. Це не тільки зменшує надійність загального процесу аутентифікації, а й призводить до нехтування іншими

факторами аутентифікації, як фактор знання, що в більшості випадків спрощується до ПІН-коду, який на додачу може бути ще й занадто простим для легкості запам’ятовування, що в свою чергу перетворює цей фактор на слабке місце процесу загалом та серйозну вразливість через відносну простоту його викрадення способами соціальної інженерії та іншими. З іншого боку, біометрія стає все більш частою ціллю нападників із розробленням все більш витончених презентаційних атак.

Для вирішення обох проблем одночасно, прототип механізму аутентифікації в цій роботі має глибоко інтегрований фактор знання у вигляді комбінації жестів обличчя. Простими словами, для успішного проходження процесу аутентифікації, користувачу необхідно не просто показати своє обличчя на камеру, а ще й зробити певну послідовність жестів, теоретично відому тільки йому. Для зручності, будемо називати цю послідовність біометричним паролем. В той час як така глибока інтеграція має спірну простоту використання, вона надає серйозні покращення в надійності загального процесу аутентифікації. По-перше, фактор знання перестає бути слабким місцем та вразливістю, оскільки:

- саме введення послідовності тісно пов’язано із біометрією обличчя, що означає, що навіть викрадення цієї послідовності окремо не дає можливості для зламу механізму;
- природа біометричного пароля робить його менш вразливим до атак соціальної інженерії, які є одним із найпопулярніших способів зламу фактору знання, причиною чутливості паролів та ПІН-кодів до таких атак є те, що здебільшого вони складаються із букв алфавіту та цифр, що можуть складати будь-яку інформацію, пов’язану із життям користувача: дати народження, визначні дати, імена та назви, улюблені фрази і т.д., вся ця інформація часто використовуються в якості фактору знання, оскільки це те, що користувач добре знає та завжди пам’ятатиме, з іншого боку біометричний пароль складається із жестів обличчя, які неможливо використати для закладання соціальної інформації, а отже

ніякі питання або прямі знання про людину не дозволять наблизитись до його зламу.

По-друге, сам біометричний фактор аутентифікації стає надійнішим та складнішим для зламу:

- так само як біометрична природа жестів посилює фактор знання, глибока інтеграція фактору знання посилює біометрію, оскільки тепер ніякі статичні презентаційні атаки, такі як маски, скульптури, фото та інші навіть теоретично не зможуть зламати механізм аутентифікації, незалежно від рівня надійності базової системи біометрії обличчя, а створення динамічних презентаційних атак які можуть відтворювати жести обличчя є на порядок складнішою задачею, хоч і не є неможливим, що буде покрито в наступних підрозділах;
- введення біометричного пароля, призводить до додаткового часу сканування обличчя базовою системою біометрії, що саме по собі ускладнює злам, порівняно із випадком, коли одноразового співпадіння біометрії достатньо для успішного результату.

Будь-який пароль представляє собою послідовність із символів певного алфавіту. Класично цей алфавіт символів є стандартним набором символів клавіатури, тобто англійські літери, цифри та декілька спеціальних символів. У випадку популярного у сучасності ПІН-кода, або одноразових паролів, найчастіше, алфавіт символів зводиться тільки до цифр для простоти. Способом вводу таких паролів, відповідно, служить вбудована або віртуальна клавіатура пристрою. Біометричний пароль не є винятком, в ролі окремих символів алфавіту служать стандартні жести обличчя, а способом вводу є відтворення цих жестів користувачем на камеру пристрою.

В нашому випадку не існує єдиного стандартного алфавіту символів, тому необхідно визначити його, що є дуже важливою ключовою задачею, оскільки від підбору жестів та виразів обличчя із яких складається алфавіт будуть напряму залежати:

- рівень надійності пароля, що залежить від розміру алфавіту;
- зручність використання, що залежить від того наскільки складними для відтворення є жести;
- доступність використання, що залежить від фізіологічних особливостей, вад або травм обличчя, що можуть заважати відтворювати певні жести.

В цьому контексті слід зазначити, що концептуально алфавіт жестів обличчя може бути змінною частиною механізму аутентифікації, який описується в цій роботі та підбиратися окремо в залежності від аудиторії користувачів та сценаріїв використання. В якості базового нейтрального випадку підберемо такі жести, що є відносно нескладними та відносно доступними для більшої частини людей. На рисунку 2.2 зображений базовий алфавіт жестів, який використовується для прототипу механізму у цій роботі, до нього входять наступні жести:

- блимання очима, обидва ока закриті;
- ліве підморгування, ліве око закрите, та ліва брова злегка опущена та вирівняна;
- праве підморгування, праве око закрите, та права брова злегка опущена та вирівняна;
- підняті брови, обидві брови високо підняті, а очі широко відкриті, чимось нагадує вираз подиву;
- посмішка, кутки рота припідняті, при цьому рот закртий або майже закритий;
- відкритий рот.

Всі ці жести представляють собою стандартні вирази обличчя, які більшість людей використовують у повсякденному житті, а отже точне відтворення цих жестів не повинне представляти великої складності.

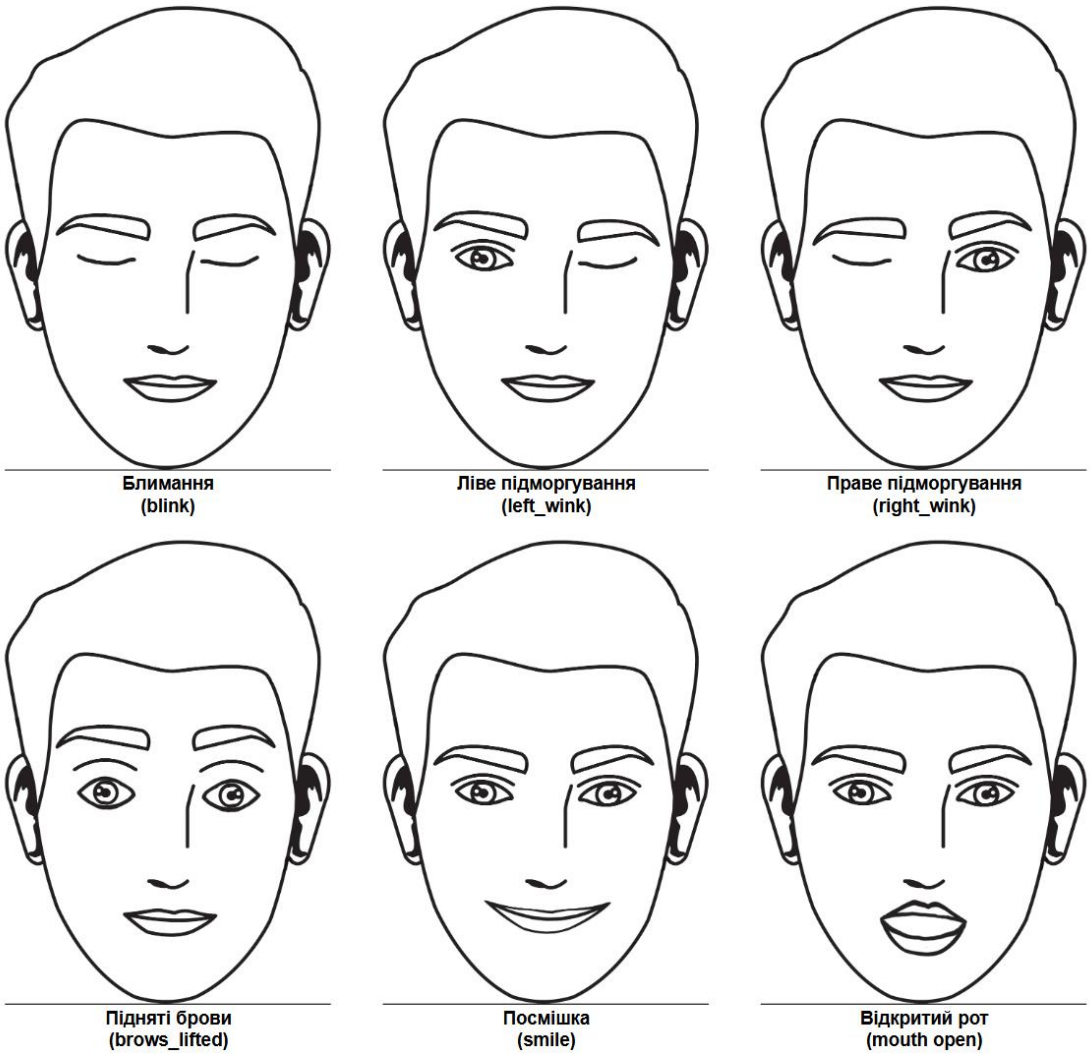


Рисунок 2.2 – Базовий алфавіт жестів обличчя

Для введення біометричного пароля механізм аутентифікації повинен вміти розпізнавати кожний із цих жестів, для цього будуть застосовуватись технології машинного навчання. Спосіб введення пароля складатиметься із двох окремих нейромережевих моделей:

- моделі розпізнавання орієнтирів обличчя, задачею якої є побудова сітки із основних точок обличчя;
- моделі розпізнавання жестів обличчя, на основі сітки опорних точок.

Причиною розділення на дві моделі є паралельне використання орієнтирів обличчя для задачі виявлення аномалій міміки обличчя, яка буде розгорнута у наступних підрозділах.

Розпізнавання орієнтирів обличчя є добре відомою та поширеною задачею й на даний момент вже існують моделі із високою точністю для її

вирішення, враховуючи достатньо високу складність створення та тренування такої моделі, раціональним рішенням є використання готової моделі. У випадку цієї роботи буде застосована Google Mediapipe Face Mesh V2 [38]. Ця модель, розроблена компанією Google створює сітку із 478 основних точок обличчя, зображену на рисунку 2.3, що забезпечує більш ніж достатню деталізацію для розпізнавання всіх необхідних жестів, що використовуються у прототипі механізму цієї роботи або будь-яких інших жестів обличчя, що можуть бути використанні у загальному застосуванні цього механізму аутентифікації. Модель була натренована на 1700 екземплярах обличь, рівномірно розподілених між 17 географічними регіонами, беручі до уваги расові та регіональні особливості будови обличчя [39]. Іншою великою перевагою цієї моделі є високий рівень її підтримки та експертизи розробників, зважаючи на авторитет Google в сфері машинного навчання та інформаційних технологій загалом.

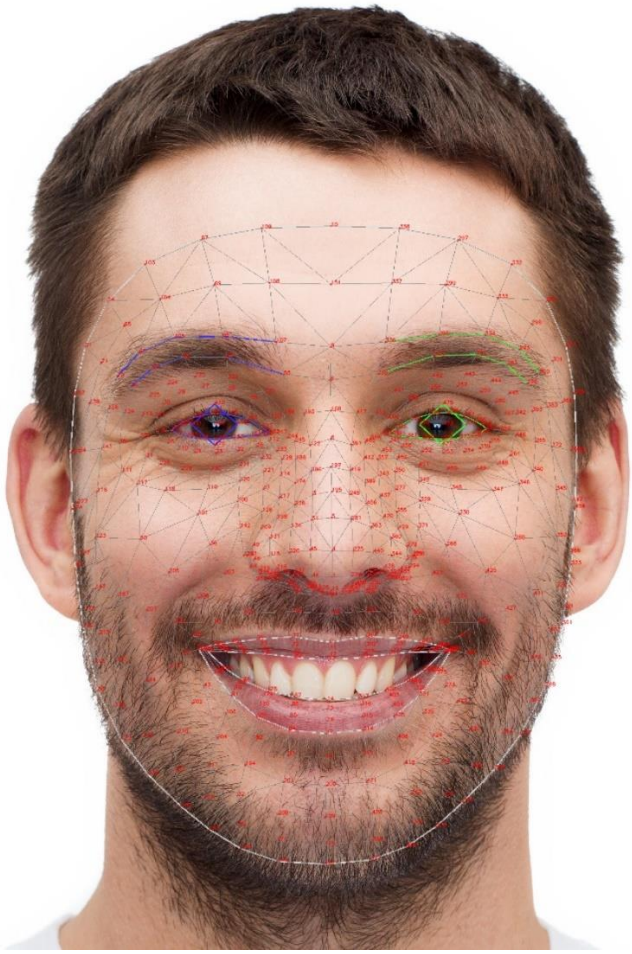


Рисунок 2.3 – Сітка точок обличчя Google Mediapipe Face Mesh V2

Google Mediapipe Face Mesh V2 також має достатню швидкість роботи для розпізнавання орієнтирів обличчя із потоку зображень в режимі реального часу, що є дуже важливою деталлю для механізму аутентифікації цієї роботи. Враховуючи зосередженість механізму аутентифікації даної роботи на певних діялнках та точках обличчя, можливим є відкидання великої кількості точок сітки для легшої та більш надійної роботи, проте це буде більш детально описано в розділі реалізації механізму.

Другою частиною введення є модель для розпізнавання заданих жестів обличчя, яка зможе відрізняти жести із алфавіту від нейтральних виразів обличчя та інших жестів та класифікувати жести заданого алфавіту. Під час дослідження існуючих моделей та задач не було виявлено універсальних моделей для розпізнавання жестів обличчя, а тим більше жестів конкретного набору, найбльш наближеною поширеною задачею є Facial Emotion Recognition, розпізнавання емоцій на обличчі, що має десятки готових моделей, проте розпізнавання емоцій, що можуть виражатись широким спектром рухів обличчя та розпізнавання конкретних жестів є принципово різними задачами. Виходячи з цього, в рамках цієї роботи буде створено нову модель для розпізнавання заданого набору жестів. Тут, знову ж таки, зручним є те, що в якості вхідних даних ця модель буде використовувати не зображення напряму, а сітку із основних точок обличчя від першої моделі, ця деталь, є величезною перевагою у тренуванні та складності моделі, оскільки класичним способом роботи із зображеннями є згорткові нейромережі, задачею яких є зведення великої кількості інформації із пікселів зображення до цільових характеристик, що вимагає окремої уваги до певних аспектів зображень, що використовуються для навачання та більшої їх кількості. В нашому випадку розмір вхідних даних нейронної мережі буде оцінюватись в сотнях, в той час як при прямому використанні зображення кількість інформації дорівнює якнайменше кількості пікселів у зображенні у випадку його бінаризації [40], а у випадку використання кольору, помножена на три канали, що зазвичай складає вхідні дані у розмірі десятків тисяч. Цей факт забезпечить як легший

процес навчання так і більшу швидкодію. Для вирішення поставленої задачі достатньо добре підходить узагальнення до задачі багатокласової класифікації [41], що має стандартні підходи для вирішення у нейронних мережах.

У випадку функціонування другої моделі у механізмі аутентифікації, невід'ємною частиною буде початкове введення пароля для його створення, що завжди надаватиме додаткові дані про обличчя конкретного цільового користувача, а отже, гарним рішенням може бути застосування стратегій оновлення моделей нейромереж [41] для точнішого регулювання механізму під користувача.

Разом із новою моделлю необхідно буде створити і новий датасет із необхідними жестами обличчя для її тренування та тестування. Процес побудови моделі нейромережі, створення датасету та її тренування буде описаний у розділі реалізації механізму.

2.3 Математична модель сили пароля

Говорячи про біометричний пароль в механізмі даної роботи необхідно згадати про базове поняття сили пароля [43]. Сила пароля S представляє собою функцію від довжини, складності та передбачуваності:

$Str(L, N, P) = S$, де $L -$ довижна, $N -$ складність, $P -$ передбачуваність

Складність пароля майже завжди зводиться до кількості можливих символів алфавіту, що використовуються в ньому. Передбачуваність пароля залежить від наявності будь-яких сторонніх факторів, що можуть допомогти його передбачити. Як вже згадувалося в попередньому розділі, передбачуваність є перевагою біометричного пароля над стандартними алфавітами символів, оскільки інформаційне значення символів біометричного пароля не здатне містити будь-яку соціальну інформацію користувача, навідміну від цифр та літер. Враховуючи цей факт, можна зробити припущення, що біометричний пароль є непередбачуваним, або, іншими словами, рандомним, хоча й існують деякі інші фактори передбачуваності, окрім соціальної інформації, вони є

набагато менш вагомими. Таким чином для оцінки складності біометричного пароля, будемо нехтувати значенням змінної P.

Стандартною мірою сили пароля є ентропія H, яка обчислюється на основі кількості бітів, необхідних для кодування за наступною формулою:

$$H = L\frac{\log N}{\log 2} \tag{2.1}$$

Важливою також є посимвольна ентропія, яка розраховується за допомогою прирівняння $L = 1$. Як згадувалося в попередньому розділі найважливішим порівнянням із біометричним паролем є набираючі популярність ПІН-коди, використовуються в багатьох ключових сценаріях. Алфавіт ПІН-кодів складається із арабських цифр, та найчастіше мають довжину у 6 символів, а отже $A_{pin} = \{0,1,2,3,4,5,6,7,8,9\}, N_{pin} = 10, L_{pin} = 6$. Біометричний пароль у прототипі механізму цієї роботи має алфавіт із 6 жестів та буде мати довжину в 4 символи для збереження простоти та швидкості використання при розробці, а отже $A_{bio} = \{b, lw, rw, bl, s, mo\}, N_{bio} = 6, L_{bio} = 4$. Використовуючи ці значення змінних можемо обчислити, що посимвольна ентропія ПІН-коду та біометричного пароля дорівнює:

- $H_{1pin} = \frac{\log N_{pin}}{\log 2} = \frac{\log 10}{\log 2} = 3.3$
- $H_{1bio} = \frac{\log N_{bio}}{\log 2} = \frac{\log 6}{\log 2} = 2.6$

А інформаційна ентропія кінцевих паролів відповідно дорівнює:

- $H_{pin} = L_{pin}\frac{\log N_{pin}}{\log 2} = 6\frac{\log 10}{\log 2} = 19.9$
- $H_{bio} = L_{bio}\frac{\log N_{bio}}{\log 2} = 4\frac{\log 6}{\log 2} = 10.3$

Тут також слід зазначити, що передбачуваність P для легкого порівняння нехтувалась не тільки для біометричного пароля, а і для ПІН-коду, беручи до уваги алфавіт символів A_{pin}, можна було б стверджувати, що передбачуваність ПІН-кода є хоча б на 30% вищою ніж передбачуваність біометричного пароля, яка припустимо може прямувати до 0, тобто з урахуванням P сили цих двох видів паролів могли б бути приблизно рівними, проте вплив передбачуваності

на силу пароля є неоднозначним фактором. Навіть нехтуючи P для обох паролів ми можемо бачити, що їх сили є порівнюваними, а згадуючи про глибоку інтеграцію біометричного пароля із біометричним фактором аутентифікації, сила біометричного пароля стає ще більш прийнятною. Також за допомогою комбінаторики тут варто зазначити, що кількість можливих біометричним паролів із даними параметрами складає $P = \frac{6!}{(6-4)!} = 360$, що є достатньо великою кількістю паролів для перебору, щоб ефективно помічати спроби вгадати пароль.

Не дивлячись на інтегровану природу біометричного пароля та набагато менше значення його сили як окремо стоячого пароля, варто пам’ятати про оцінку його складності та враховувати її при використанні механізму аутентифікації цієї роботи в різних сценаріях, відповідно змінюючи довжину пароля та розмір алфавіту символів.

2.4 Задача виявлення аномалій міміки обличчя

Використання поведінкової біометрії стає все більш перспективним шляхом розвитку систем аутентифікації, оскільки надає додатковий вимір вхідної інформації для прийняття рішень. Наприклад, для введення класичних паролів із клавіатури використовується характеристика поведінкової біометрії під назвою Keyboarding Dynamics [32], тобто динаміка клавіатурного вводу, яка використовує проміжки часу між натисненнями різних клавіш в якості поведінкового фактору. Однією з основних задач цієї роботи є спроба інтегрувати фактор поведінкової біометрії до загального механізму аутентифікація для, теоретично, досягнення ще більшої стійкості до презентаційних атак. В даному випадку в ролі поведінковоого фактора буде використовуватись міміка обличчя користувача в рухах при введенні біометричного пароля. Обличчя людини містить біля 30 окремих м’язів на кожному боці, тобто всього 60, більшість із яких є міметичними м’язами, тобто м’язами які відповідають за візуальний вираз обличчя [44]. Така висока

деталізація та мобільність обличчя на рівні м’язів як раз і робить його хорошою модальністю біометричного фактору, те саме можна сказати і про рухи обличчя, враховуючи таку різноманітність, рухи певних ділянок та точок обличчя в різних людей є достатньо унікальними, що робить їх потенційно хорошим вибором для поведінкової біометрії в цій роботі.

Ідея цієї частини механізму аутентифікації полягає в тому, щоб слідкувати за динамікою основних точок в певних ділянках обличчя при введенні жестів біометричного пароля, які будуть надаватись вже згаданою вище моделлю розпізнавання орієнтирів обличчя Google Mediapipe Face Mesh V2. В той час як задачею першої частини механізму є вирізнення конкретного жесту обличчя із різних виразів обличчя, ця частина механізму, навпаки, зацікавлена в загальній динаміці обличчя при введені того чи іншого жесту, що може відрізнятися в різних людей, наприклад, при підморгуванні, хтось може більше рухати кутками рота, а хтось сильно рухає бровами, такі особливості є індивідуальними для кожної людини та кожного жесту, який вона робить. З технічної точки зору, система аутентифікації буде використовувати алгоритм машинного навчання по виявленню аномалій – “запам’ятовувати” певну кількість останніх положень основних точок обличчя та при розпізнаванні жеста, порівнювати запам’ятовану динаміку із зразком, що був введений користувачем при початковому створенні пароля.

Слід зазначити, що ця частина механізму аутентифікації є досить складною, оскільки в якості зразкових даних для початкового налаштування алгоритму виявлення аномалій буде слугувати лише невелика кількість даних отриманих під час створення пароля користувачем, хоча оновлення моделі при подальшому використанні є можливим. Більше того, у випадку цих даних немає однозначного розуміння що є чи не є аномаліями міміки для конкретного користувача, оскільки всі початкові зразки з великою ймовірністю є нормальними, це означає, що для вирішення цієї задачі необхідно обрати алгоритм машинного навчання без нагляду, тобто алгоритм при якому не існує однозначної категоризації даних під час навчання [45]. Цей

аспект робить вибір алгоритму виявлення аномалій критично важливим кроком.

Найважливішою вхідною інформацією для вибору алгоритму виявлення аномалій є розуміння типу аномалій, що будуть зустрічатись при аналізі цільових даних. Згідно з дослідженнями, попереднє знання про тип аномалій переважувати використання підкріпленого навчання і роботи алгоритми без нагляду більш ефективними [46]. Слідуючи типології аномалій даних [47], аномалії діляться за двома основними критеріями – типом даних атрибутів та кардинальністю залежностей. Типи даних атрибутів поділяються на:

- неперервні – атрибути з числовою природою;
- категоріальні – атрибути поділяються на фіксовані категорії;
- мішані – атрибути мають ознаки неперервних і категоріальних водночас.

За кардинальністю залежностей атрибути розрізняють на:

- уніваріативні – аномальність залежить від однієї незалежної змінної;
- мультиваративні - аномальність залежить від кількох залежних змінних.

За комбінаціями цих двох критеріїв виділяють шість основних типів аномалій. За іншою класифікацією усі уніваріативні аномалії також називають глобальними, а всі мультиваріативні – локальними [47], оскільки перші виражають аномальність незалежно від інших змінних або факторів по відношенню до всього набору даних, в той час як останні виражають аномальність по відношенню до кількох змінних одночасно, тобто в певному регіоні набору даних.

У випадку цієї роботи цільовими даними є динаміка певних точок обличчя, як вже згадувалось вище, іншими словами, для кожної точки обличчя l відстежується положення p в відносний момент часу t. Обидва цих атрибути за своєю природою є неперервними, а також залежними, оскільки положення точки не має значення без контексту відносного моменту часу. Такі дані можна віднести до більш загальної категорії часових послідовностей, які належать до типу IV [47] мультиваріативних неперервних даних.

Підсумовуючи відому інформацію можна сказати, що аномалії даних належать до локального (мультиваріативного неперервного) типу, а специфіка використання алгоритму виявлення аномалій вимагає, щоб це був алгоритм без нагляду. Згідно з ADBench: Anomaly Detection Benchmark [46], що є найбільш обширним порівняльним дослдженням алгоритмів виявлення аномалій, проведеному для 30 алгоритмів на 57 наборах даних з різних предметних областей, статистично найкращим алгоритмом без нагляду для локального типу аномалій є LOF (Local Outlier Factor).

2.5 Алгоритм роботи механізму аутентифікації

Механізм біометричної аутентифікації даної роботи як і багато інших систем аутентифікації має два основних етапи роботи: початкове налаштування аутентифікації та перевірка аутентифікації, алгоритми роботи цих етапів відображені на рисунках 2.4 та 2.5 відповідно.

Як можна побачити на рисунку 2.5, одразу після успішного розпізнавання жесту ініціюється запит до базової системи біометричної аутентифікації, саме цей крок під час перевірки аутентифікації дозволяє неперервно зв’язати додатковий механізм аутентифікації до вже наявних можливостей, максимально посилюючи процес. Хоча дана робота не буде описувати інтеграцію механізму із конкретною базовою системою аутентифікації, розуміння цього кроку є критично важливим для ефективного застосування технології цієї роботи.

Також тут варто прокоментувати компонент сховища паролів, задача збереження паролів загалом заслуговує окремих робіт та досліджень, проте, в цілому, біометричний пароль, як і будь-який інший пароль повинен розцінюватись як секретна та чутлива інформація, глибока інтеграція із біометрією не применшує цього. За можливості, хорошим варіантом може бути використання нативних можливостей ОС для збереження паролів, що звичайно, буде залежати від конкретної ОС та навіть апаратного забезпечення. Іншим питанням при збереженні біометричного пароля є його кодування для

представлення у вигляді тексту, в залежності від сценарію використання можуть застосовуватись різні механізму кодування, від найпростішого мапінгу кожного жеста у визначений символ, до використання послідовностей символів та слів. В рамках цієї роботі збереження паролів не є критичною задачею оскільки розробляється лише демонстраційний додаток, тому буде використаний найпростіший механізм кодування паролю в текст.

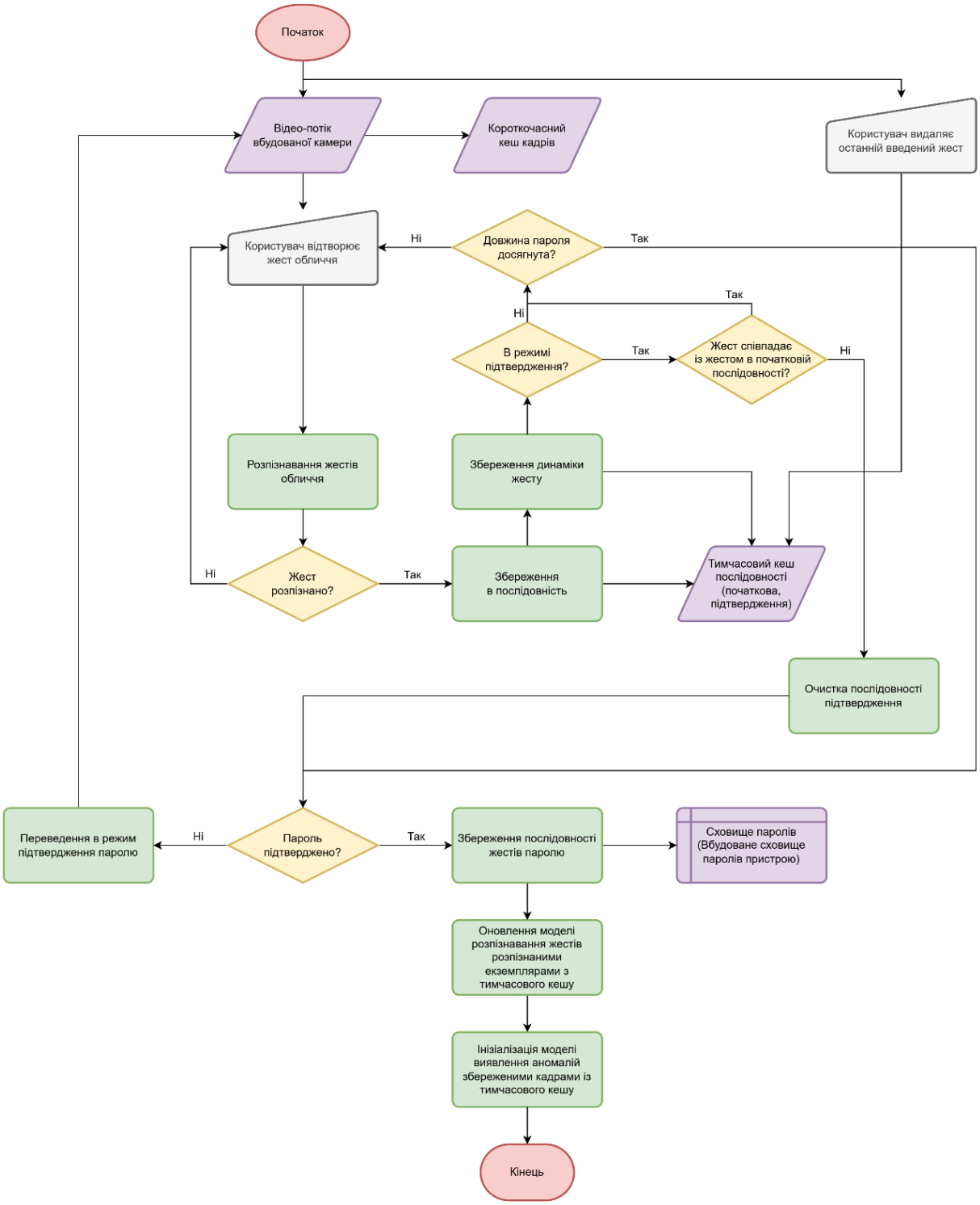


Рисунок 2.4 – Алгоритм налаштування аутентифікації

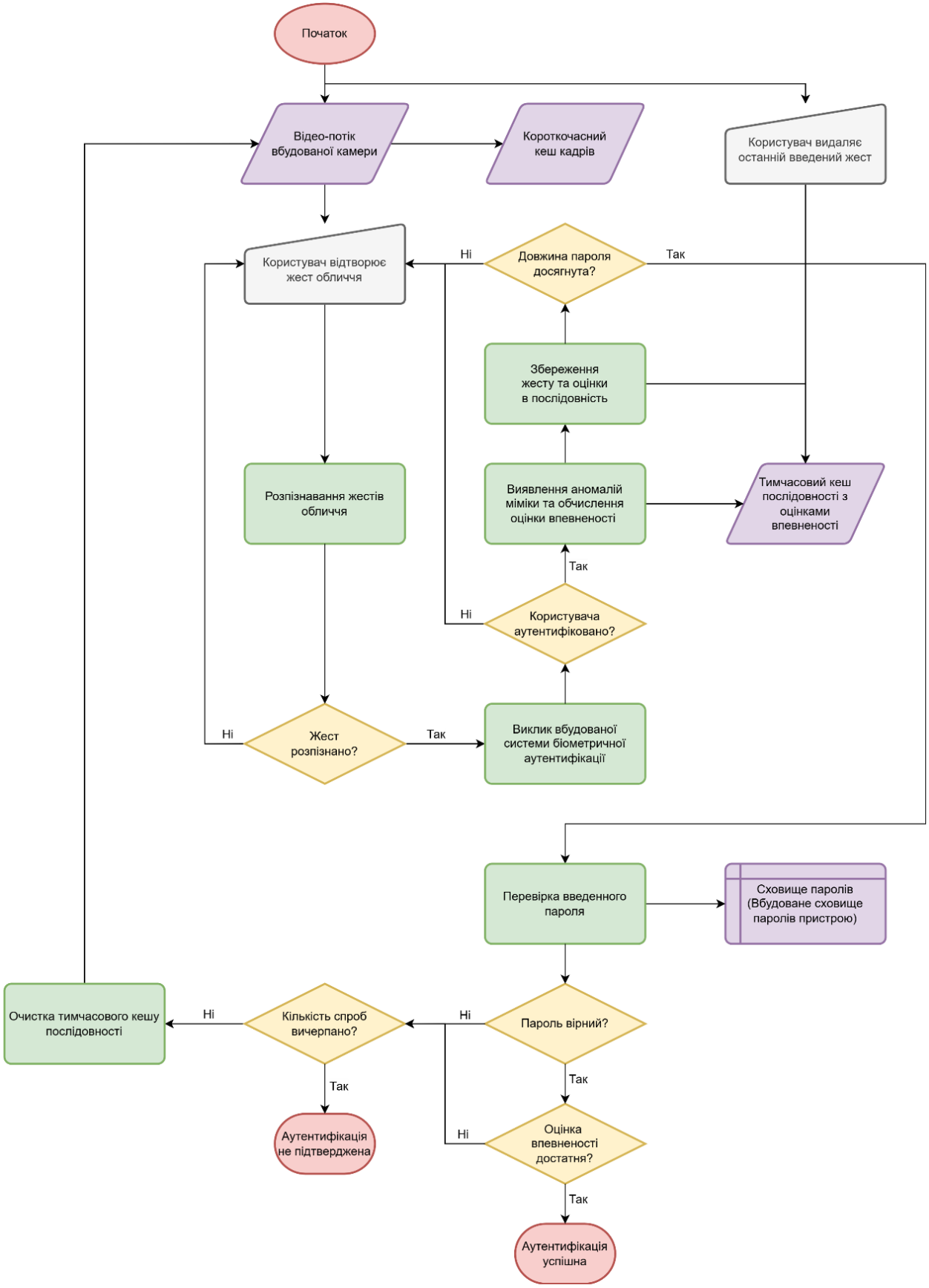


Рисунок 2.5 – Алгоритм перевірки аутентифікації

2.6 Постановка задач та вимог до програмної реалізації

На даному етапі, коли визначені функціональні компоненти механізму біометричної аутентифікації цієї роботи, можна більш детально сформувати функціональні вимоги для подальшої програмної реалізації. Як вже згадувалось в розділі 1.5 при постановці первинних задач, програмна реалізація цієї роботи буде зосереджена на двох основних частинах: розробці прототипу механізму посилення біометричної аутентифікації та розробці демонстраційного додатку, відповідно формуватимемо і функціональні вимоги.

Основною задачею реалізації прототипу механізму аутентифікації є реалізація його ключових функціональних компонентів, а саме компоненту розпізнавання жестів обличчя та компоненту виявлення аномалій міміки, в таблиці 2.1 сформовані функціональні вимоги до цієї частини роботи.

Таблиця 2.1 – Функціональні вимоги до компонентів механізму

№	Вимога	Пріоритет
1	Компонент розпізнавання жестів повинен використовувати вихідний результат моделі Mediapipe Face Mesh V2 в якості вхідних даних	Високий
2	Компонент розпізнавання жестів повинен розрізняти всі 6 жестів із набору визначеного у розділі 2.2	Високий
3	Компонент розпізнавання жестів повинен відрізняти нейтральний вираз обличчя (пасивний стан) від цільових жестів (активний стан)	Високий
4	Компонент розпізнавання жестів повинен надавати вихідний результат за яким можливо однозначно визначити введений користувачем жест або пасивність	Високий
5	Компонент розпізнавання жестів повинен надавати можливість регулювання моделі додатковими даними	Середній

Продовження табл. 2.1

№	Вимога	Пріоритет
6	Компонент виявлення аномалій міміки повинен використовувати підмножину даних вихідного результату моделі Mediapipe Face Mesh V2 в якості положення точок	Середній
7	Компонент виявлення аномалій повинен приймати два атрибути вхідних даних – положення точки та момент часу	Середній
8	Компонент виявлення аномалій повинен обробляти всю траєкторію руху точки під час введення жесту	Середній
9	Компонент виявлення аномалій повинен оцінювати та розрізняти аномальність динаміки точки для кожного жеста із визначеного набору окремо	Середній
10	Компонент виявлення аномалій повинен видавати ймовірність аномальності динаміки точки обличчя при введені певного жесту як результат	Середній

Як можна бачити майже всі вимоги компонента розпізнавання жестів мають високий пріоритет, оскільки цей компонент є основним для механізму даної роботи, при цьому пріоритет компоненту виявлення аномалій є нижчим, оскільки він надає додатковий функціонал поведінкової біометрії. Загалом в даній роботі розробляється основа функціональних частин механізму підвищення надійності аутентифікації, яка призначена для подальшого дослідження та розвитку, а отже реалізація всіх базових функцій є дуже важливою.

Основну задачу створення демонстраційного додатку можна поставити як мінімальна необхідна реалізація двох базових алгоритмів роботи, описаних в попередньому розділі, адже саме вони демонструють повну функціональність механізму. В таблиці 2.2 сформовані функціональні вимоги для додатку.

Таблиця 2.2 – Функціональні вимоги до демонстраційного додатку

№	**Вимога**	**Пріоритет**
1	Додаток повинен працювати з відео потоком із вбудованої камери пристрою в якості вхідних даних	Високий
2	Додаток повинен інтегрувати модель Mediapipe Face Mesh V2 для отримання початкових даних положення орієнтирів обличчя з відео потоку	Високий
3	Додаток повинен зберігати послідовність введених користувачем жестів	Високий
4	Додаток повинен зберігати послідовність оцінок аномальності введених користувачем жестів	Високий
5	Додаток повинен зберігати короткочасний кеш кадрів для використання в якості динаміки орієнтирів обличчя при виявленні аномалій	Високий
6	Додаток повинен зберігати налаштований пароль для подальшої перевірки аутентифікації	Високий
7	Додаток повинен тренувати моделі компоненту виявлення аномалій при закінченні налаштування аутентифікації	Високий
8	Додаток повинен надавати користувачеві можливість налаштувати (ініціалізувати) аутентифікацію	Високий
9	Додаток повинен надавати користувачеві перевірити аутентифікацію (пройти процес аутентифікації)	Високий
10	Додаток повинен надавати користувачеві можливість видаляти введені жести разом з оцінками аномальності із послідовності	Високий
11	Додаток повинен відображати базову інформацію для користувача: введені жести, поточний статус процесу	Середній

3 ПРОГРАМНА РЕАЛІЗАЦІЯ ТЕХНОЛОГІЇ

3.1 Створення датасету для розпізнавання жестів

Як вже згадувалось в попередньому розділі, готових датасетів для задачі розпізнавання жестів, визначених в цій роботі, не було знайдено. Більше того, кількість датасетів, що зосереджуються саме на жестах обличчя є дуже обмеженою. Найближчими існуючими є датасети для популярної задачі розпізнавання емоцій на обличчі (Facial Emotion Recognition), проте великим недоліком цих даних є зосередженість на загальному емоційному виразі обличчя, що може виражатись різними жестами або їх комбінаціями, в той час коли для задачі розпізнавання жестів необхідна зосередженість на конкретному ізольованому жесті.

В рамках цієї роботи був створений новий датасет зображенн Facial Gestures із фокусом на ізольовані жести людського обличчя із набору жестів, що був визначений у розділі 2.2 цієї роботи. Новий датасет із детальним описом було опубліковано на платформі машинного навчання та науки про дані Kaggle [48].

Для створення датасету було проведено пошук публічних зображень на таких ресурсах як Google Images, Gettyimages, Shutterstock та Pinterest, використовуючи їх пошукові можливості за текстом та зображеннями, а також алгоритми підбору подібних зображень. Варто відмітити, що для цільових даних цієї роботи найкращим ресурсом виявився Gettyimages, зображення з якого складають не менше половини всього датасету. В процесі підбору увага зосереджувалась на зображеннях обличь, які чітко показують конкретний жест, при цьому маючи мінімум ознак інших жестів або виразів обличчя, іншими словами – обличчя з ізольованим жестом. Знайти на 100 відсотків чисті дані в достатній кількості не виявилось можливим за обмежений час, тому певна частина зображень має комбінації декількох жестів, наприклад підморгування разом із посмішкою, з іншого боку, присутність невеликої частини таких даних на фоні більшості «чистих» даних, може навпаки дозволити моделям машинного навчання краще вирізняти категоріальні

характеристики та віддавати пріоритет одним жестам над іншими, в залежності від алгоритму. Приклади зображень всіх жестів із створеного датасету можна побачити на рисунку 3.1.

Готовий датасет містить 800 зображень, розділених на 7 підгруп – 6 підгруп по 100 зображень кожного жесту з набору цієї роботи та нейтральний (пасивний) вираз обличчя з 200 зображеннями.

Додатково була приділена увага достатній різноманітності даних. Для досягнення цієї мети було визначено 6 цільових груп людей, комбінуючи 3 базових раси: європеоїдна, монголоїдна та негроїдна, із двома базовими статями: чоловіча та жіноча. В результаті датасет рівномірно розподілений за цими групами, з майже однаковою кількістю зображень (+-2) для кожної групи як на рівні конкретного жесту, так і на рівні всього датасету. Така стратегія дозволяє використовувати датасет для цільових аудиторій по всьому світу.

Підібрані зображення були оброблені процесом нормалізації, який включав наступні кроки:

- позиціонування обличчя по центру зображення;
- обрізка зображення у співвідношенні сторін 1:1 (квадрат) із залишенням мінімального незначного простору;
- збереження у форматі JPEG із дозволом 500 на 500 пікселів

Рисунок 3.1 – Приклади зображень цільових жестів із датасету

3.2 Підготовка датасету для моделі розпізнавання жестів

Зображення людського обличчя, на кшталт тих, що представлені у датасеті є безпосередніми вхідними даними додаткового механізму аутентифікації, проте як вже згадувалось в попередніх розділах, першим кроком обробки цих даних є модель розпізнавання орієнтирів обличчя Mediapipe Face Mesh V2, яка перетворює зображення на сітку із 478 точок, які відповідають орієнтирам обличчя. Саме ці дані будуть слугувати вхідними для моделі розпізнавання жестів. Це означає, що для використання створеного датасету для безпосереднього навчання цієї моделі необхідно спочатку підготувати датасет, попередньо пропустивши його через модель розпізнавання орієнтирів.

Для виконання цієї задачі було реалізовано пайплайн на мові програмування Python, який можна побачити у Додатку А (файл images_to_landmakrs.py). Пайплайн почергово обробляє кожне зображення моделлю Mediapipe Face Mesh V2, розмічає визначену сітку точок на зображенні, відображає результат у вікні для аналізу спостерігачем та зберігає розмічене зображення і табличний файл формату CSV з координатами знайдених точок.

Схематичне зображення процесу підготовки даних можна побачити на рисунку 3.2, що містить приклади всіх трьох станів даних в пайплайні. Табличні файли слугуватимуть в якості безпосередніх вхідних даних для моделі розпізнавання жестів та її тренування, в той час як збереження зображення із розміченою сіткою точок орієнтирів обличчя дозволяє подальший зручний візуальний аналіз даних представлених у вигляді в числовому вигляді для визначення неякісних екземплярів та розуміння загальної якості підготовлених даних.

В цілому модель Mediapipe Face Mesh V2 продемонструвала дуже хорошу точність, судячи із візуальних результатів із невеликим відсотком виключень (2-3%), в яких координати деяких орієнтирів були визначені з помітною похибкою, приклади таких виключень можна побачити на рисунку

3.3. Загалом було прийнято рішення використовувати абсолютно всі оброблені дані для подальшої роботи, оскільки навіть наявні похибки не були критично вагомими для виключення даних із подальшого процесу тренування моделі розпізнавання жестів.

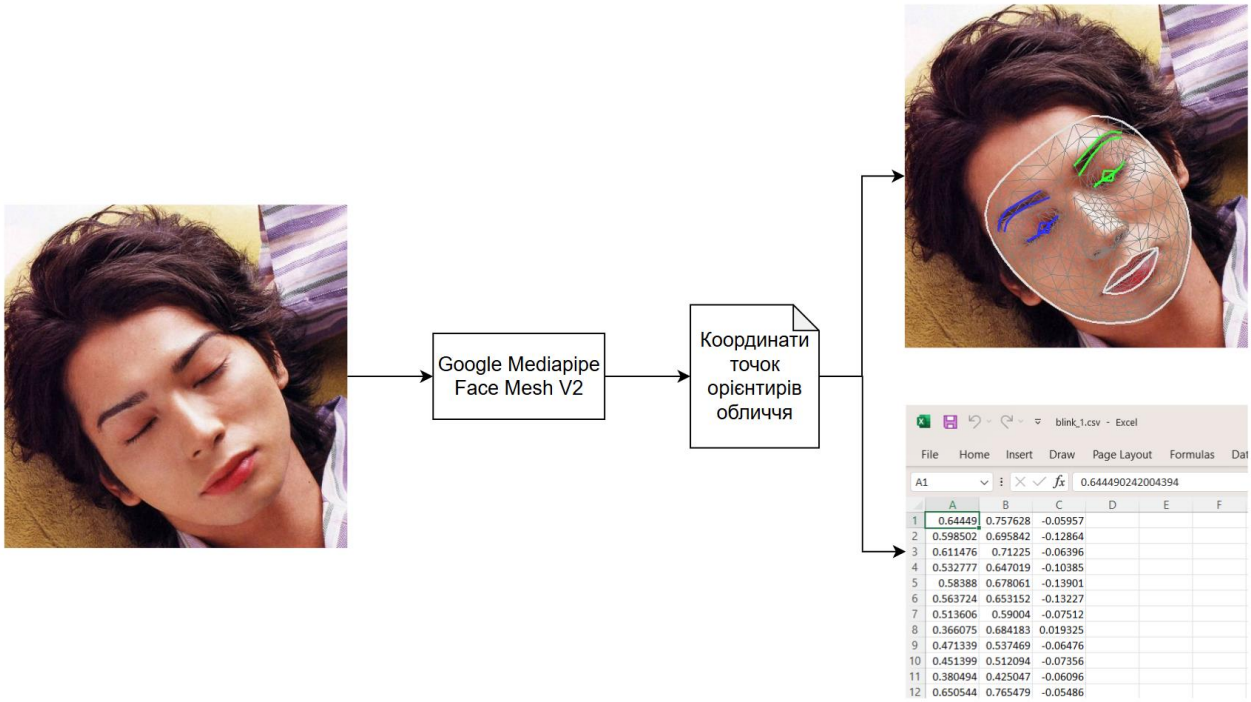


Рисунок 3.2 – Схематичне зображення процесу підготовки датасету

Рисунок 3.3 – Приклади похибок моделі Mediapipe Face Mesh V2

3.3 Побудова та тренування моделі розпізнавання жестів

Задача розпізнавання жестів обличчя може бути узагальнена до задачі мультикласової класифікації. Для виконання цієї задачі найчастіше використовуються моделі нейронних мереж, які представляють із себе шари цифрових нейронів із певною функцією активації та зв'язками з іншими нейронами, фактично наслідуючи принцип роботи біологічних нейронних зв'язків. За допомогою великої кількості нейронів та зв'язків, моделі нейронних мереж здатні «сприймати» будь-які вхідні дані та виділяти цільові характеристики із них, в залежності від бажаного результату, за допомогою налаштування числових параметрів нейронних зв'язків, таким чином, нейронна мережа може пристосовуватись до вирішення майже будь-якої задачі, так само як це робить біологічний мозок.

Особливістю моделей нейронних мереж є відносно велика кількість параметрів, які налаштовуються під час навчання порівняно із іншими типами моделей машинного навчання. В загальному випадку чим більшим є розмір вхідних даних, тим більшою є кількість параметрів [49] й, відповідно, довшим та складнішим є процес навчання моделі. Дивлячись на цільовий набір жестів для розпізнавання цієї роботи, можна побачити, що всі вони, в основному відображаються за допомогою губ та очей та брів, такі частини обличчя як ніс, щоки, підборіддя є незначними для їх розрізнення.

Беручи до уваги ці факти було прийнято рішення відсіяти незначні точки орієнтирів обличчя, що видаються моделлю Mediapipe Face Mesh V2. Повний набір вибраних значущих точок можна побачити в додатку А (файл face_landmarks_subset.py). Загалом, за допомогою цього вдалося зменшити розмір вхідних даних мережі з 478 точок до 222 точок, що є зменшенням більш ніж у два рази та відображатиметься у ще більшій кратності зменшення кількості параметрів моделі нейронної мережі. Візуальне представлення відсіювання даних та порівняння повного результату Face Mesh V2 із частковим, що використовуватиметься в якості входу мережі, можна побачити на рисунку 3.4.

а) б)

Рисунок 3.4 – Порівняння повного (а) та відсіяного (б) набору точок обличчя

Цей крок ще раз показує наскільки вдалим вибором є використання вторинних даних від моделі розпізнавання орієнтирів обличчя в якості вхідних даних для розпізнавання жестів, порівняно із використанням зображень напряму. Це дозволяє не тільки зменшити розміри вхідних даних в десятки або навіть сотні разів, як вже згадувалось в розділі 2.2, а й елементарним чином виділити підмножину найбільш значущих даних для конкретного набору жестів, це означає, що таке ефективне використання даних може бути застосоване для будь-яких інших наборів жестів за допомогою зміни значущої підмножини точок обличчя.

Задачу мультикласової класифікації можна описати наступним чином. Модель нейронної мережі M повинна віднести кожний екземпляр даних D_i із датасету D до одного із n класів множини $C, C_1 \dots C_n, P(C) = n$, створивши вектор $V_c(v_{c_1}, \dots, v_{c_n})$, в якому елементи v_{c_j} відображають ймовірність належності D_i до класу C_j $(i, j = 1 \dots n)$.

Як описувалось у попередньому розділі, датасет для навчання моделі розпізнавання жестів був представлений у вигляді CSV файлів з координатами кожної із 478 точок орієнтирів обличчя. Перед початком навчання відбувається завантаження цих файлів із відсіюванням незначних точок, усі

екземпляри збираються до датасету D. Всі файли датасету розділені на конкретні класи за допомогою структури директорій файлової системи, за допомогою цього для кожного екземпляру датасету D_i, що належить до класу C_j створюється цільовий вектор V_{c_j}, в якому елемент $v_{c_j} = 1$, а всі інші – 0, оскільки у випадку тренувальних даних належність екземпляру до класу є відомою та однозначною. Для процесу навчання датасет D повинен бути розділений на 3 частини:

- $D_{tr} \subset D$ – тренувальний датасет, який використовується безпосередньо для навчання моделі;
- $D_{val} \subset D_{tr}$ – валідаційний датасет, який використовується для валідації точності роботи моделі на відомих даних;
- $D_{test} \subset D, D_{test} \cap D_{tr} = \emptyset$ – тестовий датасет, який використовується для фінального тестування роботи моделі на нових невідомих даних.

З оглядом на невеликий розмір датасету, $P(D) = 800$, було прийнято рішення розділити датасет наступним чином:

- $P(D_{tr}) = 0.97 * P(D) = 776$;
- $P(D_{val}) = 0.06 * P(D_{tr}) = 46$;
- $P(D_{test}) = 0.03 * P(D) = 24$.

Для рівномірного розподілення екземплярів всіх класів датасет перемішувався випадковим чином. Усі необхідні функції роботи з датасетом включаючи поділ датасету та випадкове перемішування доступні у класі Tensorflow.Dataset фреймворку Tensorflow.

Наступним кроком після підготовки датасету є побудова архітектури моделі нейронної мережі. Для реалізації моделі нейронної мережі в цій роботі використовувались фреймворки Tensorflow та Keras. Почнемо із вхідного та вихідного шарів, які залежать від вхідних та вихідних даних та не залежать від архітектури моделі.

Вхідними даними моделі є підмножина із 222 точок обличчя, де кожна точка представлена трьома координатами (x, y, z), оскільки окрім положення

точки на площині, Mediapipe Face Mesh V2 також визначає глибину точки відносно центру маси обличчя. Відповідно, вхідний шар моделі буде реалізований об’єктом класу Keras Input із розмірністю (222,3).

Вихідними даними будь-якої моделі багатокласової класифікації є вектор ймовірностей, розмірність якого дорівнює кількості цільових класів, іншою типовою рисою вихідного шару є використання функції активації softmax [50], яка і дозволяє перетворити значення нейронів вихідного шару на вектор ймовірностей. Таким чином вихідний шар моделі буде реалізований шаром класу Keras Dense із розмірністю (7) та функцією активації softmax.

Архітектура внутрішніх шарів моделі будувалася на ідеї ефективного використання всіх трьох координат точок, для виконання цієї ідеї, теоретично підходить згортковий шар нейронної мережі [51]. Згортковий шар є одним із регуляризаційних шарів, тобто шарів, які узагальнюють характеристики із даних, він пристосовує фільтр, який здатний витягувати більш високорівневі характеристики із низькорівневих, детальних даних, фактично згортаючи вхідні дані до меншого розміру. У випадку даної задачі можна застосувати цей тип шару для згортання трьох координат до єдиної характеристики, що дозволить представити кожну точку обличчя одним значенням, випрямивши дані до одного виміру та розповсюдити набір точок до більшого за розміром повно зв’язаного шару для поглибленого сприйняття кожної точки. Реалізувати таку архітектуру можна за допомогою шарів класів Keras Conv1D та Keras Dense та функціонального шару випрямлення Keras Flatten. Зображення повної архітектури моделі нейронної мережі можна побачити на рисунку 3.5.

Модель було побудовано за на основі класу Keras.Sequential мережі із прямою послідовністю шарів, та вже згаданих класів шарів:

- Kears Input((255,3)) – об’єкт вхідного шару;
- Keras Conv1D(1, 30, relu) – шар одновимірної згортки з параметром filter=1 для представлення координат точок одним значенням та функцією активації ReLu;

- Keras Flatten – функціональний шар випрямлення даних;
- Keras Dense(1200, relu) – повно зв’язаний шар з функцією активації ReLu;
- Keras Dense(7, softmax) – повно зв’язаний вихідний шар з функцією активації softmax.

Реалізацію моделі в програмному коді на фреймворці Keras та опис її шарів із загальною кількістю параметрів можна побачити на рисунках 3.6 та 3.7 відповідно.

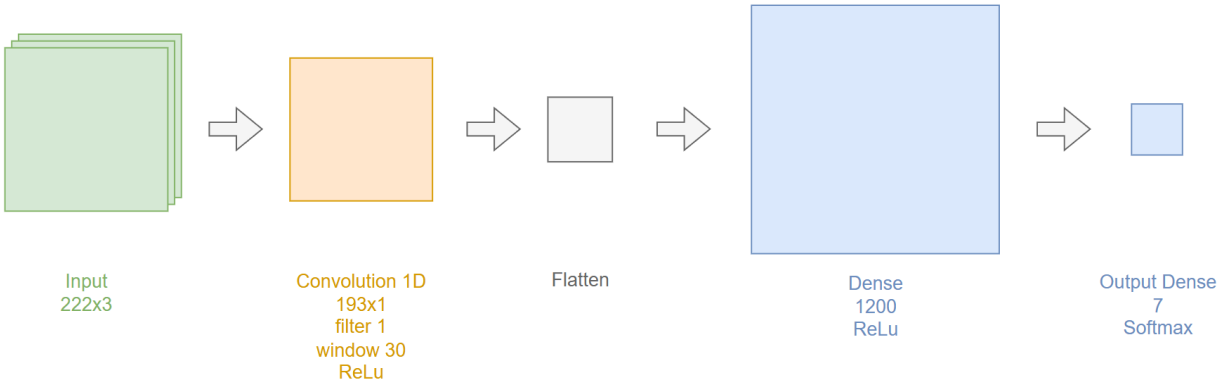


Рисунок 3.5 – Архітектура моделі нейронної мережі

```
model = Sequential([
    layers.Input((222, 3)),
    layers.Conv1D(1, 30, activation=activations.relu),
    layers.Flatten(),
    layers.Dense(units=1200, activation=activations.relu),
    layers.Dense(units=7, activation=activations.softmax),
], name='face_gesture_recognition')
```

Рисунок 3.6 – Реалізації моделі в коді за допомогою фреймворку Keras

Layer (type)	Output Shape	Param #
conv1d (Conv1D)	(None, 193, 1)	91
flatten (Flatten)	(None, 193)	0
dense (Dense)	(None, 1200)	232,800
dense_1 (Dense)	(None, 7)	8,407

Total params: 241,298 (942.57 KB)
Trainable params: 241,298 (942.57 KB)

Рисунок 3.7 – Опис шарів та параметрів побудованої моделі Keras

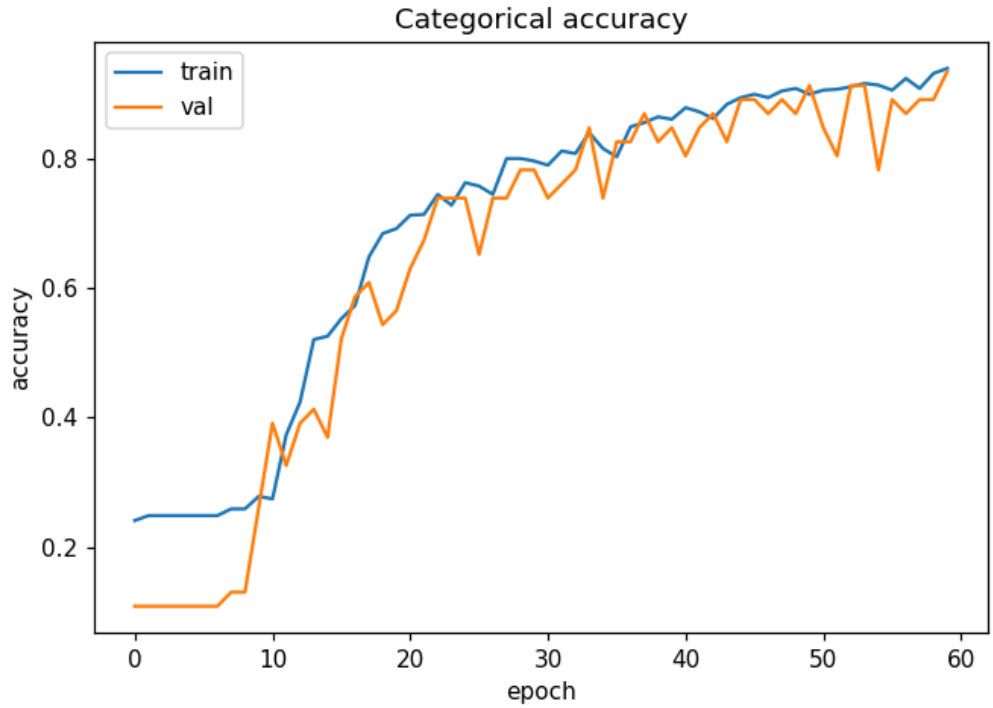
Для кінцевої компіляції моделі небхідно визначити функцію витрат та алгоритм оптимізації, які відповідають за оцінку похибки (витрати) виданих мережею результатів порівняно із цільовими результатами V_{c_j} та використання цієї інформації про витрати для оптимізації (підлаштування) ваг нейронних зв'язків відповідно. Для цих цілей були обрані стандартні для задач мультикласової класифікації функція витрат категоріальної кросентропії (Categorical Crossentropy) та алгоритм оптимізації Adam (Adaptive Moment Estimation), обидва алгоритми є частиною стандартних наборів losses та optimizers фреймворку Keras. Додатково до моделі була додана метрика Keras.metrics.CategoricalAccuracy для наочної оцінки точності класифікації моделі.

Для навчання моделі датасет було розділено на партії даних розміром 40, тобто на кожній ітерації до тренувального процесу передавалось 40 випадкових екземплярів із датасету D_{tr}, такий розмір партії забезпечує достатню кількість даних для продуктивного навчання моделі на кожній ітерації і в той же час забезпечує достатньо велику різницю між даними в кожній ітерації для запобігання перенавчанню. В процесі навчання моделі було уточнено останні два параметри моделі, які можна побачити на рисунку 3.5, а саме:

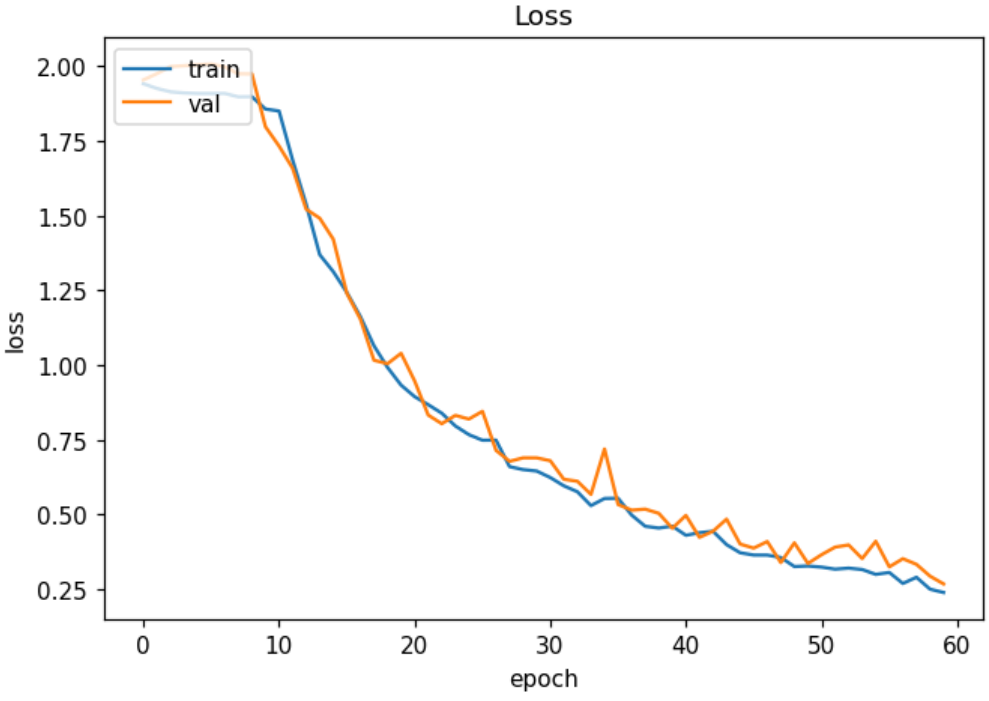
- розмір повно зв'язаного шару – 1200;
- розмір вікна одновимірної згортки (частина даних за якими навчається згортка за один крок) – 30.

Методом проб та помилок було встановлено, що модель перестає значно покращувати свою точність після 60 епохи, відповідно подальше навчання проводилось протягом цієї кількості епох. В результаті тренування було досягнуто досить хороших результатів, враховуючи обмежений розмір датасету та простоту архітектури побудованої моделі. Досягнута категоріальна точність на тренувальному та валідаційному датасетах D_{tr} та D_{val} складала 93% та більше, та сама точність, іноді трохи краща досягалася навіть на невідомих даних тестового датасету D_{test}. На рисунку 3.8 можна

побачити динаміку точності та витрат в процесі навчання моделі під час однієї із вдалих спроб, а на рисунку 3.9 кінцевий результат та результат тестування моделі на невідомих даних із відповідної спроби.



а)



б)

Рисунок 3.8 – Динаміка точності (а) та втрат (б) в процесі навчання моделі

```
Epoch 60/60
20/20 ━━━━━━━━━━━━━━━━━━━━ 0s 4ms/step - categorical_accuracy: 0.9395 - loss: 0.2511 - val_categorical_accuracy: 0.9348 - val_loss: 0.2676
1/1 ━━━━━━━━━━━━━━━━━━━━ 0s 16ms/step - categorical_accuracy: 0.9583 - loss: 0.2736
```

Рисунок 3.9 – Точність моделі 93+% на всіх трьох датасетах D_{tr} , D_{val} , D_{test}

При подальшому використання моделі також було помічено, що вона є більш чутливою до таких жестів як нейтральне обличчя, відкритий рот та підняті брови ніж до інших, тобто вихідна ймовірність цих жестів була відносно більшою. Стандартний прийом по балансуванню датасету зі зменшенням кількості екземплярів цих класів не показав значних змін, скоріше за все, це говорить про факт схожості цих жестів на інші і відповідно збільшення їх загальної ймовірності. Дана особливість, теоретично, може бути вирішена зміною кардинальною архітектури моделі, проте враховуючи те, що отримана модель все ще є достатньо чутливою до всіх жестів та показує дуже хорошу загальну точність, це не є критичним для даної роботи, хоча може бути одним із вагомих покращень механізму при подальшому розвитку.

Реалізацію завантаження та підготовки датасету, побудови та тренування моделі нейромережі можна знайти у додатку А (файл train_gesture_recognition.py).

3.4 Використання моделі для введення жестів

Підключення моделі розпізнавання орієнтирів обличчя та розробленої моделі розпізнавання жестів до відео потоку кадрів в реальному часі результуватиме у неперервну та неконтрольовану детекцію жестів на абсолютно кожному кадрі, така поведінка не підходить для введення біометричного пароля, тому необхідно створити додаткову логіку для роботи з моделями машинного навчання, яка зможе забезпечити цей процес.

Розглядаючи задачу контрольованого введення послідовності жестів, механізм може стикатися з наступними зовнішніми проблемами вхідних даних:

- початковий стан обличчя не є нейтральним і нагадує один із жестів;
- введення жесту не є достатньо швидким, через що довга послідовність кадрів класифікується до того самого жесту;
- стан обличчя після введення жесту не є повністю нейтральним і є наближеним до одного із жестів;

- неідеальне або часткове введення жесту при якому ймовірність нейтрального стану перевищує ймовірність активного жесту;
- ненавмисний частковий рух обличчя, що розпізнається як жест.

Першим прийомом для вирішення цих проблем у механізмі даної роботи є створення таймауту вводу T_i, тобто короткого проміжку часу після введення жесту в який механізм перестає розпізнавати жести, для того щоб обличчя користувача встигло повернутись у псевдо нейтральний стан. Враховуючи набір жестів механізму та швидку валідацію значення було встановлено до $T_i = 0.7$ секунди.

Другим прийомом є використання відносного збільшення ймовірності жестів між кадрами замість абсолютної ймовірності жесту в конкретному кадрі для визначення введеного жесту. Для цього необхідно зберігати значення ймовірностей жестів на попередньому кадрі $P_0 = (p_{0_0}, \dots, p_{0_n})$ та порівнювати його з поточними ймовірностями $P = (p_0, \dots, p_n)$, отримуючи значення ΔP, найбільша Δp_i і буде визначати введений жест. При цьому слід ввести граничні значення зміни для активації жестів T_{act} тільки при перевищенні яких жест буде прийнято за введений. Математичне представлення цих кроків можна побачити у формулах 3.1 та 3.2 відповідно.

$$\Delta p_{max} = \max\left(\frac{p_i}{p_{0_i}}\right), i_{\Delta p_{max}} = \arg_{\mathrm{i}} \max\left(\frac{p_i}{p_{0_i}}\right), i = 0 \dots n \tag{3.1}$$

$$act = \Delta p_{max} > T_{act}(i_{\Delta p_{max}}) \tag{3.2}$$

Програмну реалізація цього алгоритму можна побачити на рисунку 3.10.

```
def resolve_gesture_delta(cur_probs, new_probs):
    DIV_NORM = 10**6
    ACT_THRESHOLDS = [3, 5, 3, 3, 3, 3, 3]
    prob_deltas = [(n*DIV_NORM)/(c*DIV_NORM) for c, n in zip(cur_probs, new_probs)]
    max_delta = max(prob_deltas)
    gesture = prob_deltas.index(max(prob_deltas))
    if max_delta < ACT_THRESHOLDS[gesture]: return None
    return gesture
```

Рисунок 3.10 – Програмна реалізація визначення жестів на основі Δp_{max}

Цей прийом дозволяє одночасно вирішувати проблеми неідеального введення, ненавмисного введення та недостатньо нейтрального початкового стану та

стану обличчя між введенням жестів. Варто зазначити цікавий факт, під час поверхневої валідації алгоритму визначення жестів одразу було помічено, що малі ненавмисні рухи очей та повік користувача призводили до активації жесту блимання, через цю особливість граничне значення збільшення ймовірності для блимання було встановлено до 5, в той час як для всіх інших жестів значення 3 було достатнім для забезпечення адекватної чутливості.

Загалом реалізація цих двох достатньо простих прийомів забезпечила дуже хороший рівень контролю над введенням, що буде показано у розділі про демонстраційний додаток.

3.5 Інтеграція моделі виявлення аномалій

Під час розробки теоритечних основ технології в розділі 2.4 було визначено, що цільовими даними для виявлення аномалій в механізмі цієї роботи є динаміка руху точок обличчя, визначено тип аномалій та обрано алгоритм LOF. Ключовим принципом роботи цього алгоритму є оцінка відхилення локальної щільності точки по відношенню до певної кількості сусідніх точок, у випадку більшого відхилення – більша ймовірність того, що екземпляр є аномалією [52].

LOF здатний оцінювати аномальність точки за будь-якою кількістю характеристик, проте для того щоб адекватно оцінювати відхилення щільності точок необхідно забезпечити високу щільність в нормальних випадках, це означає, що чим більше нормальних даних буде мати алгоритм, тим більш точно він зможе виявляти аномальні точки. Це є найбільшою проблемою виявлення аномалій в механізмі даної роботи. На відміну від розпізнавання жестів, які мають спільні риси в усіх людей, питання аномальності руху певних точок обличчя при відтворені жеста є індивідуальним для кожного користувача, оскільки залежить від індивідуальних особливостей роботи м’язів обличчя. Це означає, що єдиними відомими нормальними даними динаміки точок обличчя в механізмі є ті, що можуть бути зібрані при проходженні користувачем налаштування аутентифікації, тобто декілька

прикладів, в залежності від кількості разів підтвердження біометричного пароля та кількості входжень жесту у пароль.

Зважаючи на проблему обмеженості нормальних даних, перш за все, необхідно уточнити вигляд вхідних даних для визначення аномалій. Так само як і у випадку з розпізнаванням жестів, використовувати всі 478 точок результату Mediapipe Face Mesh V2 не є доречним, оскільки абсолютна більшість із них не будуть мати достатньо великої амплітуди руху, тому було виділено підмножину із 12 граничних точок губ, очей та брів які повинні рухатись найбільше при введенні жестів. Набір відповідних індексів результату Mediapipe Face Mesh V2 можна побачити в додатку А (файл face_landmakrs_subset.py). На рисунку 3.11 провізуалізовано набір із 12 точок обличчя для виявлення аномалій міміки.

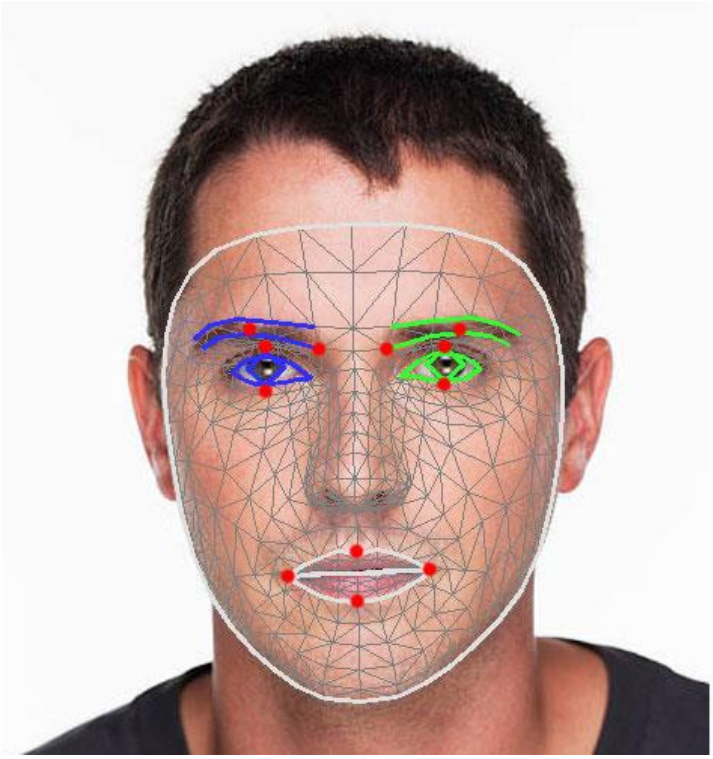


Рисунок 3.11 – Набір точок обличчя для виявлення аномалій міміки

Як уже відомо динаміка точок описується двома атрибутами: відносним моментом часу t та положенням точки p, положення точок будуть отримуватись із результату моделі Mediapipe Face Mesh V2, яка видає нормалізовані тривимірні координати (x, y, z). Теоретично, LOF може оцінювати аномальність точки за будь-якою кількістю атрибутів, проте всі

атрибути мають передаватись в одному вимірі, це означає, що при передачі всіх трьох координат p, значущість атрибута відносного моменту часу t буде зменшуватись, хоча з точки зору природи досліджуваних аномалій, момент часу є дуже важливим, оскільки одне і те саме положення певної точки в різні моменти часу може бути як нормальним, так і аномальним. Для збереження значущості атрибуту t було прийнято рішення спроектувати координати точок на один найбільш значущий вимір. Насправді, зважаючи на цільові точки та м'язи, які приводять їх до руху, рух майже всіх точок можна віднести до однієї площини, тому що вони майже не рухаються, або не можуть рухатись в інших площинах. В таблиці 3.1 наведено основні площини руху та обрані осі координат для проекції положення для кожної із 12 цільових точок.

Таблиця 3.1 – площини руху та осі проектування положення точок обличчя

Точка обличчя	**Площина руху**	**Вісь для проектування**
Лівий куток рота	горизонтальна	x
Правий куток рота	горизонтальна	x
Центр верхньої губи	горизонтальна, вертикальна	x
Центр нижньої губи	горизонтальна, вертикальна	x
Внутрішній край лівої брови	вертикальна	y
Центр лівої брови	вертикальна	y
Внутрішній край правої брови	вертикальна	y
Центр правої брови	вертикальна	y
Центр верхнього повіка лівого ока	вертикальна	y
Центр нижнього повіка лівого ока	вертикальна	y
Центр верхнього повіка правого ока	вертикальна	y
Центр нижнього повіка правого ока	вертикальна	y

Таким чином динаміка кожної точки обличчя перетворюється на залежність одного значення p від часу t, що максимізує вплив моменту часу на оцінку аномальності. На рисунку 3.12 можна побачити реалізацію функції для фільтрації точок та проектування положення на значущу вісь координат.

```
def get_ad_landmarks(detection_result) -> ad.LandmarksFrame:
    landmarks = detection_result.face_landmarks[0]
    ad_landmarks = {}
    for l in ad.AnomalyLandmark:
        l_index = ad.landmark2i_dict[l]
        l_sig_axis = ad.landmark2axis_dict[l]
        ad_landmarks[l] = landmarks[l_index].__dict__[l_sig_axis]
    return ad_landmarks
```

Рисунок 3.12 – Функція для фільтрації та проектування положень точок обличчя для виявлення аномалій

Для отримання відносного моменту часу t необхідно визначити проміжок часу T_{ad} на якому динаміка точки буде досліджуватись на аномальність, як вже було визначено, виявлення аномалій повинно відбуватися при введені жестів, це означає що досліджуваний проміжок часу повинен знаходитись перед моментом розпізнавання жесту, при цьому не перевищуючи таймаут вводу T_i, який описувався у попередньому розділі 3.4, для запобігання перетину декількох жестів. Для даної роботи було встановлено значення $T_{ad} = 0.5$ секунди. Таким чином для визначення будь-якого відносного моменту часу t на проміжку T_{ad} достатньо відняти від нього момент початку проміжку T_{ad_0}. Нарешті ще раз зазначимо, що досліджуваною аномалією є динаміка точки на проміжку T_{ad}, в кожний момент якого точка може почати рухатись аномально, тобто на вхід алгоритму виявлення аномалій буде передаватись вся траєкторія, що буде складатися із множини точок, точна кількість цих точок буде залежати від частоти кадрів вхідного відео.

Для реалізації компоненту виявлення аномалій було використано фреймворк pyod, який має готову до використання модель LOF. При створенні моделей параметр contamination (забрудненість даних аномаліями) був

виставлений до значення 0.01, оскільки при створенні до моделі передаватимуться тільки нормальні дані. У випадку LOF навчання зводиться до збереження відомих нормальних даних, в якості основи для оцінки, та обрахування кількох внутрішніх параметрів. Особливістю компоненту є те, що аномальність міміки залежить від жесту, тобто кожний використаний в паролі жест повинен мати свою модель LOF, додатково до цього, динаміка кожної цільової точки оцінюється окремо, це означає, що необхідно створити $12N_g$ моделей LOF, де N_g – це кількість жестів використаних у біометричному паролі. Для забезпечення цього процесу було реалізовано функцію, яка приймає до себе об'єкт із наборами даних для кожної із цільових точок обличчя, тренує та зберігає модель LOF для кожної з них, код можна знайти у додатку А (файл anomaly_detection.py).

3.6 Оцінка аномальності введених жестів

Знаючи деталі інтеграції моделі виявлення аномалій до механізму, сформулюємо задачу компоненту виявлення аномалій міміки обличчя. При введені жесту g_i для кожної точки обличчя $l_j, j = 1 \dots 12$ записати множину точок траєкторії $S_{l_j} = \left\{\left(t_{0,} p_{l_{j0}}\right), \dots \left(t_{k,} p_{l_{jk}}\right)\right\}$, де $p_{l_{jz}}$ – положення l_j на значущій осі координат, t_z – відносний момент часу із множини досліджуваних моментів часу $T_{ad}, P(T_{ad}) = k, z = 1 \dots k,$ сформувавши множину траєкторій $S = \{S_{l_0}, \dots, S_{l_{12}}\}$. Для кожної точки $\left(t_{z,} p_{l_{jz}}\right)$ кожної траєкторії із множини S визначити оцінку аномальності $e_{l_{jz}}$ та на основі всіх оцінок $e_{l_{jz}}$ розрахувати комплексну оцінку аномальності введеного жесту e_{g_i}. Значення k залежатиме від частоти кадрів відео потоку f, наприклад для $f = 20$ кадрів в секунду $k = f * 0.5 = 10$.

Для розрахування комбінованої оцінки аномальності жесту g_i використовувався наступний евристичний алгоритм:

1. Визначити максимум $e_{max\,l_j}$ множини оцінок точок траєкторії E_{l_j} для траєкторій S_{l_j}.
2. Відібрати підмножину значущих оцінок траєкторії $E_{sig\,l_j} = \left\{e_{l_{jz}} \in E_{l_j} \middle| e_{l_{jz}} \geq e_{max\,l_j} * r_S\right\}$, де r_S – коефіцієнт максимума значущих оцінок траєкторії.
3. Обчислити оцінку траєкторії $e_{S_{lj}}$ як середнє арифметичне множини значущих оцінок траєкторії $E_{sig\,l_j}$.
4. Визначити максимум $e_{max\,S_{lj}}$ множини оцінок траєкторій жесту $E_{g_i} = \{e_{S_{lj}}\}$.
5. Відібрати підмножину значущих оцінок жесту $E_{sig\,g_i}$ аналогічно до кроку 2 із коефіцієнтом максимума значущих оцінок жесту r_g.
6. Обчислити комплексну оцінку жесту g_i як середнє арифметичне множини $E_{sig\,g_i}$.

Ідея алгоритму полягає в тому, щоб використовувати більшу кількість оцінок при невеликій відмінності між абсолютним максимумом та іншими оцінками та меншу кількість оцінок при великій відмінності, таким чином збільшуючи вплив максимума коли він відносно більший за інші оцінки. Контроль за розмежуванням відносно великих і відносно малих відмінностей здійснюється за допомогою коефіцієнтів r_S та r_g на обох рівнях траєкторії та жесту. Візуальне представлення ідеї алгоритму можна побачити на рисунку 3.13.

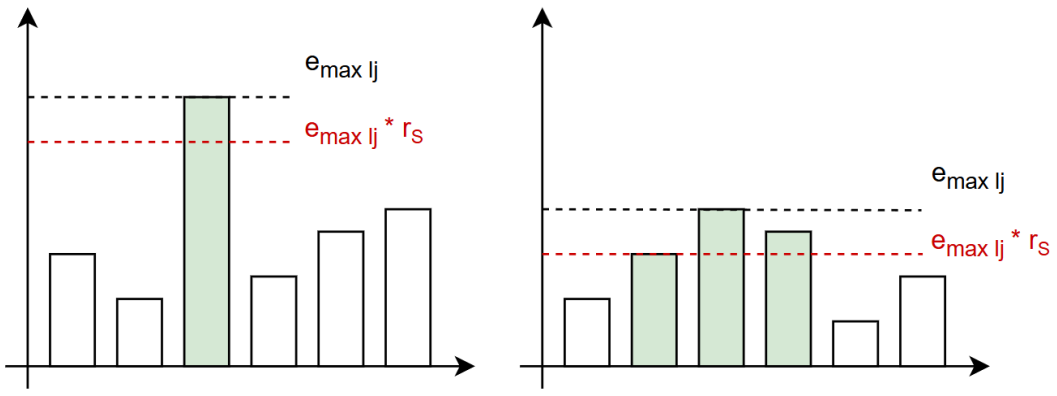
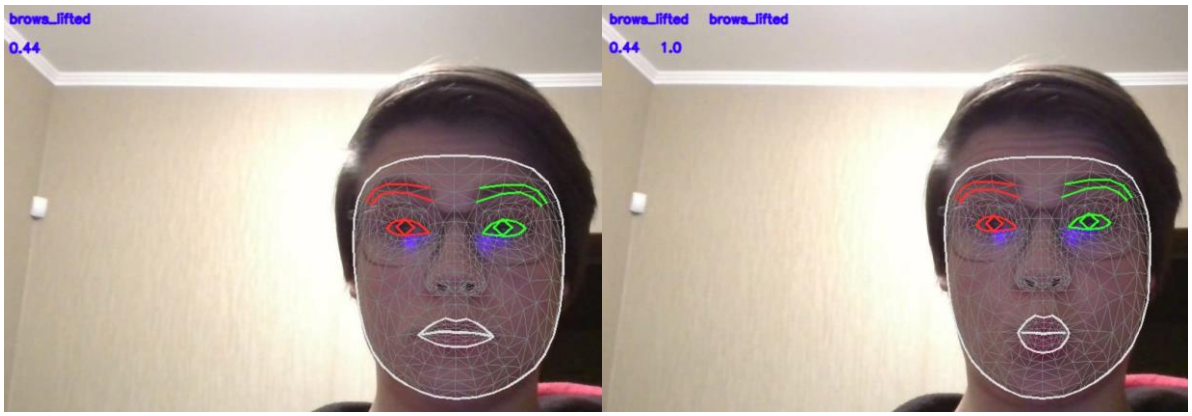


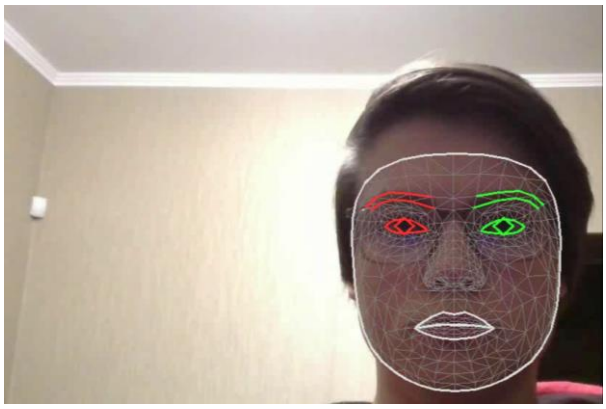
Рисунок 3.13 – Представлення ідеї алгоритму вибору значущих оцінок

Також вже із постановки задачі видно, що для оцінки аномальності одного введеного жесту доведеться виконати десятки або навіть сотні запусків алгоритму LOF, кожен з яких буде порівнювати точки принаймні із десятками сусідніх точок. Хоча LOF і є відносно легким та швидким алгоритмом, для забезпечення максимальної швидкодії було вирішено використати багатопоточне програмування за допомогою класу Python ThreadPoolExecutor для розпаралелювання обчислення оцінок траєкторій в окремі потоки. Повну реалізацію процесу оцінки аномальності жесту можна побачити в додатку А (файл anomaly_detection.py).

При тестуванні компоненту виявлення аномалій було підтверджено його функціональність, як можна побачити на рисунку 3.14(а), при введенні жесту піднятих брів в нормальному випадку оцінка аномальності складає 0.44, при введенні того самого жеста зі стисненням кутів рота оцінка складає 1.0 в результаті аномальної динаміки точок рота.



а) б)



в)

Рисунок 3.14 – Нормальний жест (а), аномальний жест (б), пасивний стан (в)

Під час тестування також було помічено, що виявлення аномалій починає працювати значно краще при наявності як мінімум 10 екземплярів нормальних траєкторій точок для одного жеста, хоча ця кількість є малою, враховуючи те, що нормальні дані отримуються під час створення пароля, користувачеві доведеться підтверджувати пароль 9 разів, що є значно більшою кількістю ніж у випадках із традиційними паролями. Отримання нормальних даних, теоретично, може відбуватись в процесі використання, проте логіка того які саме екземпляри повинні використовуватись для оновлення моделі потребує додаткових досліджень та експериментів.

Підсумовуючи компонент виявлення аномалій варто сказати, що не зважаючи на правильне функціонування цього компонента, його робота є недостатньо стабільною. Частина рішень при розробці цього компонента будувалась на гіпотетичних припущеннях і в цілому ступінь опрацьованості цього компонента є нижчим за основний компонент розпізнавання та введення жестів обличчя. Зважаючи на велику перспективність поведінкової біометрії, яка реалізована саме за допомогою виявлення аномалій міміки в механізмі цієї роботи, цей компонент потребує подальшого дослідження та розвитку для покращення роботи алгоритму та вирішення проблеми обмеженості нормальних даних для ініціалізації моделей.

3.7 Створення демонстраційного додатку

Загальна задача розробки демонстраційного додатку в цій роботі полягає у створенні базового інтерфейсу користувача, який дозволить наочно використовувати основні компоненти механізму посилення біометричної аутентифікації, що розробляється в цій роботі, та проходити основні сценарії використання, а саме процес налаштування (створення) аутентифікації та процес перевірки (проходження) аутентифікації.

Розроблений додаток представлений у вигляді двох файлів demo_setup.py та demo_verification.py, в яких повністю реалізовано два ключових сценарії використання. Додаток побудований на основі бібліотеки

комп'ютерного зору OpenCV, яка реалізована у Python модулі cv2, великою перевагою цієї бібліотеки є можливість використання вбудованої камери пристрою, що є однією із найважливіших вимог до демонстраційного додатку. В іншому cv2 не є бібліотекою для розробки інтерфейсів користувача, проте, враховуючи той факт, що демонстраційний інтерфейс в будь-якому разі повинен будуватися навколо відео потоку камери та наявність таких базових функцій як можливість перехоплювати натиснення клавіш на клавіатурі та додавати текст до зображень робить cv2 ідеальним вибором для розробки простого прототипу інтерфейсу користувача без ускладнення додатку додатковими спеціалізованими бібліотеками та архітектурою.

На рисунку 3.15 можна побачити діаграму потоку даних додатку, яка по більшій частині описує його архітектуру, оскільки обробка та збереження проміжних та кінцевих даних є основною частиною роботи додатку.

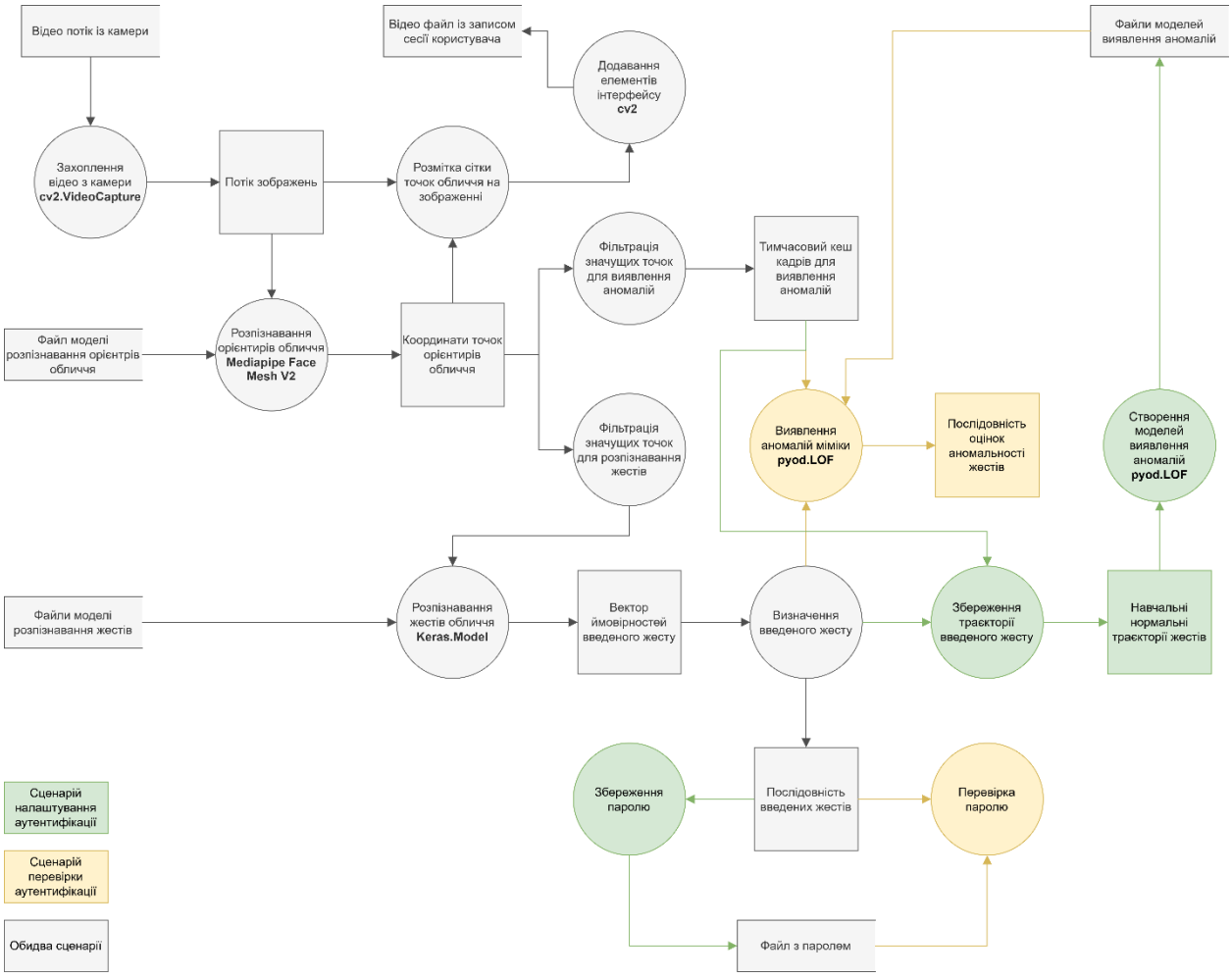


Рисунок 3.15 – Діаграма потоку даних демонстраційного додатку

Як можна побачити на діаграмі, потік даних додатку починається із відео потоку вбудованої камери, який захоплюється за допомогою класу cv2.VideoCapture. Далі додаток зв’язує усі три основні моделі механізму посилення біометричної аутентифікації у послідовний пайплайн для обробки даних, усі моделі зберігаються у спеціалізованих файлах в файловій системі.

Зручною особливістю демонстраційного додатку є запис всієї сесії користувача із розміткою сітки точок обличчя та елементами інтерфейсу, що додаються за допомогою функцій бібліотеки cv2 до вихідного відео файлу, ця функція дозволяє аналізувати та порівнювати процес використання механізму через додаток без залучення додаткового програмного забезпечення для запису екрану.

Біометричний пароль зберігається у вигляді текстового файлу в локальній файловій системі, тут необхідно ще раз наголосити, що таке збереження паролю реалізоване виключно в демонстраційних цілях, у реальних сценаріях використання біометричний пароль повинен зберігатись зі слідуванням всім правилам безпеки та збереження паролів.

Остання частина потоку даних, яка стосується виявлення аномалій та пароля відрізняється в залежності від сценарія, як можна побачити на рисунку 3.15. В сценарії налаштування аутентифікації додаток зберігає усі траєкторії точок обличчя введених жестів та при завершенні процесу використовує їх для створення моделей LOF для кожного жесту та зберігає їх у локальній файловій системі, таким чином моделі компоненту виявлення аномалій перезаписуються із кожним новим налаштуванням аутентифікації, також в цьому сценарії додаток зберігає введену послідовність жестів, тобто біометричний пароль, до текстового файлу. В сценарії перевірки аутентифікації створені моделі виявлення аномалій використовуються для оцінки аномальності при введенні кожного жесту, а послідовність оцінок аномальності зберігається і відображається як один із елементів інтерфейсу, після завершення введення послідовності жестів, вона порівнюється із збереженим у файлі паролем.

На рисунку 3.16 показаний скріншот інтерфейсу демонстраційного додатку. На рисунку можна побачити 4 основних елемента інтерфейсу:

- послідовність введених жестів у вигляді назв жестів;
- послідовність оцінок аномальності введених жестів;
- статус, що описує різні стани в процесі використання, в залежності від сценарію та етапу процесу;
- підказка про елементи управління демонстраційним додатком.

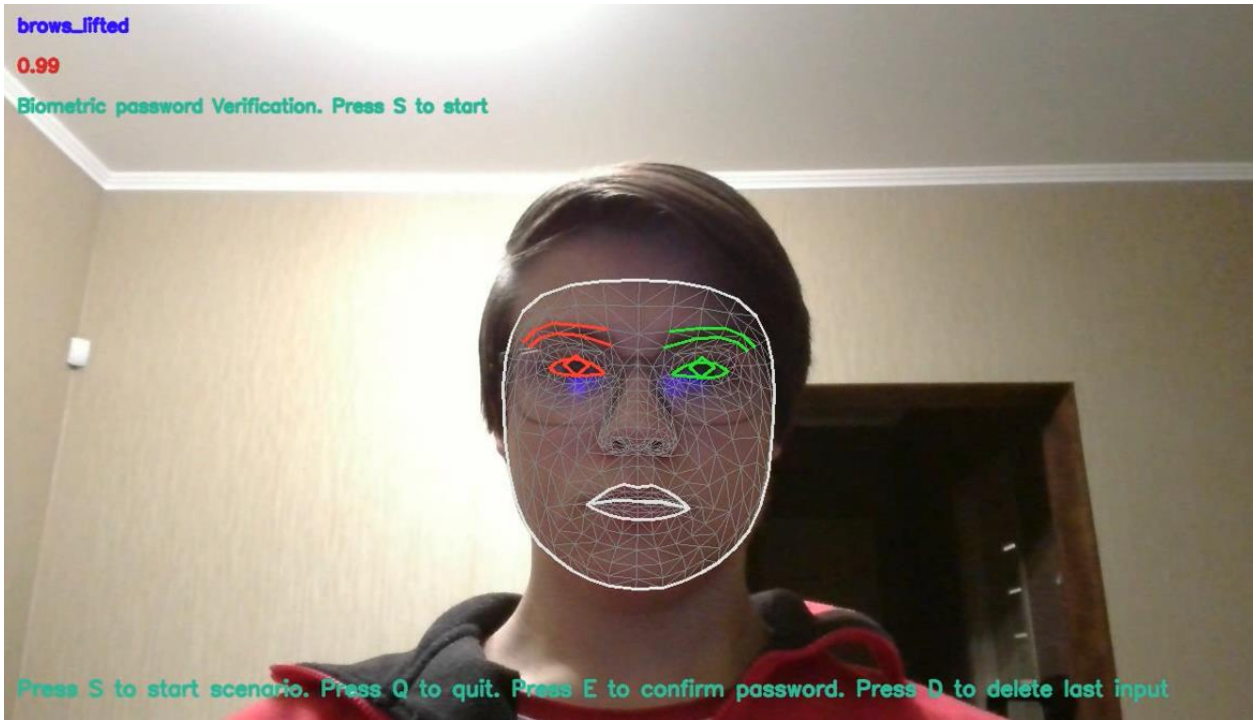


Рисунок 3.16 – Інтерфейс демонстраційного додатку

Для відображення інтерфейсу був створений функціональний модуль ui який додає кожний із елементів інтерфейсу до зображення, його реалізацію можна знайти у додатку А (файл ui.py). Елементи інтерфейсу додаються до відео за допомогою функції cv2.putText.

Елементарне управління демонстраційним додатком здійснюється через клавіатуру за допомогою функції cv2.waitKey() та можливості отримання кодів натиснених клавіш із неї. Додаток використовує наступні клавіші для управління:

- S – розпочинає сценарій та запускає відео потік в обробку моделями механізму, до цього моменту додаток працює у режимі відображення статусу та підказки управління;
- Q – перериває сценарій та завершує відео запис сесії користувача в будь-який момнет часу;
- E – підтверджує введену послідовність жестів для подальшого збереження чи перевірки;
- D – видаляє останній введений жест із послідовності разом із його оцінкою аномальності.

Загалом розроблений демонстраційний додаток задовольняє всі базові вимоги для ознайомлення із механізмом посилення біометричної аутентифікації даної роботи. Більшість параметрів додатку винесені в окремий файл конфігурації config.py для зручної зміни конфігурації та порівняння роботи із різними значеннями параметрів.

ВИСНОВКИ

Метою даної роботи було проведення загального дослідження вразливих факторів біометрії та визначення тих із них, що найбільше заслуговують додаткової уваги, в результаті розробивши технологічні методи для посилення надійності цих факторів, з фокусом на створення прототипу технології, який може бути пере використаний для подальших досліджень або розширений у більш детальні застосування.

В першому розділі роботи були зібрані та систематизовані матеріали, проведено глибокі дослідження у предметній області біометричної аутентифікації та поставлено первинні задачі для цільової технології.

Під час досліджень було виявлено, що біометрична аутентифікація є найбільш популярним типом аутентифікації у світі і стає все більш поширеним, при цьому, більш конкретно, використання розпізнавання орієнтирів обличчя є другою найпоширенішою всесвітньо модальністю біометрії, вже зараз займає перше місце в певних регіонах, та має великі шанси стати найбільш поширеною у світі. Із наявних проблем, розпізнавання обличчя піддається великій кількості презентаційних атак, певна кількість з яких є успішними; використання мультифакторної аутентифікації в найпоширеніших сценаріях, як розблокування персональних пристроїв, спрощується на користь зручності користувача, одночасно перекладаючи велику відповідальність на біометрію та, іноді, ненавмисно послабляючи фактор знання в результаті дії людського фактору користувачів. В результаті досліджень було посталено первинні задачі для розробки прототипу технологія підвищення надійності біометричної аутентифікації, який зможе зменшити вразливість до презентаційних атак, нівелювати проблему нехтування фактором знання та використовувати поведінкову біометрію як перспективний метод аутентифікації.

В другому розділі роботи було спроектовано коцепцію гібридного механізму біометричної аутентифікації та проведено дослідження і підбір технологічних методів для його реалізації.

Гібридний механізм поєднує використання глибоко інтегрованого фактору знання у формі біометричного пароля – послідовності жестів обличчя шляхом розпізнавання жестів із відео, а також використання алгоритму виявлення аномалій на даних динаміки ключових точок обличчя під час введення біометричного пароля в якості поведінкової біометрії, яка надає додатковий вимір інформації для прийняття рішень у процесі аутентифікації. Тим самим зменшуючи вразливість від презентаційних атак шляхом їх кардинального ускладнення та вирішення проблеми нехтування фактором знання за допомогою його глибокого зв’язування із біометрією обличчя. В якості первинного вузла обробки даних було обрано модель розпізнавання точок орієнтирів обличчя Google Mediapipe Face Mesh V2, яка надає дані про координати точок обличчя в якості вхідних даних для обох компонентів механізму. Механізм призначений в першу чергу для використання на основі існуючих базових систем біометричної аутентифікації для їх додаткового посилення, або використання окремо в сценаріях де це є доречним. Розробивши теоретичні основи технології, з розумінням основних функціональних компонентів було сформульовано функціональні вимоги до них.

В третьому розділі цієї роботи було виконано реалізацію спроектованого гібридного механізму аутентифікації, а також побудовано демонстраційний додаток для взаємодії із ним.

В результаті практичної реалізації було створено датасет із новим типом даних для задачі класифікації жестів обличчя та опубліковано його на платформі Kaggle. Було проведено підготовку датасету для тренування моделі та розроблено архітектуру моделі нейронної мережі для виконання задачі класифікації жестів. Побудовано модель нейронної мережі на фреймворках Keras та Tensorflow. Проведено процес навчання моделі із досягненням хороших результатів точності, також було реалізовано додатковий функціонал необхідний для використання моделі класифікації жестів для контрольованого вводу послідовності жестів користувачем. Було розгорнуто досліджено

використання алгоритмів виявлення аномалій на даних виявлення аномалій міміки обличчя (динаміки точок) та розроблено стратегію по інтеграції алгоритму LOF до механізму, що розроблявся у роботі. Було реалізовано процес створення та використання моделей LOF для загальної оцінки аномальності жесту обличчя. Проведено тестування на реальних даних та підтверджено працездатність цього компоненту механізму. Мінусом компонента виявлення аномалій є недостатня опрацьованість, що пов’язана із проблемою отримання достатньої кількості для ініціалізації моделей та відповідною нестабільністю роботи, цей компонент заслуговує на найбільшу увагу в подальшому розвитку механізму посилення надійності біометричної аутентифікації. Наприкінці роботи було створено базовий демонстраційний додаток для взаємодії із механізмом та проходження основних сценаріїв створення та перевірки аутентифікації, який добре підходить для ознайомлення та тестування механізму.

Загалом можна стверджувати, що в результаті роботи було виконано поставлені задачі до досягнуто основної мети по розробці технології для підвищення надійності біометричної аутентифікації. Одним із подальших напрямків розвитку технологій вбачаю підвищення функціональної ефективності компонента виявлення аномалій міміки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Top authentication methods in selected countries 2023. Statista. URL: https://www.statista.com/statistics/1448883/preferred-security-authentication-methods-in-selected-countries (дата звернення: 19.09.2024)
2. Quynh Anh A. Ranking 4 Most Popular Authentication Methods Today. VinCSS. URL: https://blog.vincss.net/what-is-the-best-authentication-method (дата звернення: 19.09.2024).
3. Mascellino A. Cisco report: 81 percent of all smartphones have biometrics enabled. Biometric Update. URL: https://www.biometricupdate.com/202211/cisco-report-81-percent-of-all-smartphones-have-biometrics-enabled (дата звернення: 19.09.2024).
4. Naden C. The rise and rise of biometric authentication. IEC e-tech. URL: https://etech.iec.ch/issue/2023-04/the-rise-and-rise-of-biometric-authentication (дата звернення: 19.09.2024).
5. Biometric Authentication & Identification Market Size, Share 2031. Business Research Insights. URL: https://www.businessresearchinsights.com/market-reports/biometric-authentication-identification-market-110643 (дата звернення: 19.09.2024).
6. Kosinski M. What is Authentication?. IBM - United States. URL: https://www.ibm.com/think/topics/authentication (дата звернення: 19.09.2024).
7. What Is Authentication? Definition and Methods. Microsoft | Microsoft Security. URL: https://www.microsoft.com/en-us/security/business/security-101/what-is-authentication (дата звернення: 20.09.2024).
8. The 5 factors of authentication, and what you should know about them - New York, Westchester, White Plains | Red Key Solutions. Red Key Solutions. URL: https://www.redkeysolutions.com/2019/11/the-5-factors-of-authentication-and-what-you-should-know-about-them (дата звернення: 20.09.2024).

9. Marshall-Heyman T. What is Authentication? Factors, Types, and Examples. Criipto. URL: https://www.criipto.com/blog/what-is-authentication (дата звернення: 01.11.2024).
10. Multi-factor authentication - Glossary. NIST Computer Security Resource Center. URL: https://csrc.nist.gov/glossary/term/multi_factor_authentication (дата звернення: 21.09.2024).
11. Kiennert C., Bouzefrane S., Thoniel P. Authentication Systems. Digital Identity Management. 2015. С. 95–135. URL: https://doi.org/10.1016/b978-1-78548-004-1.50003-1 (дата звернення: 21.09.2024).
12. FIDO Alliance Overview - Changing the Nature of Authentication. FIDO Alliance. URL: https://fidoalliance.org/overview (дата звернення: 21.09.2024).
13. Як зареєструватись у застосунку Дія?. Дія. Підтримка Paperless. URL: https://paperless.diia.gov.ua/instruction/yak-avtorizuvatis-u-zastosunku-diya (дата звернення: 21.09.2024).
14. Fingerprint Recognition. ucr.fbi.gov. URL: https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/fingerprint-recognition.pdf (дата звернення: 21.09.2024).
15. Evarts H. AI Discovers That Not Every Fingerprint Is Unique. Columbia Engineering. URL: https://www.engineering.columbia.edu/about/news/ai-discovers-not-every-fingerprint-unique (дата звернення: 21.09.2024).
16. Grucela A. 70+ Facts About Biometrics (+ Trends & Statistics for 2024). Passport Photo Online. URL: https://passport-photo.online/blog/biometric-statistics/ (дата звернення: 21.09.2024).
17. Global biometric usage by type 2021. Statista. URL: https://www.statista.com/statistics/1338824/global-biometric-usage-by-type/ (дата звернення: 22.11.2024).
18. Contributors to Wikimedia projects. Touch ID - Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Touch_ID (дата

звернення: 22.09.2024).

19. Contributors to Wikimedia projects. Face ID - Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Face_ID (дата звернення: 22.09.2024).
20. Apple iPhone smartphone shipments worldwide 2010-2024. Statista. URL: https://www.statista.com/statistics/299153/apple-smartphone-shipments-worldwide/ (дата звернення: 22.09.2024).
21. U.S. personal devices replacement cycle 2027. Statista. URL: https://www.statista.com/statistics/1021171/united-states-electronics-devices-replacement-cycle/ (дата звернення: 22.09.2024).
22. Wilde D. Here's what 9to5Google readers said they prefer between fingerprint scanners and face unlock. 9to5Google. URL: https://9to5google.com/2021/10/11/heres-what-9to5google-readers-said-they-prefer-between-fingerprint-scanners-and-face-unlock/ (дата звернення: 22.09.2024).
23. Smartphone market shares by vendor 2009-2024. Statista. URL: https://www.statista.com/statistics/271496/global-market-share-held-by-smartphone-vendors-since-4th-quarter-2009/ (дата звернення: 22.09.2024).
24. Samsung for Business. Which smartphone biometric authentication method is most secure?. Samsung Business Insights. URL: https://insights.samsung.com/2021/05/25/which-biometric-authentication-method-is-most-secure-3/ (дата звернення: 22.09.2024).
25. Notebook PC market share by OS worldwide 2020. Statista. URL: https://www.statista.com/statistics/1208590/notebook-pc-market-share-worldwide-by-operating-system/ (дата звернення: 22.09.2024).
26. Contributors to Wikimedia projects. Features new to Windows 10 - Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Features_new_to_Windows_10#Windows_Hello (дата звернення: 22.09.2024).

27. PC average installed base age in the U.S. 2022-2027. Statista. URL: https://www.statista.com/statistics/267474/average-life-of-pc-and-tablets/ (дата звернення: 22.09.2024).
28. Mobile Operating System Market Share Worldwide. StatCounter Global Stats. URL: https://gs.statcounter.com/os-market-share/mobile/worldwide/2023 (дата звернення: 22.09.2024).
29. Post-Pandemic Biometric Challenges and Solutions / K. Neelima та ін. Advances in Logistics, Operations, and Management Science. 2024. С. 196–208. URL: https://doi.org/10.4018/979-8-3693-1347-3.ch013 (дата звернення: 23.09.2024).
30. Presentation Attack Detection: A Systematic Literature Review / M. Pooshideh та ін. ACM Computing Surveys. 2024. URL: https://doi.org/10.1145/3687264 (дата звернення: 29.09.2024).
31. Biometric Template Attacks and Recent Protection Mechanisms: A Survey / S. M. Abdullahi та ін. Information Fusion. 2023. С. 102144. URL: https://doi.org/10.1016/j.inffus.2023.102144 (дата звернення: 29.09.2024).
32. Biometric Authentication Methods on Mobile Platforms / A. M. W. S. Edoh та ін. International Journal of Mobile Computing and Multimedia Communications. 2023. Т. 14, № 1. С. 1–16. URL: https://doi.org/10.4018/ijmcmc.334130 (дата звернення: 29.09.2024).
33. Burt C. Hack of Samsung Galaxy S10 ultrasonic fingerprint sensor suggests no liveness detection. Biometric Update | Biometrics News, Companies and Explainers. URL: https://www.biometricupdate.com/201904/hack-of-samsung-galaxy-s10-ultrasonic-fingerprint-sensor-suggests-no-liveness-detection (дата звернення: 30.09.2024).
34. Bkav’s Mask Fools Face ID, Even with ‘Attention Aware’ Feature On. Mobile ID World. URL: https://mobileidworld.com/archive/bkav-mask-fools-face-id-011295/ (дата звернення: 02.10.2024).
35. Researchers Use Tape and Glasses to Spoof Face ID Liveness Detection. ID

Tech. URL: https://idtechwire.com/biometrics-news-researchers-use-tape-and-glasses-to-spoof-face-id-liveness-detection/ (дата звернення: 02.10.2024).

36. Burt C. Hack of Samsung Galaxy S10 ultrasonic fingerprint sensor suggests no liveness detection. Biometric Update. URL: https://www.biometricupdate.com/201904/hack-of-samsung-galaxy-s10-ultrasonic-fingerprint-sensor-suggests-no-liveness-detection (дата звернення: 02.10.2024).
37. Rocha A. The Hidden Vulnerability of iOS Face ID: How Hackers Exploit PIN-Based Backup Authentication. LinkedIn. URL: https://www.linkedin.com/pulse/hidden-vulnerability-ios-face-id-how-hackers-exploit-pin-based-rocha (дата звернення: 02.10.2024).
38. Face landmark detection guide | Google AI Edge | Google AI for Developers. Google AI for Developers. URL: https://ai.google.dev/edge/mediapipe/solutions/vision/face_landmarker (дата звернення: 25.10.2024).
39. Model Card MediaPipe Face Mesh V2. URL: https://storage.googleapis.com/mediapipe-assets/Model%20Card%20MediaPipe%20Face%20Mesh%20V2.pdf (дата звернення: 27.10.2024).
40. Contributors to Wikimedia projects. Thresholding (image processing) - Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Thresholding_(image_processing) (дата звернення: 26.10.2024).
41. Contributors to Wikimedia projects. Multiclass classification - Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Multiclass_classification (дата звернення: 26.10.2024).
42. How to Update Neural Network Models With More Data. Machine Learning Mastery. URL: https://machinelearningmastery.com/update-neural-network-

models-with-more-data/ (дата звернення: 25.10.2024).

43. Contributors to Wikimedia projects. Password strength - Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Password_strength (дата звернення: 01.11.2024).
44. Anatomy, Head and Neck: Facial Muscles - StatPearls - NCBI Bookshelf. National Center for Biotechnology Information. URL: https://www.ncbi.nlm.nih.gov/books/NBK493209/ (дата звернення: 02.11.2024).
45. A Comprehensive Introduction to Anomaly Detection. Datacamp. URL: https://www.datacamp.com/tutorial/introduction-to-anomaly-detection (дата звернення: 03.11.2024).
46. ADBench: Anomaly Detection Benchmark / S. Han та ін. SSRN Electronic Journal. 2022. URL: https://doi.org/10.2139/ssrn.4266498 (дата звернення: 03.11.2024).
47. Foorthuis R. A Typology of Data Anomalies. Communications in Computer and Information Science. 2018. № 854. URL: https://doi.org/10.1007/978-3-319-91476-3_3 (дата звернення: 10.11.2024).
48. Kosiuk M. Facial gestures. Kaggle. URL: https://www.kaggle.com/datasets/mykhailokosiuk/facial-gestures (дата звернення: 06.12.2024).
49. Khanna C. Number of Parameters in a Feed-Forward Neural Network. Medium. URL: https://towardsdatascience.com/number-of-parameters-in-a-feed-forward-neural-network-4e4e33a53655 (дата звернення: 20.11.2024).
50. Contributors to Wikimedia projects. Softmax function - Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Softmax_function (дата звернення: 25.11.2024).
51. Contributors to Wikimedia projects. Convolutional neural network -

Wikipedia. Wikipedia, the free encyclopedia. URL: https://en.wikipedia.org/wiki/Convolutional_neural_network (дата звернення: 26.11.2024).

52. Belyadi H., Haghighat A. Unsupervised machine learning: clustering algorithms. Machine Learning Guide for Oil and Gas Using Python. 2021. С. 125–168. URL: https://doi.org/10.1016/b978-0-12-821929-4.00002-0 (дата звернення: 30.11.2024).

ДОДАТОК А

Посилання на репозиторій GitHub із програмною реалізацією роботи

https://github.com/MykhailKo/biometric-password