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

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____С.В. Казміруук
«___»_____20__ р.

На правах рукопису
УДК 004.056.5:510.22(043.3)

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ
ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Система біометричної автентифікації користувачів комп'ютерних систем

Виконавець: А.О. Нестерук
Науковий керівник: к.т.н. О.О. Висоцька
Нормоконтролер: к.т.н. О.О. Висоцька

Київ 2020

ВСТУП

Актуальність. Виходячи із сьогодення, технології ідентифікації особи набувають як все більшого удосконалення так і все більшої потреби у багатьох сферах життєдіяльності. Створення системи для розпізнавання особи потребує великої кількості технічних засобів для зчитування та обробки даних, зберігання бази даних та носіїв особистої інформації. Але з використанням біометричних даних таку систему можна зробити без носіїв особистої інформації, оскільки дана інформація зчитується системою з самої ж людини, що одночасно і значно підвищує стійкість до підробки. Цей факт робить актуальним створення саме біометричних систем розпізнавання. Крім того, актуальність роботи ґрунтується на збільшенні кількості об’єктів, де потрібно вести швидку та безконтактну ідентифікацію особи для правильного розмежування доступу.

Створення системи автентифікації потребує великої кількості часу та вкладання значних коштів. Її стійкість до прийняття неправильного рішення є одним із найважливіших показників, оскільки дані помилки системи можуть призвести як просто до незручностей і пауз у процесі виробництва так і до значних збитків. Тобто виникає потреба зменшити залежність системи від зовнішніх факторів задля збільшення стабільності прийняття правильного рішення.

Останні тенденції показують, що як для приватних підприємств та організацій, так і для державних органів, що працюють із цінною інформацією, розвиток технологій контролю доступу завжди актуальний. Допуск до подібного роду ресурсу компанії сторонньої особи може призвести до значних збитків.

Створення системи біометричної автентифікації дозволить здійснювати ідентифікацію особи швидко та дистанційно без потреби надавати спеціальний носій індивідуальних даних. Це дозволить як оптимізувати процес допуску до

робочого місця, так і використовувати у цьому процесі дані, які складніше скопіювати та підробити.

Відомі підходи до вирішення поставленої задачі. Існує досить велика різноманітність методів біометричної ідентифікації. Основною їх класифікацією є об’єкт аналізу, тобто: форма лиця, відбиток пальця, клавіатурний почерк, голос. Одними з найпоширеніших є методи розпізнавання по лицю. Як приклад можна привести алгоритм автоматичної побудови 3D-моделей лиця, що деформуються. Він заснований на методі відновлення ландшафтних поверхонь Шепарда та набору особистих 3D-моделей лиць. Також не менш поширеним методом є ідентифікація по відбитку пальця. Прикладом такого методу є ідентифікація відбитку по типу контрольних точок, що опирається на контрольні точки, розгалуження і кінцівки, що можуть змінювати свій тип при взаємодії з перешкодами.

Метою роботи є розробка системи біометричної автентифікації користувачів, в якій завдяки виконанню попередньої обробки зразків, забезпечується підвищена стійкість до умов виконання процесу автентифікації.

Для досягнення поставленої мети вирішуються такі **задачі**:

- проаналізувати сучасні методи біометричної ідентифікації та обрати оптимальний метод, для вирішення задачі розпізнавання в системі біометричної автентифікації користувачів комп’ютерної системи;
- розробити технологію попередньої обробки зразків для забезпечення підвищеної стійкості до умов виконання процесу автентифікації;
- розробити та провести тестування біометричної системи автентифікації користувачів комп’ютерної системи, яка використовує розроблену технологію попередньої обробки зразків.

Галузь застосування. Розроблена система біометричної автентифікації відноситься до галузі інформаційної безпеки і може бути використана для

підвищення рівня захищеності комп’ютерної системи за рахунок використання методів біометричної автентифікації.

Об’єктом дослідження є процес біометричної автентифікації користувачів комп’ютерних систем.

Предметом дослідження є технології, методи та системи біометричної автентифікації користувачів комп’ютерних систем.

Методи дослідження базуються на основі усереднення інтенсивності пікселів (для попередньої обробки зразків), статистичного аналізу (для навчання каскаду Хаара), каскаду Хаара (для розпізнавання обличь), Local Binary Pattern (для розробки методу біометричної автентифікації), та об’єктно-орієнтовного програмування (для програмної реалізації розробленої системи).

Наукова новизна одержаних результатів полягає у наступному:

- вперше розроблена біометрична система автентифікації користувачів за геометрією їх обличь, яка за рахунок використання вперше запропонованої технології додаткової попередньої обробки зображень, перед початком процесу автентифікації, здатна безпомилково отримувати біометричні характеристики незалежно від умов виконання процесу автентифікації, збільшуючи при цьому імовірність правильного розпізнавання користувачів.

Практична цінність отриманих результатів:

- розроблено систему біометричної автентифікації користувачів комп’ютерної системи, яка може використовуватися для розмежування доступу між користувачами;
- розроблено технологію виявлення особи в об’єктиві відео-камери із подальшим порівнянням її особистих характеристик із тими, що містяться у системі як еталонні, що дає змогу виконувати ідентифікацію особи, чиї дані містяться у системі.

Апробація. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Нестерук А.О. Математична модель захисту інформаційно-комунікаційної системи / Нестерук А.О. // Материали XVI международна научна практична конференция Динамиката на съвременната наука – 2020, 15 – 20 юли 2020 г.: София. «Бял ГРАД-БГ ОДД» – P. 69-71.URL: http://www.rusnauka.org/cgi-bin/search/step7_info.cgi?id=283723&idw=v2irmKULSb9LR8fZfh
- Нестерук А.О. Система біометричної автентифікації користувачів комп'ютерних систем / Нестерук А.О., Висоцька О.О. // Materials of the XVI International scientific and practical Conference Scientific horizons - 2020, September 30 - October 7, 2020: Sheffield. Science and education LTD – P. 66-69. URL: http://www.rusnauka.org/cgi-bin/search/step7_info.cgi?id=284401&idw=RqX0bg6Qz6zMgSEV2P

РОЗДІЛ 1. АНАЛІЗ НОРМАТИВНО-ПРАВОВОЇ БАЗИ В ГАЛУЗІ ЗАХИСТУ ІНФОРМАЦІЇ

1.1. Нормативно-правова база

На початку дослідження обраної теми, а саме дослідження та розробки систем біометричної автентифікації користувачів комп'ютерних систем, доцільним є проаналізувати законодавство України у сфері обробки біометричних даних. Даний аналіз дозволить визначити основні поняття, які використовуються у даній сфері.

1.1.1. Закон України «Про інформацію»

Згідно з Законом України «Про інформацію» надається визначення такої термінології [1]:

- інформація - будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді;
- захист інформації - сукупність правових, адміністративних, організаційних, технічних та інших заходів, що забезпечують збереження, цілісність інформації та належний порядок доступу до неї.

Метою створення системи автентифікації є захист інформації від несанкціонованого доступу. Для здійснення автентифікації використовується інформація, у класичній системі автентифікації це ім’я користувача (логін) та секретна комбінація символів (пароль). У випадку біометричної автентифікації як пароль використовуються певна ознака людського тіла, тобто людина у даному випадку виступає носієм інформації.

Суб'єктами інформаційних відносин є: фізичні особи, юридичні особи, об'єднання громадян, суб'єкти владних повноважень. У даному випадку суб’єктом буде виступати користувач, що намагатиметься автентифікуватися у системі.

Об'єктом інформаційних відносин є інформація. Об’єктом у даному випадку будуть виступати біометричні дані, за допомогою яких буде проводитися процес автентифікації.

Інформація з обмеженим доступом є конфіденційна, таємна та службова інформація. Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом [1].

Біометричні дані є конфіденційною інформацією особи. Користувач повинен надавати її системі виключно за своєю згодою. Для коректної роботи системи повинна існувати бібліотека зі збереженими біометричними даними всіх користувачів, тобто зберігати конфіденційну інформацію користувача.

1.1.2. Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»

Розглянемо значення термінів, що безпосередньо відносяться до процесу біометричної автентифікації. А саме біометричні дані та параметри, та ідентифікація особи.

Згідно з Законом України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» надається визначення такої термінології [2]:

- біометричні дані - сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб;
- біометричні параметри - вимірювальні фізичні характеристики або особистісні поведінкові риси, що використовуються для ідентифікації (впізнання) особи або верифікації наданої ідентифікаційної інформації про особу;
- ідентифікувати - здійснювати комплекс заходів, що дає змогу виконувати пошук за принципом "один до багатьох", зіставляючи дані (параметри) особи, у тому числі біометричні, з інформацією Реєстру;
- ідентифікація особи - встановлення особи шляхом порівняння наданих даних (параметрів), у тому числі біометричних, з наявною інформацією про особу в реєстрах, картотеках, базах даних тощо.

Біометричні дані особи складаються із сукупності біометричних параметрів, що є індивідуальними для кожної особи як самі по собі, так і у

сукупності. Збір одного із виду параметрів дозволить провести коректну ідентифікацію особи та визначити її ім’я, якщо аналогічні біометричні параметри містяться у системі.

1.1.3. Закон України «Про електронні довірчі послуги»

Згідно з Законом України «Про електронні довірчі послуги» надається визначення такої термінології [3]:

- автентифікація - електронна процедура, яка дає змогу підтвердити електронну ідентифікацію фізичної, юридичної особи, інформаційної або інформаційно-телекомунікаційної системи та/або походження та цілісність електронних даних;
- електронна ідентифікація - процедура використання ідентифікаційних даних особи в електронній формі, які однозначно визначають фізичну, юридичну особу або представника юридичної особи;
- засіб електронної ідентифікації - носій інформації, який містить ідентифікаційні дані особи і використовується для автентифікації особи під час надання та/або отримання електронних послуг;
- ідентифікаційні дані особи - унікальний набір даних, який дає змогу однозначно встановити фізичну, юридичну особу або представника юридичної особи;

Носієм біометричної інформації є сама ж людина. Дану інформацію можна привести до електронному вигляду та провести електронну ідентифікацію. Ідентифікаційні дані особи будуть індивідуальні для кожної особи, який би із

параметрів не брався до уваги. Якщо ж використовувати для електронної ідентифікації класичний метод реєстрації користувача у системі за допомогою логіну та паролю, то біометричну ідентифікацію можна використати як засіб для проведення автентифікації. Тобто ввівши самостійно ідентифікаційні дані особа повинна буде підтвердити відповідність їй цих даних за допомогою біометричної ідентифікації, що у сукупності утворить процес автентифікації

1.2. Системи біометричної автентифікації

Біометричні системи автентифікації – це системи, що використовують біометричні дані особи для її автентифікації. Сама ж біометрична автентифікація – це процес перевірки справжності особи через надання своїх біометричних параметрів, що проходять певний процес перетворень згідно з протоколом автентифікації.

Біометричні системи доступу є дуже зручними для користувачів. На відміну від паролів і носіїв інформації, які можуть бути втрачені, вкрадені, скопійовані, біометричні системи доступу засновані на людських параметрах, які завжди знаходяться разом з ними, і проблема їх збереження не виникає. Також неможлива передача ідентифікатора третім особам.

На сьогодні широко використовується велика кількість методів біометричної автентифікації, які діляться на два класи:

- Статичні методи біометричної автентифікації засновані на фізіологічних характеристиках людини, присутніх від народження до смерті, що знаходяться при людині протягом всього його життя, і які не можуть бути втрачені, вкрадені і скопійовані.

- Динамічні методи біометричної автентифікації ґрунтуються на поведінкових характеристиках людей, тобто засновані на характері підсвідомих рухів в процесі відтворення або повторення будь-якої звичайної дії.

Статистичними методами є:

- Автентифікація за відбитками пальців – найпоширеніша біометрична технологія автентифікації користувачів. Метод використовує унікальність малюнка папілярних візерунків на пальцях людей. Відбиток, отриманий за допомогою сканера, перетворюється в цифровий код, а потім порівнюється з раніше введеними наборами еталонів. Переваги використання автентифікації за відбитками пальців - легкість у використанні, зручність і надійність.
- Автентифікація по райдужній оболонці ока – досить поширена біометрична технологія автентифікації користувачів. Метод використовує унікальність ознак і особливостей райдужної оболонки ока. Райдужна оболонка - тонка рухома діафрагма очей з отвором (зіницею) в центрі; розташована за рогівкою, між передньою і задньою камерами ока, перед кришталиком. Райдужна оболонка утворюється ще до народження людини, і не змінюється протягом усього життя. Райдужна оболонка за текстурою нагадує мережу з великою кількістю оточуючих кіл і малюнків, які можуть бути виміряні комп'ютером, малюнок райдужної оболонки дуже складний, це дозволяє відібрати близько 200 точок, за допомогою яких забезпечується висока ступінь надійності автентифікації.
- Автентифікація по сітківці ока – ще одна поширена біометрична технологія автентифікації користувачів. Метод використовує унікальність малюнка кровоносних судин очного дна (що не збігається навіть за умови, що 2 людини є близнюками). Для сканування сітківки використовується інфрачервоне випромінювання низької інтенсивності, спрямоване через зіницю до кровоносних судинах на задній стінці ока. З отриманого сигналу виділяється кілька сотень особливих точок, інформація про яких зберігається в шаблоні.

- Автентифікація по геометрії руки – також поширена біометрична технологія автентифікації користувачів. Метод використовує унікальність форми кисті руки в цілому. Через те, що окремі параметри форми руки не є чимось унікальним, доводиться використовувати кілька характеристик. Скануються такі параметри руки, як вигини пальців, їх довжина і товщина, ширина і товщина тильного боку руки, відстань між суглобами і структура кістки. Також геометрія руки включає в себе дрібні деталі (наприклад, зморшки на шкірі). Хоча структура суглобів і кісток є відносно сталими ознаками, але розпухання тканин або удари руки можуть спотворити вихідну структуру.
- Автентифікація по геометрії лиця – дуже поширена біометрична технологія автентифікації користувачів. Метод використовує унікальність розміщення ХТ каркасу обличчя. Технічна реалізація представляє собою складну математичну задачу. Широке застосування мультимедійних технологій, за допомогою яких можна побачити достатню кількість відеокамер на вокзалах, аеропортах, площах, вулицях, дорогах і інших місцях скупчення людей, стало вирішальним у розвитку цього напрямку. Для побудови тривимірної моделі людського обличчя виділяють контури очей, брів, губ, носа, і інших різних елементів лиця. Потім обчислюють відстань між ними, і за допомогою нього будують тривимірну модель. Щоб знайти цей унікальний шаблон, відповідний певній людині, потрібно від 12 до 40 характерних елементів. Шаблон повинен враховувати безліч варіацій зображення на випадки повороту особи, нахилу, зміни освітленості, зміни виразу.
- Автентифікація по термограмі лиця – менш поширена біометрична технологія автентифікації користувачів. Метод використовує унікальність розподілення тепла на лиці для кожної людини. Термограма виходить за допомогою камер інфрачервоного діапазону. На відміну від автентифікації по геометрії лиця, даний метод розрізняє близнят. Використання спеціальних масок, проведення пластичних операцій, старіння організму людини, температура тіла, охолодження шкіри обличчя в морозну погоду не впливають

на точність термограми. Через невисоку якість автентифікації, метод на даний момент не має широкого поширення.

Динамічними методами є:

- Автентифікація по голосу – досить поширена технологія біометричної автентифікації користувачів. Метод використовує унікальність звукових хвиль людини. Характеризується простотою в застосуванні. Даному методу не потрібна дорога апаратура, досить мікрофона і звукової плати. Існує досить багато способів побудови шаблону по голосу. Зазвичай, це різні комбінації частотних і статистичних характеристик голосу. Можуть розглядатися такі параметри, як модуляція, інтонація, висота тону.
- Автентифікація по рукописному почерку [4, 5, 6] – малопоширена технологія біометричної автентифікації користувачів. Метод використовує унікальність специфічного руху людської руки під час підписання документів. Для збереження підпису використовують спеціальні ручки або сприйнятливі до тиску поверхні. Цей вид автентифікації людини використовує його підпис. Шаблон створюється в залежності від необхідного рівня захисту.
- Автентифікація по клавіатурному почерку – малопоширена технологія біометричної автентифікації користувачів. Метод використовує унікальність стилю набору тексту. Полягає в тому, що є однією з повсякденних задач, що вирішується людьми, є набір текстів на клавіатурі комп'ютера. В процесі того як людина вводить інформацію використовуючи клавіші у користувача виробляється свій особистий стиль набору тих чи інших слів. І цей стиль практично не повторний і залежить від таких параметрів як: кількість пальців, задіяних під час набору тексту; тривалість натискання клавіш; час між натисканнями клавіш; характер помилок у наборі тексту; використання основної або додаткової частини клавіатури; характер здвоєних або послідовних натискань; улюблені поєднання гарячих клавіш і т. д.

1.3. Статистичні методи біометричної автентифікації

Як було сказано раніше, сатистичними методами є ті, що використовують характеристики, які у людини не змінюються з часом. Такі методи поділяються на різні відносно того з якими характеристиками людського тіла вони працюють. Розглянемо детальніше методи, які є найбільш поширеними у побудові систем автентифікації.

1.3.1. Ідентифікація по відбитку пальця

Одним із найпоширеніших методів біометричної ідентифікації є метод ідентифікації за відбитком пальця. Одним із методів реалізації є метод ідентифікації по контрольних точках. Цей метод полягає в наступному.

Метод ідентифікації зображень відбитків пальців стійкий до шуму і дефектів зображень. Метод опирається на характерні точки, розгалуження і закінчення, які під впливом перешкод можуть змінити свій тип. Такі небажані зміни впливають на величину обрахунку, на топологічні та інші характеристики зображень, що може знизити надійність їх ідентифікації. Для компенсації ефекту впливу перешкод вводиться топологічний вектор і правила його нумерації для розгалужень і закінчень.

У більшості відомих підходів характерних точок (ХТ) визначають по скелетних лініях візерунка, які будують на етапі обробки зображення. В опис кожної ХТ m_i входять її координати $(x_i; y_i)$, орієнтація α_i , причому $\alpha_i \in [0;2\pi]$ і,

для повноти подачі, тип $t_i \in \{0,1\}$ зі значенням $t_i = 1$ для закінчення і $t_i = 0$ для розгалуження. Таким чином, безліч всіх ХТ записують у вигляді:

$$\{m_i\} = \{((x_i, y_i), \alpha_i, t_i)\}, i \in 1 \ldots n, \qquad (1.1)$$

де n - число ХТ, розпізнаних на зображенні. Провівши проекції від кожної ХТ перпендикулярно її орієнтації вправо і вліво на суміжні скелетні лінії (далі просто лінії). Після фіксування проекції, на лінії можуть розташовуватися закінчення, розгалуження і їх проекції [7]

Від кожної ХТ проводиться відрізок вправо і вліво перпендикулярно декількох ліній. перетин згинається паралельно напрямку кривизни ліній. Ця властивість стабілізує форму. Воно розрізає кожну перерізану лінію на дві частини, які назвемо зв'язками. Число зв'язків залежить від типу ХТ, що може змінюватися, тобто мутувати.

Мутацією першого роду називають замикання закінчення в розгалуження на суміжну лінію або розрив розгалуження в закінчення. Мутацією другого роду називають перехід закінчення через лінію в закінчення або розгалуження на суміжну лінію в розгалуження. Реалізація мутації, якщо дивитися у напрямку орієнтації ХТ, може бути виконана вправо або вліво [7].

Для закінчення 220 в перерізі, показаному точками на Рис. 1.1, зв'язку пронумеровані 0-12, а інші ХТ мають номера 110, 330, 440, 550. Від них же пунктиром проведено проекції на суміжні лінії перпендикулярно їм. Для розгалуження 220 в перерізі, показаному точками на рис. 1.2, зв'язку пронумеровані 0-12, а інші ХТ, відображені в перетині, мають ті ж номери. Розгалуження отримано як результат мутації першого роду закінчення, яке замикається на суміжну лінію вліво. Напрямок орієнтації кожної ХТ показано стрілкою [7].

Зв'язки нумерують по спіралі за годинниковою стрілкою, як показано на рис. 1.1 і рис. 1.2. При мутації ХТ, очевидно, зміна орієнтації ХТ не відбувається.

Глибина перетину, яке зазвичай симетрично в обидва боки, вибирається розробником довільно. Число зв'язків в перетині визначають у вигляді [7]:

$$w_i = 4x + 2 + (-1)^{t_i}, \qquad (1.2)$$

де t_i - тип ХТ m_i, x – кількість пересічних ліній.

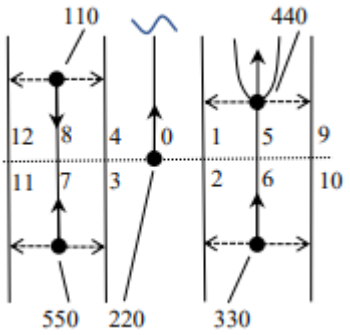

Рис. 1.1. Переріз для закінчення.

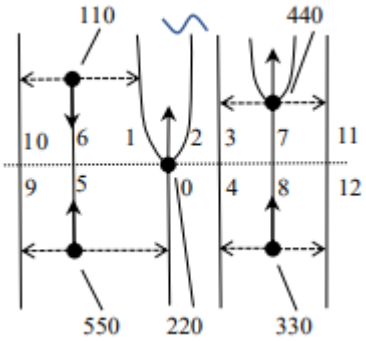

Рис. 1.2. Переріз для розгалуження.

1.3.2. Ідентифікація по радужній оболонці ока

Більшість поширених в даний час систем і технологій ідентифікації по райдужній оболонці ока засновані на принципах, запропонованих Дж. Даугманом. Цей метод полягає в наступному [8]:

1. отримання цифрового зображення;

2. сегментація;

3. параметризація.

Процес ідентифікації починається з отримання детального зображення очей людини. Зображення для подальшого використання намагаються зробити у високій якості, але це не обов'язково. Так виявити обличчя людини можна і по відеозапису.

Другим етапом є формування якісного зображення очей, на якому комп'ютер відзначає кордон оболонки, що отримав назву сегментація. У процесі сегментації на отриманій фотографії перш за все знаходять райдужну оболонку, визначають її внутрішній і зовнішній кордон. Потім знаходять межі верхніх і нижніх повік, а також виключають випадкове накладення вій на очі.

На третьому етапі райдужна оболонка умовно ділитися на концентричні кола, які скануються послідовно. У процесі сканування кожної умовної точки райдужці присвоюється певний цифрове значення в залежності від її контрасту. Далі отримані цифрові значення систематизуються, складається індивідуальний для кожної людини дескриптор. Комп'ютер порівнює його з дескрипторами бази даних [8].

1.3.3. Ідентифікація по 2D зображенню лиця

Досить поширеним методом автентифікації за біометричними даними є автентифікація по лицю. Одним з найпопулярніших є метод вектору ознак, що полягає у порівнянні векторів характерних точок лиця на подібність.

Нехай $F = \{F_1, F_2, \ldots, F_n\}$ - сукупність чорно-білих оцифрованих фотографій лиць, яка є вибіркою зразків. Сукупність характерних точок, що описують лице на фотографії, позначимо через $P = \{p_1, p_2, \ldots, p_k\}$. Задача полягає у автоматичному пошуку координат вказаних точок на фотографії лиця для подальшого вирішення задачі класифікації лиць по взаємному положенню точок[9].

Позначимо фіксований перелік характерних точок середнього лиця - $\Omega = \{\omega_1, \omega_2, \ldots, \omega_n\}$, кожна з яких має однозначний смисловий та геометричний опис. Дані точки описують середні координати, де саме містять характерні точки на лиці по середній статистиці. Координати кожної із точок будуть залежати від двох факторів: від індивідуальних рис лиця та від положення лиця на фотографії. Фактори першої групи несуть корисну для розпізнавання інформацію, а другої групи – навпаки, ускладнюють цю задачу добавляючи похибки, викривлення та шуми.

Припустимо, що кожна фотографія F_i ($F_i \in F$), яка є оброблена в ручну і на ній поставлені координати характерних точок з **Ω**, знайдений вектор:

$$p^{(i)} = (p_1^{(i)}, p_2^{(i)}, \ldots, p_n^{(i)}), \text{ де } p_k^{(i)} = p^{(i)}(\omega_k) = (x_k^{(i)}, y_k^{(i)}), \; k=1, 2, \ldots, n. \tag{1.3}$$

Вектор *p(i)* – контур лиця F_i. Всі контури, побудовані по виборці F, підлягають афінним перетворенням для найкращого вирівнювання їх друг з другом. З кожною точкою $p_k^{(i)}$, що належить контуру $p^{(i)}$, пов'яжемо вектор ознак $q_k^{(i)} = q^{(i)}(\omega_k) = (q_{k1}^{(i)}, q_{k2}^{(i)}, \ldots, q_{km}^{(i)})^T$, що характеризує окружність точки $p_k^{(i)}$ [9].

У якості таких ознак можуть використовуватися усереднена яскравість в окружності точки, наявність точок різкого перепаду. Оскільки точки $p_k^1, p_k^2, \ldots, p_k^N$ відповідають одному і тому ж геометричному описанню ω_k, то можна припустити, що в ідеальному випадку вектори $q_k^1, q_k^2, \ldots, q_k^N$ повинні бути схожими. Множина контурів $p^{(i)}$ утворює лінійний простір P^n. Встановимо ізоморфізм просторів P^n і R^n наступним чином [9]:

$$p^{(i)} = (p_1^{(i)}, p_2^{(i)}, \ldots, p_n^{(i)}) \leftrightarrow (x_1^{(i)}, x_2^{(i)}, \ldots, x_n^{(i)}; y_1^{(i)}, y_2^{(i)}, \ldots, y_n^{(i)})^T = X_i, \qquad (1.4)$$

де X_i - це по аналогії з $p^{(i)}$ - вектор. У якості статистичних характеристик класу зображень F використовується обчислення по набору контурів $X_i, i = 1,2,\ldots,N$, статистичні оцінки математичного очікування X і коваріаційної матриці S. Оцінку X математичного очікування можна інтерпретувати як контур середнього лиця, а коваріаційну матрицю – як параметр, що характеризує розкидання контурів. Клас зображень лиць характеризується усередненим значенням векторів ознак точок [9]:

$$\bar{q}_k = (\bar{q}_{k1}, \bar{q}_{k2}, \ldots, \bar{q}_{km})^T = \frac{1}{N}\sum_{i=1}^{N} q_k^{(i)} = \frac{1}{N}\sum_{i=1}^{N} (q_{k1}^{(i)}, q_{k2}^{(i)}, \ldots, q_{km}^{(i)})^T, k = 1,\ldots,n, \qquad (1.5)$$

і статистичними оцінками матриць коваріації ознак при кожній точці [9]:

$$S_k = \frac{1}{N-1}\sum_{t=1}^{N} (q_{ki}^{(t)} - \bar{q}_{ki})(q_{kj}^{(t)} - \bar{q}_{kj})^T \quad . \qquad (1.6)$$

Обрахування контуру X на вказаному лиці F є задачею із багатьма критеріями, шо складається з варіації координат $(x_1, x_2, \ldots, x_n; y_1, y_2, \ldots, y_n)^T$ точок $p_1, p_2, \ldots, p_n$ відносно середнього X так, щоб знайдені положення точок найкращим способом відповідали статистичним характеристикам векторів ознак $q_1, q_2, \ldots, q_n$. При цьому отриманий контур повинен відповідати природньому позиціонуванню характерних точок на лиці. Описаний вище метод можна

назвати етапом навчання, а саму вибірку зображень лиць F – навчальною вибіркою[9].

1.3.4. Ідентифікація по 3D зображенню лиця

Даний напрямок комп'ютерного зору стикається з двома ключовими проблемами - різні умови освітлення і різні ракурси зйомки осіб. Для вирішення цих проблем існує два шляхи: розширення бази еталонних образів додаванням зображень з різними умовами зйомки (що не завжди можливо зробити), а також моделювання умов зйомки на еталонних образах при їх порівнянні з аналізованими. Розширенням другого підходу є використання 3D моделей осіб і порівняння окремо рельєфу і текстури одержуваних тривимірних об'єктів. Даний підхід надає широкі можливості по моделюванню ракурсу і освітлення, але вимагає створення 3D моделі будь-якої людини в базі даних, що є ресурсномісткої і нетривіальним завданням. Цей метод полягає в наступному.

При наявності досить великого числа 3D моделей осіб в якості певної моделі можна взяти найближчу еталонну модель, вибравши в якості критерію віддаленість особливих точок моделі, отриманих автоматично за допомогою алгоритмів ASM, від особливих точок аналізованої особи. Однак більш точним рішенням є інтерполяція кожної точки 3D моделі виходячи з близькості до еталонних моделей.

Для обчислення моделі була застосована модифікація методу інтерполяції Шепарда для кожної особливої точки [10]:

$$W_i = \frac{(\frac{R - h_i}{R \times h_i})^2}{\sum_{q=1}^{N} \frac{R - h_q}{R \times h_q}}, \qquad (1.7)$$

де i - номер моделі особи, N - число моделей, h_i - відстань від точки моделі до точки зображення на площині (X, Y), R - заданий радіус, $R > \min(h_i)$, W_i - коефіцієнт питомої ваги моделі при обчисленні третьої координати особливої точки особи.

При цьому z-координата визначається як сума добутків z-координат моделей і відповідних ваг, отриманих з формули [10]:

$$Z_j = \sum_{i=1}^{N} Z_i \times W_i , \qquad (1.8)$$

де j - номер особливої точки зображення особи.

Пошук відповідності між знайденими особливими точками і відомими 3D моделями. Для того щоб знайти відповідність, необхідно отримати фронтальну проекцію безлічі точок 3D моделей осіб $P_i(x, y, z)$. Тобто знайти таку велику кількість точок $P_i(x^*, y^*)$, при якій координати центрів очей будуть перебувати на строго горизонтальній лінії (координата x^*), а серединні точки рота і перенісся - на строго вертикальної лінії (координата y^*). Так як в обраному для запропонованого алгоритму наборі моделей координати x та y відповідають координатам x^* і y^* фронтальної проекції, то підсумкова проекція виходить відкиданням третьої координати z. Далі, з цієї проекції можна сформувати фронтальне зображення особи за хмарами точок $P_i(x, y)$ і текстури 3D моделі[10].

Нормування особливих точок щодо масштабу моделей (наприклад, відстань між центрами очей) і центру координат (наприклад, кінчик носа). Для нормування плоского зображення необхідно визначити як мінімум дві точки, щодо яких буде проводитися масштабування інших координат і зведення центрів координат. У загальному випадку координати зображення особи

відповідають пікселям цього зображення і за визначенням лежать в площині цілих позитивних чисел, а координати проекції 3D моделі можуть бути дробовими і негативними числами (залежить від формату зберігання моделі).

У розглянутій задачі найзручніше при обчисленні коефіцієнта масштабування спертися на координати особливих точок, обчислені алгоритмом ASM. Для цього достатньо взяти дві стійкі точки, координати центрів очей для зображення проекції моделі, $E_l(x_l, y_l)$ і $E_r(x_r, y_r)$, а також для зображення аналізованого особи, $E`_l(x`_l, y`_l)$ і $E`_r(x`_r, y`_r)$. Відстані між цими точками знаходяться за формулами [10]:

$$D = \sqrt{(x_l - x_r)^2 + (y_l - y_r)^2} \text{ та } D` = \sqrt{(x`_l - x`_r)^2 + (y`_l - y`_r)^2} \qquad (1.9)$$

Обчислення відстаней для кожної особливої точки зображення особи і відповідних особливих точок кожної з 3D моделей. Так як отримані координати особливих точок для зображень нормовані по точках центрів очей E_l і E_r, а також центру носа E_n, то відстані між іншими точками масивів E і $E`$ характеризують відмінності зображення аналізованої особи і 3D моделі, використаної при формуванні фронтальної проекції [10]:

$$F_i = \sqrt{(x_i - x`_i)^2 + (y_i - y`_i)^2} \qquad (1.10)$$

Обчислення координати глибини для особливих точок зображення особи шляхом інтерполяції значень в особливих точках моделей. Обчислена на попередньому етапі відстань між відповідними особливими точками відомої моделі і заданого зображення особи дозволяє робити висновок про близькість 3D моделей до обличчя людини на зображенні. Після обчислення відстаней для проекції кожної з 3D моделей з'явиться можливість застосувати формули інтерполяції Шепарда, визначивши радіус R числом найближчих точок поверхні. Таким чином, для кожної особливої точки зображення лиця знаходиться координата глибини z, що дозволяє судити про рельєф аналізованої особи.

Визначення координати глибини для всіх інших точок шуканої моделі поступовим обчисленням нових точок між відомими особливими точками до тих пір, поки число точок моделі не досягне числа точок еталонних моделей. Для отримання більш докладної 3D моделі особи недостатньо обчислення третьої координати тільки в особливих точках, тому необхідно розширити масив до певної межі $Q \leq N$, де N - число точок, що описують вихідні 3D моделі.

1.4. Динамічні методи біометричної автентифікації

Як було сказано раніше, динамічними методами є ті, що використовують характеристики, які у людини можуть змінитися з часом. Такі методи, аналогічно із статистичними, поділяються на різні відносно того з якими характеристиками людського тіла вони працюють. Розглянемо детальніше методи, які є найбільш поширеними у побудові систем автентифікації.

1.4.1. Ідентифікація по клавіатурному почерку

Застосування ознак клавіатурного почерку в якості ідентифікаційних параметрів людей у системах ідентифікації і автентифікації особи, що активно розвивається. Одним з найбільш актуальних напрямків є ідентифікація суб'єктів по їх клавіатурного почерку [11, 12].

Особливості роботи користувачів за клавіатурою, внаслідок зміни емоційного стану, можна віднести до випадкового процесу. Відповідно, виміряні тимчасові інтервали клавіатурного почерку відносяться до випадкових величин.

Відомий метод визначення законів розподілу випадкових величин, який є апаратурним аналізом випадкових процесів, використовують еталонні гаусові сигнали. Цей метод полягає в наступному:

1) формуються еталонні сигнали гауссовського виду, які описуються функціями щільності ймовірності $W_n(x)$;

2) для кожних допоміжних сигналів $x_{ni}(t)$ та *i*-ої реалізації аналізованого процесу $x_i(t)$ формуються сигнали подібності за формулою:

$$S_{ni} = f(d_{ni}) = |1 + d_{ni}| - 1, n = 1,2 \ldots N, \qquad (1.11)$$

де d_{ni} - є відстанню між вибірками еталонних процесів і аналізованого процесу.

3) *i*-та реалізація досліджуваного процесу включається в деяку під-сукупність X_n після порівняння вихідних сигналів із заданим пороговим рівнем h_n.

Результатом порівняння сигналів подібності між собою є поділ генеральної сукупності реалізацій *I* розглянутого процесу на під-сукупності реалізацій $I_n, n = 1,2,\ldots,N$. Так як кожна *n*-на під-сукупність розглянутого процесу характеризується деяким ядром, тобто багатовимірною щільністю розподілу ймовірностей *n*-го допоміжного процесу $W_n(x)$, то багатовимірні закони розподілу заданого процесу описуються сумішами щільності розподілу із наступними ваговими коефіцієнтами[11]:

$$q_n = I_n / I, n = 1,2,\ldots,N. \qquad (1.12)$$

Для реалізації способу поділу в суміші сигналів гауссовської форми, використовуючи еталонні сигнали, статистичний аналізатор. В якості еталонних сигналів обрані тимчасові значення натискання і відпускання клавіш. При цьому еталон формують шляхом вимірювання тимчасових інтервалів натискання і

відпускання клавіш користувачами, що працюють за клавіатурою і набирають певний текст. Після формування набору вихідних характеристик клавіатурного почерку користувачів зібрані дані очищаються шляхом виключення викидів, шумів і аномальних значень. Потім на основі очищених даних обчислюють їх математичні очікування, які в подальшому приймаються в якості еталонних значень клавіатурного почерку.

1.4.2. Ідентифікація по голосовим характеристикам

Завдання верифікації диктора за голосовими даними в даний час знаходить широке застосування при побудові безпечних інформаційних систем. Як правило, її рішення ґрунтується на виявленні індивідуальних акустичних характеристик користувачів, які б дозволили ефективно і точно проводити порівняння зразків голосу, що пред'являються при спробі доступу і зберігаються в спеціалізованій базі даних. Цей метод полягає в наступному [13]:

1. Рівень обробки сигналу. Виділення ознак, істотних для завдання розпізнавання і формування так званого вектору ознак.

2. Рівень моделі. Дозволяє шляхом побудови математичної моделі проводити зіставлення векторів ознак один з одним і обчислювати ступеня подібності між зареєстрованими ознаками і збереженою моделлю.

3. Рівень прийняття рішень. Проводить прийняття кінцевих рішень на основі отриманих ступенів подоб і, якщо необхідно, заданих порогових значень.

До теперішнього часу в галузі склався типовий алгоритм попередньої обробки акустичного сигналу після його запису. Оцифрований сигнал

розбивається на блоки тривалістю 25-30 мс (Відліки позначаються в них $x_0,\ldots,x_{N-1}$). До кожного подібного блоку застосовується вагова функція і потім дискретне перетворення Фур'є. Прикладом вагової функції може служити вікно Хеммінга [13]:

$$w_n = 0{,}54 - 0{,}46 \times \cos(2\pi \frac{n}{N-1}), n = 0,\ldots,N-1, \qquad (1.13)$$

де N - довжина вікна, виражена у відліках.

Вагова функція використовується для зменшення спотворень у Фур'є аналізі, викликаних кінцівкою вибірки. Тоді дискретне перетворення Фур'є зваженого сигналу можна записати у вигляді [9]:

$$X_k = \sum_{n=0}^{N-1} x_n w_n \exp(-\frac{2\pi i}{N} kn). \qquad (1.14)$$

Значення індексів відповідають частотам [9]:

$$f_k = \frac{F_s}{N} k, \qquad (1.15)$$

де F_S - частота дискретизації сигналу.

Отримане уявлення сигналу в частотній області розбивають на діапазони за допомогою банку (Гребінки) трикутних фільтрів. Межі фільтрів розраховують в шкалі низів. Переклад в низько частотну область здійснюється за формулою [13]:

$$B(f) = 1127 \times \ln(1 + \frac{f}{700}). \qquad (1.16)$$

Нехай N_{FB} - кількість фільтрів (зазвичай використовують близько 24 фільтрів); (f_{low}, f_{high}) - досліджуваний діапазон частот. Тоді даний діапазон переводять в шкалу низів, розбивають на N_{FB} рівномірно розподілених прикритих діапазонів і обчислюють відповідні кордони в області лінійних

частот. Позначимо через $H_{m,k}$ – вагові коефіцієнти отриманих фільтрів. Фільтри застосовуються до квадратів модулів коефіцієнтів перетворення Фур'є. Отримані значення логарифмуються [13]:

$$e_m = \ln(\sum_{k=0}^{N} | X_k |^2 \times H_{m,k}), m = 0, \ldots, N_{FB} - 1. \quad (1.17)$$

Заключним етапом в обчисленні MFCC коефіцієнтів є дискретне косинусне перетворення[13]:

$$c_i = \sum_{m=0}^{N_{FB}} e_m \cos(\frac{\pi i(m + 0{,}5)}{N_{FB}}), i = 1, \ldots, N_{MFCC}. \quad (1.18)$$

Коефіцієнт c_0 не використовується, тому що являє собою енергію сигналу. Кількість коефіцієнтів N_{MFCC} на практиці вибирають від 12 до 30. На Рис. 1.3 наведено приклад графіка низько-кепстральних коефіцієнтів

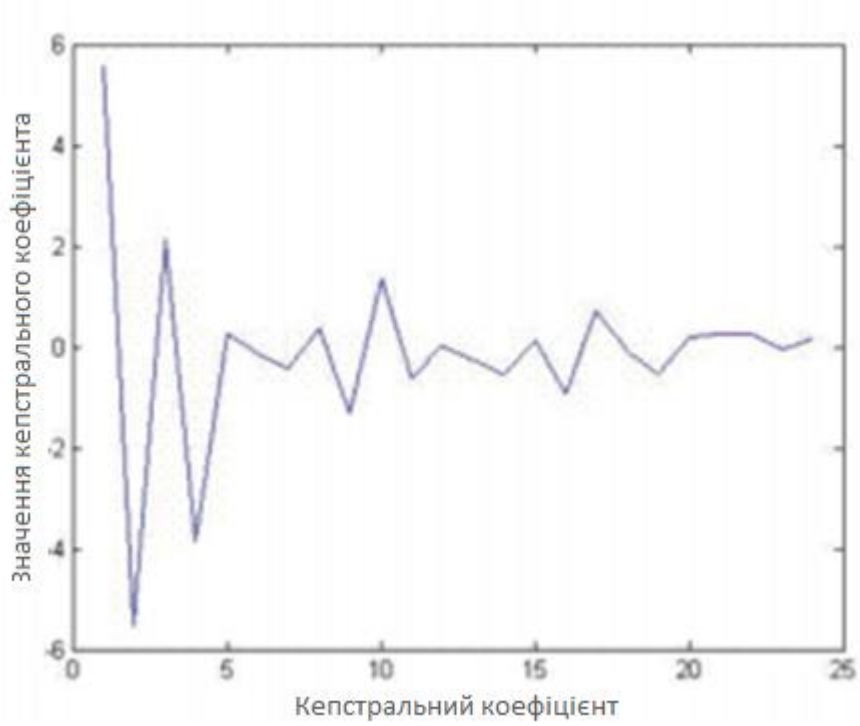

Рис. 1.3. Приклад низько-кепстральних коефіцієнтів для фрази «один-два-три»

1.5. Обґрунтування доцільності побудови системи біометричної автентифікації саме на базі методу ідентифікації по геометрії лиця

Для здійснення коректного вибору найоптимальнішої біометричної технології розпізнавання проведемо аналіз найпоширеніших методів. Оскільки статистичні методи є значно стабільнішими та легшими у реалізації ніж динамічні, то доцільно розглянути лише найпоширеніші статистичні методи.

При побудові системи біометричної автентифікації користувачів комп'ютерної системи в першу чергу потрібно звертати увагу на правильність ідентифікації особи, але такі фактори як простота у використанні, швидкість роботи, непримітність на робочому місці та ціна утримання також має свою вагу.

Дані методи біометричної ідентифікації можна порівняти за допомогою таких показників як помилка першого роду та помилка другого роду. Помилкою першого роду (ППР) є ситуація, у якій системою було прийнято рішення відхилити позитивний результат. Та помилкою другого роду (ПДР) називається ситуація, коли системою було прийнято рішення прийняти негативний результат.

Також дані методи можна порівняти зі вразливістю їх до підробки зразків для автентифікації. Даний показник є достатньо важливим оскільки яка б надійна не була б система з боку знаходження найменших відмін у зразків, вся її надійність може зводитися до нуля, якщо зрізки для системи автентифікації можна підробити.

Стійкість до змін характеристик протягом часу є важливим фактором якщо потрібно максимально довго зберігати актуальність довірених зразків у системі ідентифікації. Однак дані зміни не означають, що при не значній зміні

характеристики користувача неможливо буде ідентифікувати його по зразкам, які були зняті раніше.

Незалежність процесу ідентифікації особи від факторів навколишнього середовища достатньо сильно впливає на стабільність прийняття правильного рішення системою. У ролі таких факторів можуть виступати яскравість освітлення, температура повітря, положення освітлення, склад повітря, наявність пилі та інші.

Також дані методі можна порівняти за часом ідентифікації особи. Даний час залежить від швидкості зняття потрібних характеристик з особи при ідентифікації, розмірів шаблонів та інших ресурсів, що потрібні для обробки та складності програмних алгоритмів, що потрібні для коректної ідентифікації.

Можливість безконтактної ідентифікації дає можливість в побудові більш безпечних систем автентифікації з боку гігієни. Також відсутність необхідності прямого контакту із системою є більш комфортною для користувача.

Комфорт користувача при процесі автентифікації не слід ігнорувати при виборі методів ідентифікації для системи безпеки. Користувачам доведеться мати справу з даною системою кілька разів на добу щодня. Автентифікація може бути як сама по собі фізично не дуже комфортною, так і бути психологічно не комфортною.

Вартість реалізації системи безпеки має місце у порівнянні. Вартість залежить від призначення системи, складність методів, що використовуються для ідентифікації, додаткових модулів, що підвищують безпеку системи та іншого.

Доступність техніки для реалізації системи безпеки на базі методу ідентифікації на території України є характеристикою, яка залежить від наявності вітчизняного виробництва та економічного стану країни. Звісно доступ до техніки іноземного виробництва в Україні є, але економічний стан всередині

країни є достатньо поганим, тому перевагу має техніка вітчизняного виробництво, оскільки вона значно буде відрізнятися в ціні від іноземних аналогів.

Усі розглянуті вище критерії оцінки можна зобразити у вигляді таблиці. Об'єднавши усі дані для кожного з методів можна зробити висновок який з них найкраще. У таблиці 1.1 відображені характеристики кожного із методів [14, 15].

Таблиця 1.1.

Метод	ППР, %	ПДР, %	Можливість фальсифікації	Стійкість характеристик	Стійкість до середовища	Швидкість ідентифікації	Безконтактна ідентифікація	Комфорт	Вартість	Доступність
Відбиток пальця	0,6	0,001	В	Н	Н	В	Н	С	С	С
Райдужна оболонка ока	0,016	0,000001	Н	В	С	В	В	В	В	Н
Сітківка ока	0,4	0,0001	С	С	Н	Н	Н	Н	В	Н
Геометрія лиця	2,5	0,1	В	С	Н	С	В	В	Н	В
Вени руки	0,01	0,0008	Н	С	С	В	С	С	С	Н

У таблиці 1.1 скорочення «Н» означає «Низький», «С» означає «Середній», «В» означає «Високий».

Найбільші показники помилок першого та другого роду має ідентифікація особи за геометрією обличчя. Також недоліком даного способу є те, що можливий обман сканера через показ на камеру фотографії особи. Також на правильність розпізнавання впливає розміщення освітлення, але при використанні даного методу в офісному приміщенні освітлення буде завжди на одному і тому ж місці. Ще одним недоліком методу є можливість неправильного розпізнавання чи повного не розпізнавання, якщо особа буде в окулярах, або

медичній масці, що є дуже актуальним у даний час. Для успішного розпізнавання також потрібно, щоб користувач дивися прямо в камеру, що не є складною задачею. Але даний метод має ряд переваг, порівняно із іншими методами. Для зняття зразків для порівняння він потребує лише звичайну камеру і не вимагає від неї зйомку у високій якості, що обійдеться у закупівлі дешевше ніж обладнання для інших типів ідентифікації. Також дане обладнання виробляється в Україні кількома компаніями такими як: Ajax [16], Atis [17], Dahua Technology [18], Ezviz [19] та інші. Оскільки для ідентифікації лиця не обов'язково, щоб лице особи розміщалося на весь кадр, то це дає змогу розташовувати камеру на певній відстані від комп'ютерної системи, що значно зменшує ризики пошкоджень у випадку необережності під час роботи. Також дана перевага дозволить позбавити робоче місце від візуальних ознак способу забезпечення безпеки комп'ютерної системи, що ускладнить для зловмисника збір інформації про захист. А оскільки про факт ідентифікації при вході в систему може не знати навіть працівник, то ймовірність викриття даного способу ідентифікації є дуже низьким. Станом на 2020 рік надзвичайно актуальною є проблема особистої гігієни. Оскільки даний метод є повністю безконтактним, то потреби надмірної гігієни сьогодення є повністю задовільними. Візуально характеристики лиця з часом можуть серйозно змінюватися, але сама його геометрія буде така ж протягом всього життя людини, що дозволить ідентифікувати людину, навіть якщо візуально вона не дуже схожа на себе.

Отже, розглянувши методи ідентифікації особи по біометричним ознакам, можна зробити висновок, що метод ідентифікації по геометрії лиця найкраще підходить для даних цілей. Оскільки він має сукупний ряд переваг, які разом інші методи не мають. Результати помилок першого та другого порядку у даного методу є найслабшими, але вони не є на стільки серйозними, щоб не використовувати даний метод у дії, відсоток похибки значно не відрізняється від інших методів.

1.6. Висновки до розділу

В даному розділі дипломної роботи було проаналізовано нормативно-правова база в галузі захисту інформаційних ресурсів в інформаційно-телекомунікаційних системах. Зокрема аналізувалися такі нормативні документи: Закон України «Про інформацію» [1], Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» [2], Закон України «Про електронні довірчі послуги» [3].

Також було проаналізовано існуючі методи ідентифікації особи за її біометричними даними, а саме ідентифікація по: відбитку пальця по типу контрольних точок [7], 2D зображення обличчя по вектору ознак [9], 3D зображення обличчя [10], райдужній оболонці ока [8], голосових ознаках по низьких кептральних коефіцієнтах [10] та клавіатурному почерку по еталонних гауссовських сигналах [11, 12].

На основі проведеного аналізу було обрано метод розпізнавання за геометрією лиця для побудови системи біометричної автентифікації користувачів у системі у подальшій роботі.

РОЗДІЛ 2. АНАЛІЗ МЕТОДІВ РОЗПІЗНАВАННЯ КОРИСТУВАЧІВ ЗА ГЕОМЕТРІЄЮ ЇХ ОБЛИЧ

2.1. Каскад Хаара

Ознаки Хаара – ознаки цифрового зображення, що використовуються для розпізнавання зразків. Основною перевагою використання ознак Хаара є швидкість обробки, завдяки якій можна без проблем обробляти потокове відео. За допомогою цих ознак можна розпізнавати безліч об’єктів, одним з яких є і людське обличчя [20].

Для того, щоб налаштувати ознаки на пошук конкретного об’єкта, потрібно провести процес навчання каскаду Хаара. Даний процес відбувається із використанням кількох сотень чи тисяч зразків, що є зображеннями об’єкта, який нам потрібно знайти, а також зображення середовища, у якому буде проводитися пошук у такій самій кількості.

Метод Віоли-Джонса є популярним методом для пошуку об’єктів на зображенні через свою високу швидкодію та ефективність. В основу даного методу входить інтегральне представлення зображення за ознаками Хаара, побудова класифікатора і комбінування класифікаторів у каскадну структуру. Дані можливості дозволяють реалізувати пошук об’єктів у реальному часі.

Цей спосіб дуже швидкий в реалізації, інтуїтивний і досконально відомий. Але він звичайно має свої недоліки:

- Нестійкість при зміні освітлення;

- Нестійкість при зміні масштабу або повороті зображення;
- Нестійкість, якщо на частині зображення змінюється фон;
- Низька швидкість роботи, тобто якщо потрібно виявити область $n \times n$ на зображенні $m \times m$, то кількість операцій буде пропорційною $n^2 \times (m-n)^2$.

Але існують не складні методи боротьби із цими недоліками:

- Освітлення нейтралізується нормування або переходом до бінаризації області;
- Зміни масштабу і невеликі повороти нейтралізуються зміною дозволу при кореляції;
- Швидкість оптимізують шляхом пошуку з великим кроком.

Беручи до уваги дані недоліки, можна зробити висновок, що даний спосіб розпізнавання буде працювати не стабільно, або ж взагалі не працювати, якщо система переміщується. Але системи автентифікації часто розробляються таким чином, щоб працювати на одному місці без зміни положень, тобто ні фон, ні освітлення змінюватися не будо, а отже слабкі місця даного способу не вплинуть на якість роботи системи.

Інтегральне представлення зображень – це матриця, однакова за розмірами із первісним зображенням. У кожному елементі матриці зберігається сума інтенсивностей всіх пікселів, що знаходяться ліворуч, та вгору відносно даного елемента, тобто правого нижнього кута прямокутної області (0, 0) до (x, y). Елементи матриці L можна розрахувати за формулою:

$$L(x, y) = \sum_{i=0,\, j=0}^{i \le x,\, j \le y} I(i, j), \qquad (2.1)$$

де *I(i, j)* – це яскравість пікселя первісного зображення.

Розрахунок значень елементів матриці продовжується протягом часу, що є пропорціональним кількості пікселів у первісному зображенні, тому інтегральне

зображення прораховується за один підхід. Елементи матриці розраховуються за формулою:

$$L(x, y) = I(x, y) + L(x-1, y-1) + L(x, y-1) + L(x-1, y) \qquad (2.2)$$

За допомогою інтегрального представлення зображення можна швидко розрахувати сумарну яскравість довільної прямокутної області на зображенні. На етапі виявлення об'єкту в методі Віоли-Джонса використовується вікно одного розміру, яке рухається по зображенню. Для кожної області зображення, над якою проходить вікно, розраховується ознака Хаара, за допомогою якої відбувається пошук потрібного об'єкта.

Ознака відображення, де Df – множина допустимих значень ознаки. Якщо задані ознаки $f_1, \ldots, f_n$, то вектор ознак $x = (f_1(x), \ldots, f_n(x))$ називається ознаковим описом об'єкта *x.* Ознакові описи допустимо зіставляти із самими об'єктами. При цьому множина $X = Df_1 * \ldots * Df_n$ називають ознаковим простором.

Ознаки діляться на такі типи у залежності від множини *Df*:

- бінарна ознака, $Df = \{0,1\}$;
- номінальна ознака, *Df* – кінцевий множник;
- порядкова ознака, *Df* – кінцева згадка множини;
- кількісна ознака, *Df* – множина дійсних чисел.

Ознаки Хаара обраховуються за суміжними прямокутним областям. У стандартному методі Віоли-Джонса використовуються прямокутні примітиви, що зображені на рисунку 2.1 та рисунку 2.2.

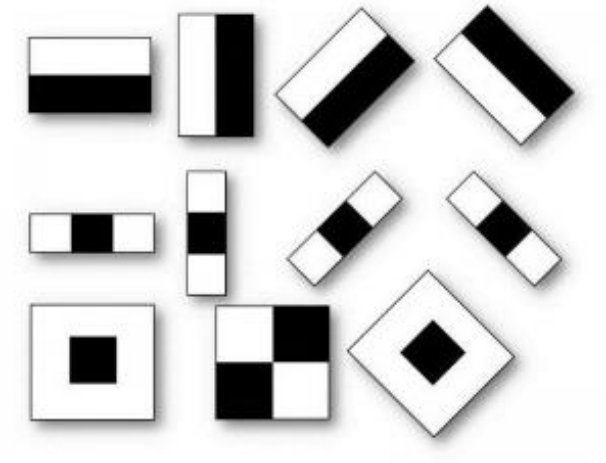

Рис 2.1. Прямокутні примітиви Хаара (А)

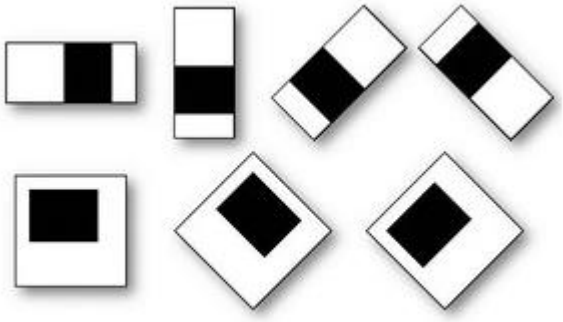

Рис 2.2. Прямокутні примітиви Хаара (Б)

Обрахованим значенням F ознаки Хаара буде:

$$F = X - Y \qquad (2.3)$$

де X - сума значень яскравості точок, які закривають світлою частиною примітиву, Y - сума значень яскравості точок, які закривають темною частиною.

Для обчислення використовується поняття інтегрального зображення, розглянуте вище, і ознаки Хаара можуть обчислюватися швидко, за постійний час. Використання ознак Хаара дає точкове значення перепаду яскравості по осі X і Y відповідно.

Оскільки ознаки Хаара мало підходять для навчання або класифікації, для опису об'єкта з достатньою точністю необхідна більша кількість ознак. Тому

ознаки Хаара надходять в каскадний класифікатор, службовець для швидкого відкидання вікон, де не знайдений необхідний об'єкт, і видачі результату «істина» або «брехня» щодо знаходження об'єкта.

Класифікатор будується на основі алгоритму бустинга (від англ. boost-поліпшення, посилення) для вибору найбільш підходящих ознак для шуканого об'єкта на даній частині зображення. У загальному випадку бустинг - це комплекс методів, що сприяють підвищенню точності аналітичних моделей. Ефективна модель, яка припускає мало помилок класифікації, називається сильною. Слабка ж, навпаки, не дозволяє надійно розділяти класи або давати точні прогнози, робить велику кількість помилок. Тому бустинг означає посилення слабких моделей і є процедурою послідовного побудови композиції алгоритмів машинного навчання, коли кожен наступний алгоритм прагне компенсувати недоліки композиції всіх попередніх алгоритмів.

В результаті роботи алгоритму бустингу на кожній ітерації формується простий класифікатор наступного вигляду:

$$h_{j(z)} = \begin{cases} 1, if \;\; p_j f_j(z) < p_j \theta_j \\ 0, else \end{cases} \qquad (2.4)$$

де p_j - напрямок знака нерівності, θ_j - значення порога, $f_j(z)$ - обчислене значення ознаки, z - вікно зображення розміром 24 × 24 пікселів.

Отриманий класифікатор має мінімальну помилку по відношенню до поточних значень ваг, задіяним в процедурі навчання для визначення помилки. Для пошуку об'єкта на цифровому зображенні використовується навчений класифікатор, представлений в форматі xml. Класифікатор формується на примітивах Хаара.

2.2. Метод головних компонентів та відстань Евкліда

Метод головних компонент (Principal Component Analysis) - один з поширених методів порівняти два обличчя різних користувачів [21].

Даний спосіб є малоефективним, якщо людина змінює вираз обличчя чи змінюється ракурс освітлення обличчя, оскільки для даного методу потрібно обирати підкласи для обчислення таким чином, щоб максимально апроксимувати набір вхідних даних, а не виконувати дискримінацію між класами обличь. Але даний недолік можна вирішити використавши лінійний дискримінант Фішера. Що робить максимальним наступне відношення:

$$\frac{\left|\phi^T \times S_b \times \phi\right|}{\left|\phi^T \times S_W \times \phi\right|}, \qquad (2.5)$$

де S_b – матриця розкиду між класами, S_W – матриця розкиду в середині одного класу, а m – кількість класів, що знаходиться в базі даних.

Матриця розкиду між класами визначається за формулою:

$$S_b = \sum_{i=1}^{m} N_i (\bar{x}_i - \bar{x}) \times (\bar{x}_i - x)^T \qquad (2.6)$$

Матриця розкиду в середині одного класу визначається за формулою:

$$S_W = \sum_{i=1}^{m} \sum_{x \in X_i} (x - \bar{x}_i) \times (\bar{x}_i - x)^T \qquad (2.7)$$

Даний метод віднаходить таку проекцію даних, при якій буде максимальний розкид по всій базі даних осіб без урахування класів. За статистикою даний метод демонструє результат розпізнавання у 95% успішності. Однак даний процес можна замінити аналогами, що є легшими у обчисленні.

Таким методом є порівняння дескрипторів лиця за допомогою відстані Евкліда. Даний метод полягає у порівняння двох векторів даних, що дозволяє визначити їх схожість між собою.

Розрахувати схожість векторів можна за формулою:

$$E = \sqrt{\sum_{i=0}^{n} (p_i - q_i)^2}\ , \qquad (2.8)$$

де n – кількість елементів у векторі, p – значення першого вектору, а q – значення другого вектору.

2.3. Нейронна мережа Хопфілда та LBP

Велике коло задач можна вирішити за допомогою застосування нейронних мереж. Але для їх функціонування потрібні великі обчислювальні потужності.

Мережа Хопфілда [22] складається із одного слою нейронів, кількість яких рівна кількості входів та виходів мережі. Усі нейрони пов’язані синапсасами друг з другом а також із одним із входів. Кожен синапс має свій числовий коефіцієнт w, вага, що у фізичному розумінні була б еквівалентною його електричній провідності. Візуальне представлення нейрона зображено на рисунку 2.3.

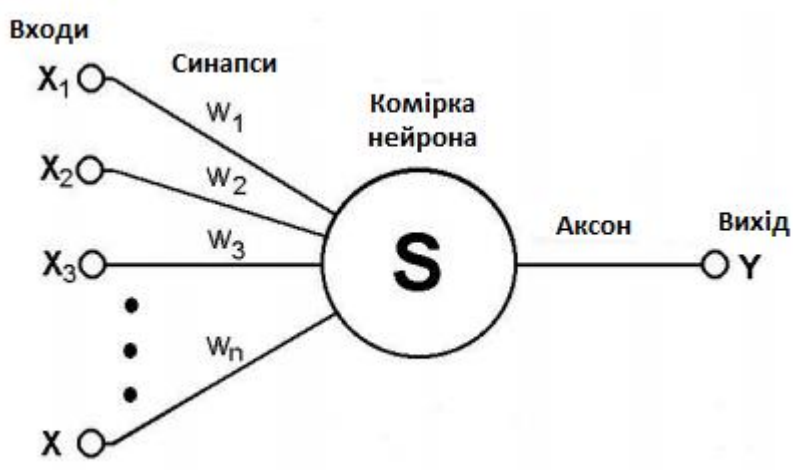

Рис. 2.3. Штучний нейрон

Стан кожного *i*-того нейрона визначається як сума його входів об'єднана із його масою. Обчислюється це за формулою:

$$S = \sum_{i=0}^{n} x_i \times w_i \qquad (2.9)$$

Відповідно до визначення 2.8 можна визначити, що вихід є функцією стану нейрона і обчислюється як:

$$y = f(s) \qquad (2.10)$$

Мережа Хотфілда може вирішити задачу, при якій є набір двійкових сигналів, які вважаються еталонними. Мережа повинна розпізнати сигнал-зразок у середовищі із шумом та визначити чи відповідає даний сигнал одному із еталонних.

На початковій стадії обрахунку мережі вагові коефіцієнти синапсів визначаються за формулою:

$$W_{ij} = \begin{cases} \sum_{k=0}^{m-1} x_{ik} \times x_{jk}, i \neq j, \\ 0, i = j \end{cases}, \qquad (2.11)$$

де x_{ik}, x_{jk} – *i*-ий та *j*-ий елементи вектору *k*-го зразку.

У випадку, якщо провідність синапсу $i=j$, то можна зробити висновок, що синапсис, що веде на той же нейрон, з якого він бере початок, відсутній. У подальшій роботі мережа функціонує по наступному алгоритму:

- На входи подаються невідомі сигнали
- Стан нейронів обновляється для кожного нового заходу даних:

$$S_j(p+1) = \sum_{i=0}^{n-1} w_{ij} y_i(p),\ j = 0 \ldots n-1 \qquad (2.12)$$

та нові значення аксонів:

$$y_j(p+1) = f\left|S_j(p+1)\right|, \qquad (2.13)$$

де f – функція активізації у вигляді різкого збільшення.

Перевірка на зміну вихідних значень аксонів за останню ітерацію. Якщо значення змінилися, то система переходить назад до попереднього пункту функціонування, якщо ж ні, то алгоритм закінчує роботу.

Вихідний вектор являє собою зразок, що найкращим чином представляє вхідні дані.

Також ХТ можна визначити за допомогою методу LBP, який є легшим та швидшим у обрахунку відносно нейронної мережі Хопфілда. А також є стійким до шумів та варіацій текстур на зображенні.

Даний спосіб використовується для опису направлення, у якому яскравість фрагменту зменшується, що дозволить визначати межі елементів обличчя, яскравість на яких менша ніж на областях поряд. Даний аналіз можна проводити у різних радіусах навколо точки. Чим більший радіус бере участь у обрахунку, тим точніше можна визначити напрямок згасання яскравості. Але для коректного визначення достатньо лише радіуса розміром в 1 піксель. На рисунку 2.4 зображені приклади визначення кількості точок відносно радіуса.

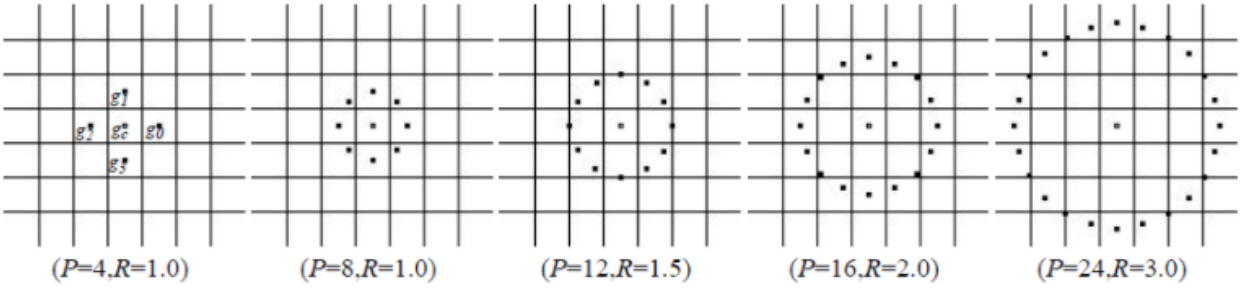

Рис 2.4. Визначення точок відносно радіуса

Якщо різниця між сусідніми пікселями є негативною, то це означає, що яскравість стає меншою. Позначивши кожен піксель відповідними позначками (0 у випадку, якщо яскравість більша у сусідньому пікселі, 1 у випадку, якщо яскравість навпаки менша ніж у сусідньому пікселі). Склавши це у один ряд, ми отримаємо двійкове число розмірністю у кількість точок, визначених у рисунку 2.4. Вигляд даного процесу зображений на рисунку 2.5.

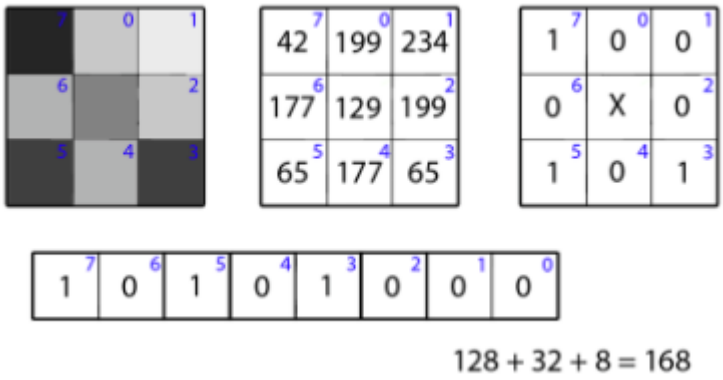

Рис. 2.5. Визначення дескриптору точки

Розрахувавши даний дескриптор для кількох сусідніх точок кожної із Характерних точок обличчя можна визначити опис лиця у вигляді вектору, який відповідно можна використати у порівнянні за допомогою відстані Евкліда.

2.4. Висновок до розділу

У даному розділі були розглянуті поширені методи, за допомогою яких можна розпізнати обличчя на фотографії та провести порівняльний аналіз.

Метод розпізнавання за допомогою каскаду Хаара є ефективним методом для визначення об’єктів на зображенні. Його можна налаштувати на пошук різних об’єктів, одним з яких є лице. Також даний метод є гнучким завдяки можливості настройки процесу пошуку. Але даний метод є нестійким до зміни освітлення та середовища, що є незначним для систем автентифікації, що не будуть переміщуватися у просторі.

Також були розглянуті метод головних компонент та нейронна мережа Хопфілда. Дані методи підходять для порівняння вхідних даних із еталонними. Але мережа Хопфілда є достатньо складною у реалізації та потребує досить великі потужності техніки для її обрахунку. Метод головних компонент має достатньо високу успішність обчислювання, але має більш ефективні аналоги.

РОЗДІЛ 3. АЛГОРИТМ СИСТЕМИ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА НА БАЗІ МЕТОДУ РОЗПІЗНАВАННЯ ПО ГЕОМЕТРІЇ ЛИЦЯ

3.1. Обґрунтування вибору середовища для реалізації методу автентифікації по геометрії лиця

Перед початком підготовки ознак для розпізнавання для системи автентифікації та опису алгоритму доцільно обрати середовище для розробки та бібліотеки із функціоналом, що знадобиться для процесу, а саме підготовка каскаду Хаара, обробка зображення, визначення характерних точок та їх порівняння. Почати доцільно із вибору середовища для розробки системи.

3.1.1. Середовище для розробки системи автентифікації користувачів комп’ютерної системи

Python [23] – високорівнева мова програмування, що орієнтована на підвищення продуктивності і читабельності програми. Синтаксис ядра Python є мінімалістичним, що значно підвищує простоту як написання програми, так і розуміння сторонніх програм. Також це дозволяє легко та швидко модифікувати програму під різні потреби. Реалізацією Python являється інтерпретатор CPython,

що підтримується більшістю платформами, які активно використовуються на сьогодні.

Для написання програмного забезпечення знадобиться відповідне середовище для розробки. Одним із середовищ для розробки на Python є крос-платформне середовище PyCharm [24]. Воно дозволяє об’єднати в собі весь проект в одному вікні із великою кількістю налаштувань. Серед можливостей середовища можна виділити:

- зручний редактор коду з підсвіченням синтаксису;
- швидкий перегляд документації для будь-якого елемента;
- інтегрована консоль Python;
- швидкий доступ до всіх компонентів проекту.

3.1.2. Обробка зображень та створення компонентів для розпізнавання обличчя

OpenCV (Open Source Computer Vision Library) [25] – бібліотека алгоритмів, комп’ютерного зору, обробки зображень та чисельних алгоритмів загального призначення. Дану бібліотеку можна використовувати при написанні програми на мові програмування Python.

Дану бібліотеку можна використовувати для багатьох дій, які потрібні при реалізації системи автентифікації на базі методі ідентифікації по геометрії лиця, що в свою чергу вимагає взаємодії із відео камерою або ж просто із фотографією. Бібліотека дозволяє використовувати такі можливості для взаємодії як:

- фільтрація зображення, геометричні перетворення, перетворення кольорових просторів;
- введення та виведення зображень та відео;
- моделі машинного навчання;
- розпізнавання, аналіз руху та відслідковування об’єктів;
- настройка камери

Отже, дана бібліотека буде корисною для введення відеоряду до програми для подальшої її обробки, яка буде виконуватися за допомогою цієї ж бібліотеки. А також окрім обробки відеоряду даною бібліотекою можна здійснити один із найважливіших етапів виконання автентифікації користувача – знаходження обличчя людини у кадрі.

Для знаходження обличчя людини у кадрі найкраще підходить використання примітивів Хаара. Але для того, щоб програмі було зрозуміло, який саме об’єкт їй потрібно знайти у кадрі, спочатку потрібно створити каскад Хаара для обличчя людини. Даний каскад дозволить детектувати обличчя шляхом накладання маски із примітивів Хаара на частини зображення із покроковим переміщенням по всьому зображенню, поки не буде знайдений шуканий об’єкт. У бібліотеці OpenCV містяться необхідні програми для створення каскаду Хаара. Для їх роботи необхідно зібрати певну кількість позитивних та негативних зображень об’єкта, що потрібно знайти на фото.

3.1.3. Розпізнавання Характерних точок та їх порівняння

Dlib [26] - це сучасний набір інструментів, що містить алгоритми машинного навчання та інструменти для створення складного програмного забезпечення для вирішення реальних проблем. Він використовується як у промисловості, так і в наукових колах у широкому діапазоні доменів, включаючи робототехніку, вбудовані пристрої, мобільні телефони та великі високопродуктивні обчислювальні середовища.

Аналогічно із бібліотекою OpenCV, за допомогою Dlib можна реалізувати розпізнавання лиця у кадрі. Дане розпізнавання буде більш стійким за умови, що люди на буде дивитися прямо у камеру, але у випадку, якщо людина трішки поверне голову, то ймовірність успішного розпізнавання значно зменшується і реалізація за допомогою OpenCV буде стабільнішою.

Але для автентифікації особи лише знайти присутність самої особи буде замало, потрібно визначити хто конкретно здійснює спробу увійти до системи. Для ідентифікації особи потрібно на щось опиратися, а саме на певні ознаки, які притаманні лише для однієї людини і у іншої вони будуть відрізнятися. У випадку людського лиця даною опорою для ідентифікації можуть стати точки лиця. А саме точки на краях очей, роту, брів, носу та обрис обличчя, що у сукупності мають різне розташування у кожної людини. Бібліотека Dlibдає змогу зняти з лиця положення даних точок. Для цього спочатку накладається спеціальна маска, на якій розташовані середньостатистичні опорні точки лиця, після чого дані точки підганяються до знайденого лиця шляхом переміщення її на найближче місце, де знаходить різкий перепад кольору на фотографії, що в свою чергу виступає краєм частини лиця (носа, рота чи ока).

Таким чином, дізнавшись розміщення опорних точок лиця можна визначити особистість людини, яка намагається увійти до системи.

3.2. Створення каскаду Хаара

Створення каскаду Хаара поділяється на 2 етапи [27]. Першим етапом є збір і підготовка необхідних зразків, що будуть брати участь у навчанні каскаду. Другим етапом є саме навчання каскаду. Розглянемо дані кроки детальніше та проведемо процес навчання каскаду Хаара для системи біометричної автентифікації на базі ідентифікації по геометрії лиця.

3.2.1. Збір і підготовка зразків для побудови каскаду Хаара

Першим етапом для побудови каскаду Хаара є збір і підготовка зразків для його навчання та інших компонентів для даного процесу – списки із переліком зразків та координат. Класифікатор формується на примітивах Хаара шляхом розрахунку значень ознак. Для того щоб вивчити каскад Хаара потрібно виконати наступні умови:

- Підготовити набір фотографій одного формату, де буде зображений об’єкт, який у подальшій роботі нам потрібно буде шукати, у звичайному середовищі (позитивні зразки);
- Підготовити набір фотографій одного формату, де буде зображене середовище (без об’єкта, який потрібно буде шукати), у якому у подальшій роботі нам потрібно буде шукати потрібний об’єкт (негативні зразки);
- Файл із переліком позитивних зразків у файловій системі операційної системи комп’ютера відносно даного файлу, у якому також вказана кількість шуканих об’єктів на зображенні, а також їх координати (координати верхньої лівої точки та координати нижньої правої точки);
- Файл із переліком негативних зразків у файловій системі операційної системи комп’ютера відносно даного файлу.

Для підготовки позитивних зразків краще використовувати фото з лицями реальних робітників, оскільки чим більше схожі зразки на реальні об’єкти, тим стабільніша буде проводитися пошук. Також дуже важливим є надати для навчання фотографії у середовищі, де буде проводитися пошук, враховуючи освітлення та ракурс камери, оскільки це теж сильно впливає на стабільність успішного знаходження об’єкта. Оскільки середовище та точки освітлення будуть стабільні в умовах, для яких проектується дана система, то дані недоліки методу (значно менша ймовірність успішного розпізнавання при відмінностях у середовищі та ракурсі освітлення) впливати не будуть. Для стабільної роботи каскаду рекомендується зробити 3000-4000 позитивних зразків. Приклад бібліотеки позитивних зразків показаний на рисунку 3.1.

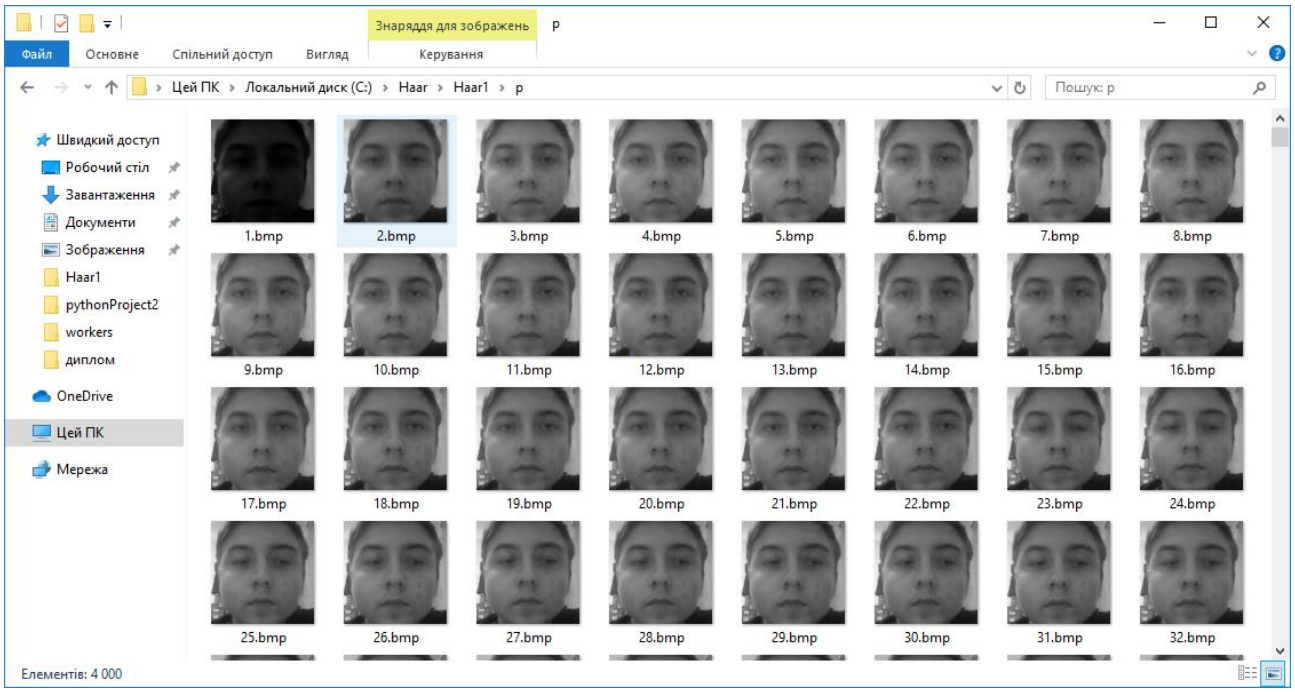

Рис 3.1. Приклад бібліотеки позитивних зразків у файловій системі Windows

По аналогічним причинам при наповненні бібліотеки негативних зразків слід робити їх на місці розпізнавання при робочому освітленні та ракурсі камери. Для стабільного розпізнавання також рекомендується зробити 3000-4000 зразків. Приклад бібліотеки негативних зразків показаний на рисунку 3.2.

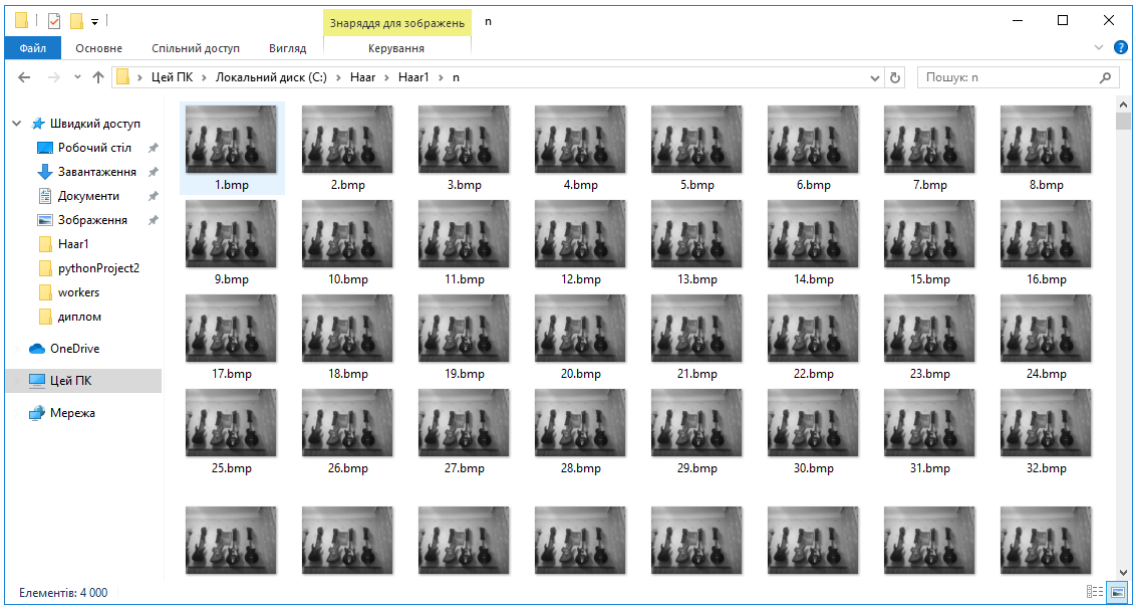

Рис 3.2. Приклад бібліотеки негативних зразків у файловій системі Windows

Для правильного заповнення файлу із переліком потрібно вказати координати об’єкта на фото, але цю частину можна полегшити. Бібліотеку позитивних зразків можна зробити із фотографій, на яких на повну фотографію зображений шуканий об’єкт і лише по краям видно навколишнє середовище. У такому випадку у даному файлі як координати об’єкта можна буде вказати повний розмір фотографії. Приклад заповненого файлу із переліком позитивних зразків та приклад заповненого файлу із переліком негативних зразків зображено на рисунках 3.3 та 3.4.

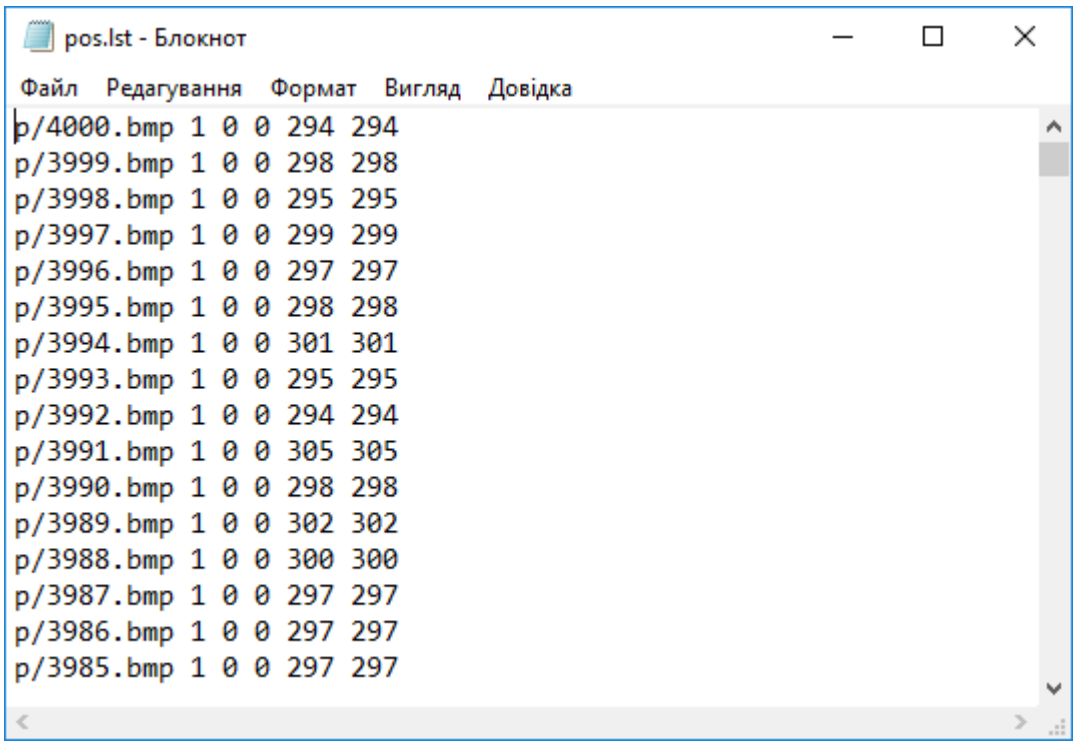

Рис 3.3. Приклад заповненого файлу із переліком позитивних зразків у файловій системі Windows

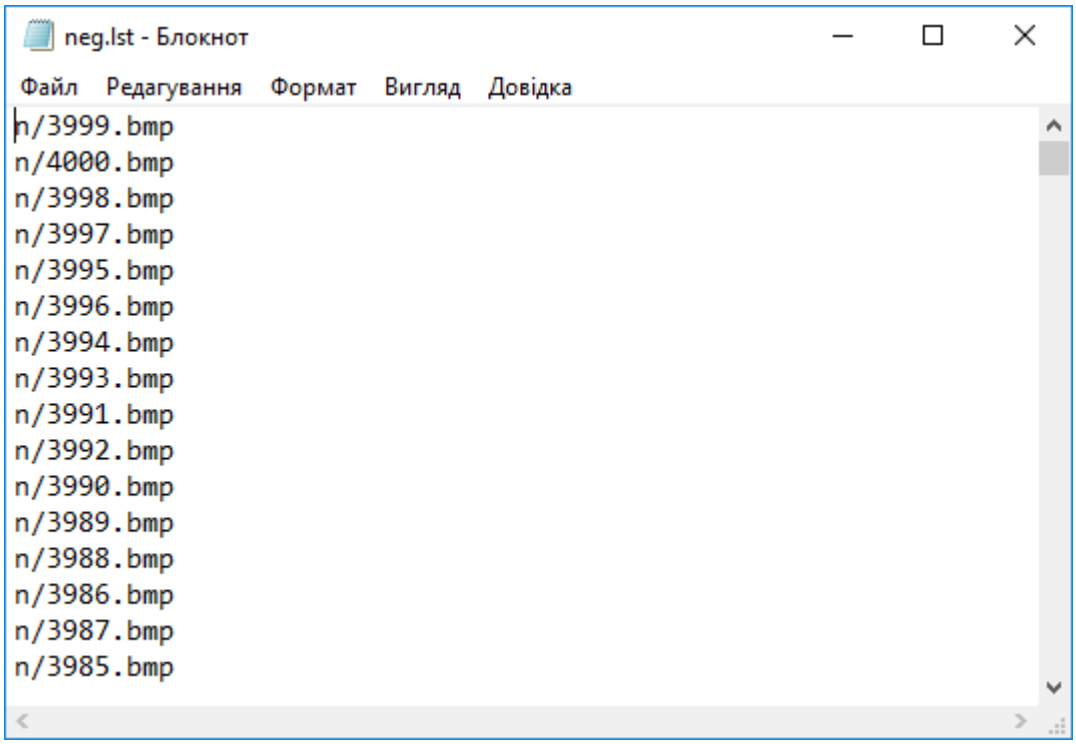

Рис 3.4. Приклад заповненого файлу із переліком негативних зразків у файловій системі Windows

3.2.2. Побудова каскаду Хаара

Побудова каскаду Хаара проводиться у 2 етапи. Обидва етапи можна виконати вбудованими програмами бібліотеки OpenCV. При завантаженні OpenCV версії 3.4.11 дані програми містяться за адресом «…\opencv\build\x64\vc15\bin». Приклад розміщення програм зображений на рисунку 3.5.

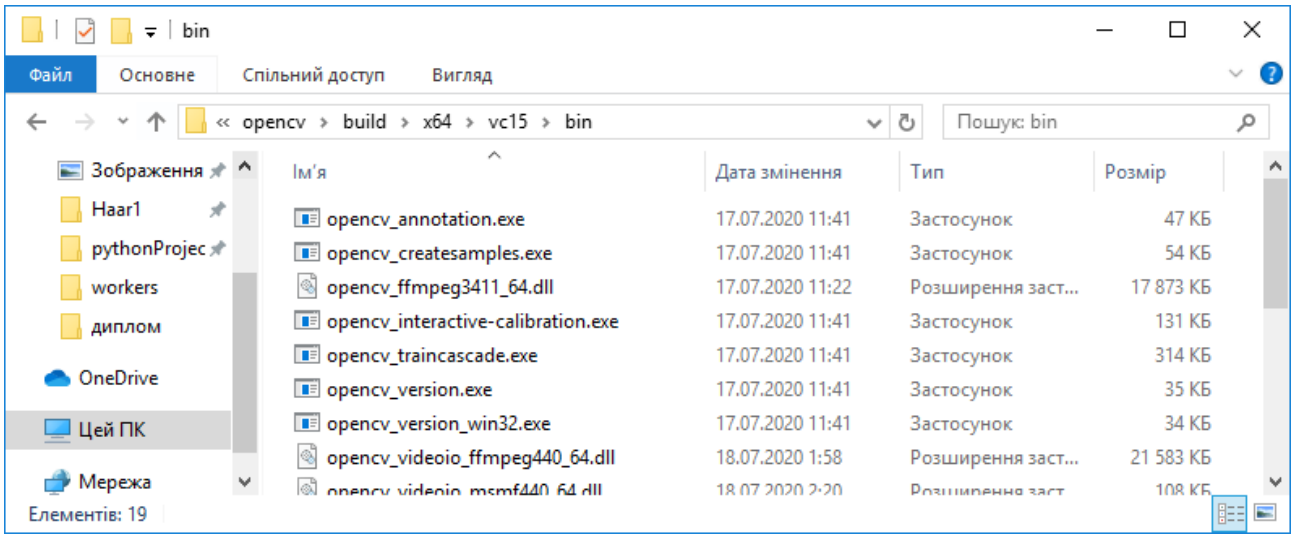

Рис 3.5. Розміщення вбудованих програм OpenCV 3.4.11

Першим етапом є створення файлу «samples.vec», у якому будуть міститися всі позитивні зразки у форматі близькому до bmpта у вказаному розмірі. Для його створення потрібно у командному рядку операційної системи ввести команду «opencv_createsamples.exe -infoC:\Haar\Haar1\pos.lst -vecsamples.vec -w 24 -h 24», де:

- opencv_createsamples.exe – назва програми, яка буде використовуватися для роботи;
- -infoC:\Haar\Haar1\pos.lst – повний шлях до файлу pos.lst, у якому вказаний опис позитивних зразків (також може бути вказаний шлях до даного файлу відносно програми opencv_createsamples.exe);
- -vecsamples.vec – шлях до файл, у який буде збережена доведена до загального формату база позитивних зразків, відносно програми opencv_createsamples.exe (також може бути вказаний повний шлях до файлу);
- -w 24 -h 24 – розміри шаблону, а саме «w», від слова «width» - ширина шаблону, а «h», від слова «height» - висота шаблону. Розміри вказуються у пікселях. Для лиця доцільно створити квадратний шаблон.

Другим етапом є створення самого каскаду. Для його створення використовується програма «opencv_traincascade.exe». Дана програма міститься

у тій же папці, що і попередня програма. Процес створення каскаду може займати від кількох хвилин до кількох годин в залежності від кількості позитивних та негативних зразків. Для вибірки у 4000 зразків створення каскаду буде тривати близько чотирьох годин. Для початку процесу потрібно у командній стрічці операційної системи ввести команду «opencv_traincascade.exe -dataC:\Haar\Haar1\classifier -vecsamples.vec -bgC:\Haar\Haar1\neg.lst -numStages 20 -minhitrate 0.99 -maxFalseAlarmRate 0.1 -numPos 3960 -numNeg 4000 -w 24 -h 24-mode ALL -precalcValBufSize 10240 -precalcIdxBufSize 10240», де:

- opencv_traincascade.exe – назва програми, що буде використовуватися для навчання каскаду Хаара;
- -dataC:\Haar\Haar1\classifier – повний шлях до папки, у якій буде зберігатися каскад Хаара після закінчення процесу його створення (також шлях може бути вказаний відносно програми opencv_traincascade.exe);
- -vecsamples.vec – шлях до файлу із приведеними до одного формату позитивними зразками відносно програми opencv_traincascade.exe (також може бути вказаний повний шлях);
- -bgC:\Haar\Haar1\neg.lst – повний шлях до бібліотеки із негативними зразками (також може бути вказаний шлях відносно програми);
- -numStages 20 – кількість рівнів каскаду Хаара, які програма буде створювати. Для стабільної роботи каскаду достатньо зробити 16-25 рівнів навчання. Оскільки вибірка фотографій достатньо велика, а кожен наступний рівень навчається значно довше за попередній, то у даному випадку доцільно взяти 20 рівнів;
- -minhitrate 0.99 – коефіцієнт, що визначає якість навчання каскаду, а саме мінімальний відсоток правильних знаходжень об’єкта серед бібліотеки позитивних зразків. Оскільки у вибірці позитивних зразків можуть бути фотографії низької якості, які програма не прийме на навчання, то доцільно цей коефіцієнт зробити меншим одиниці;

- -maxFalseAlarmRate 0.1–рівень фальшивої тривоги;
- -numPos 3960 – кількість позитивних зразків, але не повна, а пропорційна коефіцієнту minhitrate;
- -numNeg 4000 – кількість негативних зразків у вибірці;
- -w 24 -h 24 – розмір примітиву Хаара, повинен співпадати із розміром, вказаним у першому етапі при створенні файлу samples.vec;
- -mode ALL –вказуємо програмі які примітиви Хаара будуть використовуватися у формуванні каскаду. У даному випадку Allозначає, що програма буде використовувати всі примітиви Хаара;
- -precalcValBufSize 10240 -precalcIdxBufSize 10240 – розмір пам’яті комп’ютера, яка буде виділена для процесу навчання каскаду Хаара.

Після закінчення роботи програми буде створена папка по вказаному шляху та із вказаною назвою, куди буде поміщений результат роботи програми – файл «cascade.xml». Для використання даного каскаду у подальшій роботі в програмі слід підключати даний файл. Результат проведеного навчання каскаду Хаара зображений на рисунку 3.6.

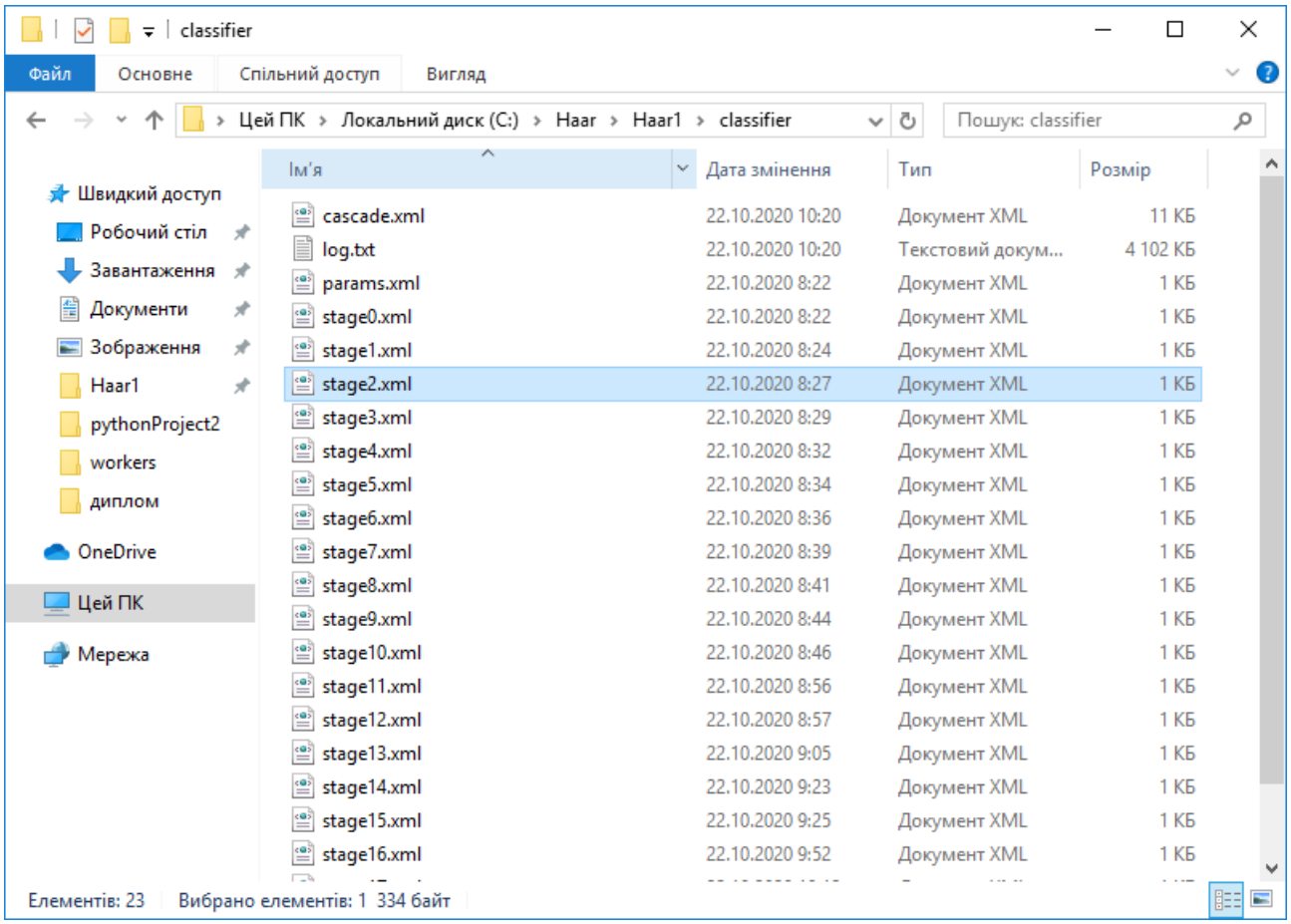

Рис 3.6. Результат закінчення навчання каскаду Хаара

3.3. Опис алгоритму розпізнавання користувача

За допомогою системи автентифікації можна визначити чи співпадає особистість людини, що намагається увійти до комп'ютерної системи, із тими, що внесені до списку довірених осіб у системі. При використанні методів біометричного розпізнавання із системою повинен взаємодіяти пристрій, що може зчитати біометричні характеристики із особи, які потрібні для подальшого

розпізнавання. У даному випадку як засіб для зчитування біометричних даних буде використовуватися веб-камера, кадри якої мають розмір 640 на 480 пікселів.

Процес автентифікації складається з 4 основних етапів:

- Перший етап це зчитування біометричних характеристик із людини та особистих даних;
- Другий етап це обробка зображення перед початком розпізнавання для підвищення успішності процесу;
- Третій етап це є ідентифікація координат людського лиця на зображенні та зняття з нього характеристик, за допомогою яких буде проводитися порівняння із довіреними зразками.
- Четвертий етап це порівняння знятих характеристик із тими, що були внесені до системи як еталонні.

Розглянемо розроблений алгоритм автентифікації за геометрією лиця більш детально:

1. Підключення заздалегідь встановлених бібліотек OpenCV та Dlib для подальшої роботи процесу;
2. Підключення створеного у 2 розділі дипломної роботи каскаду Хаара для пошуку людського лиця на зображенні за допомогою функцій OpenCV;
3. Підключення маски із характерними точками для середньо-статистичного людського лиця;
4. Підключення моделі для визначення дескриптора;
5. Ввід користувачем логіну та пароля;
6. Ввімкнення веб-камери для подальшого зняття біометричних характеристик із особи;
7. Зчитування зображення з веб-камери у вигляді відео-потоку;
8. Виділення області у відео-потоці, у яку користувач повинен помітити своє лице;

9. Фіксація кадру із відео-потоку по натисканню користувачем відповідної клавіші, що вказана у кадрі;
10. Визначення розмірів кадру;
11. Створення маски для обробки кадру перед початком роботи;
12. Накладання створеної маски на отримане зображення;
13. Пошук координат людського лиця на обробленому зображенні;
14. Виділення лиця на зображенні;
15. Накладання маски характерних точок на лице, що було знайдене раніше;
16. Корекція положення для кожної точки маски, щоб вони співпадали із лініями знайденого лиця;
17. Визначення дескриптору лиця;
18. Завантаження фотографій, на яких зображені еталонні лиця;
19. Накладання маски із характерними точками на завантажені еталонні лиця;
20. Корекція положення характерних точок;
21. Визначення дескрипторів еталонних лиць;
22. Визначення Евклідової відстані між дескриптором знайденого лиця та дескрипторами еталонних лиць;
23. Створення масиву знайдених Евклідових відстаней;
24. Визначення найменшої Евклідової відстані;
25. Визначення та позначення на кадрі імені особи, яка була знайдена у попередніх етапах, якщо її біометричні характеристики, логін та пароль співпали із еталонними;
26. У разі, якщо біометричні характеристики знайденої особи не співпали із еталонними, то на кадрі позначається, що дана особа є невідомою;
27. У разі, якщо пред’явлене лице співпадає із еталонними, але не співпадає логін чи пароль, що були пред’явлені разом із лицем, то на кадрі позначається відповідне повідомлення;

28. У разі, якщо лице не було визначено у кадрі, то на кадрі позначається відповідне повідомлення;
29. Візуальне представлення висновку процесу.

3.3.1. Отримання необхідних даних

До першого етапу (зчитування біометричних характеристик) відносяться перші 9 пунктів процесу. Даний етап є підготовчим у процесі автентифікації особи у комп'ютерній системі, а саме збір даних.

Для підключення створеного каскаду Хаара знадобиться XML файл із створеним раніше у 2 розділі каскадом Хаара. Аналогічно і для підключення маски із характерними точками та моделі для визначення дескриптора лиця потрібно мати відповідні файли, у яких описуються дані моделі.

Першими даними, які користувач вводить у процес є особистий логін. Дана інформація вказує під яким іменем користувач намагається увійти до комп'ютерної системи. Біометричні дані слугують підтвердженням того, що до комп'ютерної системи намагається увійти саме та особа, якій належить вказаний логін.

Ввімкнення веб-камери відбувається за допомогою функціоналу OpenCV. У нашому випадку нам потрібно, щоб зображення до процесу надавалося із веб-камери. Відтворити даний відео-потік у реальному часі можна шляхом по-кадровому показу у нескінченному циклі. Оскільки дана процедура не містить складних обчислювальних процесів, то це відбувається дуже швидко що дає змогу створити ефект відтворення відео.

Наклавши текст із інструкцією для користувача можна значно полегшити розуміння процесу. Також оскільки у наступних кроках зображення буде додатково оброблятися, то варто окреслити область, де користувачу варто розмістити своє обличчя, що дозволить максимально якісно користувачу надати свої біометричні дані для обробки.

Переривати даний потік доцільно натисканням клавіші, оскільки, якщо використовувати фіксовану кількість кадрів для збору біометричних характеристик людини, дані кадри можуть бути низької якості, що не дозволить провести коректне розпізнавання. Причиною цьому можуть стати як поворот голови по вертикалі, розмиті кадри через рух, так і повна відсутність у кадрі. Зняття характеристик по натисканню клавіші робітником дозволить уникнути даних проблем. Після натискання відповідної клавіші оновлення актуального кадру припиняється і ми отримуємо кадр, який буде брати участь у подальшому розпізнаванні особи.

3.3.2. Попередня обробка отриманих зразків

До другого етапу (обробка кадру) відносяться пункти з 10 по 12 включно. У даному етапі проводиться робота над отриманим зображенням лиця людини, а саме обробка кадру таким чином, щоб мінімізувати шанс розпізнавання об’єктів у навколишньому середовищі як лиця людини чи уникнути подвійного розпізнавання у випадку, якщо поряд знаходяться інші люди і їх лиця попадають у поле зору камери.

Реалізувати це можна за допомогою розмиття областей кадру, у яких не передбачується розміщення лиця користувача. Оскільки положення голови людини буде розміщене у одній і тій же області за посадкою на робочому місці, то це дає змогу обробити максимально велику область і лишити для розпізнавання максимально малу область. У випадку, якщо область лиця при обробці та реальне розміщення лиця у користувача будуть мати відхилення між собою, то користувач має змогу правильно скоректувати положення голови за рахунок позначення області майбутньої обробки на кадрі на попередньому етапі. Для цього потрібно створити фото, що повністю наповнене шумом та маску, у якій будуть виділені координати, які потрібно лишити без шуму.

Саме ж розмиття відбувається наступним чином. Ядро - це розмір матриці, яка буде брати участь в обчисленні значення пікселя. Обчислюється воно за формулою:

$$K = \frac{1}{Ksize.width \times Ksize.height} \times \begin{bmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ 1 & 1 & 1 & \dots & 1 & 1 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 1 & 1 & 1 & \dots & 1 & 1 \end{bmatrix} \qquad (3.1)$$

де $Ksize.width$ -ширина ядра, а $Ksize.height$ - висота ядра.

Піксель фото, який ми обчислюємо, є центром матриці ядра. Усі пікселі, які попадають під вплив матриці ядра беруть участь у обчислюванні, тобто, якщо у нас ядро розміром 3 на 3, то участь у обчислюванні будуть брати усі пікселі, що попадають у матрицю розміром 3 на 3 із центром у пікселі, що буде обчислюватися. Дана область виділяється із фотографії, множиться на матрицю ядра, після чого всі отримані значення додаються в одне ціле, що є новим значенням пікселя.

Чим більший радіус ядра, тим сильніше замилювання створюється у результаті даного обчислення. На рисунку 3.7 зображені приклади використання

ядер різної величини (А – без замилювання, Б – ядро розміром 11 на 11, В – ядро розміром 23 на 23).

Рис. 3.7 Приклад замилювання для різних ядер

3.3.3. Обчислення ХТ та їх порівняння

Наступним етапом є створення маски, по якій будуть додаватися розмите зображення та звичайне зображення. Для початку потрібно створити масив заповнений нулями із таким же розміром як отриманий кадр. Оскільки фото складається із значень трьох кольорів, а саме червоного (Red), зеленого (Green) та синього (Blue), що сукупно утворюю RGB модель. Тобто у числовому вигляді фото можна представити наступним чином:

$$R=\begin{pmatrix} r_{00} & r_{10} & \dots & r_{m0} \\ r_{01} & r_{11} & \dots & r_{m1} \\ \dots & \dots & \dots & \dots \\ r_{0n} & r_{1n} & \dots & r_{mn} \end{pmatrix},\quad G=\begin{pmatrix} g_{00} & g_{10} & \dots & g_{m0} \\ g_{01} & g_{11} & \dots & g_{m1} \\ \dots & \dots & \dots & \dots \\ g_{0n} & g_{1n} & \dots & g_{mn} \end{pmatrix},\quad B=\begin{pmatrix} b_{00} & b_{10} & \dots & b_{m0} \\ b_{01} & b_{11} & \dots & b_{m1} \\ \dots & \dots & \dots & \dots \\ b_{0n} & b_{1n} & \dots & b_{mn} \end{pmatrix}, \quad (3.2)$$

де r, g, b – значення яскравості пікселів для відповідного кольору, а m, n – порядкові номери стовбців та рядків матриць.

Після чого місце ймовірного розташування лиця суцільно заповнюється значенням 255. У результаті ми отримаємо числовий масив, який якщо зобразити у вигляді фотографії RGB моделі, то ми отримаємо зображення на рисунку 3.8.

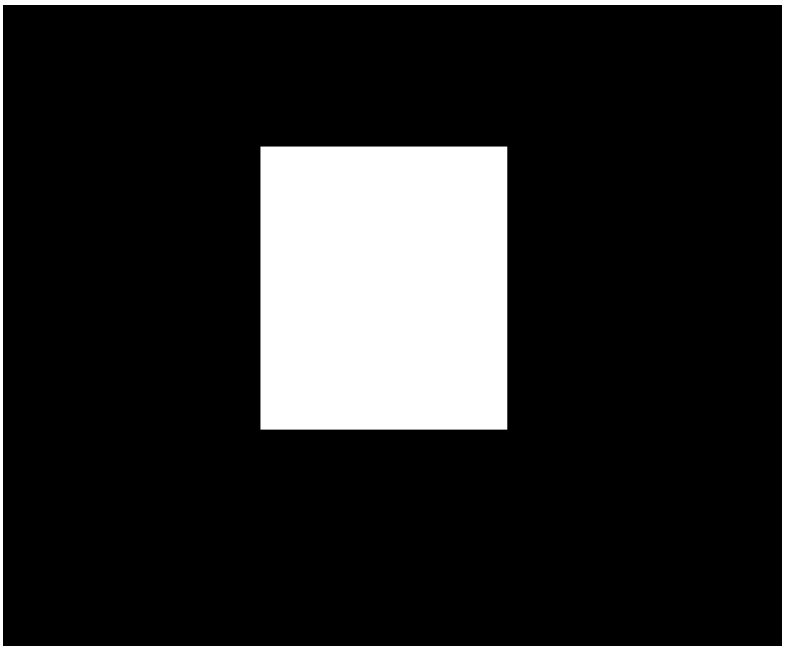

Рис. 3.8. Маска для нанесення blur ефекту

Скористатися даною маскою можна наступним чином. На місця, де значення матриці рівне 0, ми підставляємо значення пікселів із розмитого фото. А на місця, де значення матриці рівне 255, ми підставляємо значення звичайного фото. Після проведення даної операції ми отримуємо кадр, що зображений на рисунку 3.9.

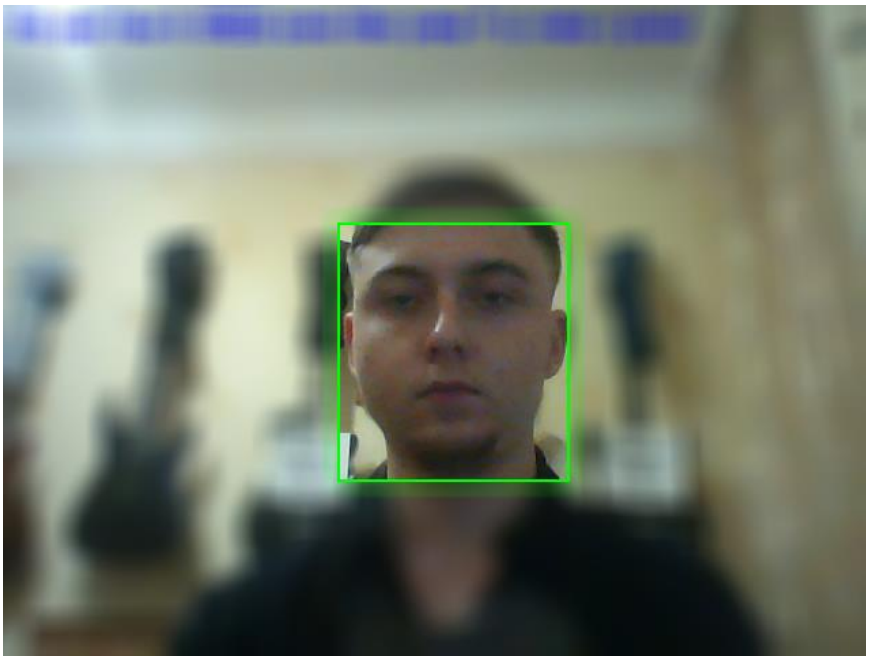

Рис. 3.9. Результат обробки фото перед процесом ідентифікації

Обробивши отримане зображення, процес пошуку координат лиця за допомогою каскаду Хаара стане значно стабільнішим, оскільки об’єкти, які каскад міг би сплутати з лицем занадто розмиті на кадрі а єдиний не розмитий об’єкт у кадрі це лице, яке потрібно розпізнати.

До третього етапу (розпізнавання обличчя та розрахунок дескриптору) відносяться кроки від 13 до 17 включно. Спочатку координати лиця знаходяться за допомогою каскаду Хаара. Після чого за допомогою методу LBP на ньому визначаються ХТ, н основі яких проводиться розрахунок дескриптору.

Відповідність зображенню примітивам Хаара визначається різницею сум яркостей пікселів на прямокутних підобластей примітиву Хаара.

Оскільки примітиви Хаара у каскаді створені для лиця фіксованого розмір, а також саме лице не буде розміщене на всю фотографію, то потрібно накладати примітиви Хаара на частини зображення із по-кроковим переміщенням та зміною масштабу вікна при закінчення аналізу всього фото. Для пошуку об’єктів за допомогою каскаду Хаара використовується метод вікна, що переміщується. На частину зображення накладаються примітиви з каскаду Хаара після чого

порівнюється яскравість білих та чорних областей. Розглянемо детальніше параметри пошуку каскадом.

Шкала збільшення не може бути менший одиниці та більший значення 1.4 . Чим більше даний показник, тим сильніше збільшується поле пошуку при закінченні сканування всього фото. При більшому коефіцієнті сканування буде проводитися швидше, але зростає шанс пропустити шуканий об’єкт у кадрі.

Кількість сусідніх квадратів пошуку не може бути меншою одиниці. Більший параметр дозволить зробити ретельніший аналіз, але це негативно вплине на швидкість пошуку, оскільки поле пошуку буде повільніше рухатися. Оптимальне значення для даного параметру є 3-6.

Мінімальна розмірність шаблону визначає початковий розмір області, у якій буде вестися пошук. Для лиця краще брати квадратну область розмірністю 30 на 30 пікселів. Також є параметр максимального вікна, але при його ігноруванні, вікно буде збільшуватися до тих пір, поки не заповнить все зображення, що збільшить час пошуку, але і збільшить шанс на успішне виявлення об’єкта.

Після виявлення лиця на фотографії потрібно визначити його характерні точки, за якими можна визначити особистість людини та провести автентифікацію. Визначити дані точки можна розмістивши на зображення маску із середньо-статистичними характерними точками та підрівнявши їх під конкретне лице шляхом застосування методу Local Binary Pattern (LBP) [28]. Стандартна маска середньо-статистичних характерних точок зображена на рисунку 3.10.

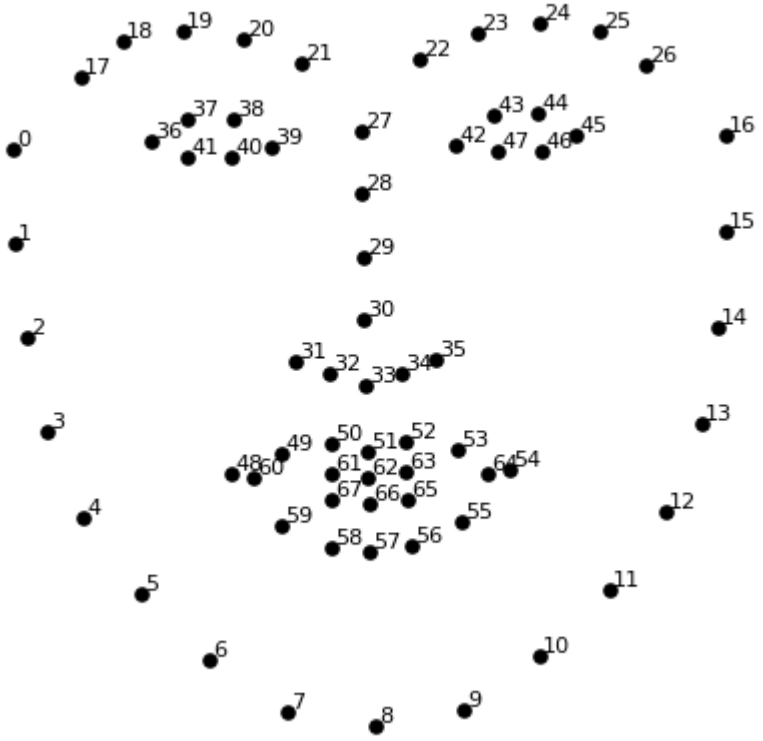

Рис. 3.10 Маска середньо-статистичних характерних точок

Метод LBP дозволяє визначити у якому напрямку зменшується яскравість відносно точки на фото по нормалі. Дана операція дозволить визначити у якому напрямку та як далеко розташований краї скул (0-16 точки), роту (48-67 точки), носу (27-35 точки), очей (36-47 точки) та брів (17-26 точки). Розрахунок проводиться за формулою:

$$LBP(g_{Px}, g_{Py}) = \sum_{p=0}^{P-1} S(g_P - g_C) \times 2^p \ , \qquad (3.3)$$

де *gc* це інтенсивність центрального пікселя у вибірці, а *gp* це інтенсивність сусідніх пікселів. Функція *S* описується наступним чином:

$$S(x) = \begin{cases} 1 \, if \ \ x \geq 0 \\ 0 \, if \ \ x < 0 \end{cases} \qquad (3.4)$$

Дані результаті складаються у двійкове число та переводяться у десяткове. Після чого будується гістограма (рисунок 3.11) залежності інтенсивності та

відхилення від центральної точки, що є точкою маски характерних точок середнього лиця. Дане відхилення будується по нормалі відносно контуру маски.

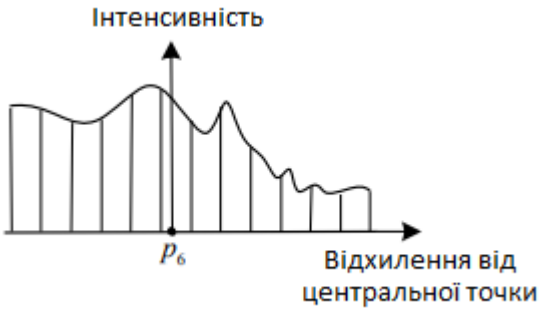

Рис. 3.11 Приклад гістограми залежності інтенсивності від відхилення

Наступним кроком є визначення дескриптора лиця. Дескриптор – набір характеристик, що описують лице не залежно від сторонніх факторів, таких як стать, вік, зачіска та тому подібне. Аналізуються спеціальні ознаки, а саме характерні точки обличчя, які були визначені у минулому кроці.

Четвертий етап (порівняння отриманих даних із еталонними) є завершальним. Під час нього до програми завантажуються фотографії, на яких зображені еталонні лиця, із якими проводяться ті ж самі маніпуляції, доки не буде визначений дескриптор для кожного з них. Дескриптор є результатом згортки сусідніх пікселів ХТ, що розраховується за формулою 3.1.

Порівняти отримані дескриптори можна розрахувавши відстань Евкліда для кожної пари дескрипторів. Дана відстань це є довжина між точками простору. Розраховується вона по наступній формулі:

$$d(p,q) = \sqrt{\sum_{k=1}^{n} (p_k - q_k)^2} \qquad (3.5)$$

, де p це точка одного простору, а q це відповідно точка другого простору.

Чим менше значення Евкліда тим більша ймовірність, що дане лице це лице тієї ж людини, що зображена на еталонному зображенні. Якщо значення більше ніж 0.6, то дане лице не співпадає із еталонним.

Якщо лице співпадає із еталонним, то наступним кроком є порівняння логіну та паролю, що були введені раніше, чи співпадають вони із тими, що належать знайденому лицю. Якщо ж лице не співпало із еталонними, то таким же чином доцільно вказати дану інформацію на фотографії. Якщо лице не було знайдене на фотографії, то також доцільно вивести відповідне повідомлення на фотографію. Якщо лице було ідентифіковане успішно, але не співпав логін чи пароль, то аналогічно із попередніми ситуаціями доцільно повідомити даний результат на зображенні.

3.4. Висновок до розділу

У даному розділі було обрано середовище для розробки системи біометричної автентифікації користувачів комп’ютерної системи, а саме PyCharm. А також було обрано бібліотеки для виконання основного функціоналу системи, а саме OpenCV для обробки зображень та розпізнавання лиця та Dlib для визначення ХТ та їх порівняння.

Був розглянутий процес запропонованої підготовки зразків для навчання каскаду Хаара для пошуку людського лиця. А також було по-кроково розглянуто розроблений процес навчання даного каскаду із використанням раніше підготовлених зразків та функціоналу OpenCV.

Також був детально розглянутий вдосконалений алгоритм біометричної автентифікації користувача у комп’ютерній системі. Який був розділений на чотири етапи, кожен з яких має свій набір кроків, направлених на:

- виконання збору інформації;

- попередню обробку отриманих даних;
- розпізнавання лиця та визначення особливих характеристик;
- порівняння отриманих даних із еталонними.

Для підвищення стабільності виконання процесу та мінімізації виникнення помилок через сприйняття алгоритмом навколишнього середовища як шуканого об’єкта перед початком виконанням основної роботи, тобто розпізнавання, прийняті зразки додатково обробляються. Дана обробка являє собою приведення зображення до такого вигляду, щоб система не змогла розпізнати навколишнє середовище як шуканий об’єкт або ж прийняти у процес лиця сторонніх осіб.

Також оскільки фото оброблене таким чином, що всі сторонні об’єкти є неможливими у розпізнаванні, то зростає коректність розпізнавання лиця. Оскільки єдиним чітким об’єктом на зображенні є лице користувача, то система не може надати подальшим крокам алгоритму зображення, на якому є лише частина лиця і частина навколишнього середовища, що схожа на відсутню частину лиця.

4 РОЗДІЛ. ПРАКТИЧНА РЕАЛІЗАЦІЯ АЛГОРИТМУ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА КОМП'ЮТЕРНОЇ СИСТЕМИ

1.1. Програмна реалізація алгоритму

Перед початком роботи потрібно підключити всі потрібні для роботи бібліотеки. Виконується це за допомогою команді import. Для роботи алгоритму знадобляться бібліотеки OpenCV, для виконання операцій пов'язаних із обробкою зображень, Dlib, для виконання операцій, пов'язаних із обробкою XT, Numpy [29], для операцій, пов'язаних із числовими обрахунками, CascadeClassifier, для операцій, пов'язаних із методом Хаара, та distance, для операцій, пов'язаних із визначенням довжини Евкліда.

1.1.1. Перший етап алгоритму

Початковим кроком є прийняття логіну від користувача. Для цього скористаємося вбудованою командою input(). Користувачу виводиться повідомлення з інструкцією «Input your LOGIN, thereafter press ENTER», що має наступний переклад – «Введіть свій логін, після чого натисніть на ENTER».

Після введення всіх даних, починається процес надання фотографії. За допомогою функції VideoCapture() можна вести зйомку кадрів із веб-камери комп'ютера. Оскільки дана зйомка ведеться по-кадрово, то виведення її

користувачу доцільно із використанням циклу for. Через функцію read() надаємо змінній зображення, на яке перед показом накладаємо інструкцію для користувача та позначаємо зону, у яку користувач має помістити своє лице. У якості інструкції добавляємо текст «Put your face in GREEN zone! Thereafter press P to make a photo!», що має переклад «Помістіть своє лице у ЗЕЛЕНУ зону! Після цього натисніть P, щоб зробити знімок!». Додаємо дану інструкцію за допомогою putText(). І за допомогою rectangle() позначаємо кордони області, у якій повинно бути лице. По натисканню клавіші P цикл оновлення актуального кадру припиняється за допомогою waitKey().

1.1.2. Другий етап алгоритму

Отримавши актуальний кадр можна приступити до попередньої обробки зображення для підвищення успішності процесу. Як було визначено у 3 розділі роботи, даний етап проходить у 2 кроки – розмиття повного фото та з’єднання розмитого фото та фото без обробки за допомогою створеної маски. За допомогою blur() створюємо повністю розмите фото. Дана функція використовує формулу 3.1 і задаємо розмір ядра 23 на 23. За допомогою zeros() створюємо повністю заповнену матрицю нулями і заповнюємо область лиця значенням 255. Оскільки даний масив можна інтерпретувати як зображення, то для виділення лиця використовуємо знову ж rectangle(), але на цей раз вказуємо суцільне заповнення вказаним кольором, що є (255, 255, 255). Таким чином ми отримаємо закінчену маску. Скористатися даною маскою можна за допомогою where(), що підставить на місця заповнені нулями значення із масиву розмитої фотографії, а на всі інші – знамення із масиву не обробленої фотографії.

1.1.3. Третій етап алгоритму

Отримавши оброблене зображення, можна приступати до розпізнавання лиця. Для запуску процедури пошуку обличчя за допомогою каскаду Хаара використовується detectMultiScale(). Вказуємо параметри пошуку, а саме крок збільшення 1.1, мінімальна кількість сусідніх областей 6 та мінімальній розмір вікна 30 на 30 пікселів. Після закінчення розпізнавання функція повертає значення, що є координатами верхнього лівого кута області з лицем та ширину і висоту області. Використовуючи дані значення можна окреслити зону із лицем.

Отримавши координати лиця, тобто переконавшись, що лице дійсно присутнє на фото, стає можливим визначити особистість зображеної людини. Перед самим визначенням ХТ потрібно визначити додаткові координати лиця за допомогою detector() у вже визначеній області каскадом Хаара. Визначення ХТ відбувається за допомогою predictor(), що використовує стандартну модель середньостатистичного розміщення ХТ, зображена у другому роздала на рисунку 3.4. Дана маска накладається на лице та за допомогою методу LBP ХТ коректуються відповідно до зображеного лиця за допомогою виразів 3.3 та 3.4. як результат ми отримуємо координати кожної із 68 ХТ. Використавши координати даних точок можна позначити їх на зображення точками за допомогою circle().

Отримавши координати ХТ стає можливим визначити унікальний для кожної особи дескриптор. Виконується це за допомогою compute_face_descriptor(), що поверне масив унікальних значень.

1.1.4. Четвертий етап алгоритму

Отримавши всі дані від користувача наступним кроком є виконання всіх тих же дій для всіх користувачів системи. Даний процес починається із загрузки фотографії, на якій міститься лише лице користувача за допомогою imread(). Після чого аналогічним чином проводиться визначення ХТ та дескриптору лиця для подальшого порівняння. Виконується дана операція для кожного зображення окремо.

Після чого для кожного із отриманих дескрипторів визначається Евклідова відстань, а саме між дескриптором заявленого лиця і між кожним із дескрипторів еталонних лиць за формулою 3.5. Після визначення усіх відстаней формується масив із отриманих значень, із якого вибирається найменше значення. Чим менше значення відстані Евкліда, тим більша вірогідність, що дескриптори були зняті з однієї людини.

Фінальним кроком є порівняння усіх отриманих значень із тими, що належать кожному користувачу, а саме відстань Евкліда, логін та пароль. У випадку, якщо всі дані співпали із одним із користувачів, то на фотографію накладається його ім’я, та інструкція про подальші дії, а саме «Press E to exit», тобто «Натисніть Е для виходу». У випадку якщо відстань менша 0.6, але логін не співпав із користувачем, якому належить лице, то виводиться відповідне повідомлення «THE LOGIN DOES NOT MATCH THE DETECTED FACE!» - «Логін не відповідає знайденому лицю». У випадку якщо найменша відстань більша 0.6, то це означає, що знайдене лице не належить жодному із користувачів системи. У цьому випадку виводиться повідомлення «UNKNOWN PERSON» - «Невідома особистість». У випадку, якщо лице зовсім не було розпізнане, то виводиться повідомлення «NO FACE DETECTED» - «Лиць не розпізнано».

1.2. Приклад роботи програми

Розглянемо приклад автентифікації для користувача Andrii із використанням веб камери із розширенням 640 на 480 пікселів. Після ввімкнення програми виводиться повідомлення, що вказує на потребу ведення логіну користувача, зображена на рисунку 4.1.

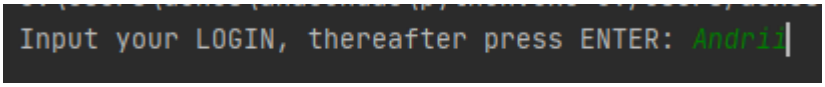

Рис. 4.1. Повідомлення про введення логіну користувача

Після отримання цих даних включається веб-камера, на якій зображений користувач, інструкція для користувача та зона, у яку йому потрібно помістити лице. Вигляд даного кроку зображений на рисунку 4.2.

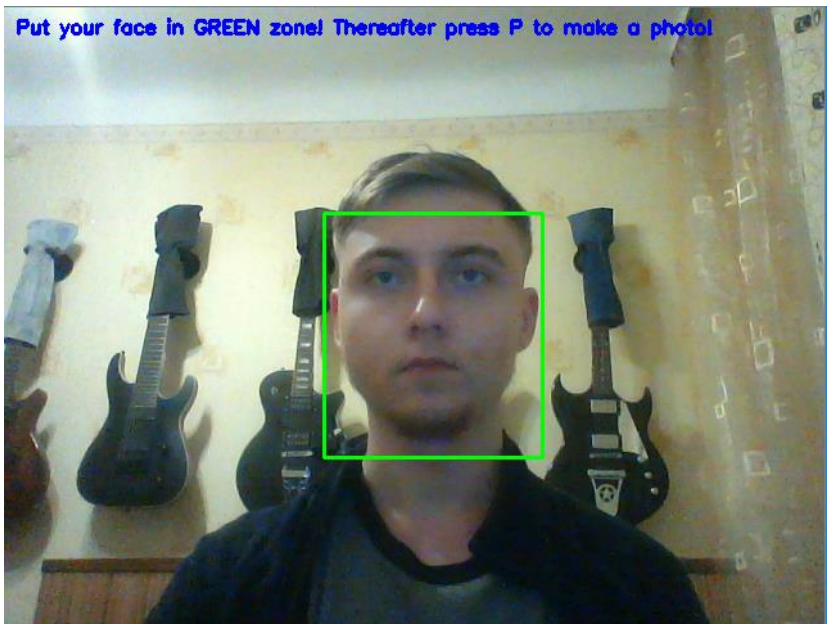

Рис. 4.2. Створення фотографії користувача

Після натискання на клавішу P даний кадр фіксується та бере участь у подальшій обробці. Наступним етапом є обробка зображення, а саме розмиття

навколишнього середовища для уникнення шансу не коректного розпізнавання. На рисунку 4.3 зображений оброблена фотографія.

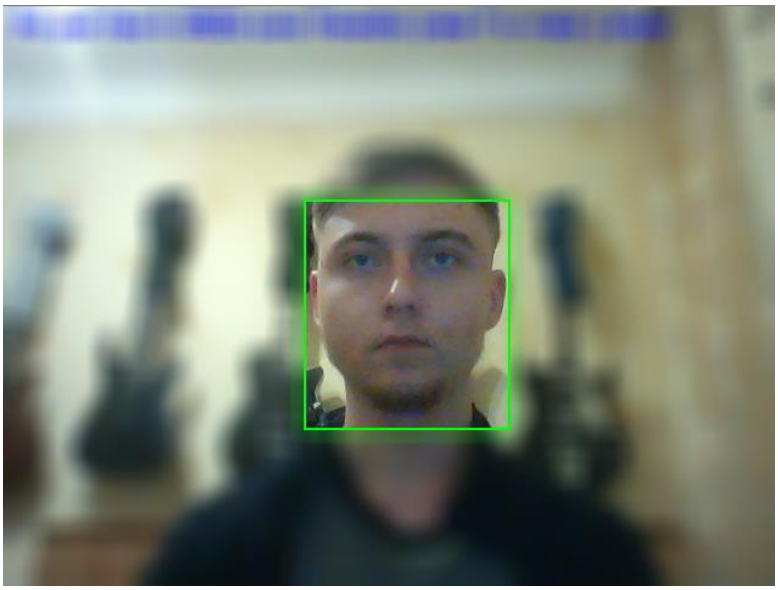

Рис. 4.3. Оброблена фотографія

Після того як ми отримали оброблене зображення, починається процес розпізнавання лиця. Знайдене лице виділяється на зображенні. Після виділення лиця на зображенні проходить процес знаходження ХТ, кожна з яких також позначається на зображенні. На рисунку 4.4 зображена фотографія після розпізнавання лиця каскадом Хаара та з позначеними ХТ.

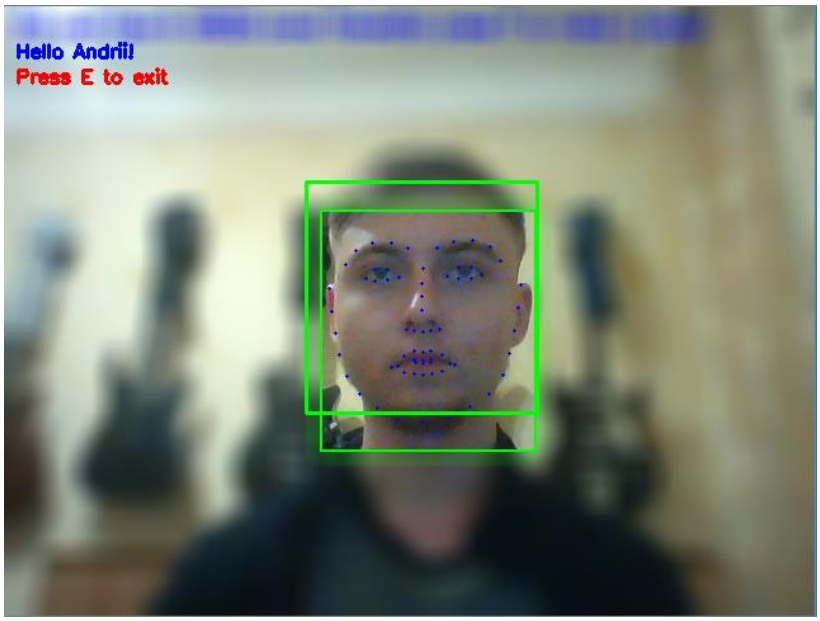

Рис 4.4. Кінцевий кадр після проведення автентифікації

Після визначення дескриптору лиця та евклідових відстаней проходить процес порівняння всіх отриманих даних із тими, що присвоєні кожному еталонному лицю. У випадку якщо всі дані співпали із одним із користувачів, то на екран виводиться привітання з іменем користувача, що зображено у правому верхньому куті на рисунку 4.4.

Тепер спробуємо ввести логін користувача John, але лице надати користувача Andrii. Введення логіну та пароля зображене на рисунку 4.5.

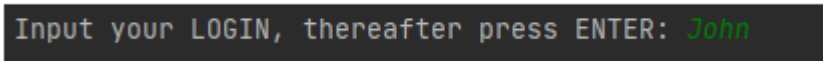

Рис. 4.5. Введення даних користувача John

На рисунку 4.6 зображений результат автентифікації користувача Andrii із введеним логіном користувача John. Програма розпізнала що пред’явлене лице співпадає із одним з еталонних, але логін не співпав із тими, що належать користувачу із даним лицем.

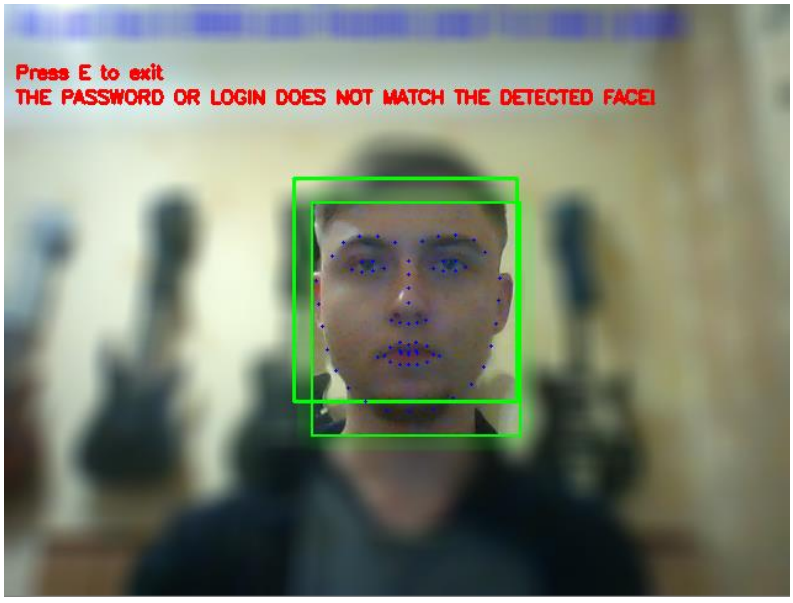

Рис. 4.6. Результат автентифікації із чужими даними

Тепер спробуємо надати програмі лице особи, що не міститься у списку еталонних. Вводимо пароль та логін користувача Andrii. Результат проведеної автентифікації зображений на рисунку 4.7.

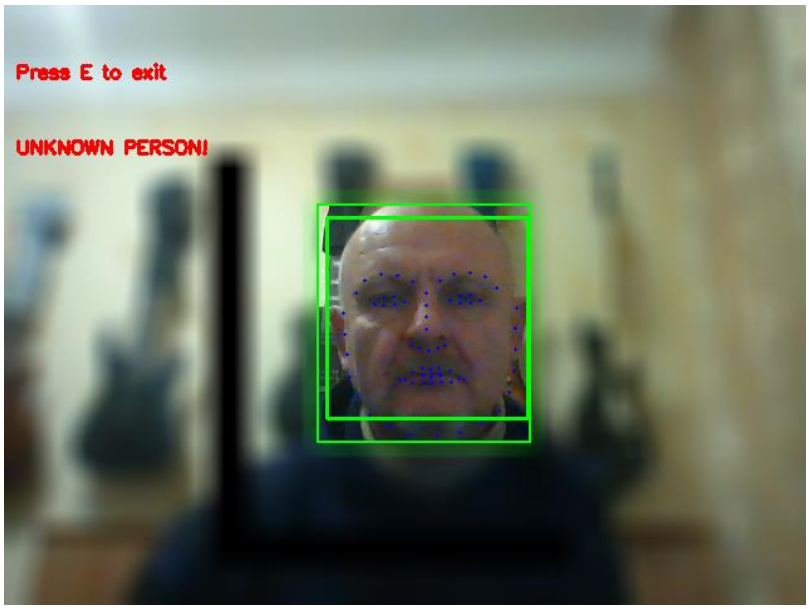

Рис. 4.7. Автентифікації невідомої особи

Тепер перевіримо реакцію програми, у випадку, якщо у зелену зону не попало лице. Результат автентифікації зображений на рисунку 4.8.

Рис. 4.8. Автентифікація без лиця

1.3. Порівняння із алгоритмом без попередньої обробки

Для представлення важливості етапу попередньої обробки фотографії слід порівняти даний алгоритм із аналогічним, але без попередньої обробки. Тобто після фіксації кадру одразу буде починатися процес пошуку лиця каскадом Хаара. Спочатку проведемо розпізнавання користувача Andrii у звичайному середовищі. Результат розпізнавання зображений на рисунку 4.9.

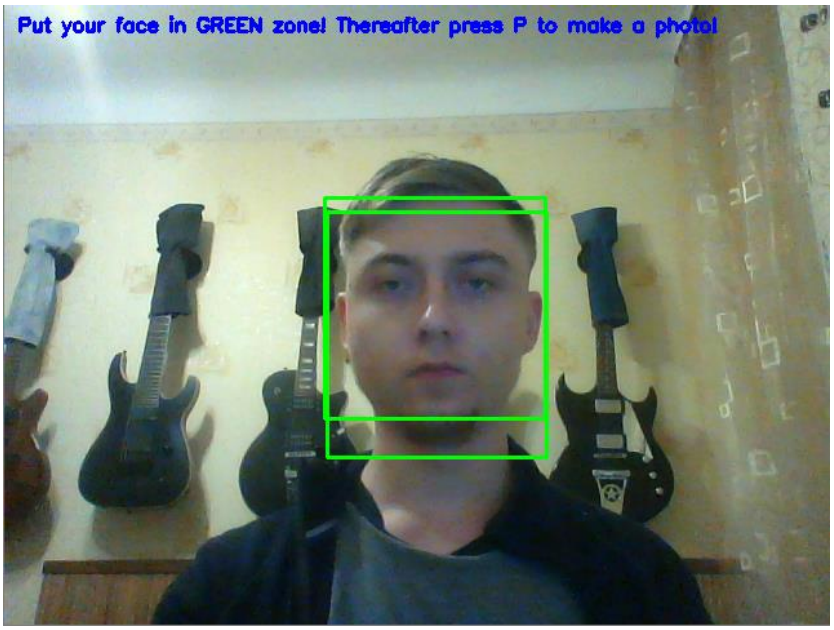

Рис. 4.9. Розпізнавання без попередньої обробки

Розпізнавання пройшло успішно не зважаючи на те, що етап попередньої обробки не проходив. Тепер додамо у навколишнє середовище об’єкти, що схожі на людське лице та проведемо розпізнавання знову. Результат зображений на рисунку 4.10.

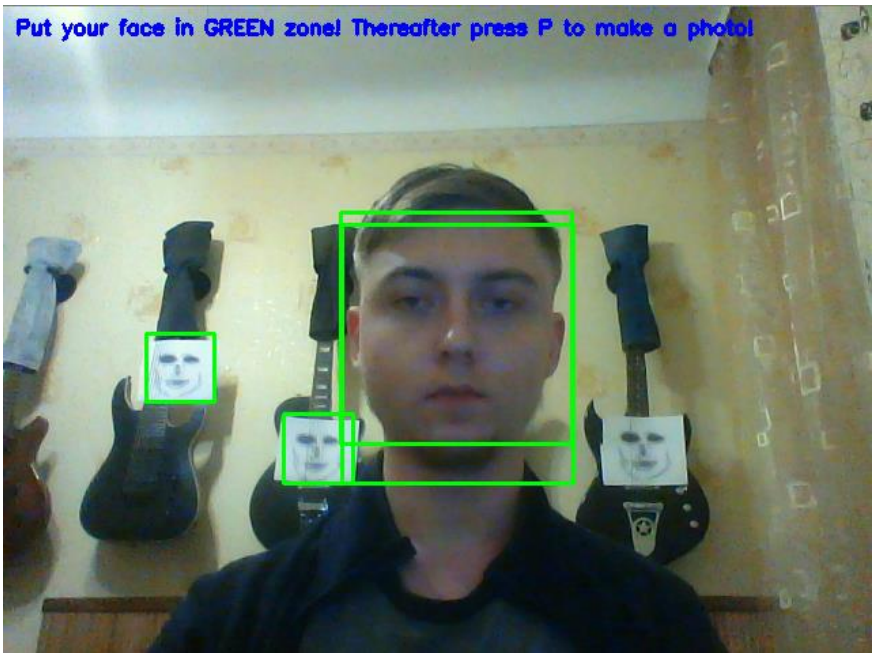

Рис. 4.10. Результат розпізнавання без обробки із сторонніми об’єктами

Розмістивши у середовищі об’єкти, що дуже схожі на лице людини своєю формою, ми у результаті отримали 3 області, на яких на думку системи розташоване лице людини. При порівнянні дескрипторів можуть виникнути проблеми із винесенням правильного висновку, оскільки лиць знаходиться кілька на зображенні. Тепер проведемо спробу розпізнавання обличчя із таким самим середовищем, але у системі із попередньою обробкою. Результат зображений на рисунку 4.11.

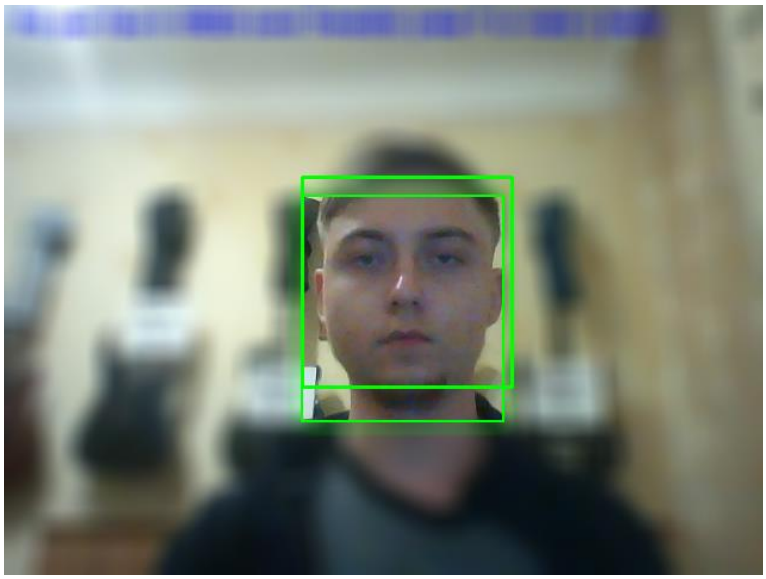

Рис. 4.11. Результат розпізнавання з обробкою зі сторонніми об’єктами

Отже можна зробити висновок, що розмиття середовища дійсно впливає на якість розпізнавання.

1.4. Оцінка ефективності системи

Для оцінки ефективності системи біометричної автентифікації користувача комп’ютерної системи слід розрахувати наступні показники:

- Помилка першого роду, що являється імовірністю виникнення ситуації при якій була відхилена правильна гіпотеза;
- Помилка другого роду, що являється імовірністю виникнення ситуації при якій була прийнята неправильна гіпотеза;
- Середній відсоток помилки, що визначає точність системи.

Для знаходження середнього відсотку помилки потрібно спочатку побудувати графіки на одному полотні залежності ППР та ПДР від порогу відстані Евкліда. Значення середнього відсотку помилки буде мати таке ж значення як і ППР та ПДР у місці свого перетину.

Визначення ПДР проводиться по наступному алгоритму на основі результатів 100 запусків програми:

- Обчислюються дескриптори для кожного із еталонних лиць даної особи в системі;
- Обчислення дескриптору для розпізнаного лиця;
- Обчислення відстаней Евкліда для кожної пари дескрипторів;
- Обчислення середньої відстані Евкліда (сума всіх знайдених відстаней Евкліда поділена на кількість еталонних зразків);

- Якщо обчислена середня відстань Евкліда більше за поріг, то дане значення вважається помилковим;
- Значення відношення кількості помилок до загальної кількості спроб є значенням ПДР.

Результат обчислення ПДР зображені у таблиці 4.1.

Таблиця 4.1

Значення порогу	Значення ПДР для порогу
0,01	100
0,02	100
…	…
0,35	98
0,36	97
0,37	95
0,38	93
0,39	88
0,40	84
0,41	79
0,42	73
0,43	66
0,44	56
0,45	48
0,46	41
0,47	34
0,48	26
0,49	19
0,50	15
0,51	14
0,52	11

Значення кроку	Значення ПДР для кроку
0,53	8
0,54	6
0,55	5
0,56	4
0,57	2
0,58	1
0,59	1
0,60	1
…	…
0,99	0
1,00	0

Наступним кроком є визначення значень ППР для кожного порогу. Їх визначення проходить за наступним алгоритмом для 100 запусків програми:

- Обчислюються дескриптори для кожного із еталонних лиць сторонніх осіб в системі;
- Обчислення дескриптору для розпізнаного лиця;
- Обчислення відстаней Евкліда для кожної пари дескрипторів;
- Обчислення середньої відстані Евкліда (сума всіх знайдених відстаней Евкліда поділена на кількість еталонних зразків);
- Якщо обчислена середня відстань Евкліда менша за поріг, то дане значення вважається помилковим;
- Значення відношення кількості помилок до загальної кількості спроб є значенням ППР.

Результати обчислення ППР зображені у таблиці 4.2.

Таблиця 4.2

Значення порогу	Значення ППР для порогу
0,01	0
0,02	0
…	…
0,57	1
0,58	2
0,59	2
0,60	3
0,61	5
0,62	7
0,63	13
0,64	17
0,65	25
0,66	33
0,67	39
0,68	45
0,69	50
0,70	57
0,71	66
0,72	71
0,73	76
0,74	82
0,75	87
0,76	90
0,77	92
0,78	95
0,79	97
0,80	99
…	…

Значення порогу	Значення ППР для порогу
0,99	100
1	100

Побудуємо графік із отриманих значень. Результат зображений на рисунку 4.12.

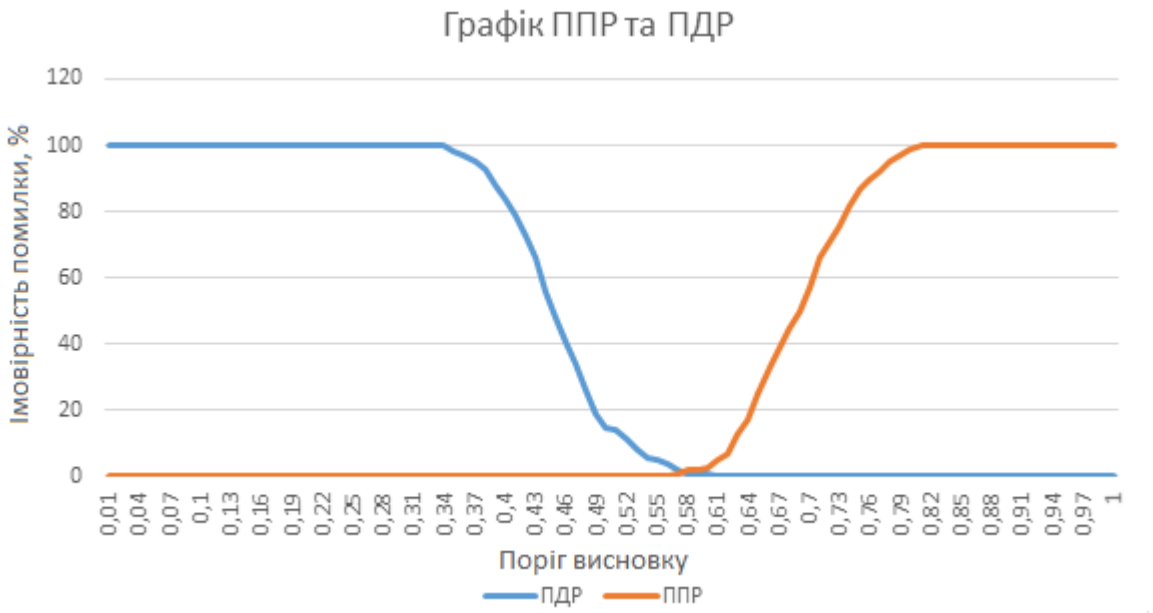

Рис. 4.12. Графік ППР та ПДР

Оскільки зона, яка потрібна для визначення ППР, ПДР та середньої помилки є надто дрібною при виведенні всіх даних одночасно, доцільно виділити лише зону, де відбувається перехрещення ППР та ПДР. Результат зображений на рисунку 4.13.

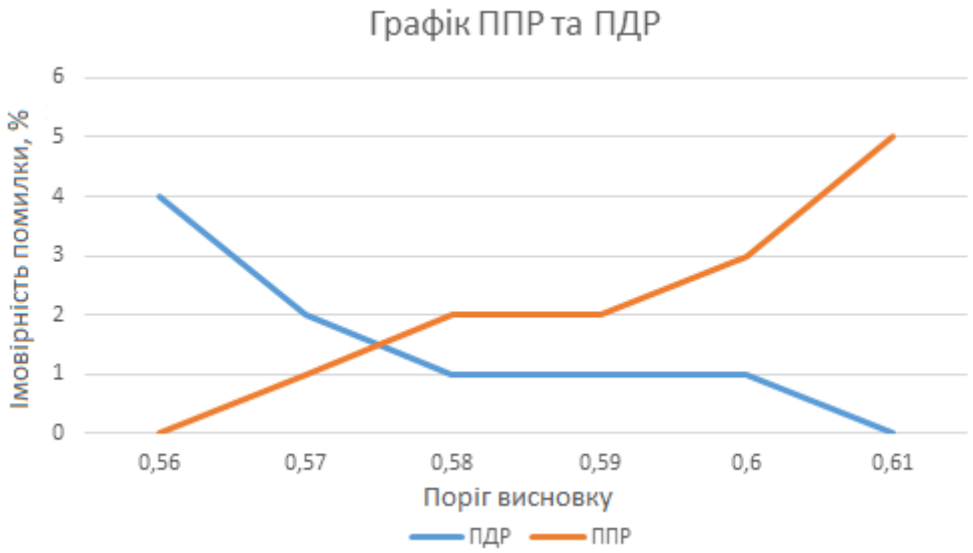

Рис. 4.13. Перехрестя ПДР та ППР

Як видно із отриманого графіку, середній відсоток помилки є 1,5%, та має поріг 0,575. Оскільки у даній точці перетинаються ППР та ПДР. Зобразимо даний висновок на рисунку 4.14.

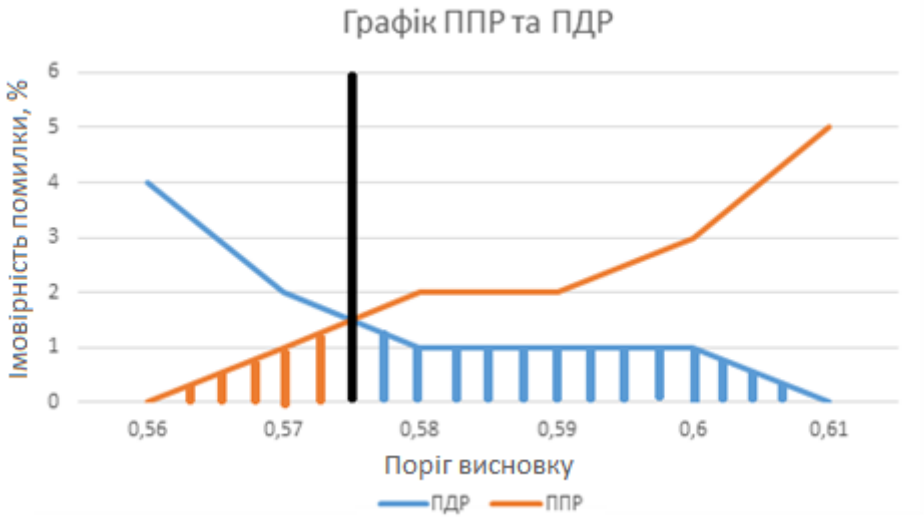

Рис. 4.14. Виділення зон ПДР та ППР для середньої помилки

Також слід розрахувати ПДР та ППР для порогу створеної системи біометричної автентифікації. Даний поріг має значення 0,6, оскільки саме на це значення опирається система при розпізнаванні лиця. У даному порозі значення ППР є 1%, а значенням ПДР є 3%. Аналогічно середній помилці зобразимо виділені зони ПДР та ППР для системи на рисунку 4.15.

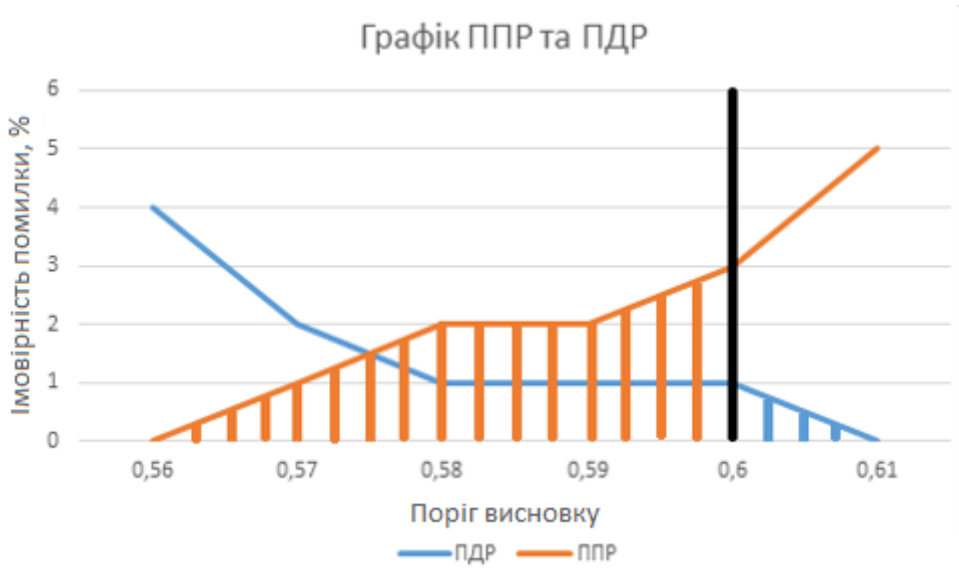

Рис. 4.15. Виділення зон ППР та ПДР для системи

Отримані результати, а саме ППР рівна 1%, а ПДР рівна 3% є повністю задовільними для системи біометричної автентифікації за допомогою методу розпізнавання по геометрії лиця. Також дана система є чутливою до зміни освітлення, оскільки розпізнавання проводиться за допомогою каскаду Хаара, та зміни ракурсу зйомки, оскільки при відхиленні обличчя значення ХТ будуть різними, що може призвести до некоректної обробки даних.

1.5. Висновки до розділу

У даному розділі роботи було проаналізована розроблена програмна реалізація системи біометричної автентифікації користувачів комп’ютерної системи, продемонстрований приклад її роботи. А саме приклад успішної автентифікації, автентифікації із неправильно введеними особистими даними,

автентифікація лиця, що не відповідає еталонним, та автентифікація без пред’явлення лиця.

Було проведено порівняння створеної системи, яка містить етап попередньої обробки зображення перед початком розпізнавання особистості, та системи, що не містить даний етап у алгоритмі роботи. Було практично доведено необхідність використання даного етапу у системі біометричної автентифікації, опираючись на результати практичного експерименту із доповненням навколишнього середовища сторонніми об’єктами, що схожу на людське лице. Результатом експерименту стало те, що система із етапом обробки успішно ідентифікувала обличчя користувача на зображенні, а система без обробки окрім користувача прийняла до процесу розпізнавання сторонні об’єкти із навколишнього середовища.

Було оцінено ефективність роботи системи за допомогою визначення помилки першого роду та помилки другого роду для порогу оцінки системи. Помилка першого роду становить 3% та помилка другого роду становить 1% для системи, у якій зареєстровано 5 користувачів. Дані значення помилок є задовільними для системи біометричної автентифікації, побудованої на базі розпізнавання за геометрією обличчя.

ВИСНОВКИ

У процесі виконання роботи були отримані наступні результати:

1. Проведено аналіз принципів реалізації біометричної автентифікації. Проведено класифікацію біометричних методів автентифікації та наведені приклади найпоширеніших систем, на їх основі. Проведено порівняльний аналіз найпоширеніших статистичних методів біометричної автентифікації та виявлено їх недоліки, що дало основу для подальших досліджень в даній області. На основі проведеного аналізу методів розпізнавання обличчя, визначення їх характеристик та подальшого їх порівняння було визначено найбільш підходящий метод для використання його у розробці системи біометричної автентифікації користувачів комп'ютерної системи.

2. Розроблено технологію попередньої обробки зразків для забезпечення підвищеної стійкості до умов виконання процесу автентифікації, що обробляє зображення поза обмеженою зоною таким чином, щоб воно було нерозбірливим і з нього неможливо було зняти ніяких показників у процесі розпізнавання, що дозволяє уникнути недоліків системи розпізнавання.

3. Було створено систему біометричної автентифікації користувачів комп'ютерної системи, алгоритм виконання якої поділений на 4 етапи: отримання даних від користувача, попередня обробка зразків, розпізнавання лиця та його характеристик, порівняння отриманих характеристик із еталонними. Було проведено тестування створеної системи автентифікації користувачів комп'ютерної системи. Оцінено ефективність роботи системи та визначені відсотки ППР та ПДР, що становлять 3% для ППР та 1% для ПДР.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Закон України «Про інформацію» № 2657-XII від 02.10.1992: зі змінами внесеними згідно із Законом України № 692-IX від 16.06.2020

2. Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» № 5067-VI від 05.07.2012: зі змінами внесеними згідно із Законом України № 720-IX від 17.06.2020

3. Закон України «Про електронні довірчі послуги» № 2155-VIII від 14.01.2020: зі змінами внесеними згідно із Законом України № 440-IX від 13.02.2020

4. Vysotska O. Authentication of information systems users, based on the analysis of their handwriting / O.Vysotska, A.Davydenko // Scientific and Practical Cyber Security Journal (SPCSJ). 2018. – V.2. No 4. – 51-63. URL: https://journal.scsa.ge/wp-content/uploads/2018/12/2.4_04_dec_18.pdf

5. Vysotska Olena. The usage of handwriting recognition systems of information systems users for their authentication / Vysotska Olena, Davydenko Anatolii // La science et la technologie à l'ère de la société de l'information: coll. de papiers scientifiques «ΛΌΓΟΣ» avec des matériaux de la conf. scientifique et pratique internationale, Bordeaux, 3 mars, 2019. Bordeaux : OP «Plateforme scientifique européenne», 2019. – Vol. 9. – P. 48-51.

6. Корченко О. Метод автентифікації користувачів інформаційних систем за їх рукописним почерком з багатокроковою корекцією первинних даних / О. Корченко, А. Давиденко, О. Висоцька // Захист інформації. 2019. – Том 21, №1. – С. 40-51. DOI: 10.18372/2410-7840.21.13546

7. Гудков В. Ю. Ідентифікація відбитків пальців по типу контрольних точок/ Гудков В. Ю.// Південно-Уральський національний університет (2019)

8. Зенович В. М. Ідентифікація особистості по радужній оболонці ока/ Зенович В. М., Хлус А. М.// 126-128 (2019)

9. Каркищенко А. Н. Статистичне розпізнавання лиць по геометрії характерних точок для системи транспортної безпеки/ Каркищенко А. Н., Гречухін І. А.// Інформаційні технології в управлінні, №38, 65-77 (2012)

10. Небаба С. Г. Алгоритм побудови деформованих 3D моделей лиця і обґрунтування його застосування в системах розпізнавання особистості/ Небаба С. Г., Захарова А. А.// SPIRAS Proceedings, №3, 157-179 (2017)

11. Шаріпов Р. Р. Методи аналізу клавіатурного почерку користувачі в використанням еталонних гауссовських сигналів/ Шаріпов Р. Р., Катасьов А. Р., Кірпічников А. П.// Вісник технологічного університету, №13, 157-160 (2016)

12. Висоцька О.О. Моніторинг роботи користувачів комп'ютерних систем за допомогою технологій розпізнавання за клавіатурним почерком / О.О. Висоцька// Моделювання та інформаційні технології. Збірник наукових праць інституту проблем моделювання в енергетиці ім. Г.Є. Пухова НАН України. – К.:ІПМЕ, 2018. – Вип. 84. - С. 119-125.

13. Заковряшин А. С. Застосування розподілень низько-частотних кепстральних коефіцієнтів для голосової ідентифікації особистості/ Заковряшин А. С., Малинін П. В., Лепендін А. А.// Відомості Алтайського національного університету, 156-160 (2014)

14. Калуцький І. В. Аналіз сучасних статистичних методів біометричної ідентифікації/ Калуцький І. В., Матюшин Ю. С., Спевакова С. В.// Відомості Південно-Західного національного університету, 84-94 (2019)

15. Біометрична ідентифікація [Електронний ресурс] / Techportal: Галузевий медіаканал. Режим доступу: World wide web. URL: http://www.techportal.ru/glossary/biometricheskaya_identifikaciya.html (Переглянуто 05 грудня 2020)

16. Ajax Systems [Електронний ресурс] / Ajax Systems CH: Офіційний сайт. Режим доступу: World wide web. URL: https://ajax.systems/ua/about/ (Переглянуто 05 грудня 2020)

17. Advanced Technologies In Security [Електронний ресурс] / ATIS: Офіційний сайт. Режим доступу: World wide web. URL: https://atis-security.com/ (Переглянуто 05 грудня 2020)

18. Dahua Tecnology [Електронний ресурс] / Dahua Tecnology: Офіційний сайт. Режим доступу: World wide web. URL: https://dahua-technology.com.ua/ (Переглянуто 05 грудня 2020)

19. EZVIZ [Електронний ресурс] / EZVIZ.IN.UA: Офіційний сайт. Режим доступу: World wide web. URL: https://ezviz.in.ua/about (Переглянуто 05 грудня 2020)

20. Використання каскаду Хаара для порівняння зображень [Електронний ресурс] / А. Мальцев – Електрон. дан. – Хабр, 2013. – Режим доступу: World wide web. URL: https://habr.com/ru/post/198338/ (Переглянуто 05 грудня 2020)

21. Недоля Д. Розпізнавання обличь як частина теорії розпізнавання образів/ Недоля Д., Гречко Є.// Молода наука 2016, №4, 285-287 (2016)

22. Потапкін К. О. Штучні нейронні мережі. Нейронна мережа Хопфілда/ Потапкін К. О.// XLVI ОГАРЁВСКИЕ ЧТЕНИЯ, 315-320 (2018)

23. Python [Електронний ресурс] / Python Software: Офіційний сайт. Режим доступу: World wide web. URL: https://www.python.org/about/ (Переглянуто 05 грудня 2020)

24. PyCharm [Електронний ресурс] / JetBrains s.r.o.: Офіційний сайт. Режим доступу: World wide web. URL: https://www.jetbrains.com/ru-ru/pycharm/ (Переглянуто 05 грудня 2020)

25. OpenCV [Електронний ресурс] / OpenCV Team: Офіційний сайт. Режим доступу: World wide web. URL: https://opencv.org/about/ (Переглянуто 05 грудня 2020)

26. Dlib [Електронний ресурс] / Dlib C++ Library: Офіційний сайт. Режим доступу: World wide web. URL: http://dlib.net/ (Переглянуто 05 грудня 2020)

27. Навчання OpenCV каскаду Хаара [Електронний ресурс] / А. Мальцев – Електрон. дан. – Хабр, 2014. – Режим доступу: World wide web. URL: https://habr.com/ru/post/208092/ (Переглянуто 05 грудня 2020)

28. Огляд дескрипторів зображення Local Binary Pattern (LBP) та їх варіації [Електронний ресурс] / П. Садовников – Електрон. дан. – Хабр, 2016. – Режим доступу: World wide web. URL: https://habr.com/ru/post/280888/ (Переглянуто 05 грудня 2020)

29. Numpy v1.19 Manual [Електронний ресурс] / The SciPy Comunity: Офіційний сайт. Режим доступу: World wide web. URL: https://numpy.org/doc/stable/ (Переглянуто 05 грудня 2020)