Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Електронної та біомедичної інженерії
(повна назва)

Кафедра Фізичних основ електронної техніки
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти другий (магістерський)

ОПТОІНФОРМАЦІЙНІ БІОМЕТРИЧНІ ТЕХНОЛОГІЇ
(тема)

Виконав:
студент 2 курсу, групи ЛОЕТм-22-1
Новіков І.В.
(прізвище, ініціали)

Спеціальність 152 Метрологія та інформаційно- вимірювальна техніка
(код і повна назва спеціальності)

Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)

Освітня програма «Лазерна і оптоелектронна техніка»
(повна назва освітньої програми)

Керівник проф. каф. ФОЕТ Курський Ю.С.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Гнатенко О.С,
(підпис) (прізвище, ініціали)

2024 р.

Харківський національний університет радіоелектроніки

Факультет Електронної та біомедичної інженерії
(повна назва)
Кафедра Фізичних основ електронної техніки
(повна назва)
Рівень вищої освіти другий (магістерський)
Спеціальність 152 Метрологія та інформаційно-вимірювальна техніка
(код і повна назва)
Тип програми освітньо-професійна
(освітньо-професійна або освітньо-наукова)
Освітня програма «Лазерна і оптоелектронна техніка»
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри
_____
(підпис)
«_____»_____ 20 ___ р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студенту Новікову Іллі Валерійовичу
(прізвище, ім'я, по батькові)
1. Тема роботи Оптоінформаційні біометричні технології
затверджена наказом університету від « 03 » листопада 2023 р. № 1284 Ст
2. Термін подання студентом роботи до екзаменаційної комісії 22 січня 2024 р.
3. Вихідні дані до роботи Біометрія; розпізнавання образів; гармонічний сигнал; спотворений сигнал; програмний пакет «Scilab»; перетворення Фур'є.
4. Перелік питань, що потрібно опрацювати в роботі
1 Дослідження основних завдань біометрії. 2 Дослідження оптичних методів систем розпізнавання людини. 3 Дослідження математичних методів систем. 4 Дослідження труднощів із забезпеченням розпізнавання людини.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій
Демонстраційний матеріал – 14 слайдів.

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Інформаційно-тематичний пошук та огляд літературних джерел про основні завдання біометрії	01.09.23–28.09.23	Виконано
2	Дослідження математичних методів систем розпізнавання	04.10.23–22.10.23	Виконано
3	Виконання перетворення Фур'є гармонічного та спотвореного сигналу	25.10.23–10.11.23	Виконано
4	Аналіз резрахунків та труднощів із забезпечення розпізнавання образів	16.11.23–02.12.23	Виконано
5	Оформлення пояснювальної записки	04.12.23–24.12.23	Виконано
6	Оформлення графічних та демонстраційних матеріалів	27.12.24–10.01.24	Виконано
7	Проходження нормоконтролю і отримання рецензії	12.01.24–18.01.24	Виконано
8	Проходження перевірки на плагіат	19.01.24–20.01.24	Виконано
9	Підготовка та захист кваліфікаційної роботи	21.01.24–23.01.24	

Дата видачі завдання 01 вересня 2023 р.

Студент _____
(підпис)

Керівник роботи _____ проф. каф. ФОЕТ Курський Ю.С.
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка кваліфікаційної роботи: 40 с., 13 рис., 1 додаток, 14 джерел.

ДІЕЛЕКТРИЧНИЙ ХВИЛЕВІД, ДИФРАКЦІЙНЕ ВИПРОМІНЮВАННЯ, ПОДВІЙНА РЕШІТКА, ДІЕЛЕКТРИЧНА ПРОНИКНІСТЬ, ПАКЕТ COMSOL MULTIPHYSICS.

Об’єкт дослідження – біометричні системи розпізнавання образів.

Мета – роботи дослідження принципів функціонування та застосування оптоінформаційних біометричних технологій систем ідентифікації образів.

Метод дослідження – аналітичний та чисельний за допомогою програмного пакету Scilab.

У роботі було розглянуто системи розпізнавання образів, їх алгоритм роботи, різні методи розпізнавання образів, загальні труднощі які можуть впливати на розпізнавання системи та проаналізовано реалізацію фур'є аналізу при розпізнаванні образів.

Розрахований та порівняняний гармонічний сигнал зі зміною деяких параметрів та величини.

ABSTRACT

Explanatory note of the attestation work: 40 pp, 13 fig, 1 application, 14 sources.

BIOMETRY, CORRELATOR, LASER SCANNING, PATTERN RECOGNITION, VANDERLUGHT FILTER, FOURIER TRANSFORM.

The object of research is biometric systems of pattern recognition.

The purpose of the work is to study the principles of operation and application of opto-informational biometric technologies of the image identification system.

The research method is analytical and numerical using the Scilab software package.

The paper considered pattern recognition systems, their work algorithm, different methods of pattern recognition, general difficulties that can affect system recognition, and analyzed the implementation of Fourier analysis in pattern recognition.

Calculated and compared harmonic signal with changes in some parameters and values.

ЗМІСТ

Вступ 7
1 Біометрія 8
1.1 Визначення біометрії 9
1.2 Історія біометрі 11
1.3 Типи біометричних ознак 12
1.4 Виклики та перспективи 13
2 Оптоінформаційна реалізація біометричних технологій 14
2.1 Методи оптоінформатики 14
2.2 Техніки сканування обличчя та їх застосування в біометричних дослідженнях 15
2.3 Активні та пасивні підходи до сканування обличчя в системах біометрії 19
3 Застосування перетворення Фур’є в оптоінформаційних технологіях 25
3.1 Використання аналізу Фур'є для розпізнавання зображень 25
3.2 Процес фільтрації згідно з методологією Вандерлюгта 29
3.3 Аналіз переваг та недоліків сканування обличчя 36
Висновки 38
Перелік джерел посилання 39
Додаток А Демонстраційний матеріал 41

ВСТУП

В сучасному світі широко використовують паролі для різноманітних задач автоматичного контролю, управління та вимірювань. Проте, останнім часом їх популярність зменшується через можливість легко втратити або забути. У цьому контексті, розпізнавання обличчя набуває все більшої актуальності, зокрема для забезпечення безпеки, верифікації особи та онлайн спілкування. Хоча розроблено різні системи для виявлення та відстеження облич, надійне розпізнавання залишається складною задачею для вчених у галузі комп'ютерного зору та розпізнавання образів.

Останнім часом спостерігається зростаючий інтерес до розпізнавання обличчя, що пояснюється збільшеною тривожністю суспільства стосовно безпеки, необхідністю перевірки особистості в цифровому просторі та потребою в аналізі обличчя та методах моделювання в управлінні мультимедійними даними та розвагами.

Розпізнавання обличчя розглядається як перспективний напрямок майбутнього розвитку, з численними потенційними перевагами, такими як ненав'язливість, низькі витрати на обладнання та відсутність необхідності отримання згоди користувача під час збору даних. У цьому контексті пропонується перспективний підхід, використовуючи Фур'є-перетворення для досягнення ефективного розпізнавання обличчя.

Об’єкт дослідження – біометричні технології ідентифікації людини.

Мета роботи – аналіз принципів функціонування та застосування оптоінформаційних біометричних технологій систем ідентифікації обличчя.

Мета нашого дослідження включає розгляд:

а) основних завдань біометрії;

б) оптичних методів у системах розпізнавання;

в) математичних методів у таких системах.

1 БІОМЕТРІЯ

1.1 Визначення біометрії

Біометрія – це наукова галузь, яка аналізує унікальні фізичні та поведінкові особливості людини для її точної ідентифікації та перевірки. Ця дисципліна об'єднує методи з різних галузей знань, таких як біологія, математика, соціологія та інженерія. В сучасному світі біометричні технології широко використовуються в системах безпеки, електронній комерції, медицині та інших сферах для підвищення ефективності і точності ідентифікації особи [1].

Визначення біометрії в контексті наукових досліджень відноситься до дисципліни, яка вивчає фізичні та поведінкові характеристики живих організмів для їхнього ідентифікації або верифікації. Основна ідея полягає в використанні унікальних параметрів, таких як відбитки пальців, розпізнавання обличчя, голосовий та інші біометричні ознаки, для встановлення особистості.

Біометрія стала ключовим напрямком в сучасних технологіях індивідуальної ідентифікації через свою ефективність та надійність. Застосування біометричних технологій включає безпекові системи, інформаційні технології, медицину та інші галузі.

Наукове вивчення біометрії широко охоплює аналіз основних завдань, які є актуальними для цієї галузі. Воно розглядає оптичні та математичні методи в системах розпізнавання, а також вирішує проблеми та труднощі, пов'язані з ефективністю процесу розпізнавання особи. Ця область постійно розвивається, використовуючи нові технології та наукові досягнення для поліпшення якості і точності біометричних систем.

Основні принципи біометрії базуються на концепції використання унікальних біологічних параметрів для встановлення особистої ідентичності. Це охоплює різноманітні фізіологічні ознаки, такі як відбитки пальців,

розпізнавання обличчя, слід очей, або поведінкові характеристики, наприклад, голосовий аналіз чи динаміка набору тексту.

Застосування біометрії розповсюджене в різних галузях, таких як безпека, інформаційні технології, медицина та фінанси. В сучасному суспільстві біометричні технології активно використовуються для підвищення рівня захисту та ефективності ідентифікаційних систем. Однак це також породжує важливі питання щодо приватності та етики використання таких даних, а також технічних викликів у вдосконаленні систем біометричного розпізнавання та їхніх перспективах у майбутньому.

1.2 Історія біометрії

Біометричні системи в останнє століття пройшли значний етап еволюції завдяки досягненням в галузі обробки комп'ютерних даних. Багато з цих нововведень мають своє коріння в ідеях, які були сформовані століття тому.

У давнину на стінах печер виявлено малюнки, свідченням творчості давніх людей, що проживали понад 31 000 років тому. Ці твори мистецтва оточують відбитки рук, які, ймовірно, служили символічним "підписом" їхніх авторів.

У давньому Вавилоні та Ассирії близько трьох тисяч років тому жителі вже знали, що кожен має унікальний відбиток пальця, що свідчить про їхнє розуміння дактилоскопії. В Китаї, за дослідженнями Жо де Барроса, біометрію використовували ще у XIV столітті, а першою формою біометричної ідентифікації вважається встановлення особистості за відбитками пальців.

Китайські купці використовували відбитки пальців для підпису торгових угод, а також для відрізняння дітей. Для цього вони макали пальці та долоні в чорнило. Завершальний образ біометрії сформувався в XIX

столітті. Теоретиками біометрії вважають Френсіса Гальтона, Карла Пірсона та Рональда Фішера.

В 1890-х роках Альфонс Бертильйон ввів техніку вимірювання параметрів тіла, що отримала назву "бертильонаж". Проте ефективність цього методу стала відчутною, коли виявилося, що різні люди можуть мати однакові параметри. Першим, хто врахував відбитки пальців у криміналістиці, був доктор Генрі Фолдс. У 1880 році він опублікував статтю, де висловив свої ідеї щодо унікальності відбитків пальців.

Однак остаточно біометрія сформувалася завдяки роботі Френсіса Гальтона, який у 1889 році вжив вираз "біометрія" в своїй роботі про природну наслідуваність. У 1938 році було створено Біометричний відділ Американської статистичної асоціації, а в 1947 році відбулася перша міжнародна біометрична конференція. З того часу біометрія продовжує розвиватися та знаходить застосування в різних галузях науки і технологій [1].

До вересня 2001 року біометричні системи переважно використовувались для забезпечення безпеки у військових секторах і рідше для важливої комерційної інформації. Проте після терактів у США 11 вересня 2001 року вони стали ширше використовуватись, зокрема в аеропортах, торгових центрах та інших місцях масового збору людей.

Завдяки розвитку високих технологій біометрія стала широко використовуватися у багатьох галузях. Аутентифікація, ідентифікація, удостоверення особистості, оплата покупок, пошук злочинців і зниклих – це лише частина завдань, які мають вирішувати біометричні методи.

Найпоширеніші методи біометрії на сьогодні – відбиток пальця, райдужка ока, зображення обличчя, венозний малюнок пальців і долоні, а також голос. Технології біометричної ідентифікації діляться на динамічні та статистичні. Перші базуються на поведінкових характеристиках людини, таких як розпізнавання по почерку, голосу і т.д. Другі ґрунтуються на фізіологічних характеристиках, таких як відбиток пальця, райдужка ока, ДНК тощо.

Біометричні методи поділяються на автоматизовані та ручні. Основними інструментами автоматизованого методу є алгоритм порівняння біометричного шаблону і сканер для вимірювання характеристик. У ручному методі, наприклад, при дактилоскопії, відбиток пальця фіксується безпосередньо на носії, і цей спосіб документується біометричним.

Сучасні тенденції в розвитку біометрії включають використання пристроїв як біометричних токенів доступу, мультимодальність, біометричні сенсорні карти, використання в сфері фінансів та здравоохоронення. Очікується, що до 2024 року світовий ринок біометрії перевищить 50 мільярдів доларів США. Загальна мета таких інновацій - спрощення життя.

1.3 Типи біометричних ознак

Біометричні ознаки поділяються на різні типи, враховуючи різноманітні фізіологічні та поведінкові характеристики. Біометричні ознаки включають 8 основних типів [2].

1. Відбиток пальця: Заснований на унікальних рисах папілярних ліній та випинань на пальцях.
2. Райдужка та сітківка ока: основані на унікальних характеристиках внутрішніх структур ока, таких як райдужка та сітківка.
3. Зображення обличчя: використовує унікальні риси обличчя для ідентифікації особи.
4. Венозний малюнок пальців та долоні: заснований на унікальних венозних структурах у пальцях та долонях.
5. Голосові характеристики: використовують унікальні особливості голосу для ідентифікації особи.
6. Геометрія руки та пальців: заснована на розмірах та формі руки та пальців.
7. Динамічні характеристики: включають рухові характеристики, такі як ходьба або почерк, для ідентифікації особи.

8. Генетичні характеристики (ДНК): використовують генетичні відмінності для ідентифікації особи.

Ці типи біометричних ознак можуть використовуватися окремо або в комбінації (мультимодальність) для підвищення точності ідентифікації. Кожен тип має свої переваги та обмеження, і вибір конкретного типу залежить від конкретних вимог та контексту застосування.

1.4 Виклики та перспективи

У світі, де технологічний прогрес невпинно крокує вперед, біометрія стає ключовим елементом сучасного суспільства, проте вона також породжує низку питань і обговорень з точки зору соціології. Загальне використання біометричних технологій впливає на соціальні відносини та викликає рефлексії стосовно приватності, етики та культурних відмінностей.

Проблеми конфіденційності та приватності стають актуальними в умовах загального спостереження за громадянами. Використання камер спостереження, біометричних сканерів та голосових асистентів піднімає питання щодо можливості втрати особистої приватності в умовах технологічного просунутку. Це спонукає до обговорення ефективної захисту особистих даних та узгодження зручності та приватності в сучасному суспільстві.

Культурні наслідки використання біометрії також потребують уваги соціологів. Різні культури реагують на ці технології по-різному, відзначаючи їх як прояв прогресу чи загрозу традиційним цінностям. Важливо розуміти, як використання біометрії впливає на соціокультурні особливості кожного суспільства.

Пошук рівноваги між зручністю та ризиками є необхідним завданням. Сучасне суспільство стоїть перед завданням знайти баланс між прагненням до зручності, яку принесли біометричні технології, та свідомим ставленням до ризиків, які вони можуть представляти для особистої приватності.

Біометричні технології стають не лише інструментами технологічного світу, але і важливим аспектом взаємодії людини та суспільства, вимагаючи глибокого аналізу соціальних наслідків.

Біометрія, як наука і технологія, пережила дивовижний ріст за останні роки і відкрила нові можливості для суспільства. Очікується, що майбутнє розвитку цієї галузі принесе ряд нових тенденцій та переваг:

– зростання точності та надійності: постійне дослідження та розвиток алгоритмів призведуть до ще більш точних систем біометричної ідентифікації, зменшуючи кількість помилок ідентифікації;

– більша інтеграція з повсякденним життям: біометричні системи будуть все більше вплітатися у наш повсякденний досвід, від смартфонів до автомобілів, надаючи зручність та ефективність;

– отичні аспекти та стандартизація: розвиток біометрії також породжує етичні питання щодо конфіденційності особистих даних.

Стандартизація, така як та, яку веде Міжнародна організація зі стандартизації (ISO), є ключовим елементом для забезпечення етичного використання цих технологій та захисту прав людини.

Усі ці тенденції визначають майбутнє біометрії як важливої галузі, яка може вносити значний вклад у соціальний та технологічний прогрес.

2 ОПТОІНФОРМАЦІЙНА РЕАЛІЗАЦІЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ

2.1 Методи оптоінформатики

Оптоінформатика представляє собою галузь науки, яка займається вивченням застосування оптичних методів та технологій для обробки, передачі, зберігання та відображення інформації. Ця наука об'єднує в собі різноманітні методи, що можуть бути класифіковані за кількома ключовими напрямами, кожен з яких вносить свій внесок у розвиток та застосування оптичних технологій.

Перший напрям – це методи оптичної інформатики, які базуються на використанні оптичних принципів та елементів для різноманітних завдань, таких як кодування, декодування, модуляція, демодуляція, фільтрація, перетворення та візуалізація інформації. Ці методи є елементом створення нових оптичних пристроїв та систем обробки інформації.

Другий напрям – це методи оптоелектроніки, які використовують електрооптичні явища для створення пристроїв обробки, введення та виведення інформації, а також для розробки пристроїв запам'ятовування та логічних схем. Ці методи взаємодіють з електричними сигналами за допомогою оптичних засобів, що розширює можливості обробки інформації.

Третій напрям – методи лазерної інформатики, використовують лазерне випромінювання для генерації, зчитування, запису, переносу, обробки та аналізу інформації. Ці методи відкривають широкі перспективи для створення швидших та більш потужних оптичних пристроїв для обробки інформації.

Четвертий напрям – методи голографії, що базуються на принципах та техніках голографії для запису, відтворення, обробки та зберігання інформації у вигляді тривимірних зображень. Голографічні методи відкривають можливості для створення вражаючих інтерактивних візуальних

систем та забезпечують нові можливості для зберігання та відтворення об'ємних зображень.

2.2 Техніки сканування обличчя та їх застосування в біометричних дослідженнях

Біометричні системи аутентифікації визначаються як високоефективні лише у разі включення до їхнього складу криптографічних механізмів аутентифікації. Ці механізми співпрацюють з біометричними методами аутентифікації, перетворюючи нечіткі біометричні зображення в чіткий криптографічний ключ або довгий пароль (рис. 2.1).

Рисунок 2.1 – Приклад біометричної аутентифікації

Застосування таких систем звільняє користувача від потреби зберігати ключ чи пам'ятати довжину випадкового паролю, оскільки він сам стає ключем (паролем) доступу (аутентифікації) завдяки власній біометрії [3].

Наукові системи високоефективної біометрично-криптографічної аутентифікації класифікуються за допомогою біометричних механізмів або їх комбінацій, включаючи перспективні біометричні методи, такі як аналіз кровоносних судин очного дна, аналіз радужної оболонки ока, геометричний аналіз обличчя у видимому та інфрачервоному спектрах, аналіз ушних

раковин, аналіз голосу, аналіз папілярних відбитків пальців, аналіз форми ладоні, аналіз рисунка кровоносних судин, аналіз рукописного та клавіатурного почерку, аналіз геометричних співвідношень частин тіла, аналіз походки тощо [2].

Особливий погляд на методи сканування обличчя вказує на важливість виявлення живості у біометричних системах. Виявлення живості є програмним забезпеченням, яке відрізняє живу людину від спроб шахрайства, таких як фотографії, маски, аватари чи відео, і науково відоме як виявлення атак на презентації (PAD). Цей аспект стосується запобігання шахрайству в біометрії загалом, в той час як визначення живості зазвичай використовується для розпізнавання обличчя. Не вимагаючи спеціального апаратного забезпечення, виявлення живості використовує аналіз одного або двох селфі, зроблених стандартною камерою, для визначення "жвавості" особи, яка намагається ідентифікуватися [4]. Без ефективного виявлення живості можуть виникати загрози від використання фотографій, відео або масок для шахрайського доступу до системи або даних користувача. Таким чином, виявлення живості стає ключовим елементом безпечної біометричної системи.

Методи виявлення живості можуть бути класифіковані на активні та пасивні. Активне виявлення живості вимагає навмисного підтвердження присутності користувача, наприклад, шляхом взаємодії з системою (наприклад, "Я не робот"). Для активного виявлення живості використовують два зображення: перше фіксується негайно, а друге захоплюється природнім рухом голови. Цей природний рух, такий як "кивок, якщо згоден", є інтуїтивно зрозумілим для користувача [1]. Технологія активного виявлення живості базується на аналізі руху та використанні штучного інтелекту для розрізнення руху 3D-обличчя від 2D-фото.

Пасивне виявлення живості відбувається без додаткових дій від користувача. Зазвичай використовується одне зображення, яке аналізується за допомогою штучного інтелекту. Методи пасивного виявлення можуть

включати зйомку повного відеосеансу або аналіз блискавки особи для отримання додаткової інформації [5]. Процес пасивного виявлення може відбуватися в фоновому режимі, не заважаючи користувачеві та не вимагаючи його взаємодії.

Кожен з вищезазначених методів біометричної аутентифікації вносить свій унікальний біометричний образ людини. Біометричні дані поділяються на статичні (обмежена інформативність, незмінні) та динамічні (необмежена інформативність, змінюються). Статичні біометричні дані, як правило, фіксуються від народження, мають обмежену інформативність і не піддаються змінам. Для забезпечення конфіденційності статичних біометричних даних необхідно використовувати анонімізацію користувача. Динамічні біометричні дані є більш інформативними, але їх легко можна змінити. Конфіденційність динамічних біометричних даних забезпечується тим, що власник зберігає в секреті голосові фрази, рукописні слова, текстові паролі клавіатури і т.д. [6].

Системи високоефективної біометрично-криптографічної аутентифікації мають стандартну структуру перетворень, яка дозволяє об'єднати різноманітні методи біометричного визначення та забезпечити високий рівень безпеки (рис. 2.2).

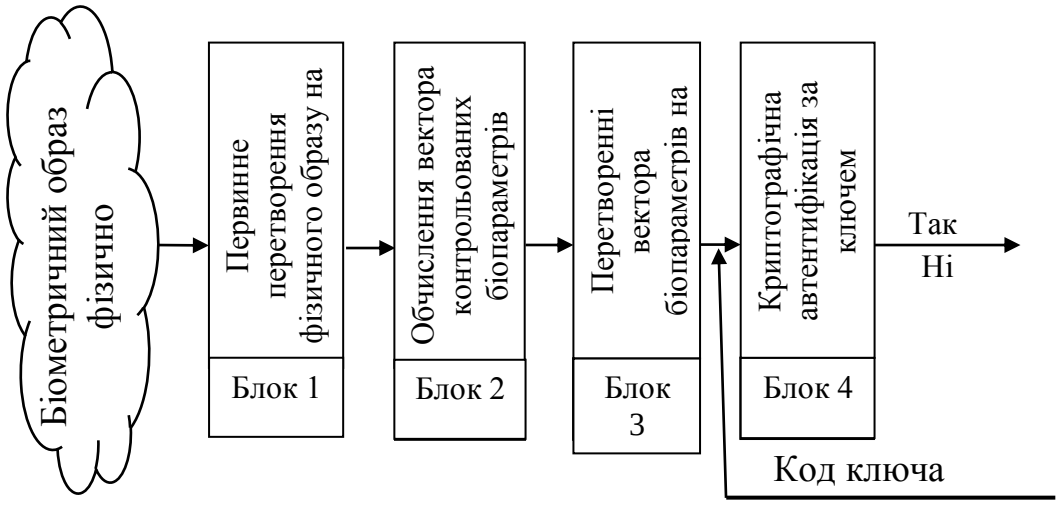

Рисунок 2.2 – Організаційна структура обробки інформації у високонадійних засобах біометричної аутентифікації

У цій структурі блок 1 здійснює перетворення фізичного нечіткого біометричного образу людини в електронний біометричний нечіткий образ через первинні перетворювачі фізичних величин в електронні цифрові дані. Блок 2 нормує електронні образи та обчислює вектор біометричних параметрів (наприклад, у вигляді коефіцієнтів Фур'є в системах аутентифікації за динамікою відтворення рукописного пароля). Блок 3 перетворює вектор біометричних параметрів в код ключа (пароля) для подальшої криптографічної аутентифікації. Блок 4 здійснює криптографічну аутентифікацію людини за його ключем або паролем, видаючи на вихід рішення "Так" або "Ні" [7].

З метою підвищення стійкості біометричного захисту від атак вивчення та модифікації програмного забезпечення, високоефективні варіанти технічної реалізації не повинні містити зразки біометричних зображень користувача, біометричних еталонів зображень користувача та коду ключа (паролю) користувача. Ця інформація є конфіденційною та має бути захищена під час зберігання. Крім того, сліди цієї конфіденційної інформації повинні бути гарантовано знищені після виконання кожної конкретної процедури аутентифікації. Для засобів високоефективної біометричної аутентифікації допустимо приховування конфіденційної інформації про код ключа (пароль) користувача та його біометричні зображення в таблицях параметрів та зв'язків нейромережевого перетворювача біометричних параметрів у ключ (пароль) [8].

Система високоефективної біометрично-криптографічної аутентифікації повинна видачу результат біометричної аутентифікації "Так" або "Ні", а також кількість незмінних бітів коду ключа (кількість спроб підбору та результат підбору, якщо підбір дозволений за діючою політикою інформаційної безпеки). Прилад високоефективної біометричної аутентифікації повинен надавати користувачеві можливість бачити (знати) свій ключ (пароль) та можливість його збереження (наприклад, на аварійному паперовому носії, що знаходиться в опечатаному конверті). Якщо

така можливість суперечить прийнятій безпеці, то вона повинна бути відключена адміністратором безпеки. Засіб високоефективної біометричної аутентифікації повинен мати безпечний аварійний вхід у вигляді можливості ручного введення коду ключа (пароля) на випадок, якщо користувач повністю втратив здатність відтворення свого біометричного зображення [9].

2.3 Активні та пасивні підходи до сканування обличчя в системах біометрії

Системи біометрії використовують різні підходи до сканування обличчя для забезпечення надійності та ефективності процесу ідентифікації. Активні та пасивні методи сканування представляють дві основні стратегії в цьому контексті. Активні підходи включають в себе використання спеціальних джерел світла або інших сигналів для збору інформації, тоді як пасивні методи використовують наявність природного освітлення.

Сканування активним методом. Метод активного сканування використовує тривимірний лазерний сканер, що направляє лазерний промінь на об'єкт, такий як обличчя людини. Лазерний промінь сканує поверхню об'єкта, а зображення отримується за допомогою камери із зарядовим зв'язком, яка реєструє відбите світло. Тривимірні дані формуються триангуляцією, яка надає інформацію про глибину об'єкта. Лазерні сканери мають великий діапазон захоплення, до 8 футів, що вище, ніж інші методи збору даних, які працюють на відстані від 1,6 футів до 5 футів.

На рисунку 2.3 зображено основний принцип роботи системи сканування обличчя за допомогою лазерного променя [6].

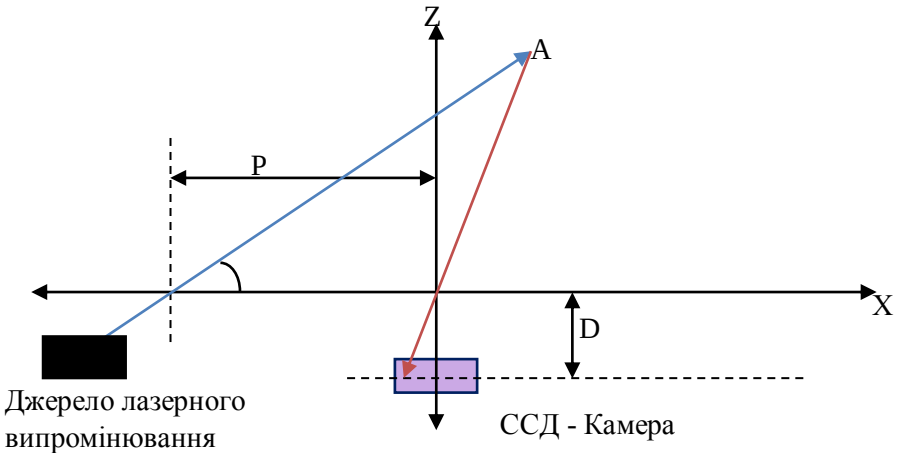

Рисунок 2.3 – Отримання глибини одноточкового лазерного променя

Оцінка глибини покладається на врахування викривлення випромінюваного лазерного світла. Лазерне джерело спрямовує лазерний промінь однієї довжини хвилі на точку A в тривимірному просторі під кутом β відносно базової лінії. Точка перетину лазерного джерела та базової лінії розташована на відстані P одиниць від початку координат. Фокусна відстань ССД-камери позначається як D. Тривимірне положення точки A, визначене координатами (X, Y, Z), виражається наступним чином:

$$X\ Y\ Z\ = \frac{P}{D\ cot(\beta - x)}(X\ Y\ Z\ ). \qquad (2.1)$$

Метод активної тріангуляції, який застосовується у даному випадку, включає в себе лазерне джерело як засіб освітлення та камеру з ПЗС-матрицею як датчик. Камера з ПЗС-матрицею налаштована на довжину хвилі лазерного світла, яке проходить через простір. Цей метод сканування лазерним променем відрізняється високою точністю за рахунок вузького фокусу лазерного джерела, надійністю освітлення завдяки використанню єдиної стандартної довжини хвилі та зменшеними потребами в електроенергії.

Однак цей метод характеризується невеликою швидкістю, оскільки вимагає поетапного сканування повної тривимірної поверхні. Пристрої, які використовують цей метод, є вартішими порівняно з іншими пристроями для тривимірного моделювання (рис. 2.4) [4].

Рисунок 2.4 – Прилад сканування активним методом (Revopoint POP2)

В цілому, система лазерного сканування була визнана найбільш ефективною з таких причин:

Швидкий та простий збір даних забезпечується лазерним сканером:

– можливість швидкої обробки даних за допомогою лазерного сканера та зменшена залежність від програмних систем;

– застосування лазерного сканера забезпечує більш точні вимірювання орієнтації точок;

– лазерний сканер полегшує спостереження за площинами, нахиленими до експонованого обличчя [1].

Сканування пасивним методом.

Сканування пасивним методом – це новаторський спосіб виявлення живості, що використовується у системах розпізнавання обличчя на основі штучного інтелекту (ШІ). Цей метод гарантує, що обличчя, яке представлене системі розпізнавання обличчя, є живим. Пасивна активність не повідомляє

користувачів про те, що вони проходять тестування, і не вимагає від них додаткових рухових завдань.

Пасивне виявлення живості відбувається в фоновому режимі, а технологія базується на алгоритмах, які ідентифікують та оцінюють частини зображення, що вказують на його вміст, такі як шкіра, контури, текстура, наявність масок або вирізів, а також будь-які додаткові індикатори того, що представлене зображення є реальним обличчям користувача. Оскільки процес не повідомляє користувача, шахраям ускладнено розуміти, як обійти цю технологію [10].

Пасивна перевірка автентичності має ряд переваг:

– швидко та легко: цей підхід ідеально підходить для приваблення нових клієнтів, особливо, якщо клієнти банку шукають швидку реєстрацію для доступу до свого облікового запису в Інтернеті або через додаток, що особливо актуально при впровадженні систем розпізнавання облич;

– без перешкод: клієнти можуть швидко завершити процес реєстрації або входу, гарантуючи відсутність труднощів та забезпечуючи високу якість взаємодії з користувачем;

– відсутність руху: немає необхідності в масштабуванні камери, поворотах голови або додаткових активних заходах, що важливо для забезпечення безпеки систем розпізнавання обличчя та уникнення можливості «підробки обличчя».

Методи Брунеллі та Поджіо розкривають систему розпізнавання обличчя, яка базується на 22 геометричних особливостях для визначення різниці між обличчями:

– товщина брів і їх вертикальне положення;
– вертикальне положення та ширина носа;
– вертикальне положення рота, його ширина і висота;
– одинадцять радіусів, що описують форму підборіддя;
– бігональна ширина (ширина щелепи);
– ширина виличної кістки (ширина обличчя поперек вилиці) [11].

Гібридна система нейронної мережі об'єднує локальну вибірку зображень, самоорганізуючу карту (СОК) та згорткову нейронну мережу. Нейронна мережа СОК використовується для зменшення розмірності та формування інваріантності до незначних змін у тестовому зображенні перед його класифікацією за допомогою згорткової нейронної мережі. Остання, у свою чергу, частково стійка до зсувів, обертань, масштабу та деформацій. Процедура вибірки локального зображення включає сканування зображення локальним вікном та створення вектора інтенсивності пікселів. Під час просування вікна по зображенню формуються вектори для побудови векторного представлення всього зображення. Кожному вузлу СОК призначається опорний вектор mi з вхідного простору, а сама СОК навчається порівнювати вектори вхідних зображень з опорними векторами вузлів у навчальному наборі.

Обирається найближчий збіг, і вузли оновлюються відповідно до наступного рівняння:

$$m_j(t+1) = m_j(t) + h_{cj}(t)\left(x(t) - m_j(t)\right), \qquad (2.2)$$

де t – ітерація навчання;

h – форма ядра згладжування, функція сусідства, в якій локальна область сусідства в СОК зменшується зі зростанням часу t [7].

Результатом є топологічно впорядкований набір вузлів в значно меншому просторі. Кожен вимір СОК є цілісною характеристикою, подібною до граней у методі аналізу головних компонент. Цей вимір можна також розглядати як зображення. Кожне зображення в навчальному наборі обробляється за допомогою СОК і подається у вигляді трьох зображень (карт функцій), які використовуються для навчання згорткової мережі з використанням алгоритму градієнтного спуску зворотнього розповсюдження. Мережа має один вихід для кожного класу у навчальному наборі (кожен

вихід ідентифікує конкретну особу) і включає кілька прихованих шарів, що з'єднані вручну вузлами.

Шляхом ручної локалізації набору орієнтирів на навчальному наборі зображень обличчя використовується метод часткових квадратів (ПСІ) для створення статистичної моделі варіації форми та текстури (2.5) [2].

Рисунок 2.5 – Пасивний сканер (Skyline F23)

Ці активні моделі зовнішнього вигляду можуть бути використані для точного передбачення орієнтації обличчя в межах п'яти градусів. Після визначення кута позиції та вибору оптимальної моделі, програмні системи автоматизованого аналізу (ПСА) та інші можуть використовувати ту ж саму модель зовнішнього вигляду для створення передбаченого обличчя під різними оглядовими кутами.

3 ЗАСТОСУВАННЯ ПЕРЕТВОРЕННЯ ФУР'Є В ОПТОІНФОРМАЦІЙНИХ ТЕХНОЛОГІЯХ

3.1 Використання аналізу Фур'є для розпізнавання зображень

Більшість методів оптичної обробки інформації (ОМОІ) використовують перетворення Фур'є чи інші інтегральні перетворення, які пов'язані з ними. Математичне перетворення Фур'є є конкретним випадком інтегрального перетворення Фредгольма з ядром у вигляді експоненти з уявним, лінійним аргументом, показником. В оптиці воно реалізується за допомогою аналогового пристрою – позитивної лінзи. Основні властивості цього перетворення можуть бути продемонстровані при розгляді пропускання світлових хвиль через оптичну систему, яка включає лінзи, діафрагми, оптичні транспаранти та інші (рис. 3.1) [3].

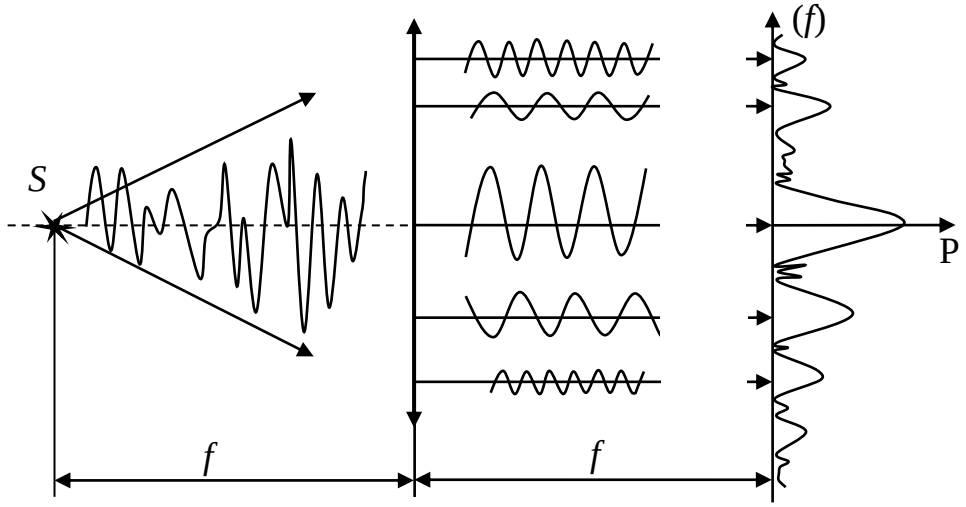

Рисунок 3.1 – Розкладання сигналу на просторові гармоніки

Виділяють прямий (та зворотній) процеси Фур'є-перетворення:

$$F\big(f(x,y)\big) = F(u,v) = \int_{-\infty}^{+\infty}\int f(x,y)e^{-j2\pi(ux+vy)}dxdy \tag{3.1}$$

$$F^{-1}\big(f(u,v)\big) = F(x,y) = \int_{-\infty}^{+\infty}\int f(u,v)e^{j2\pi(ux+vy)}dudv \tag{3.2}$$

де u та v представляють собою просторові частоти і мають розмірність [1/см].

Функцію $F(u, v)$, яка визначає фур'є-спектр вихідної функції, іноді називають Фур'є-образом цієї функції.

Властивості перетворення Фур'є.

1. Перетворення Фур'є лінійне:

$$F[ag(x) + bh(x)] = aF[g(x)] + bF[h(x)]. \tag{3.3}$$

У виразі $g(x)$ і $h(x)$ представляють вихідні функції, a і b є константами (для лаконічності наведені одновимірні функції). Це означає, що через одну лінзу, яка виконує перетворення Фур'є, одночасно може проходити багато світлових сигналів.

2. Виконується особливість подоби:

$$F[g(ax, by)] = \frac{1}{ab} G\left(\frac{u}{a}, \frac{v}{b}\right). \tag{3.4}$$

Коли масштаб зображення на вході системи змінюється, це веде до стиснення або розтягування області його просторового спектру.

3. Теорема зміщення:

$$F[g(x - a, y - b)] = e^{-j2\pi(au+vb)} G(u, v). \tag{3.5}$$

Коли зображення зсувається, це викликає зміну фази спектральної функції, але її амплітуда залишається незмінною.

4. Теорема о похідній:

$$F\left[\frac{\partial}{\partial x} f(x, y)\right] = j2\pi u F(u, v). \tag{3.6}$$

5. Для функції з обмеженим спектром виконується теорема Парсеваля:

$$\int_{-\infty}^{+\infty} \int |f(x, y)|^2 dxdy = \int_{-\infty}^{+\infty} \int |f(u, v)|^2 dudv. \tag{3.7}$$

Ця характеристика вказує на те, що сумарна потужність (квадрат амплітуди) випромінювання, яке проходить через ідеальну прозору лінзу, залишається постійною.

6. У Фур'є-аналізі термін "згортка" використовується для опису взаємодії двох функцій. Це визначається як інтеграл від їхнього добутку, зсунутого одна відносно одної вздовж координатних вісей. Зсув виступає як аргумент в інтегралі згортки [6].

Якщо відомі Фур'є-перетворення двох функцій:

$$F[g(x,y)] = G(u,v), \tag{3.8}$$

$$F[h(x,y)] = H(u,v). \tag{3.9}$$

Тоді теорема згортки стверджує, що Фур'є-перетворення від згортки функцій дорівнює добутку їхніх Фур'є-зображень:

$$F[\Phi(x,y)] = F[g \emptyset h] G(u,v) H(u,v). \tag{3.10}$$

7. Теорема автокореляції є частковим випадком теореми згортки у більшості випадків:

$$F[g \emptyset g^*] = [G(u,v)]. \tag{3.11}$$

Використання символу «*» для позначення комплексного спряження дозволяє корисно виражати операції згортки та автокореляції, особливо при описі оптичних систем просторової фільтрації зображень.

8. Однією з характеристик дельта-функції Дірака є те, що вона може бути виражена як результат перетворення Фур'є від постійної функції.

$$F[1] = \int_{-\infty}^{+\infty} \int e^{-j2\pi(ux+vy)} dxdy = \delta(u,v). \tag{3.12}$$

Символічна дельта-функція досягає нескінченності при аргументі, рівному нулю, та дорівнює нулю в інших областях. Це описує точкове джерело світла із невеликими розмірами, але з обмеженою потужністю. Інтеграл від дельта-функції є скінченим. Функції з постійною комплексною амплітудою та фазою відповідають плоскій хвилі, що поширюється вздовж оптичної осі. Її спектр локалізований у центрі задньої фокальної площини лінзи, близько до точки фокусування (нульова просторова частота). Плоскі хвилі, що рухаються під кутами до оптичної осі, характеризуються просторовими частотами за межами фокусу лінзи [9].

Результат зворотного перетворення Фур'є від дельта-функції рівний константі:

$$F^{-1}[\delta(u,v)] = 1. \tag{3.13}$$

Даний вираз вказує на те, що просторовий спектр точкового джерела світла містить нескінченний, однорідно розподілений у спектральній області набір просторових частот, що відповідає білому шуму.

Згідно з визначенням, результат згортки дельта-функції і звичайної функції дорівнює значенню звичайної функції в точці, де дельта-функція має нескінченні значення:

$$f \emptyset \delta = \int_{-\infty}^{+\infty} \int f(\xi - x, \eta - y) d\xi d\eta = f(x,y). \tag{3.14}$$

Застосовуючи наведені теореми, проводиться двовимірний частотний аналіз характеристик оптичних систем перетворення зображень, що аналогічний спектральному аналізу одновимірних сигналів у радіотехніці. У цьому контексті проходження оптичного сигналу через систему призм, лінз, діафрагм і т. д. подібно проходженню електричного сигналу через електронний фільтр (чотириполюсник) із заданою амплітудно-частотною (передавальною) характеристикою. Функція з постійною комплексною

амплітудою і постійною фазою відповідає плоскій хвилі, яка поширюється по оптичній осі [10].

3.2 Процес фільтрації згідно з методологією Вандерлюгта

Розроблено декілька оптичних методів обробки зображень із спільними концепціями. Один із них включає в себе використання просторової фільтрації Вандерлюгта для обробки зображень та запису інформації про двовимірне перетворення Фур’є об’єкта на фоточутливу плівку [4].

Для виконання оптичної обробки зображень застосовується простий та ефективний метод, відомий як "налаштування 4f", який ілюструється на рис. 3.2. Ця система дозволяє досягти кореляції між двома зображеннями. При цьому одне зображення розташовується на вхідній площині, а відфільтрована форма іншого — на площині Фур’є [1].

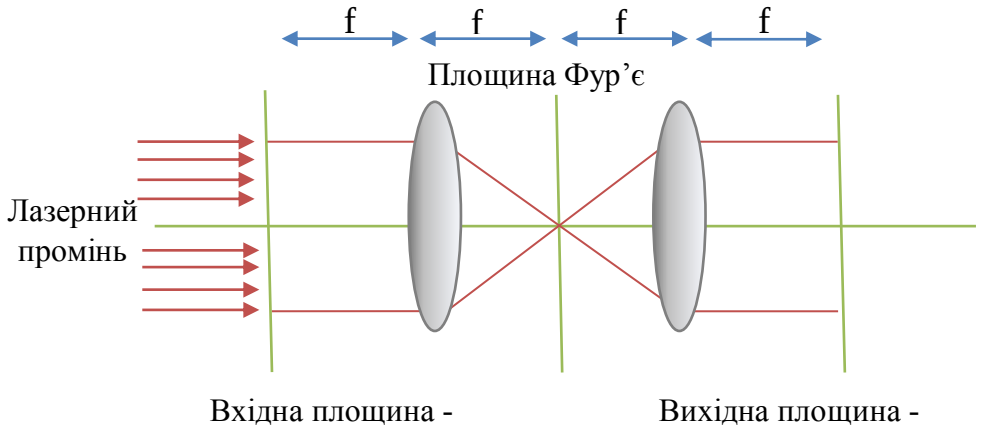

Рисунок 3.2 – Установка корелятора 4f

Лазерний промінь, проходячи через перше зображення та оптичну лінзу, створює Фур’є-перетворену форму цього зображення на площині Фур’є. Фільтр Вандерля, що містить інформацію про частотну область, створює перешкоди для цієї Фур’є-перетвореної форми на другому зображенні. Застосовуючи зворотне перетворення Фур'є, інтерференція проходить через другу оптичну лінзу, що практично реалізовує зворотне

перетворення. Отже, зворотне перетворення Фур'є, включаючи множення фільтра Вандерлюгта на вхідне зображення у частотній області, формується на вихідній площині і розглядається як кореляція між двома зображеннями. Шляхом вимірювання інтенсивності кореляції та порівняння її з автокореляцією зображень можна оцінити ступінь їх схожості [11].

На рисунку 3.2. зображено схематичну конфігурацію для створення просторового фільтра Вандерлюгта для зображення на плівці. Лінза L1 випромінює паралельне світло в площину P1, де міститься зображення з просторовою імпульсною характеристикою $h(x_1, y_1)$. Після того, як світло зображення проходить через лінзу L2 на відстані фокусної відстані L2, формується просторове перетворення Фур'є-зображення на площині P2 [6].

В результаті отримаємо: $\frac{1}{\lambda f} H(\frac{x_2}{\lambda f} \frac{y_2}{\lambda f})$ на площині P2, яку можна замінити фоточутливою плоскістю. Крім того, призма P напряму спрямовує частину світла джерела на площину P2, тобто світло від джерела та світло, що надходить від лінзи L2, інтерферують на площині P2. Таким чином, інтерференція світла від джерела та Фур'є-перетворення зображення будуть зафіксовані на фоточутливій плівці, яка розташована замість площини P2 [2].

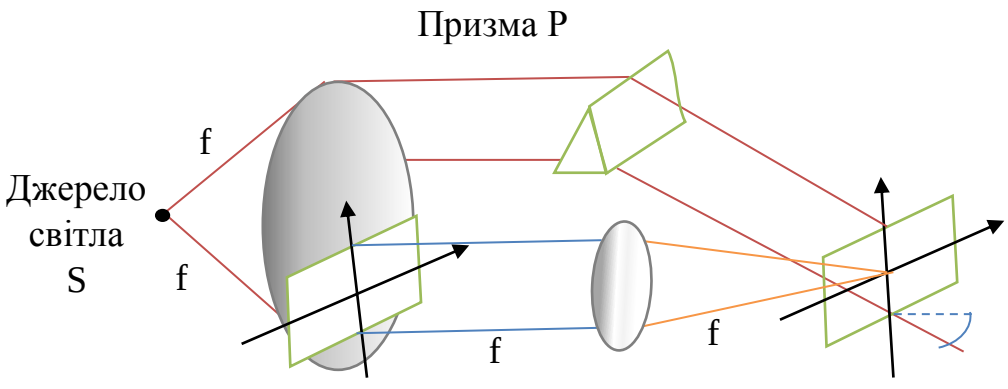

Рисунок 3.3 – Установка синтезу фільтра Вандерлюгта

У випадку, коли нахилена плоска хвиля проходить через призму, вона викликає формування розподілу поля $U_r\ (x_2, y_2)$ на площині Р2, як це ілюстровано нижче:

$$g_r =(x_2, y_2)=r_0 ex\, p(-j2\pi\alpha y_2). \tag{3.15}$$

У ситуації, коли $\alpha = \frac{sin\theta}{\lambda}$, модель інтерференції на площині Р2 буде виражатися таким чином:

$$g =(x_2, y_2)= (\, r_0 exp(-j2\pi\alpha y_2) + \frac{1}{\lambda f} H(\frac{x_2}{\lambda f}\frac{y_2}{\lambda f}))^2. \tag{3.16}$$

Поскільки фоточутлива плівка реагує лише на інтенсивність світла, у рівнянні (3.16) модель зводиться до квадрату. Застосовуючи рівняння (3.16), отримаємо:

$$g =(x_2, y_2)= r_0 + \frac{1}{\lambda f^2}(H\left(\frac{x_2}{\lambda f}\frac{y_2}{\lambda f}\right)^2 + exp(-j2\pi\alpha y_2)\frac{r_0}{\lambda f} H\left(\frac{x_2}{\lambda f}\frac{y_2}{\lambda f}\right) + \\ + exp(-j2\pi\alpha y_2)\frac{r_0}{\lambda f} H\left(\frac{x_2}{\lambda f}\frac{y_2}{\lambda f}\right). \tag{3.17}$$

На заключному етапі процесу синтезу просторового фільтра Вандерлюгта плівка зафіксовує прозорий знімок, де його амплітуда, позначена як $t(x_2, y_2)$, корелює з інтенсивністю світла, яке походить від обох зображень та джерела [10].

$$t(x_2, y_2)= {r_0}^2 \frac{1}{\lambda f^2}\, H^2 + \, exp(-j2\pi\alpha y_2)\frac{r_0}{\lambda f} H\left(\frac{x_2}{\lambda f}\frac{y_2}{\lambda f}\right) H^*. \tag{3.18}$$

Третій член у рівнянні (3.18) представляє собою точне перетворення Фур'є імпульсної характеристики зображення, тому його можна використовувати для оптичної обробки в просторово-частотній області. Обробка зображень за допомогою фільтра Вандерлюгта передбачає

використання синтезованого фільтра Вандерлюгта, який можна замінити площиною Фур'є на рис. 3.3. Якщо вхідне зображення, яке потрібно відфільтрувати, позначене як g (x_1, y_2), його просторовий розподіл частот буде еквівалентним $\frac{1}{\lambda f}\ G(\frac{x_2}{\lambda f}\frac{y_2}{\lambda f})$ [8].

Стосовно виразу (3.18), оптичний сигнал, отриманий на площині Фур'є корелятора $4f$, який зображений на рис. 3.2., може бути представлений наступним чином:

$$U_2 = \frac{{r_0}^2 G}{\lambda f} + \frac{1}{(\lambda f)^2} H^2 G + exp(-j2\pi\alpha y_2)\frac{{r_0}^2}{(\lambda f)^2} HG + \\ + exp(-j2\pi\alpha y_2)\frac{{r_0}^2}{(\lambda f)^2} H^* G. \tag{3.19}$$

U_2 представляє собою результат множення фільтра Вандерлюгта та частотного перетворення вхідного зображення. Після того як ця інтерференція проходить через другу лінзу корелятора $4f$ і пройде відстань фокусування лінзи, застосовується зворотне перетворення Фур'є, і U_3 формується на вихідній площині [7].

$$U_3 = {r_0}^2\, g(x_3, y_3) + \frac{1}{(\lambda f)^2}\left(h(x_3, y_3)\, h^*(-x_3, -y_3) g(x_3, y_3)\right) \\ + \frac{{r_0}^2}{(\lambda f)^2}\,(h(x_3, y_3) g(x_3, y_3)\delta(x_3, y_3 + \alpha\lambda f)) + \\ + \frac{{r_0}^2}{(\lambda f)^2}\left(h^*(-x_3, -y_3) g(x_3, y_3)\delta(x_3, y_3 - \alpha\lambda f)\right). \tag{3.20}$$

Третій компонент у рівнянні (3.20) представляє собою згортку між h та g, яка здійснюється в області з центром $(0, -\alpha\lambda f)$ на вихідній площині. Четвертий компонент можна виразити у вигляді:

$$h^*(-x_3, -y_3) g(x_3, y_3)\delta(x_3, y_3 - \alpha\lambda f) = \tag{3.21}$$
$$= \int\int_{-\infty}^{+\infty} g(\varphi, \mu) h^*(\varphi - x_3, \mu - y_3 + +\alpha\lambda f) d\varphi d\mu.$$

Кореляція між h та g виникає в зоні з центром (0,+αλf) на вихідній площині [10]. При великому куті відхилення джерела світла від площини P2 при створенні фільтра Вандерлюгта області згортки та кореляції на вихідній площині корелятора 4f розташовані віддалено одна від одної. Це дозволяє використовувати просторову високочастотну фільтрацію вихідної площини для індивідуальної кореляції та згортки між вхідним зображенням та фільтром Вандерлюгта.

Перші та другі компоненти рівняння (3.20), які виникають навколо центру вихідної площини, слабо впливають на бажаний результат, оскільки вони піддаються просторовій фільтрації високих частот.

На рисунку 3.4 відображена вихідна площина корелятора 4f, де видно області згортки та перехресної кореляції.

Якщо максимальні просторові розміри h та g позначити як Wh та Wg відповідно, то максимальне значення чотирьох розглянутих компонентів може бути визначено так:

1. $r_0{}^2\, g(x_3, y_3) \longrightarrow W_g{:}\, ma,$ (3.22)
2. $\frac{1}{(\lambda f)^2}(h(x_3, y_3)\ h^*(-x_3, -y_3) g(x_3, y_3)) \longrightarrow (2W_h + W_g){:}\, max,$ (3.23)
3. $\frac{1}{(\lambda f)^2}\left(h(x_3, y_3)\ h^*(-x_3, -y_3) g(x_3, y_3)\right) \longrightarrow \left(2W_h + W_g\right){:}\, max,$ (3.24)
4. $\frac{1}{(\lambda f)^2}(h^*(-x_3, -y_3) g(x_3, y_3) \delta(x_3, y_3 - \alpha\lambda f) \longrightarrow (W_h + W_g){:}\, max.$ (3.25)

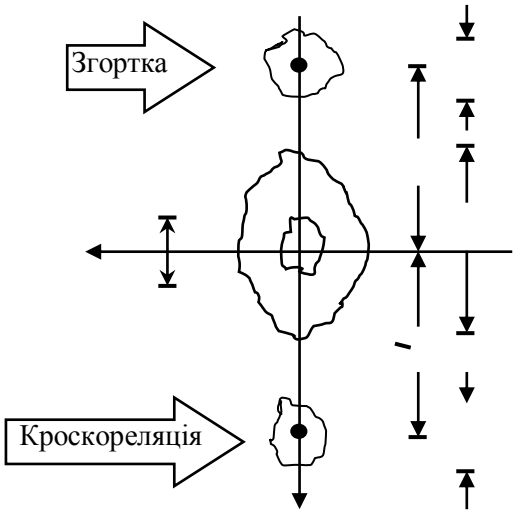

Рисунок 3.4 – Розташування вихідних елементів корелятора

Для ефективного просторового розділення чотирьох компонент на вихідній площині, значення α і θ повинні задовольняти умови, визначені обмеженнями у рівнянні (3.26) і рівнянні (3.27) [12]:

$$\alpha > \frac{1}{\lambda f}\left(\frac{3W_h}{2} + W_g\right) \ (\alpha = \frac{sin\theta}{\lambda}), \tag{3.26}$$

$$\gg \theta > \frac{3}{2}\frac{W_h}{f} + \frac{W_g}{f} \ (sin\theta \approx \theta)\,. \tag{3.27}$$

Установка 4f автоматично обчислює просторову імпульсну характеристику зображення із швидкістю світла, уникаючи складних обчислень. Фільтр Вандерлюгта записує амплітуду і фазу зображення на високороздільній плівці. Далі кожне зображення обличчя порівнюється з усіма фільтрами Вандерлюгта через корелятор 4f. Отримані значення кореляції використовуються для визначення схожості; чим вище значення, тим більша схожість. Система розпізнає зображення з високою точністю, досягаючи практично 100 % правильності. Це свідчить про те, що вхідне зображення точно збігається з фільтром Вандерлюгта, оскільки вони мають найвищу оптичну кореляцію серед усіх. Схема алгоритму розпізнавання зображень показана на рис. 3.5 [6].

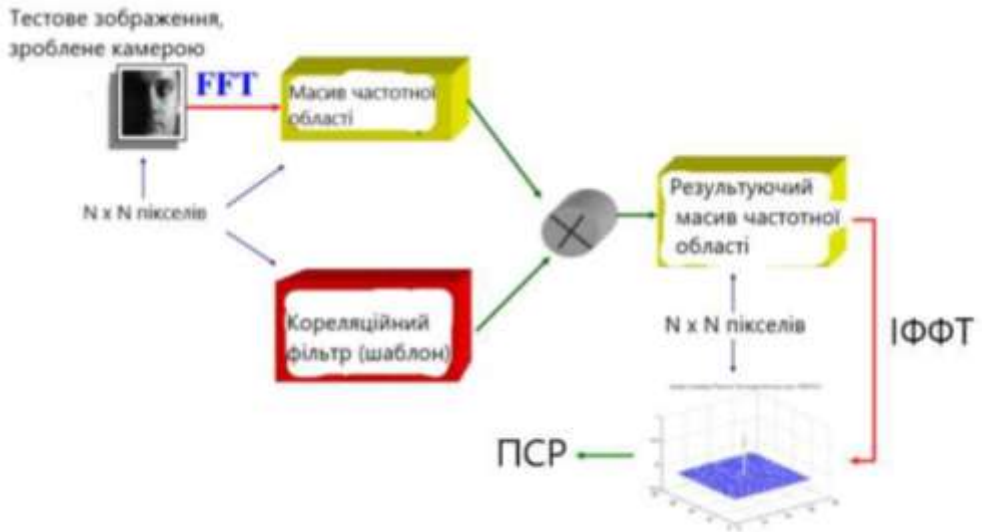

Рисунок 3.5 – Алгоритм розпізнавання образів

Тестове зображення, зняте камерою, спочатку проходить обробку кореляційним масивним фільтром, результатом якої є масив частотної області з N пікселями. Співвідношення піку до бічної пелюстки (ПСІ), яке служить індикатором збігу, оголошується в разі великого значення ПСІ, що вказує на необхідність великого піку та невеликих бічних часток (рис. 3.6.)

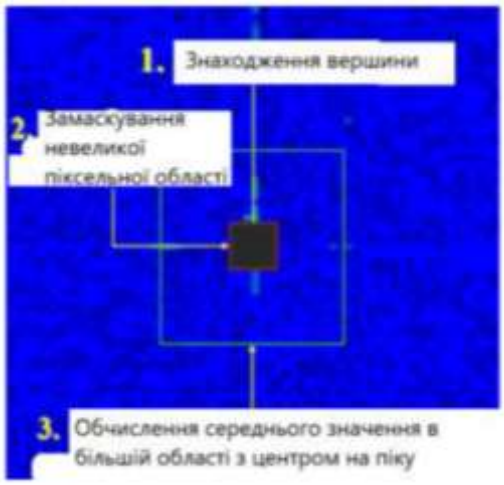

Рисунок 3.6– Робота ПСІ системи

Для точного моделювання кореляції важливо ураховувати всі параметри та константи. На рис. 3.7 два зображення та відповідні фільтри Вандерлюгта. На рис. 3.8 стовпчасті діаграми нормалізованої оптичної кореляції між першими зображеннями шести суб'єктів з набору даних. Кореляція вхідного зображення з фільтром Вандерлюгта є найвищою, забезпечуючи високу достовірність розпізнавання. Другі піки відносяться до того ж предмета з різними позиціями. Це демонструє високу ефективність системи в розпізнаванні [13].

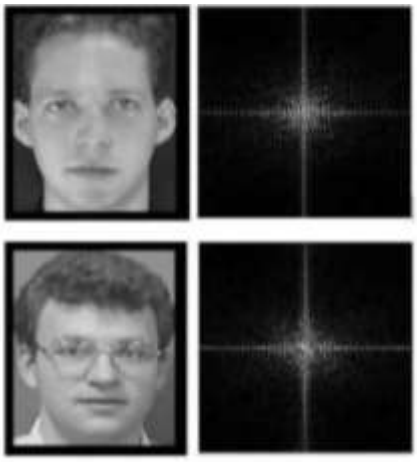

Рисунок 3.7 – Суб’єкт 1 та його фільтрація у верхньому рядку; суб’єкт 2 та його фільтрація у нижньому рядку

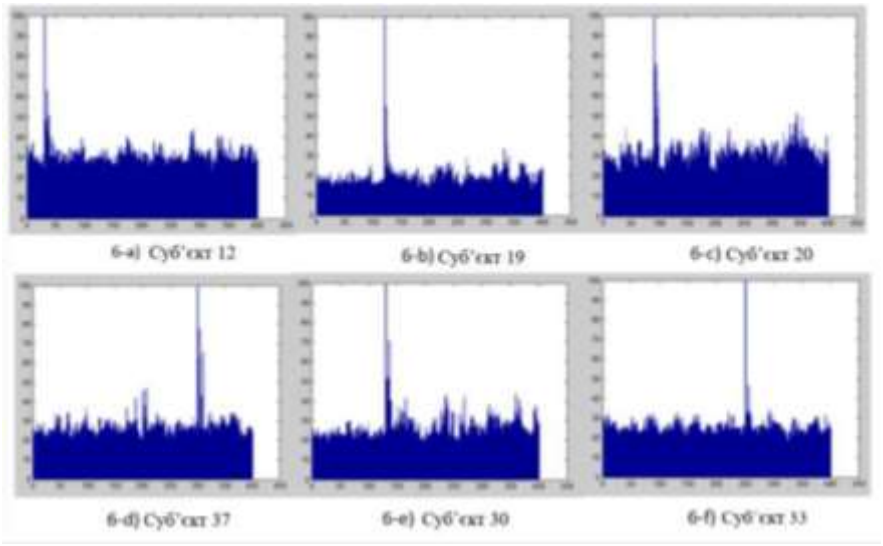

Рисунок 3.8 – Оптична кореляція між першим зображенням шести суб’єктів і фільтрами Вандерлюгта для двох типів обличчя

3.3 Аналіз переваг та недоліків сканування обличчя

Аналізуючи переваги та недоліки розпізнавання обличчя, можна відзначити кілька позитивних аспектів:

– використання для розблокування пристроїв;

– застосування в аеропортах;

– покращення та розширення розпізнавання облич за допомогою машинного навчання та ШІ;

– підвищення рівня безпеки;

– захист від поширення хвороб;

– захист важливої інфраструктури;

– покращення ефективності процесів;

– розпізнавання підроблених паспортів;

– ускладнення ухилення злочинців;

– запобігання різноманітним видам шахрайства.

Проте наряд з перевагами виявляються й недоліки:

– високі витрати на розпізнавання обличчя;

– обмеження свободи та приватності;

– можливість зловживань з боку уряду;

– ризик викрадення конфіденційних даних хакерами;

– технологія ще не є повністю зрілою;

– різні правила та норми у різних регіонах;

– проблеми зберігання даних;

– потенційна небезпека від надмірної залежності від розпізнавання обличчя;

– можливе неприйняття широкою громадськістю;

– підвищення рівня безробіття внаслідок автоматизації.

Враховуючи усі зазначені вище недоліки та переваги перед службовцями, що виконують завдання кібербезпеки, постає задача від несанкціонованого відео- та фотозапису. Але маємо відзначити, що його реалізація здійснюється за допомогою лазерних оптико-електронних систем (ЛОС), що дозволяють виявляти приховані оптичні пристрої (ОД), такі як біноклі, відео- та фотокамери [14].

Незважаючи на очевидні переваги розпізнавання обличчя, важливо усвідомлювати, що конфіденційність і свобода є значущими цінностями [3].

ВИСНОВКИ

Основні завдання біометрії включають в себе впровадження ефективних методів ідентифікації особистості на основі унікальних фізіологічних та поведінкових ознак.

Оптичні методи грають ключову роль в системах розпізнавання, забезпечуючи точність і швидкість ідентифікації. Методи оптоінформатики та техніки сканування обличчя є важливими складовими цього процесу, визначаючи успішність впровадження біометричних систем у практиці.

Математичні методи, зокрема перетворення Фур'є, виявляються невід'ємною частиною оптоінформаційних технологій. Використання аналізу Фур'є для розпізнавання зображень та процес фільтрації за методологією Вандерлюгта сприяють підвищенню точності і швидкості біометричних систем.

Однак, при всіх перевагах сканування обличчя, необхідно ретельно розглядати його недоліки. Високі витрати, можливість обмеження свободи та конфіденційності, ризик зловживань урядами та злочинцями – це аспекти, які потрібно враховувати при розгляді застосування біометрії.

Заключно, важливо підкреслити, що використання біометричних технологій несе великий потенціал для покращення безпеки та зручності у різних галузях. Однак, зберігаючи високі стандарти приватності та конфіденційності, можна забезпечити ефективність та прийняття цих технологій широкою громадськістю.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Біометрія як універсальний спосіб ідентифікації людини. URL: http: //bablyukh .clan. su/publ/ i-i-Q -4 (Дата звернення 14.11.2023).

2. KurskoyYu.S., Gnatenko A.S. System for recognition of optical tools, based on fractal mathematic views // Метрологія та прилади. 2021. Т. 85, № 1. С. 14–18.

3. Decarlo. D., Metaxas D. Optical flow constraints on deformable models with applications to face tracking. // Journal of Computer Vision. 2000. Vol. 38, No 2. P. 99–127.

4. Zhou S.K. Face Recognition using more than One Still Image: what is More?: lecture Notes In Computer Science. // Sinobiometrics. Springer Verlag. 2004. P. 212–223.

5. Васильев В.Н., Павлов А.В. Оптические технологии искусственного интеллекта: учеб. пособ. 2-е изд., дополненное. В 2-х т. Санкт-Петербург: Университет ИТМО, 2017. Т.1. 80с.

6. Lin. I.C. Mirror mocap: automatic and efficient capture of dense 3d facial motion parameters from video // The Visual Computer.2005. Vol. 21, No 6. P. 355–372.

7. Perez P., Gangnet M., Blake A. Poisson image editing // ACM Trans. Graph. Vol. 22, No 3. P. 313–318.

8. Richard D. Zakia, Stroebel L. The Focal Encyclopedia of Photography. 3 Ed. English: Focal Press, 1996. 928 p.

9. Roivainen Li. H. 3-d motion estimation in model-based facial image coding. IEEE Trans. on Pattern Analysis and Machine Intelligence. 1993. Vol. 15. P. 545–555.

10. David D. Zhang. Biometric Solutions: for the Authentication in an E-World. USA: Ed. Kluwer Academic Publishers, 2002. 465 p.

11. Heidari F., Kaatuzyan H., Alizadeh A. Frequency domain approach for face recognition using optical Vanderlugt filters // Optics and Photonics. Vol. 6, No 8B. P. 94–100.

12. Williams L. Performance-driven facial animation // Siggraph Comput. Graph. 1990. Vol. 24, No 4. P. 235–242.

13. David D. Zhang. Automated Biometrics: technologies and Systems. USA: Kluwer Academic Publishers, 2000. 332 p.

14. Kurskoy Y.S., Hnatenko O.S., Machekhin Y.P., .Orazalieva S., Smailova S. Optical system recognition via topological methods Proceedings of SPIE - The International Society for Optical Engineering, 2020, 11581.