Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ПОЯСНЮВАЛЬНА ЗАПИСКА
Дипломної роботи

магістра
(назва освітньо-кваліфікаційного рівня)

галузь знань: *12 Інформаційні технології*
(шифр і назва галузі знань)

напрям підготовки *125 Кібербезпека*
(код і назва напряму підготовки)

освітній рівень ***магістр***

кваліфікація
(назва освітнього рівня)

на тему: Застосування біометричних методів ідентифікації користувачів в інформаційно-комунікаційних системах

Виконавець: студент II **курсу, групи** КБМ-21

(підпис) Бондаренко Максим Сергійович
(прізвище ім'я по-батькові)

	Прізвище, ініціали	Оцінка	Підпис
Науковий керівник	Наконечний В.С.		

Рецензент			

Нормоконтроль			

Київ
2021

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
завідувач кафедри
кібербезпеки та захисту
інформації
_____ Лукова-Чуйко
Н.В.
«_____» _____ 2021 року

ЗАВДАННЯ
на виконання дипломної роботи

спеціальності *125 Кібербезпека*
(код і назва напряму підготовки)

студенту КБМ-21 (група) Бондаренку Максиму Сергійовичу (прізвище ім'я по-батькові)

Тема дипломної роботи Застосування біометричних методів Ідентифікації користувачів в інформаційно-комунікаційних системах

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол №2 від 08.10.2020 р.

2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень процеси ідентифікації та автентифікації об'єктів за біометричними параметрами з використанням ІТ.

Предмет досліджень методи, моделі, алгоритми та ІТ для ідентифікації та автентифікації персоналу.

Мета дослідження залежностей між індивідуальними біометричними параметрами людини для її унікальної ідентифікації та розробка алгоритмів і програми реалізації методів створення еталонів для ІТ біометричної ідентифікації.

Вихідні дані для проведення роботи Механізми біометричної ідентифікації

3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна це спроектування та розробка сайту для роботи з мультимодальним пристроєм, що покращить захищеність систем шляхом зменшення ймовірності виникнення помилок виду FAR та FRR.

Практична цінність Визначення найоптимальнішого методу ідентифікації користувачів біометричними методами

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Робота повинна виконуватися згідно діючої законодавчої та нормативної бази в сфері аудиту інформаційної безпеки

5. ЕТАПИ ВИКОНАННЯ РОБОТИ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Уточнення постановки задачі	

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Пошук та аналіз літератури	
Збір даних	
Обґрунтування вибору рішення	
Розробка програмного забезпечення	
Проведення аналізу отриманих результатів	
Робота над висновками	
Оформлення презентації	

6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект мінімальні витрати на впровадження, використання та супроводження системи бімодальної біометричної ідентифікації

Соціальний ефект Впровадження результатів роботи дозволить ефективно проводити ідентифікацію користувача в інформаційній системі за допомогою мультимодального пристрою.

7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ (підпис) Наконечний В.С. (ініціали, прізвище)

Завдання прийняв до виконання _____ (підпис) Бондаренко М. С. (ініціали, прізвище)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

УДК 621.391

РЕФЕРАТ

Пояснювальна записка до дипломної роботи «Застосування біометричних методів ідентифікації користувачів в інформаційно-комунікаційних системах» складається зі вступу, основної частини, що містить 3 розділи, висновків, списку літератури та джерел. Загальний обсяг роботи – 99 сторінки. Робота містить 18 рисунків, графіків, формул. Список використаних джерел включає 22 джерела.

Об’єкт дослідження – процеси ідентифікації та автентифікації об’єктів за біометричними параметрами з використанням ІТ.

Мета - дослідження залежностей між індивідуальними біометричними параметрами людини для її унікальної ідентифікації та розробка алгоритмів і програми реалізації методів створення еталонів для ІТ біометричної ідентифікації.

Предмет дослідження – методи, моделі, алгоритми та ІТ для ідентифікації та автентифікації користувачів.

Метод дослідження – теоретичний: аналіз наукових джерел (дисертацій, авторефератів дисертацій, монографій, статей тощо) та пошук з метою визначення нерозв’язаних частин проблеми дослідження; моделювання – з метою визначення біометричних параметрів, суттєвих для різних типів людей.

Ключові слова : безпека, інформація, біометрія, біометричні системи, захист інформації, доступ, конфіденційність, захищеність, ідентифікація.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

ІС – інформаційна система

ІТ – інформаційні технології

БД – база даних

ПК – персональний комп’ютер

НСД – Несанкціонований доступ

ПЗ – програмне забезпечення

ПЛР – полімерази

ННМ – приховані моделі Маркова

АЦП – аналого-цифрове перетворення

ВСТУП

Сучасні біометричні інформаційні системи та технології розпізнають людей на основі їх анатомічних особливостей (відбитків пальців, образу обличчя, малюнка ліній долоні, райдужної оболонки, голосу) або поведінкових рис (підпису, ходи). Біометричні інформаційні системи також володіють унікальними перевагами – вони не дозволяють відмовитись від досконалої транзакції і дають можливість визначити, коли індивідуум користується декількома посвідченнями (наприклад, паспортами) на різні імена. Отже, при грамотній реалізації у відповідних додатках інформаційної технології (ІТ) ідентифікації людини, яка використовує біометричні параметри, забезпечує високий рівень захищеності.

Актуальність теми ідентифікації особистості людини обумовлена активною інформатизацією сучасного суспільства та збільшенням потоків конфіденційної інформації. Аналіз сучасних систем контролю доступу свідчить про очевидний рух у бік біометричних методів завдяки їх зручності, надійності та достовірності.

У даний час ІТ все активніше застосовуються в різних галузях промисловості. Це насамперед пов’язано з тим, що сучасні завдання ідентифікації, розпізнавання та авторизації об’єктів (наприклад, службовців, обслуговуючого персоналу, фінансових агентів тощо) вимагають досить високого ступеня точності та ефективності їх вирішення в режимі реального часу. Як правило, перераховані завдання є складними і багатофакторними. Одним з найбільш перспективних підходів у даному випадку є мультимодальні методи, засновані на одночасному використанні кількох класифікаційних ознак. У разі використання однієї біометричної характеристики для розпізнавання об’єктів існує ймовірність помилки системи. Це пов’язано з неправильним використанням технології, умовами навколишнього середовища і якістю зразка.

Потрібно також зазначити, що однією з основних проблем в області біометричних технологій, що гальмують їх розвиток, є відсутність на даний момент основних стандартів [1].

На даний момент усе більше українських та зарубіжних компаній із різних сфер діяльності переходять на біометричний облік робочого часу. Потрібно також зазначити, що за даними соціологічного дослідження компанії Unisys 68% клієнтів у світі вважають за краще, щоб банки, платіжні системи та державні органи для ідентифікації використовували біометрію замість паролів і карток [1].

Мета дослідження – дослідження залежностей між індивідуальними біометричними параметрами людини для її унікальної ідентифікації, пошук оптимальних методів покращення захищеності інформаційно-комунікаційних систем за допомогою біометричних засобів захисту на прикладі підприємства, де проходила виробнича практика.

Об’єкт дослідження – процеси ідентифікації та автентифікації об’єктів за біометричними параметрами з використанням ІТ.

Предмет дослідження – методи, моделі, алгоритми та ІТ для ідентифікації та автентифікації персоналу.

Виходячи з поставленої мети задачами дослідження мають бути:

1. Проаналізувати існуючі алгоритми, моделі, методи біометричної ідентифікації та розглянути переваги мультимодальних ІТ перед унімодальними системами для вибору оптимальних біометричних характеристик.

2. Проаналізувати існуючі прототипи та аналоги ІТ-розробок у галузі біометрії.

3. Розглянути та класифікувати існуючі характеристики статичних біометричних систем, пов’язаних із помилками ідентифікації, для визначення доцільності використання біометричної технології в залежності від початкових умов, а також визначити переваги мультимодальних ІТ перед унімодальними

системами для оцінки точності роботи біометричної системи та побудувати відповідні DET-криві.

4. Визначити шляхом аналізу найкраще поєднання для мультимодальної ідентифікації та можливості її застосування.

5. Розробити алгоритми і програми реалізації методів створення еталонів для ІТ біометричної ідентифікації та експериментально перевірити їх.

6. Спроектувати, реалізувати та випробувати мультимодальний пристрій для розпізнавання об’єктів.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ ПЕРСОНАЛУ

Загальні проблеми використання біометричних технологій досліджували вітчизняні та зарубіжні вчені, зокрема: Ахмєтов Б. С., Завгородній В. В., Іванов О. І., Крак Ю. В., Кухарев Г. О., Мельников Ю. Н., Ушмаїв О. С., John Carter, John R. Vacca, Mark Nixon, Samir Nanavati та інші. Проте наукові праці, в яких би висвітлювалися в повній мірі комплексні підходи біометричних технологій, практично відсутні.

Постановка завдання розділу 1. Розглянути існуючі методи ідентифікації персоналу за біометричними параметрами. Виявити їх переваги та недоліки. Запропонувати комплексний підхід, який включає комбінацію біометричних характеристик – мультимодальний метод.

1.1 Сучасний стан ІТ біометричної ідентифікації

Біометричні технології ідентифікації особистості, засновані на розпізнаванні людини за зовнішніми ознаками, мають глибокі історичні корені. Здатність людей розпізнавати одне одного за зовнішнім виглядом, голосом, запахом тощо – це елементарна біометрична ідентифікація. В кінці 19 століття був розроблений систематичний біометричний підхід писарем префектури паризької поліції Альфонсом Бертільоном. Запропонований ним метод заснований на вимірюванні антропологічних параметрів людини (зріст, довжина та об'єм голови, довжина рук, пальців, стоп тощо) з метою ідентифікації людини [2].

Біометричні системи сьогодні є другим поколінням систем безпеки, оскільки саме біометрія використовує вимірювання окремих параметрів людини для її ідентифікації. Як відомо, головною особливістю систем безпеки

першого покоління є унікальність та послідовність у часі та просторі параметра ідентифікації, тоді як системи безпеки другого покоління, біометричні параметри особистості, завжди є змінними, залежно від багатьох факторів. Завдання надійної ідентифікації біометричних параметрів набагато складніше, ніж ідентифікація постійних параметрів для систем першого покоління.

З інформаційної точки зору, саме системи біометричної ідентифікації людини найкраще відповідають вимогам часу, здійснюючи ідентифікацію людини автоматично та використовуючи нестабільні значення [2].

В даний час біометрія, як наука про ідентифікацію особи, має кілька практично незалежних наукових галузей, кожна з яких має свої технічні вдосконалення. Слід зазначити, що в дослідженнях біометрії беруть активну участь десятки дослідницьких центрів при університетах, деякі дослідницькі організації та комерційні фірми [2]. Вже сформовано специфічний ринок біометричних апаратних пристроїв та програмного забезпечення для них, а також послуг з підтримки, тестування та адаптації біометричних систем на практиці. Сучасні біометричні системи ідентифікації персоналу наведені в додатку А , а їх технічні характеристики - у додатку Б .

Усі системи біометричної ідентифікації виконують дві основні функції [2]:

• реєстрація за кількома вимірами. Цифрове подання (шаблон або модель) біометричної характеристики (залежно від методу: відбиток пальця, малюнок райдужної оболонки ока тощо), що відповідає зареєстрованій особі, формується із зчитувального біометричного пристрою;

• розпізнавання одного або декількох вимірювань біометричної характеристики зчитувача перетворюється у придатну для використання цифрову форму, а потім порівнюється з:

1) єдиним шаблоном, що відповідає людині. Шаблон вибирається заздалегідь затвердженим номером або кодом. Результати порівняння повертаються до програми, процедура називається верифікацією або індивідуальним порівнянням. Результатом порівняння зазвичай є число -

ймовірність того, що порівняні шаблони належать одній людині. Потім, використовуючи будь-який математичний критерій, приймається рішення про ідентичність шаблонів.

2) усіма зареєстрованими шаблонами (без попереднього вибору шаблону та введення номера чи коду). Результат - список декількох найбільш подібних шаблонів (з найвищими можливостями порівняння). Потім, як і в попередньому випадку, за допомогою будь-якого математичного критерію приймається рішення про ідентичність шаблонів. Це називається ідентифікацією або порівнянням "один до багатьох" [3].

З розвитком комп'ютерних технологій біометричний метод широко застосовується у багатьох сферах діяльності. Біометрія може виконувати завдання ідентифікації, автентифікації та авторизації особи, пошуку людей (злочинців, терористів, зниклих безвісти), оплати покупок та послуг, фіксації використання робочого часу тощо.

Активно розвивається нормативна, технічна та правова база біометричних технологій. У рамках Міжнародної організації зі стандартизації (ISO) було створено підкомітет SC37 з біометрії, завдання якого включають оперативну розробку та затвердження єдиних міжнародних стандартів щодо використання, обміну та зберігання біометричних даних. Подібні комітети створені у багатьох національних органах з питань стандартів.

Розглянемо детальніше основні досягнення біометрії, що отримали практичне застосування, проаналізуємо їх недоліки, переваги та перспективи розвитку.

В даний час сучасні технології ідентифікації технологічної біометрії поділяються на дві групи [4]: статистичні та динамічні. Статистичні технології базуються на унікальних фізіологічних особливостях людини. До них належать такі методи [4]:

1) Відбитків пальців. Найбільш широко застосовуваний метод біометричної ідентифікації, цей метод заснований на унікальних особливостях кожної шкіри. Зображення відведення великого пальця, отримане за допомогою

спеціального сканера, трансформується в цифровий код (конвергенція) і підтверджується за допомогою раніше вставлених шаблонів (посилань) або набору шаблонів (у разі розпізнавання).

2) Форма долоні. Ця методика базується на ідентифікованих геометричних зображеннях кисті. За допомогою спеціального пристрою, що дозволяє отримати тривимірне зображення, виходить вимірювання, необхідне для одного цифрового повороту, який ідентифікує людей.

3) Розташування вен на долоні. За допомогою інфрачервоної камери зображення можна відображати на тильних сторонах кисті або руки, які забезпечують зображення та форму цифрових стовпчиків залежно від положення.

4) За сітківкою ока. За своєю швидкістю це метод ідентифікації, заснований на формуванні судин ока. Щоб побачити зображення, потрібно поглянути на світлову точку, воно так само підсвічується і спочатку сканується за допомогою спеціальних камер.

5) За райдужкою оболонки ока. Метод, заснований на унікальних зображеннях райдужної оболонки ока. Метод вимагає спеціальної камери та відповідного програмного забезпечення, що дозволяє записати отримані зображення за допомогою цифрового коду.

6) Форма обличчя. Цей метод ідентифікації створює двовимірний або тривимірний образ людської форми обличчя. Використовуються камери та спеціалізоване програмне забезпечення (ПЗ) для ідентифікації позначених предметів, носів, губ тощо. Обчислюється відстань між ними. На основі цих даних було створено цифрове зображення для порівняння.

7) За термограмою. Цей метод використовує унікальний розподіл формування артерій на шкірі, що виділяють тепло. Для відображення зображень використовуються спеціальні інфрачервоні камери.

8) Інші методи. Існують також унікальні методи, такі як ідентифікація ДНК, піднігтьового шару шкіри, форма вух, запах тіла тощо.

Динамічні методи засновані на (динамічних) характеристиках поведінки людини, тобто з урахуванням характеристик, характерних для підсвідомих рухів у процесі відтворення будь-якої дії [6]:

- Рукопис. Цей метод використовує підпис людини (іноді він пише кодове слово). Цифровий код формується відповідно до динамічних властивостей письма, тобто. Створюється сертифікат, який отримує інформацію про графічні параметри, часові характеристики підпису та динаміку поверхневого тиску тощо.

- Почерк на клавіатурі. Метод подібний до описаного вище, але замість підпису використовується слово код. Основною характеристикою, на якій базується переконання, є динаміка набору кодових слів.

- Голос. Існує багато способів складання коду розпізнавання голосу, як правило, різні комбінації частоти голосу та статистичних характеристик.

- Інші методи. Для цієї групи, методи настільки ж унікальні, як розпізнавання губ, динаміка повороту ключа в дверному замку тощо.

При цілому спектрі біометричних підходів на практиці в основному використовуються три [5]: ідентифікація відбитків пальців, зображення обличчя (двовимірне 2D та 3D) та ідентифікація за райдужною оболонкою ока. Однак будь-яка з них базується на порівнянні ідентифікованих даних об'єкта та біометричного стандарту. Таке порівняння неможливе без запису та зберігання біометричної інформації, тобто без документів.

Основними інструментами автоматизованого біометричного методу є сканер для вимірювання біометричних характеристик та алгоритм, що дозволяє порівняти його з тим раніше зареєстрованим об’єктом (так званий біометричний шаблон). Наприклад, при ідентифікації людини за допомогою відбитка пальця стандартною процедурою є перетворення відбитків пальців сканера спочатку у графічний файл, а потім у спеціальний файл шаблону, форма якого залежить від конкретної техніки.

Отже, в процесі ідентифікації біометрії ми маємо справу з особливим способом документування інформації - біометрією. Вивчення методів

документування є одним із завдань теорії документознавства. Відповідно до термінологічного стандарту ведення діловодства та архівування, документація - це запис інформації на різні носії відповідно до встановлених правил [6]. Правила оформлення документації - це вимоги та норми, що встановлюють порядок оформлення документації [6].

1.2 Статичні методи біометричної ідентифікації

Статичні методи ідентифікації біометрії базуються на фізіологічних (статичних) характеристиках людини, тобто на унікальній ознаці, яку вони отримують від народження та є невід'ємною частиною її. Розглянемо більш детальні методи статичної ідентифікації.

1.2.1 Ідентифікація за відбитками пальців

Сканування відбитків пальців є найдавнішим з усіх, але в той же час воно вважається одним з найперспективніших. Кожна людина має унікальні незмінені відбитки пальців, що доведено судово-медичними науками та підтверджено професійною практикою [5]. Відбитки пальців умовно складаються з рельєфних ліній - папілярного малюнка, структура якого є результатом ряду гребінцевих виступів на шкірі, розділених борознами. Ці лінії утворюють складні шкіряні зображення - арки, петлі, завитки, які зазвичай мають такі властивості, як: індивідуальність, стійкість, повторюваність (показано на рисунку 1.1). Індивідуальність - це різноманітний набір папілярних ліній, які утворюють візерунок відповідно до його конфігурації, положення, відносного положення та унікальності в іншому візерунку [5].

Рисунок 1.1 – Процес дактилоскопічного розпізнавання

Відносна стабільність - це вторгнення зовнішньої структури папілярного малюнка у людей від народження, протягом життя та через деякий час після смерті. При поверхневих розладах шкіри папілярні лінії відновлюються за початковим типом. Ці властивості папілярних візерунків дозволяють, безсумнівно, ідентифікувати людину за відбитками пальців.

Система біометричної ідентифікації використовує два основних методи ідентифікації відбитків пальців [7]:

- перший заснований на візерунку на великому пальці;
- інші - за допомогою кореляційного підходу.

Вони постійно вдосконалюються та мають свої переваги та недоліки. Ці методи засновані на фізіологічних властивостях структури папілярних малюнків та апаратних пристроїв із відповідним ПЗ.

Дактилоскопічна ідентифікація особи, яка бажає отримати доступ до об’єкта, що охороняється, виконується за допомогою телевізійної камери, яка сканує папілярний малюнок пальців і порівнює його за співвідношенням із еталонним зображенням. Кількість інформації в стандартах може значно зменшитись, якщо класифікувати зображення за типом папілярних візерунків та виділити характерні мікрофункції, що представляють початок або кінець папілярних ліній, що їх об’єднують. Існує три типи папілярних візерунків (дугоподібні, круглі та вигнуті) та два типи макро-ознак (дельта та центри).

Біометричні системи розпізнавання відбитків пальців, як правило, відмовляють у доступі до об'єкта доволі часто (система не розпізнає справжність відбитків пальців зареєстрованого користувача), з певною можливістю неправильного або помилкового доступу до об'єкта (можливість того, що система помилково "ідентифікує" відбитки пальців користувач, який не зареєстрований у цій системі).

В даний час розробляються алгоритми, стійкі до шуму, на зображеннях відбитків пальців для підвищення точності та швидкості ідентифікації об'єктів у реальному часі. Цей метод ідентифікації набув широкого розповсюдження в судових та охоронних системах[7].

Переваги та недоліки методу:

Переваги методу. Висока надійність - статистичні показники методу кращі, ніж показники обличчя, голосу, зображення. Дешеві пристрої, які сканують зображення відбитків пальців. Досить проста процедура сканування відбитків пальців.

Недоліки: папілярний малюнок відбитків пальців дуже легко пошкодити дрібними подряпинами, порізами. Люди, які використовували сканери в компаніях, штат яких становить кілька сотень людей, повідомляють, що вони відмовляються від даного типу ідентифікації. Багато сканерів погано обробляють суху шкіру і не дозволяють літнім людям пройти даний етап перевірки. Також бракує захисту від злиття зображення, частково через широке використання методу. Для деяких людей з «неправильними» пальцями (особлива температура тіла, вологість) ймовірність відмови у доступі може досягати 100%. Ці цифри коливаються від декількох відсотків (для дорогих сканерів) до десяти відсотків (для дешевих).

1.2.2 Біометричні інформаційні системи розпізнавання обличчя

Усі основні типи технологій розпізнавання обличчя призначені для пошуку бажаного об'єкта індивідуально, тобто для ідентифікації конкретного обличчя серед тисяч облич, внесених до бази даних.

Якісні характеристики таких систем залежать від технологічних можливостей відеокамер з роздільною здатністю 320x240 пікселів на дюйм при швидкості відеопотоку не менше 3-5 кадрів в секунду і які підключені до мережі за допомогою ПК. Чим вища швидкість потокового відео, тим краща роздільна здатність системи, тим краща якість отриманої ідентифікації.

У існуючих біометричних системах поверхня сканується приблизно протягом 20-30 секунд, в результаті чого створюється кілька зображень. Якісне розпізнаване зображення обличчя зазвичай вимагає приблизно 150-300 Кб даних, а шаблони зображень займають приблизно (1,3 Кб) інформації.

Процес сканування відео на обличчі базується на створенні оригінального "живого" шаблону в режимі реального часу та порівнянні його з прикладом файлу шаблону. Ступінь надійності об'єктів зображення, що перевіряються, - це певний рівень вірогідності, який може бути не однаковим для різних типів завдань, або який може залежати від персоналу, комп'ютерів, часу та інших факторів. Розпізнаючи людину з великої відстані, існує значний зв’язок між якістю та результатами ідентифікації [8].

Існує три основних методи розпізнавання обличчя. Вони включають аналіз зображення для визначення типових рис обличчя [8]:

- аналіз "ідентифікованих рис обличчя" - найбільш поширених та адаптованих до змін у виразів обличчя;

- аналіз на основі "нейронних мереж" - на основі порівняння "особливих точок", яке може ідентифікувати людей, що перебувають у складних умовах;

- метод "автоматичної обробки зображень" - визначення відстані між встановленими рисами обличчя людини.

Останній метод не такий ефективний, як інші, але його можна використовувати для ідентифікації зображень у кімнатах без освітлення. Основними проблемами, що суттєво впливають на ефективність цих біометричних систем, є зміни освітлення, різні варіації положення обличчя під час руху, труднощі з виділенням інформативної частини обличчя, включаючи портретну поверхню, та несприятливий фон, що ускладнює обличчя визнання. Ці частини можна частково вирішити шляхом автоматичного виділення певних точок на поверхні та вимірювання відстані між ними. Тому на обличчі виділяються контури очей, брів, носа, щелепи та вух. Відстань між типовими точками цих контурів утворює унікальний і компактний стандарт конкретної людини, який легко масштабується.

Проблема особистої ідентифікації значно спрощується, якщо перетворити систему біометричного спостереження на широкий діапазон інфрачервоного світла. Цей метод дозволяє виконати (сканувати) термографію ідентифікованої людини, одночасно виявляючи спеціальну мережу поверхневих кровоносних судин. Існує проблема адекватного освітлення для цього класу біометричних приладів, оскільки вони лише виявляють і реєструють зміни температури поверхні і можуть працювати в повній темряві. На результати ідентифікації не впливають такі фактори, як перегрів обличчя або переохолодження, природне старіння шкіри обличчя, пластичні операції тощо, оскільки вони не змінюють внутрішнє розташування кровоносних судин людини.

Система розпізнавання обличчя поділяється на дві області: 2-D розпізнавання та 3-D розпізнавання [7]. Всі вони мають переваги та недоліки, але багато з них також залежать від обсягу та вимог певного алгоритму.

Двовимірне розпізнавання поверхні є одним із найбільш статистично ефективних біометричних методів (показано на рисунку 1.2). Він з’явився давно і використовувався переважно в криміналістиці, що сприяло його розвитку. В результаті з’явилися обчислювальні інтерпретації методу, що роблять його більш надійним, але поступаються іншим методам біометричної ідентифікації. В даний час він використовується в мультимодальних даних чи,

як це також відомо, у перехресних біометричних даних або в соціальних мережах через погану статистику.

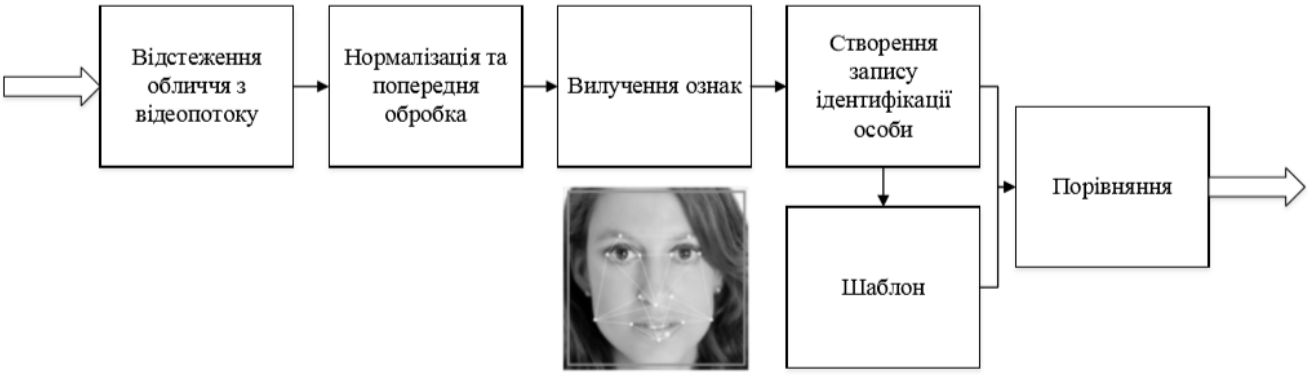


Рисунок 1.2 – Процес 2-D розпізнавання особи

Переваги та недоліки методу [8].

Переваги методу. Двовимірне розпізнавання не вимагає дорогого обладнання, на відміну від більшості біометричних методів. Завдяки необхідному обладнанню, є можливість розпізнавати обличчя на великій відстані від камери.

Недоліки. Низька статистична надійність. Вимоги до освітлення. Для багатьох алгоритмів неприйнятними є будь-які зовнішні бар'єри, такі як окуляри, борода, деякі елементи зачіски. Іноді нечітке зображення обличчя, з невеликими відхиленнями. Багато алгоритмів не враховують можливі зміни виразу обличчя, тобто. Вираз повинен бути нейтральним.

3-D розпізнавання обличчя. В даний час існує безліч методів ідентифікації тривимірних граней. Методи не можна порівнювати між собою, оскільки вони використовують різні сканери та бази даних.

Перехід від двовимірного підходу до тривимірного є методом, який застосовує накопичення персональних даних. При цьому використовується лише одна камера. При введенні об'єкта в базу даних він повертає голову, і алгоритм приєднується до зображення, створюючи 3D-шаблон (показано на рисунку 1.3).

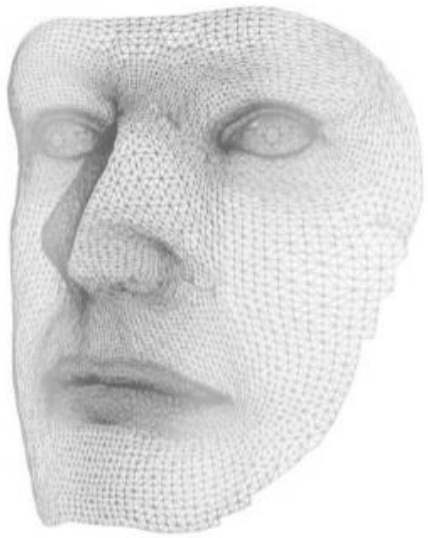


Рисунок 1.3 – 3-D шаблон для розпізнавання особи

Найбільш класичний підхід - метод дизайну шаблону. Він передбачає проектування мережі на об’єкті (людині). Потім камера знімає десятки кадрів в секунду, а отримані зображення обробляються спеціальною програмою. Промінь, який падає на криволінійну поверхню, згинається - чим більше кривизна поверхні, тим сильніше вигин променю. Спочатку використовувалося видиме джерело світла. Потім видиме світло замінюється інфрачервоним. На першому етапі обробки робляться зображення там, де поверхня взагалі не видна або є сторонні предмети, які заважають ідентифікації.

Згідно з отриманими знімками, тривимірна модель особи підлягає редагуванню, де призначено та видалено непотрібні перешкоди (зачіска, борода, вуса та окуляри). Потім проводиться аналіз моделі - антропометричні ознаки, які, відповідно, записуються в унікальний код, поміщаються в базу даних. Запис та обробка зображень займає 1-2 секунди для найкращих моделей.

Переваги та недоліки методу [8].

Переваги методу. Не потрібно зв’язуватися зі сканером. Низька чутливість до зовнішніх факторів, до людини (зовнішній вигляд окулярів,

бороди, зміна зачіски) і в його оточенні (освітлення, поворот голови). Високий ступінь надійності порівняно з методом ідентифікації відбитків пальців.

Недоліки методу. Дуже дороге обладнання. Зміни у вираженні поверхні та поверхневих перешкодах погіршують статистичну надійність методу. Метод все ще недостатньо розроблений, що ускладнює широке використання.

1.2.3 Біометричні інформаційні системи розпізнавання особи за кистю руки

Метод ідентифікації геометрії людини вручну за технологічною структурою та рівнем надійності подібний до ідентифікації відбитків пальців, але все ще використовується рідко. Така математична модель ідентифікації вимагає невеликої кількості інформації - всього 9 байт. Це дозволяє зберігати велику кількість необхідної інформації про людей, яких потрібно розпізнати, та швидко здійснювати пошук. Найдосконаліший пристрій - Handkeu, який сканує не тільки внутрішню, але й зовнішню сторону долоні, використовуючи вбудовану відеокамеру. Подібні системи, де можна сканувати інші ручні параметри, в даний час розробляються такими компаніями, як VioMetRagtners, Palmetrics та BTG.

Більш складними є системи, які також вимірюють профіль кисті - об’єм пальців, об’єм кисті, нерівність долоні, площа шкірних складок на суглобах тощо. (показано на рисунку 1.4).

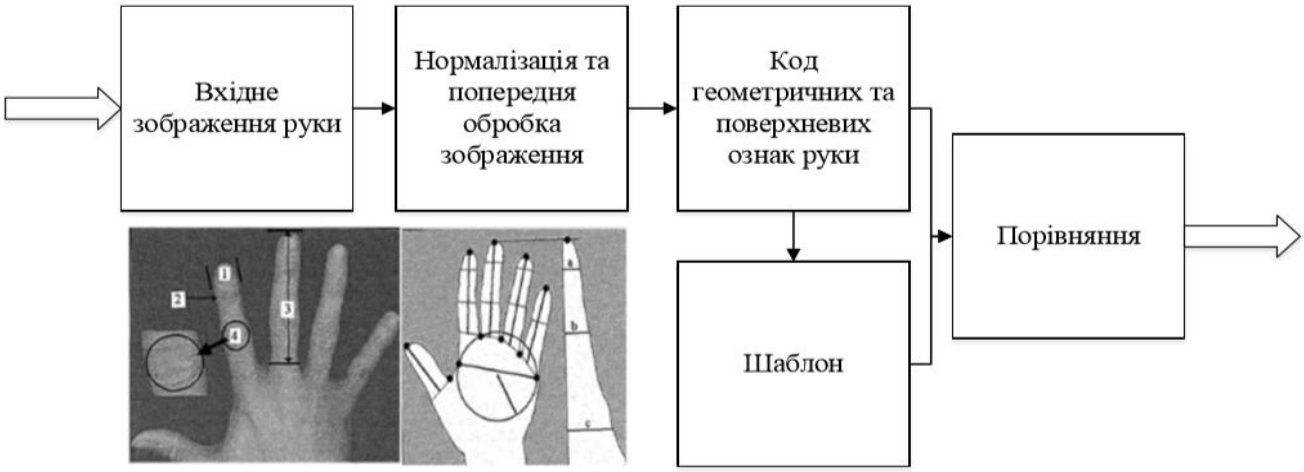


Рисунок 1.4 – Процес розпізнавання особи за кистю руки

Дані про тривимірну геометрію руки отримують за допомогою однієї телевізійної камери та інфрачервоного підсвічування під різними кутами. Поворот декількох світлодіодів поспіль для освітлення дає тіньові проекції тривимірної геометрії руки, що включає інформацію про її об'єм та відповідні індивідуальні властивості. Ці пристрої досить громіздкі, оскільки вимагають видалення джерел світла на відстані 10-15 см і відносно дорогі - коштують від 600 до 3000 доларів.

1.2.4 Біометричні інформаційні системи розпізнавання особи за мережею кровоносних судин долоні руки

У цьому випадку біометричним об'єктом є термографія судин поза долонею, що відрізняється унікальністю і послідовністю протягом усього життя, що дозволяє використовувати їх для ідентифікації людини.

Формування судинної системи починається до народження і відрізняється навіть у близнюків. Процес сканування судин за межами долоні відбувається в інфрачервоному діапазоні світлових хвиль, що дозволяє отримати досить чітке зображення судин. У цьому випадку порівняно невеликі порізи або забруднення

поверхні шкіри не завадять успішній реєстрації, а швидкість обробки отриманих даних дуже висока, порівняно з іншими біометричними системами.

Зареєструвавшись у цій біометричній системі, користувач зберігає свої дані в терміналі або корпоративній базі даних або зберігає їх на смарт-картці. У цьому випадку порівняння проводиться за планом "разом" і триває мінімум часу.

Це нова технологія в галузі біометрії, широке використання якої розпочато 6-10 років тому. Інфрачервона камера робить зображення зовні на внутрішній стороні руки. Картина вен формується тому, що гемоглобін у крові поглинає інфрачервоне випромінювання. В результаті швидкість відбиття зменшується, і вени з'являються на камері у вигляді чорних ліній. Спеціальна програма, що базується на отриманих даних, створює переконання в цифровій формі. Не потрібен контакт людини із скануючим пристроєм.

Існує два методи отримання зображення вени на долоні [8]. Режим відображення дозволяє встановити всі компоненти пристрою в одному корпусі, що зменшує розмір. Це також знижує психологічний бар’єр (не потрібно нікуди класти руку).

Метод передачі інфрачервоного світла (Transmission) полягає в установці інфрачервоних ліхтарів на тильну сторону долоні, а камера з фільтром встановлена на долоні і приймає інфрачервоне випромінювання, що проходить через всю долоню. За допомогою методу пропуску отримані зображення є більш детальними (показано на рисунку 1.5) [8].

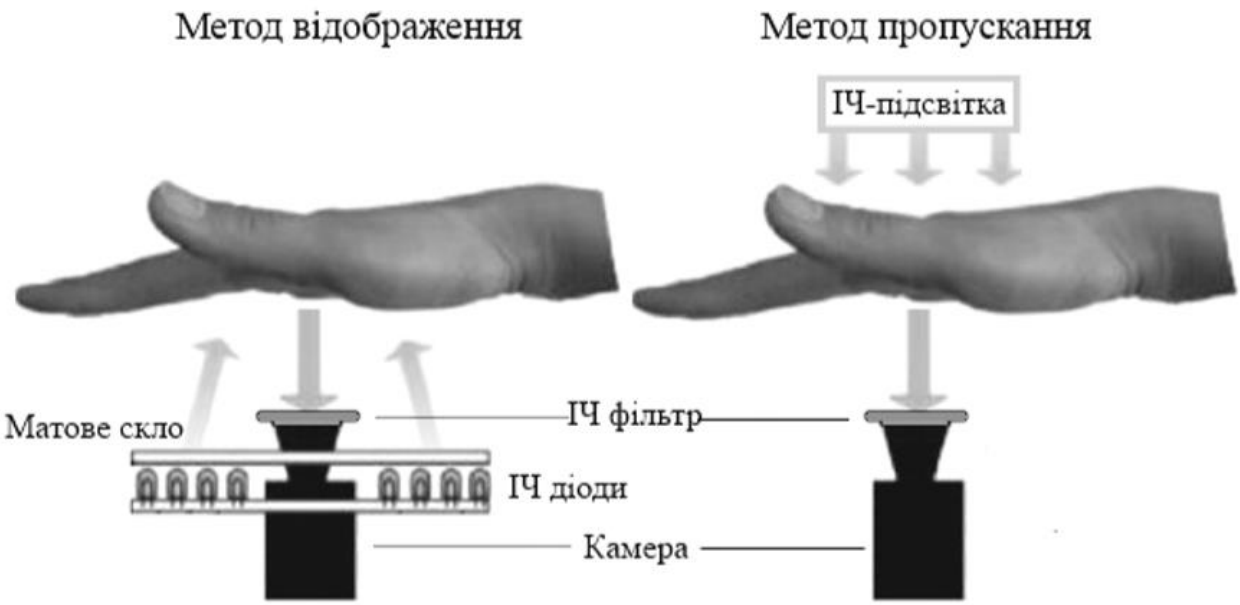


Рисунок 1.5 – Методи отримання зображення малюнка вен долоні

Переваги та недоліки методу [7].

Переваги методу. Відсутність необхідності контактувати зі скануючим пристроєм. Висока достовірність - статистичні показники методу можна порівняти з показаннями райдужної оболонки ока. Цю характеристику дуже важко отримати від людини «з вулиці», наприклад сфотографувавши її фотоапаратом.

Недоліки методу. Неприпустиме засвічення сканера сонячними променями і променями галогенних ламп. Метод менш вивчений в порівнянні з іншими статичними методами біометрії.

1.2.5 Біометричні інформаційні системи розпізнавання особи за райдужною оболонкою ока

Око - єдиний внутрішній орган людини, видимий із зовні. Оскільки внутрішні органи людини є унікальними, а зображення ока також легко доступне за допомогою звичайної цифрової камери, постало питання, чи можна

використовувати зображення райдужки ока як код, який відрізняє одну людину від іншої.

Візерунок райдужки ока є випадковим і чим вища випадковість, тим більша ймовірність того, що певна картина буде унікальною.

Ідея використання текстури райдужки ока для ідентифікації людини була запропонована в 70-80-х роках минулого століття. У 1981 р. Флом (учений) та Аран Сапфір (офтальмолог) розпочали вивчення наукових медичних звітів про будову ока і, зокрема, райдужки ока людини [8].

У 1987 році вони подали заявку в Кембридж про співпрацю вчених у галузі обчислювальної техніки. Вчений на ім'я Джон Догман відгукнувся на його заклик.

Вперше Доугман опублікував результати своїх досліджень у 1992 році на конференції. Донині робота Догмена є основною у цій галузі. У 1994 році запатентована система ідентифікації райдужки на основі досліджень Даугмана (патент 5291560).

1996. Річард П. Уайлдс запропонував альтернативний метод зберігання текстурної інформації, а в 1998 р. Вчений запропонував альтернативний метод. Серед компаній, що займаються ідентифікацією, можна назвати Iridian, IriTech, Evermedia.

Унікальність малюнка райдужки ока обумовлена генотипом людини, а значні відмінності в райдужці помічаються навіть у близнюків. Деякі захворювання викликають появу характерних пігментних плям на райдужці і зміну кольору очей. У технічних системах використовуються лише чорно-білі зображення з високою роздільною здатністю, щоб зменшити вплив результатів особистої ідентифікації на здоров'я.

Унікальність структури райдужки дозволяє компаніям виробляти значну кількість високонадійних систем біометричної ідентифікації. Цей клас систем сканує зображення ока на відстані 20-30 см від відеокамери, автоматично вибираючи зіницю та райдужку. Немає даних про спроби зробити модель райдужки. Ціни на ці системи коливаються від 500 до 6500 доларів. Основні

патенти цієї системи ідентифікації знаходяться в руках однієї компанії – IriScan [9].

Однак ця система має певні недоліки через фізіологічні зміни в організмі людини. З роками розташування плям на райдужці людини може істотно змінюватися, наприклад, райдужка ока дитини може змінюватися з роками, так що система біометрії не може її ідентифікувати. Крім того, негативні помилки в ідентифікації можуть траплятися при незначних травмах очей або навіть в результаті безсоння або сильного перенапруження очей. Зміни такого роду є тривіальними, але система ідентифікації в таких випадках може не ідентифікувати райдужку.

Для біометричних систем сканування сітківки вони ідентифікуються за інтенсивним інфрачервоним світлом, спрямованим через зіницю до кровоносних судин у задній частині ока. Зареєстровані користувачі мережевих сканерів мають найнижчий відсоток відмов, і помилок доступу практично немає. Однак малюнок райдужки повинен бути чітким.

Одним із ранніх і найнадійніших способів ідентифікації людини є використання зразка судин ока. Кровоносні судини та артерії, що постачають кров до ока, добре видно, коли зіницю ока осяяє зовнішнє джерело світла.

Око освітлюється інфрачервоними променями, які випромінюють мережу кровоносних судин, які потім порівнюють зі стандартними.

Однак ця система може спричинити помилки внаслідок відхилення голови людини від встановлених меж або неправильного фокусування погляду на віддаленому джерелі світла. Прилади цього класу є найдорожчими - 4000 доларів і найменш популярні, оскільки споживачі вважають, що використання приладів для інфрачервоного освітлення зіниці ока шкодить їх здоров'ю [8].

Методи ідентифікації особи за допомогою райдужки базуються на одному і тому ж принципі - вибір частоти або іншої інформації про текстуру райдужки з зображення та збереження цих даних як спеціального коду (код для Даугмена так і називається - IrisCode). Цей код порівнюється та вноситься у базу даних.

1) Виділення "круга" райдужної оболонки загальної картини показано на рисунку 1.6;

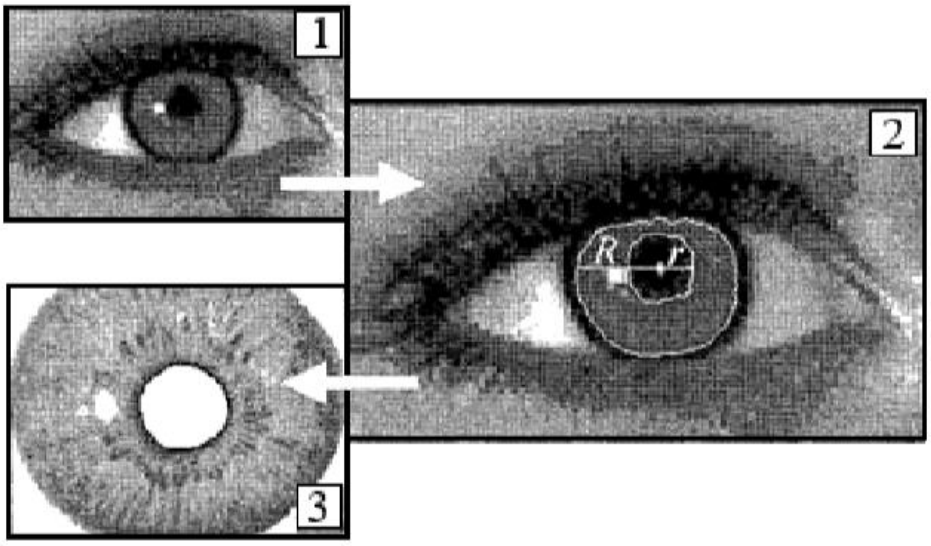


Рисунок 1.6 – Отримання «кола» райдужки

2) Попередня обробка отриманого зображення - наприклад, видалення шуму, поліпшення зображення, включаючи вирівнювання гістограми, видалення відблисків. Деякі методи «розвивають» круговий вигляд зіниці в прямокутне зображення - відбувається перенесення полярних в декартові координати. Іноді після такої «програми» частина зображення обрізається, тому помилка в цей момент може вплинути на подальше розпізнавання, як показано на рисунку 1.7;

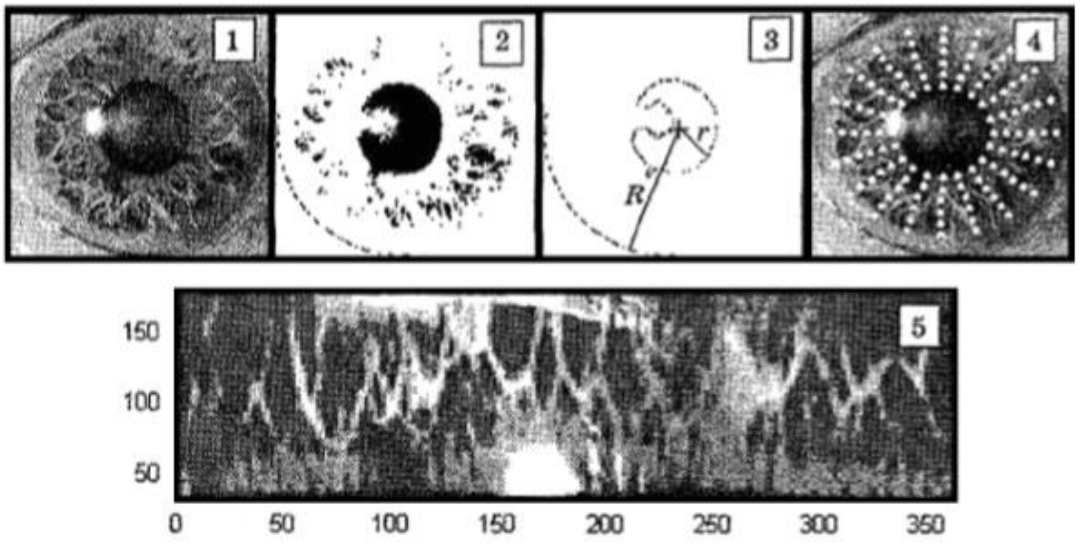


Рисунок 1.7 – Обробка отриманого зображення

3) Компілювати код. Оброблене раніше зображення фільтрується способом, який залежить від конкретного методу. Згідно з результатами фільтру, подання коду показано на рисунку 1.8 [8].

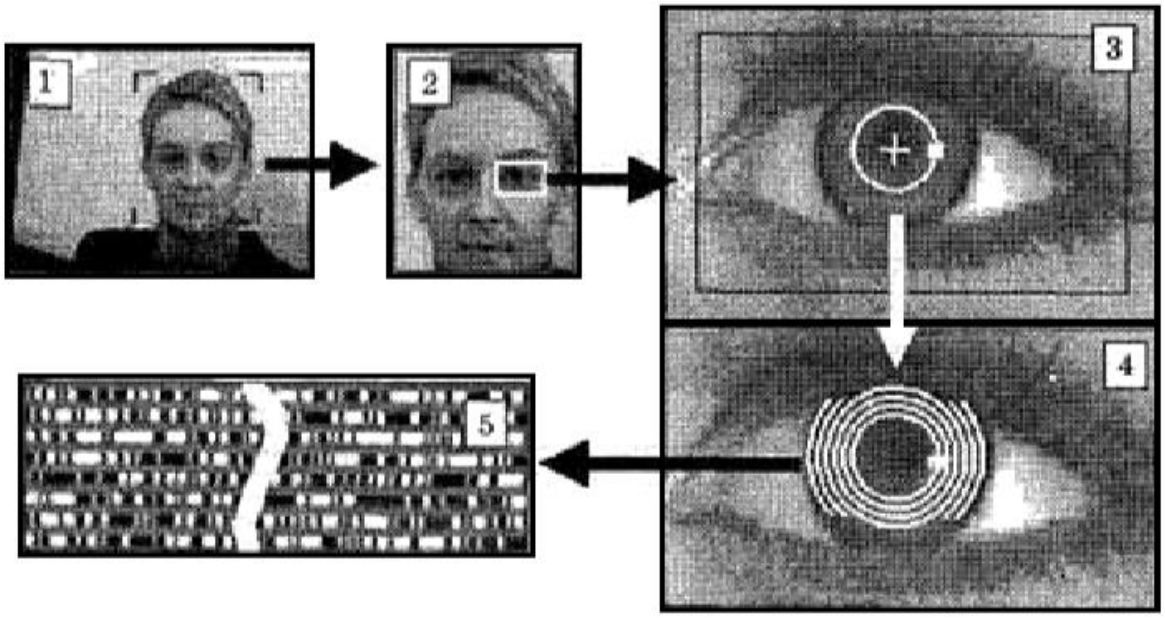


Рисунок 1.8 – Складання коду

Для порівняння потрібно розробити коди. Код часто пишеться у вигляді серії фрагментів, а критерієм для порівняння є код Хеммінга. Зокрема, код Хеммінга використовується в системах Даугмана [9].

Якщо для захоплення зображення не використовуються спеціальні інструменти, можливо, доведеться заздалегідь усунути побічні ефекти, такі як спалах зіниці від спалаху або іншого яскравого джерела світла, якщо ці ефекти заважають правильній роботі алгоритму райдужної оболонки.

Класичні методи компіляції коду включають ослаблення просторової частоти зображення за допомогою фільтрів Габора, запропоновані Даугманом [9]. Кожен фрагмент коду визначається сигналом ефекту двовимірного фільтра Габора на якомусь невеликому сусідстві текстури райдужної оболонки. Для

коду Догмена та подібних йому для порівняння використовується відстань Хеммінга (кількість різних фрагментів коду).

Ще однією модифікацією коду на основі фільтрів Габора є підсумовування коду на основі середнього абсолютного відхилення відфільтрованого зображення від оригіналу [9].

Переваги та недоліки методу [7].

Переваги методу. Статистична надійність алгоритму. Зображення райдужки може бути зроблено на відстані від декількох сантиметрів до декількох метрів, тоді як фізичний контакт людини з пристроєм цього не робить. Райдужна оболонка захищена від пошкоджень, тому з часом вона не зміниться. Також можна використовувати велику кількість методів, щоб уникнути підробки.

Недоліки методу. Вартість системи на основі райдужної оболонки вища, ніж вартість системи розпізнавання пальців або розпізнавання обличчя. Низька доступність готових рішень. Продаються найдорожчі системи великими компаніями, такими як Iridian або LG.

1.2.6 Ідентифікація за сітківкою ока

Ця система ідентифікації біометричних даних має невелику пропускну здатність і є досить дорогою у використанні, але її надійність у рази вища. Вона поєднує в собі найкращі ідентифікаційні ознаки відповідно до малюнка вен та ключових точок райдужки (показано на рисунку 1.9).

Рисунок 1.9 - Процес розпізнавання особи за сітківкою ока

На відміну від змінної, в залежності від освітленості, ваги та присутності наркотиків в тілі райдужки, сітківка залишається нерухомою і не змінюється з часом [10]. Помилки можливі лише при очних захворюваннях, таких як катаракта, але такі випадки - лише винятки. А венозний малюнок потиличного дна - це ще одне постійне «захисне кільце», унікальне для кожної людини. Ідентифікація сітківки завоювала почесне місце в системах безпеки державних спецслужб [5].

Процедура цієї ідентифікації полягає в скануванні сітківки вузьким пучком світла в інфрачервоному діапазоні, спрямованим через зіницю до резервуара. Останні моделі сканерів використовують інфрачервоне світло замість лазера. Людина повинна наблизити своє обличчя до сканера, відзначити його положення та подивитися на спеціальну позначку на екрані сканера. Це, мабуть, єдиний недолік таких систем - необхідність тривалого обслуговування. Тобто сканери сітківки не підходять для установки на входах та контрольних точках заводу: це просто перешкоджатиме виробництву. Такі системи призначені насамперед для охорони приватних кабінетів, скарбниць та сховищ.

Одна з найновіших та вдосконалених систем розпізнавання сітківки називається EueDentifu [10]. Системи цього класу мають камеру з датчиками

короткої дальності (близько 3 см). Цей пристрій допомагає зменшити час сканування масиву в хвилину, час порівняння стандартів та зразків - до 5 секунд і, отже, збільшує вхід до 3-5 людей за 5 хвилин.

Переваги та недоліки методу [7].

Переваги. Високий рівень статистичної надійності. Через низьку поширеність системи, існує дуже мало способів її обійти

Недоліки. Важко використовувати систему з тривалим часом обробки. Висока вартість системи. Відсутність широкого попиту на ринку та, як наслідок, неадекватна інтенсивність підходу.

1.2.7 Ідентифікація за ознакою ДНК

Генні відбитки або метод генетичних відбитків пальців - метод розрізнення особин за допомогою зразків ДНК [6].

Перша версія методу була розроблена Алеком Джеффрісом з Лестерського університету в 1985 році. Більшість послідовностей нуклеотидних ДНК кожних двох особин зазвичай ідентичні. Однак метод відбитків пальців використовує різні послідовності, що відрізняють різних людей. Двоє незнайомих людей навряд чи матимуть однакове зображення ДНК у певному локусі.

Генетичні відбитки пальців - не єдиний метод, а сукупність методів розрізнення цих різних послідовностей. Наприклад, метод профілювання STR використовує повторювані сайти, мінісателіти, посилені ланцюговою реакцією полімерази (ПЛР), щоб знайти кількість повторень у декількох локусах.

Таким чином, можна визначити особу людини, яка, як правило, навряд чи помилиться, за винятком однояйцевих близнюків з однаковими геномами.

При судово-медичній експертизі метод відбитків пальців використовується для виявлення підозрюваних з кров'ю, волоссям, слиною або спермою. Це вже призвело до затримання багатьох підозрюваних, навіть після оголошення вироку. Цей метод також використовується для визначення

ідентичності останків людини, тестів на батьківство, відповідності донорів, популяцій дикої природи та походження їжі. Цей метод також може бути використаний для перевірки гіпотез про походження етнічних груп [11].

Метод відбитків пальців вимагає, щоб певні закони мали юридичну силу. Зазвичай тест є добровільним, але може бути необхідним за рішенням суду чи заявою. Кілька юрисдикцій почали збирати бази даних, що містять кримінальну інформацію про ДНК.

Найбільші у світі бази даних ДНК підтримуються США (NDNAD) та Великобританією, кожна з яких містить понад 4,5 мільйона записів з 2007 року. Обсяг баз даних і право держави збирати дані стосуються деяких правозахисних організацій обох штатів [1].

1.3 Динамічні методи біометричної ідентифікації

Динамічні методи біометричної ідентифікації базуються на (поведінкових) характеристиках поведінки людини, тобто на характеристиках, характерних для підсвідомих рухів у процесі відтворення будь-якої дії.

1.3.1 Біометрична ідентифікація за рукописним почерком

Підпис - одна з класичних форм ідентифікації, яка впродовж століть використовується в юридичній практиці, банківській та комерційній діяльності. Автор приносить власноручний автограф і детально розробляє його. Бажано, щоб підпис не повторював звичайне написання літер і мав додаткові елементи (штрихи, букви, що перекриваються тощо).

Є два незалежних способи позначення [11]:

- ідентифікувати, намалювавши підпис на документі;
- визначити динаміку підпису, введеного на комп’ютері.

У першому методі порівнюються два зображення. Людина впорається з цим краще. Другий метод має дані про коливання пера при відтворенні підпису

в тривимірному просторі (Ks, B - координати і Z - вага на планшеті). З цим може впоратись лише комп’ютер.

Якщо система аналізу сигнатур враховує лише загальні параметри, то біометричний стандарт формулюється досить просто. Якщо враховувати локальні особливості (та сама функція, але для окремих елементів підпису), то біти підпису можуть з’являтися та зникати (об’єднуватись). Як результат, важко розділити підпис на частини. Розглядаються всі варіанти або вибираються зображення для середнього варіанту (показано на рисунку 1.10).

Однією з головних проблем цієї біометричної системи є залежність від психологічного стану людей та стабільність їх почерку.

Система розпізнавання почерку передбачає наявність планшетів. Може використовуватися будь-який (VACOM, CALCOM, Genius). Ці системи також можуть бути застосовані в сенсорних екранах пристроїв і часто використовуються для зберігання конфіденційних даних.

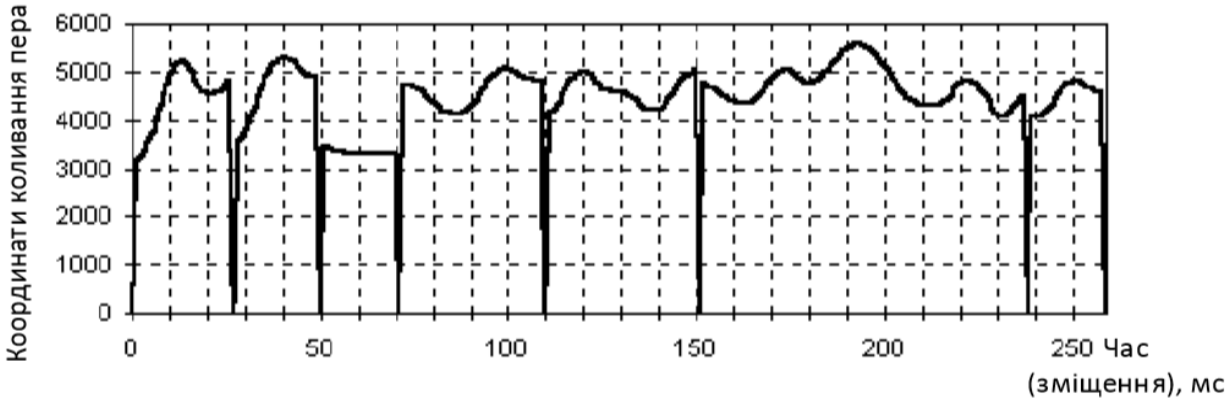


Рисунок 1.10 – Вертикальне коливання пера. Нульові значення функції відповідають моментам відриву пера від планшета

Переваги такого підходу [7]:

- низька ціна;
- практичність використання.

Недоліки:

- високий рівень помилок першого та другого типу;

- необхідність навчитися працювати з планшетом перед реєстрацією (процедура сильно відрізняється від написання звичайною ручкою через розмір пера, інші ваги та неможливість одночасного контролю процесу та результатів);

- тривалий час реєстрації користувача (більше 2 хвилин);

- користувачі можуть відображати нестабільний почерк, якщо вони не довіряють системі.

1.3.2 Біометрична ідентифікація за клавіатурним почерком

Сучасні дослідження показують, що клавіатура користувача має певну стійкість до рукописного вводу, що дозволяє однозначно ідентифікувати користувача. Інтервали часу між натисканням клавіш на клавіатурі та час їх утримання використовуються як вихідні дані. У той же час часові інтервали між натисканням клавіш характеризують швидкість роботи, а час утримання клавіш характеризує стиль роботи з клавіатурою - швидкий постріл або тихе погладжування [10].

Почерк клавіатури можливий наступними способами [10]:

- серія ключових фраз;

- набравши будь-який текст.

Основна різниця між цими двома методами полягає в тому, що в першому випадку використовується ключова фраза, введена користувачем під час реєстрації в системі (пароль), а в другому випадку використовуються ключові фрази, сформовані системою.

Існує 2 підходи: навчання та ідентифікація [11]. На етапі навчання користувач вводить тестові вирази, пропоновані кілька разів, одночасно обчислюючи та посилаючись на посилальні характеристики користувача. На етапі ідентифікації розрахункові оцінки порівнюються з еталонними, за якими робиться висновок про випадковість або невідповідність параметрів клавіатури.

Вибір тексту, який вводитиметься на системі, є дуже важливим кроком для нормальної роботи цієї системи. Вирази, запропоновані користувачем, повинні бути підібрані таким чином, щоб символи, що використовуються в них, повністю і однаково відповідали їхньому клавіатурному почерку.

Однак існує кілька обмежень у застосуванні цього методу на практиці. Застосування методу рукописного вводу на клавіатурі підходить лише для користувачів, що мають досить великий досвід роботи з комп'ютером та рукописного вводу, що виробляється на клавіатурі, тобто програмістів, переписувачів тощо.

В іншому випадку ймовірність неправильної ідентифікації користувача доступу значно збільшується, і це означає, що ця ідентифікація не може бути використана на практиці.

Спираючись на теорію набору тексту та ведення записів за допомогою клавіатури, може бути вказаний час формування рукопису, який досягає необхідної ймовірності ідентифікації користувача: приблизно 6 місяців [10].

Довідкові функції користувача, отримані на етапі системного навчання, дозволяють робити висновки про ступінь стабільності рукописного вводу користувача на клавіатурі та визначати довірчий інтервал дисперсії параметра для подальшої ідентифікації.

Важливим етапом завдання ідентифікації користувачів за допомогою рукописного вводу на клавіатурі є обробка основних даних. В результаті такої обробки вхідний потік даних поділяється на ряд ознак, що характеризують деякі якості ідентифікованої людини [11]. Ці функції, які підлягають статистичній обробці, дозволяє отримати певну кількість ознак користувацьких посилань.

Початковий етап обробки даних - фільтрація. На цьому етапі інформація про "сервісні" клавіші витягується з потоку даних - клавіші зі стрілками, функціональні клавіші тощо.

Потім надається інформація про такі характеристики користувача [11]:

- кількість помилок друку;

- інтервали між ключовими зверненнями;
- час утримання ключа;
- кількість перекриттів між клавішами;
- ступінь аритмічності при наборі;
- швидкість набору.

1.3.3 Біометрична ідентифікація за голосом

Існує багато способів складання коду розпізнавання голосу, як правило, поєднання частоти та статистичних його особливостей.

Розпізнавання голосу - одна з традиційних форм ідентифікації, яка використовується всюди [12]. Ви можете легко ідентифікувати абонента, не бачившись. Також можна визначити психологічний та емоційний стан голосу.

Оскільки розпізнавання голосу не вимагає особливих зусиль, триває робота над створенням голосового блокування та обмеження доступу до інформації.

На сьогоднішній день існує два методи ідентифікації людини за голосом, засновані на структурі мовного сигналу [12].

Індивідуальні відмінності у розподілі потужності сигналу в центральному спектрі - це перші категорії біометричних систем розпізнавання голосу. Вони базуються на декількох вузькосмугових фільтрах, які випромінюють голосові коливання різних частот (показано на рисунку 1.11).

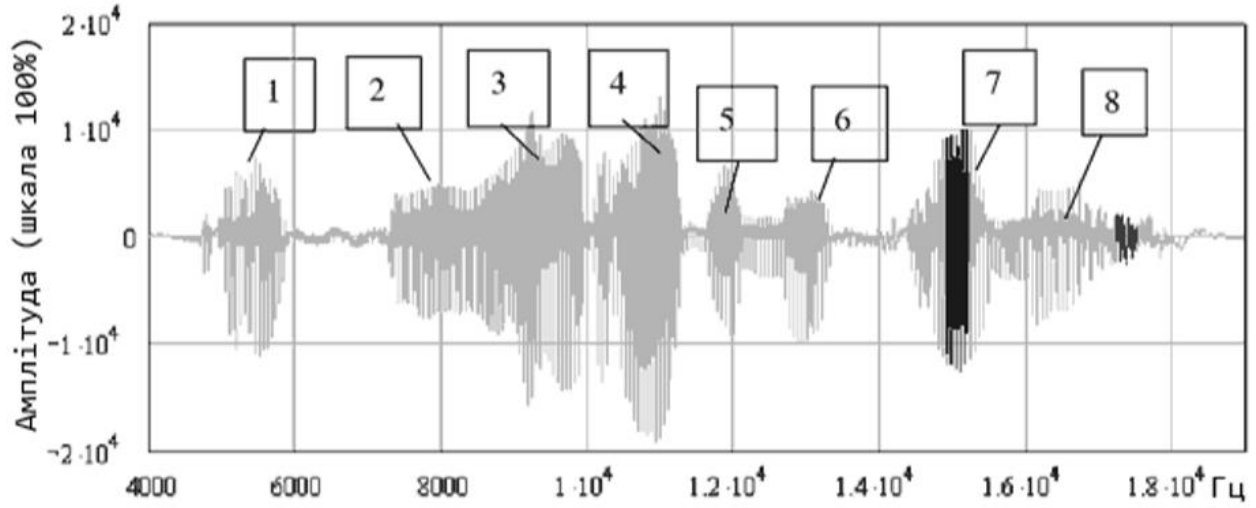


Рисунок 1.11 - Приклад голосової фрази і виділення з неї 8 фрагментів

Пропускна здатність фільтра вибирається при проектуванні системи, але вона не повинна бути занадто вузькою, щоб не покладатися на зміни в спектрі голосових частот. При цьому вони не повинні бути занадто широкими. Необхідно вибрати оптимальну ширину, достатню для надійної ідентифікації.

Зазвичай для збільшення значень при виборі частоти використовуються 16 розширювальних фільтрів (показано на рисунку 1.12). Це пов’язано з нестабільністю високих частот енергії (порівняно з низькими частотами).

Захист голосу легко передається, якщо ключова фраза перехоплюється або записується. Тому розробники зараз намагаються створити систему, яка захищена від перехоплення. Ви можете використовувати перевірку голосу з іншими засобами захисту. Наприклад, геометрія поверхні. Потім можна слідкувати за рухом губ та їх синхронізацією зі звуком.

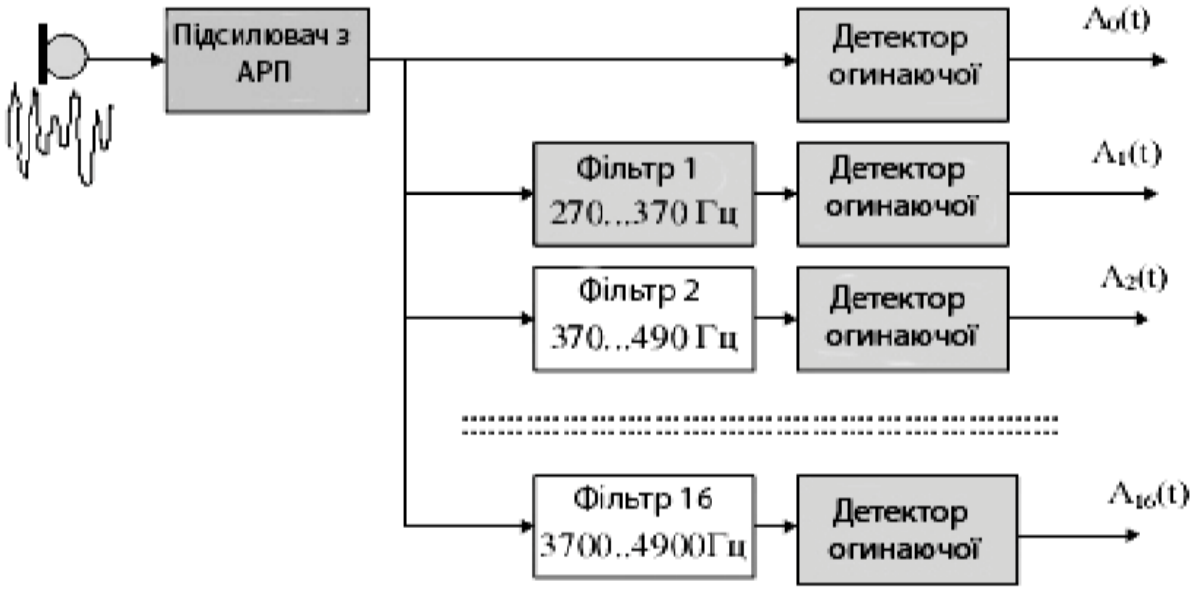


Рисунок 1.12 - Накладення фільтрів на голос

Один з ефективних способів захисту від перехоплення кодової фрази заснований на використанні мовної інформації, яка вводиться за допомогою чутливого динаміка ларингофону.

Ларингофон суттєво змінює індивідуальний колір звуку залежно від точки контакту з тілом (показано на рисунку 1.13).

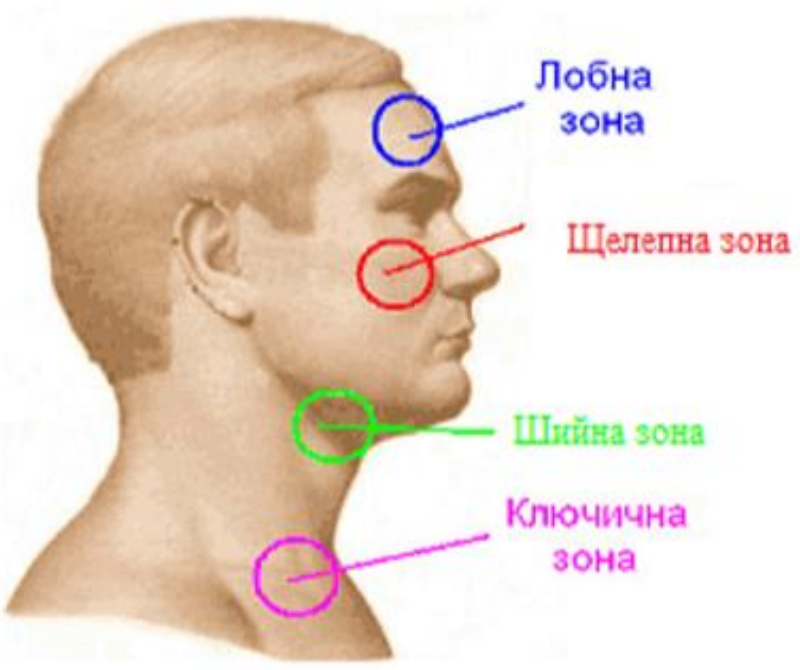


Рисунок 1.13 - Зони для запису інформації, що вводиться з ларингофона

Відсутність інформації про зону абстрагування сигналу ускладнює подолання біометричної ідентифікації, тому сигнал залежить від місця розташування ларингофона. Його неможливо описати сучасними технічними засобами через індивідуальну будову та взаємодію м'язів, кісток та хрящів конкретної людини.

При випромінюванні мовний сигнал коливається всередині тіла. Це виявляється складна звукова система різного роду. Як результат, кожна із контактних зон по-різному. На рисунку 1.14 зображений той самий сигнал, який приймається з шийної (зеленої) та ключичної (рожевої) області.

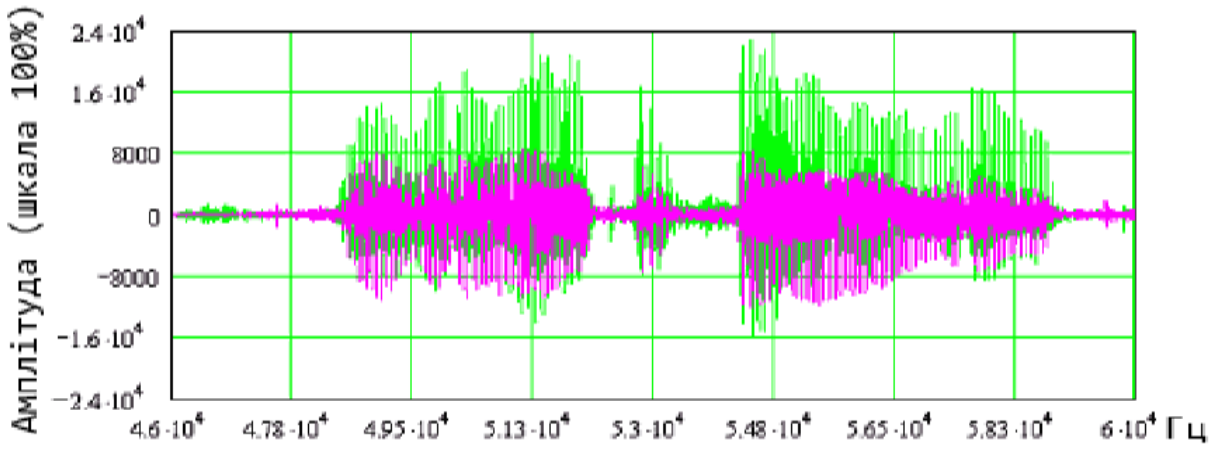


Рисунок 1.14 – Графік проходження звуку в різних зонах

Тривалість основного тону повторюється дуже докладно, але форма коливань зовсім інша. Отже, навіть якщо зловмисник має пароль та інформацію про місцезнаходження ларингофона, його неможливо ідентифікувати через різницю в голосі [12].

Переваги цього методу ідентифікації:

- звичайний спосіб ідентифікації особи;

- низька ціна (найнижча з усіх біометрій);

- не вимагає контакту.

Недоліки:

- високий рівень помилок першого та другого типу;

- необхідність спеціальної звукоізоляції в ідентифікаційних кімнатах;

- здатність перехоплювати фразу за допомогою диктофона;

- якість розпізнавання залежить від багатьох факторів (інтонація, швидкість публікації, психологічний стан, захворювання горла);

- необхідність підбору певних фраз.

1.4 Мультимодальні методи біометричної ідентифікації

Інтегрована (мультимодальна) біометрична система використовує різні програми для поєднання різних типів біометричних даних [13]. Це дозволяє використовувати два або більше типів розпізнавання біометрії. Мультимодальна система включає комбінацію розпізнавання відбитків пальців, контурів обличчя, голосу - плюс смарт-карту або будь-яку іншу комбінацію біометричних функцій. Ця розширена структура використовує весь спектр біометричних даних людини і може бути використана там, де потрібні кілька біометричних функцій [13].

Якщо для ідентифікації людини використовується одна біометрична характеристика (одна біометрична форма), існує ймовірність системної помилки. Це пов’язано з неправильним використанням системи, екологічними умовами та якістю зразків, наприклад:

1) не кожен має специфічні біометричні особливості. За різними даними, близько 5% населення не мають чітких відбитків пальців, особливо деформовані та відбитки пальців людей похилого віку та дітей. Все це також збільшує ймовірність помилки при реєстрації зразків біометрії в системі біометрії;

2) неправильна взаємодія користувача з біометричною системою в процесі реєстрації: вибір неправильного жесту тіла або виразу обличчя під час фотографування призводить до збільшення ймовірності неправильної ідентифікації;

3) подібність окремих біометричних ознак (наприклад, голосів чи почерку) у різних людей призводить до збільшення подібності. Це головним чином призводить до збільшення помилки ідентифікації.

Мультимодальні біометричні системи можуть подолати багато обмежень нелінійних систем, оскільки деякі біометричні особливості компенсують вади, властиві іншим характеристикам.

Переваги мультимодальної ідентифікації [13]:

- зменшити ймовірність відмови у реєстрації;

- збільшити охоплення населення за рахунок зменшення помилки відмови у реєстрації (замість однієї ознаки ми використовуємо іншу ознаку);

- підтримувати точність ідентифікації на великих базах даних;

- деякі особливості біометрії можуть заповнити недоліки, властиві іншим ознакам;

- зменшити кількість неправильних збоїв;

- зменшити чутливість до шуму та розширити діапазон умов навколишнього середовища, де це можна розпізнати за допомогою декількох методів;

- підвищення стійкості до нападів хуліганів та підробок - одразу декілька біометричних характеристик важко сформувати [7].

На рисунку 1.15 представлені статистичні дані щодо використання різних біометричних методів для ідентифікації людей за 2007 рік. На наступному рисунку 1.16 показано використання цих систем у 2018 році (надана компанією з аналізу ринку для біометрії, автоматизованих систем контролю доступу та захисту документів) [13].

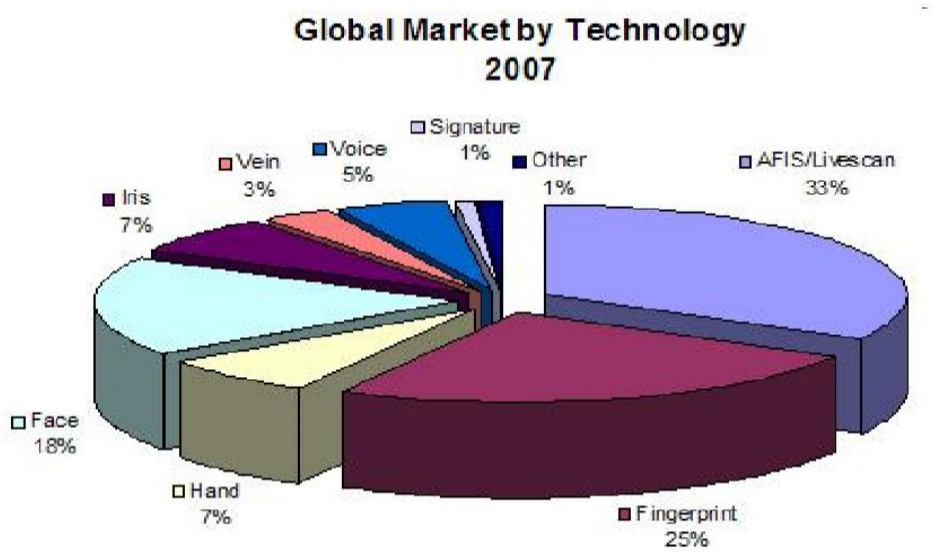


Рисунок 1.15 – Статистика 2007 (Acuity Market Intelligence)

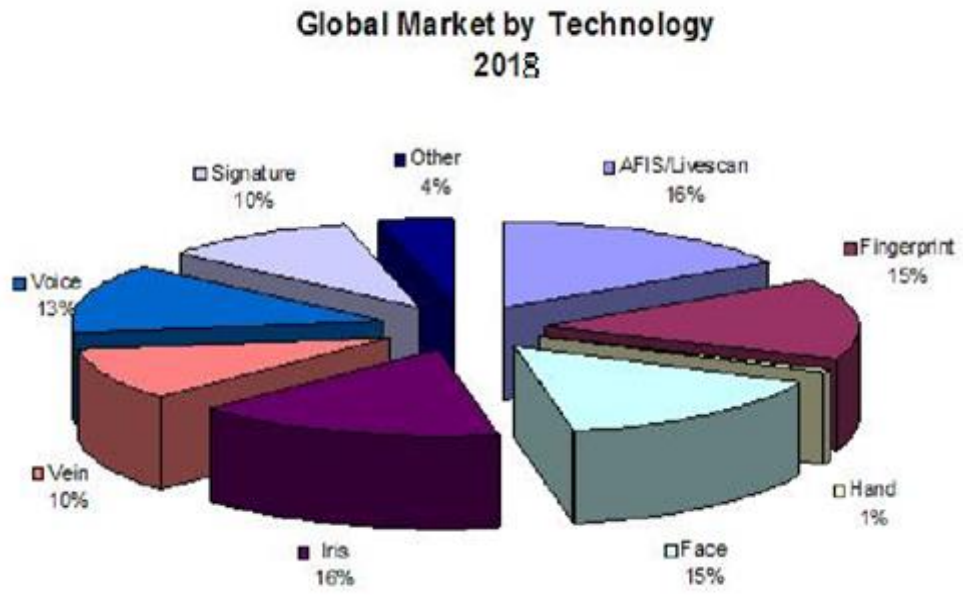


Рисунок 1.16 – Статистика 2018 (Acuity Market Intelligence)

Щоб підтвердити свою особу під час використання банкомату, мобільного телефону, планшета чи ноутбука, найбільш підходящими технологіями є біометрія обличчя та голосу, оскільки:

- "домашні" зразки голосу та обличчя легко отримати, не вимагають особливих навичок;

- для отримання зразків голосу та обличчя не потрібне спеціальне обладнання;

фотографія робиться за допомогою камери, а голос записується через мікрофон;

- фотографія обличчя та запис голосу є простими та зрозумілими для всіх, тому технологію легко побачити.

Слід зазначити, що останнім часом біометричні системи для розпізнавання голосу та обличчя мали набагато гірші показники (точність ідентифікації, розмір біометричної моделі тощо), ніж, наприклад, біометричні відбитки пальців. Однак за останні кілька років було досягнуто значного прогресу у розробці автоматизованих методів класифікації та машинного навчання, що наблизило ефективність цих методів до інших.

Поєднання голосової та лицевої біометрії є природним розвитком біометричних технологій завдяки широкому використанню відповідних «бімодальних» пристроїв: мобільних телефонів, комунікаторів, цифрових камер та відеокамер, ноутбуків. Наявність таких бімодальних пристроїв значно спрощує процес отримання біометричних зразків, процес зарахування людини до системи біометрії, зниження вартості самої системи тощо.

Висновки за розділом 1

1. Біометричні системи сьогодні є другим поколінням систем безпеки, оскільки біометрика використовує вимірювання окремих параметрів людини для їх ідентифікації. Актуальність розробки ІТ-біометричної ідентифікації виникає через зростаючу кількість засобів та інформаційних потоків, які необхідно захищати від несанкціонованого доступу, а саме: банківські, судово-медичні, системи контролю доступу, системи персональної ідентифікації, інформаційна безпека.

2. Статичні методи ідентифікації біометрії базуються на фізіологічних (статичних) характеристиках людини, тобто на унікальній рисі, яка надається їй і від народження. Переваги статичних методів включають низькі зусилля споживачів, а також низьку залежність від їх психологічного стану.

3. Динамічні методи розпізнавання біометрії базуються на (динамічних) поведінкових характеристиках людини, тобто на характеристиках, типових для підсвідомих рухів у процесі відтворення будь-якої дії. До переваг динамічної біометрії належать низькі витрати, оскільки їх можна вбудувати лише за допомогою програмного забезпечення (клавіатури, звукової карти, планшета, мобільного телефону - що вже можна вбудувати в апаратне забезпечення), а також швидкої зміни персонального комп’ютера. відтворене слово чи фразу.

4. Підсумовуючи, можна сказати, що мультимодальна біометрична ідентифікація використовується в системах, які вимагають особливих вимог безпеки. Використання біометричних інструментів впорядковує процес

ідентифікації, а також підвищує надійність систем безпеки. Для підтвердження особи при використанні банкомату, мобільного телефону, планшета чи ноутбука найбільш підходящі ІТ-біометричні дані особи та голосу.

РОЗДІЛ 2
ОЦІНКА НАЙБІЛЬШ ЗАХИЩЕНИХ БІОМЕТРИСЧНИХ СИСТЕМ ТА РОЗРОБКА НАЙБІЛЬШ ОПТИМАЛЬНОГО МУЛЬТИМОДАЛЬНОГО МЕТОДУ

2.1 Дослідження відомих біометричних параметрів людини, пов'язаних із помилками ідентифікації

Помилки першого та другого типів можна прийняти як дві основні ознаки будь-якої біометричної системи. Наприклад, в радіолокаційній теорії їх зазвичай називають "помилковими тривогами" або "відмовами цілей", а в біометрії найпоширенішими поняттями є FAR (коефіцієнт помилкового прийняття) і FRR (коефіцієнт помилкової відмови).

Перше значення характеризує ймовірність неправильного узгодження біометричних характеристик двох осіб. Інша можливість полягає у забороні доступу людині, яка має доступ [14]. Чим краща система, тим нижче значення FRR (помилка першого типу) при тих самих значеннях FAR (помилка другого типу). Іноді використовується відносно типовий EER - точка перетину графіків FRR та FAR (рис. 2.1).

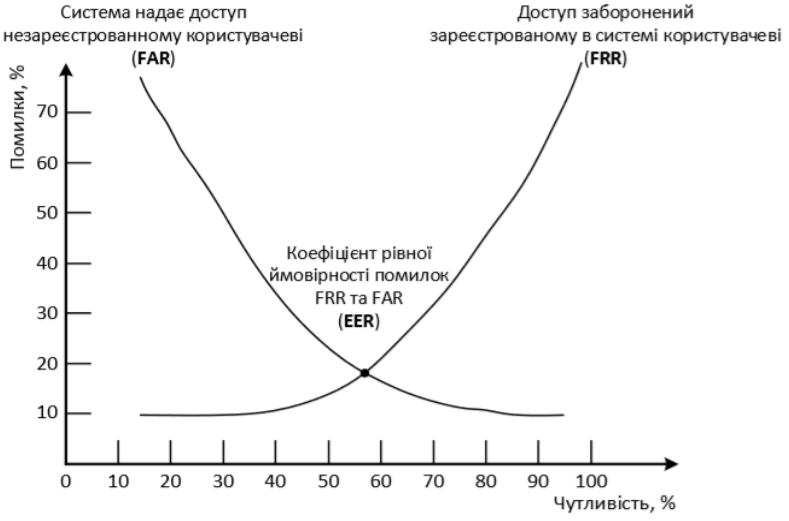


Рисунок 2.1 – Порівняльна характеристика EER

Щоб зрозуміти ймовірності FAR та FRR, можна оцінити частоту неточних збігів, якщо в транзитній організації встановлена система ідентифікації з персоналом *N*-осіб.

Ймовірність помилкового узгодження сканера відбитків пальців для бази даних із відбитком *N* дорівнює FAR · *N*. А щодня для людей *N* проходить через точку контролю доступу. Тоді ймовірність помилки за робочий день становить FAR · (*N* · *N*).

Звичайно, залежно від цілей системи ідентифікації, ймовірність помилки за одиницю часу може сильно відрізнятися, але якщо взяти одну допустиму помилку протягом робочого дня, ми отримаємо формулу 2.1:

$$FAR \times N^2 \approx 1 \Rightarrow N \approx \sqrt{\frac{1}{FAR}} \qquad (2.1)$$

Тоді очевидно, що стабільна робота системи ідентифікації при FAR=0.1%=0.001 можлива при чисельності персоналу *N*≈30.

Розпізнавання відбитків пальців - це найдосконаліший на сьогодні метод біометричної ідентифікації. Кожна людина має унікальний папілярний відбиток пальців, що дозволяє ідентифікувати.

Статистичні дані Verifinger SDK, отримані за допомогою сканерів відбитків пальців U.are.U DP, використовувались як джерела даних FAR та FRR. За останні 5-10 років функції дактилоскопії зробили великий крок вперед, тому ці цифри показують хороші середні показники сучасних алгоритмів.

Типове значення FAR для методу ідентифікації відбитків пальців становить 0,001%. З формули 2.1 ми робимо можливим стабільну роботу системи ідентифікації при FAR = 0,001% з персоналом *N*≈300.

Райдужка - це унікальна особливість людини. Метод є одним з найточніших серед біометричних.

Характеристики FAR та FRR райдужки є найкращими у класі сучасних біометричних систем (за винятком можливо розпізнавання сітківки). Представлені особливості бібліотеки алгоритму ідентифікації райдужної оболонки ока - EueR SDK, що відповідає випробуваному алгоритму з тих самих баз даних VeriEue. Типове значення FAR становить 0,00001% [14].

За формулою 2.1 $N \approx 3000$ - чисельність персоналу організації, де ідентифікація працівника є досить стабільною.

Тут варто згадати важливу особливість, яка відрізняє систему розпізнавання райдужки від інших систем. Використовуючи 1,3-мегапіксельну камеру, можна захопити два ока в одному кадрі. Оскільки ймовірності FAR і FRR статистично незалежні, при розпізнаванні парою очей значення FAR буде майже рівним квадрату значення FAR для одного ока. Наприклад, для FAR 0,001%, коли використовуються два ока, ймовірність неправильної толерантності становитиме 8-10%, а FRR лише вдвічі перевищує відповідне значення FRR для одного ока при FAR = 0,001% [14].

Тривимірне розпізнавання обличчя є складним завданням. Повні дані FRR та FAR для алгоритмів цього класу не доступні на веб-сайтах виробника. Але для найкращих моделей Bioscript (3D EnrollCam, 3D FastPass), яка працює за методом проекції шаблону, при FAR = 0,0047% FRR становить 0,103%. Вважається, що статистична надійність методу порівнянна з надійністю методу ідентифікації відбитків пальців [14].

Що стосується надійності, технологія порівнянна з розпізнаванням райдужної оболонки, в чомусь перевершує її і в чомусь поступається.

Для сканера Palm Wayne вказані значення FRR та FAR. На думку розробника FAR, 0,0008% FRR становить 0,01% [14].

Результати досліджень стабільності систем ідентифікації персоналу для різних біометричних методів наведені в таблиці. 2.1. додається у додатку Б.

Таким чином, підсумовуючи результати для методів, можна сказати, що сканування райдужки ока повинна використовуватися як метод біометрії, визнаних для середніх та великих об'єктів, а також для об'єктів з найвищими

вимогами безпеки. Для закладів, де працює персонал до сотні людей, доступ зі скануванням відбитків пальців буде оптимальним.

Системи 3D-розпізнавання обличчя дуже специфічні. Вони можуть знадобитися в тих випадках, коли розпізнавання не вимагає фізичного контакту або коли неможливо встановити систему контролю райдужки. Наприклад, якщо особу потрібно ідентифікувати без її участі, прихованої камери чи зовнішньої камери виявлення, це можливо лише за невеликої кількості об'єктів у базі даних та невеликого потоку людей, що потрапили на камеру.

2.2 Оцінка точності роботи та переваги мультимодальної біометричної ІТ ідентифікації персоналу перед унімодальними системами

На основі аналізу сучасних біометричних систем для розпізнавання людини в розділі 1 пропонується використовувати мультимодальну (бімодальну) систему ідентифікації, яка складається з двох ознак: обличчя та голосу.

Мультимодальна система біометричної ідентифікації визначає персонал як багатофакторний, що складається з двох основних статичних компонентів:

1) ідентифікація за образом людини;

2) ідентифікація допомогою фрази пароля.

В даний час розпізнавання обличчя виконується в режимі реального часу під час взяття або наближення обличчя до камери. Для реєстрації та ідентифікації достатньо трьох зображень.

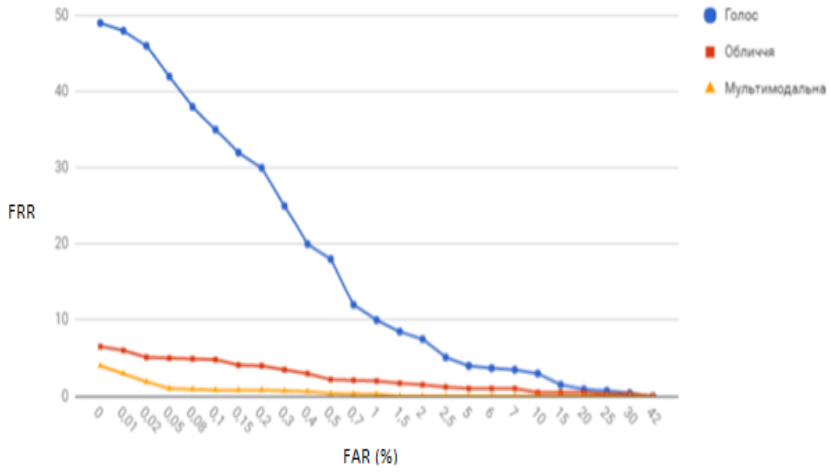
Розпізнавання голосу базується на використанні статичної фрази доступу. На етапі реєстрації фразу потрібно повторити кілька разів, щоб максимізувати надійність та оцінити мінливість вимови.

Мультимодальне рішення полягає в узагальненні результатів, отриманих за допомогою розпізнавання голосу та обличчя. Обробка цих модулів призводить до математичної схожості голосу та обличчя контрольної вибірки

користувачів, які ввели вхід під час аудіо / відеопотоку. На основі цих значень розраховуються ймовірності мультимодальної ідентифікації.

Рішення про доступ користувачів - це логічний план, який враховує наслідки всіх модулів системи ідентифікації. Для оцінки точності будь-якої біометричної системи зазвичай використовують характерні криві: ROC (прийняття функціональних ознак) або DET (помилка виявлення), які встановлюють взаємозв'язок між помилками FRR та FAR у таблиці 2.2. в додатку Б. Для мультимодальної роздільної здатності отримуємо таку криву DET (рис. 2.2).

Отже, з таблиці 2.2 (додаток Б) видно, що якщо ви використовуєте плаваючу або мультимодальну систему в організації з чисельністю персоналу: (осіб), система голосового зв'язку не втратить 48% (FRR) персоналу з доступом, обличчя - 6,5% (FRR), мультимодальні - 3% (FRR).



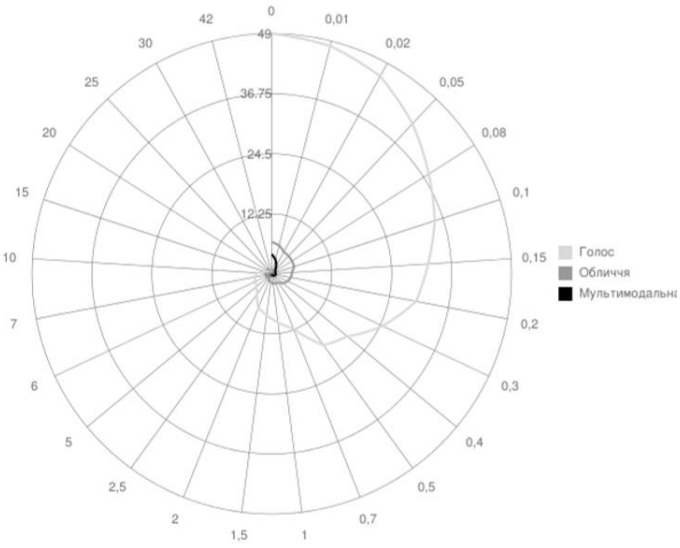


Рисунок 2.2 – Оцінка точності роботи біометричної системи (DET-криві)

При аналізі останнього рядка таблиці 2.2 (додаток Б) (15) видно, що якщо в організації 10 (осіб), то мультимодальна система у 33 рази надійніша ніж унімодальні системи: голос – 38% (FAR), обличчя – 42% (FAR), мультимодальна (голос та обличчя) – 1.2% (FAR) [15].

2.3 Вибір моделі для ідентифікації за голосом та обробка звукового сигналу

Завдання розпізнавання голосу залишається актуальною проблемою і сьогодні. Для оптимізації цього процесу в цьому розділі використовуються різні алгоритми та методи.

Розпізнавання мови в режимі реального часу за допомогою сучасних методів вимагає великих обчислювальних ресурсів, часто обмежених розмірів. Неможливість широко використовувати багато алгоритмів сьогодні, наприклад, у мобільних пристроях, змушує дослідників шукати більш ефективні та оптимізовані методи. Через свою простоту та малу кількість операцій на кожній ітерації розглянуті алгоритми можуть бути запропоновані як альтернатива існуючим методам розпізнавання голосу в режимі реального часу.

Кілька основних моделей використовуються в задачах розпізнавання мови та розпізнавання [15].

1) Моделі, що використовують приховані моделі Маркова (HMM), де модельований процес описується за допомогою скінченного набору станів, змінних на кожному кроці у довільному, але статистично передбачуваному напрямку (рис. 2.3). Такі підходи базуються на припущенні, що мову можна розділити на сегменти (провінції), де мовний сигнал можна вважати нерухомим, а перехід між цими провінціями є негайним. Також передбачається, що ймовірність спостережуваного символу, виробленого моделлю, залежить лише від

поточного стану моделі та не залежить від раніше створених символів. По суті, жодне з цих двох припущень не стосується мовного сигналу. Однак стандартні HMM є основою для більшості сучасних систем розпізнавання мови.

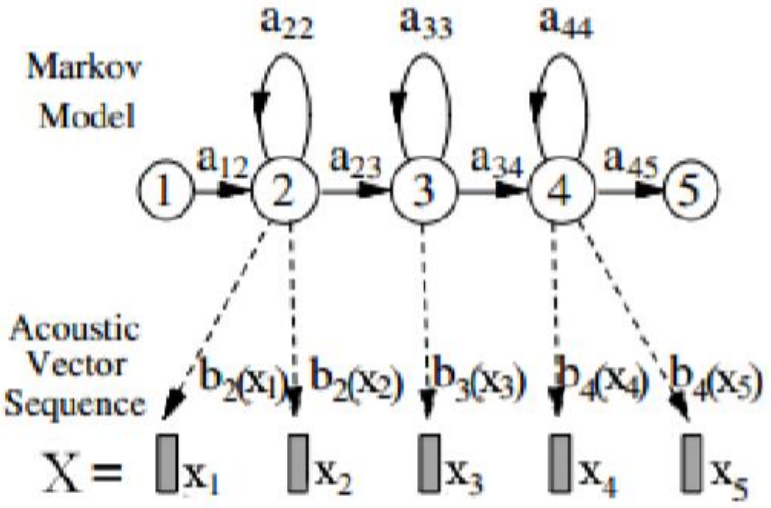


Рисунок 2.3 – Прихована модель Маркова

2) Моделі, що використовують метод опорних векторів (Support Vector Machine - SVM).

Метод SVM здійснює пошук такої гіперплощини в просторі всіх можливих входів для відокремлення та якомога далі від різних класів даних. Використання методу еталонного вектора дозволяє функцію розподілу з принаймні максимальною оцінкою очікуваного ризику (рівень помилки розподілу), а також використання лінійного класифікатора для роботи з нелінійно відокремленими даними, поєднуючи простоту та ефективність (рис. 2.4).

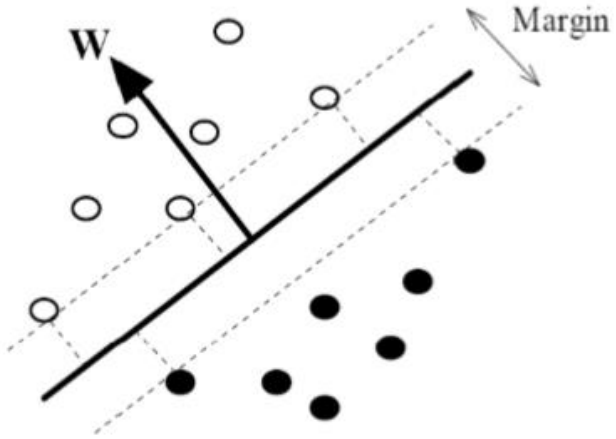


Рисунок 2.4 – Метод опорних векторів

2.4 Опис цифрової системи обробки голосу

Цифрова система обробки аудіосигналів дозволяє передавати аналоговий мовний сигнал у цифровій формі. В результаті аналого-цифрового перетворення (АЦП) безперервний сигнал перетворюється в ряд дискретних часових моделей, кожен з яких відсутній. Це число характеризує сигнал у точці з певною точністю. Точність відображення залежить від ширини діапазону отриманих чисел і, відповідно, від значного розміру АЦП.

Процес вилучення числових значень із сигналу називається кількісною оцінкою. Процес поділу сигналу на вибірки називається дискретизацією. Кількість проб за секунду називається частотою дискретизації [16]. У деяких випадках для визначення кількісної оцінки - кількості бітів, що обробляються в секунду, використовується поняття швидкості передачі даних (швидкості передачі даних).

Знаючи частоту та швидкість дискретизації, ви можете отримати ширину діапазону отриманих чисел.

Обробка звукових хвиль схематично показана на рисунку 2.5.

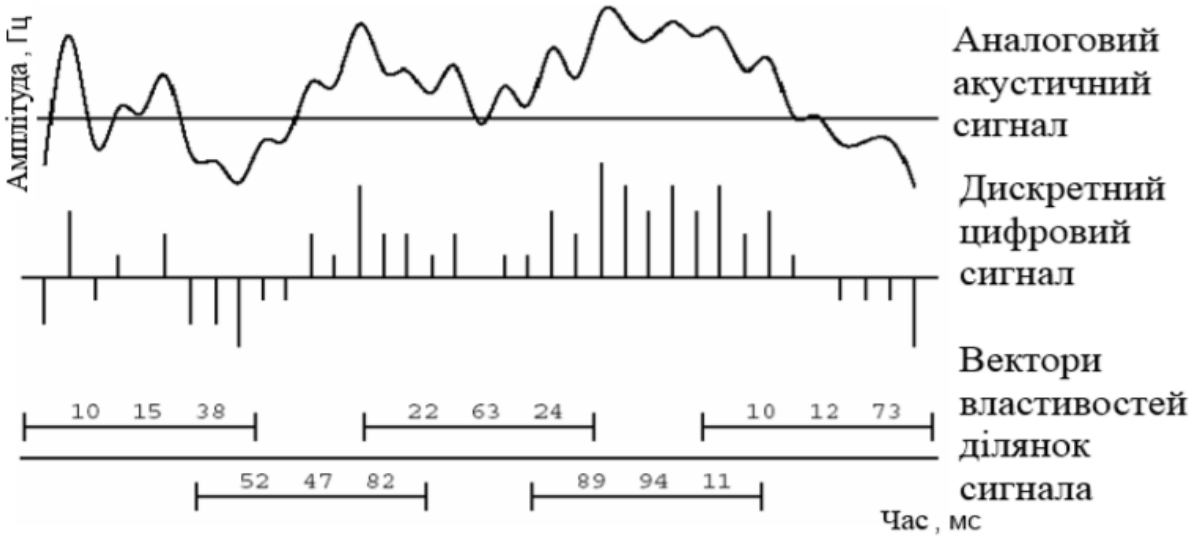


Рисунок 2.5 – Етапи обробки звукової хвилі

Аналоговий звуковий сигнал, що надходить від мікрофона, відбирається та кількісно визначається за допомогою АЦП. Так звана аудіореалізація, тобто цифровий запис публікації слів (аудіо), має форму серії вибірок аудіосигналу {Sk}. Використання слова (звуку) у цифровій обробці поділяється на ряд кадрів {Xi}. Кадр Ks (довжина *N*) є послідовністю зразків звукових сигналів S_1, S_2, ..., S_n. Довжина кадру фіксується в часі. Наприклад, при *N* = 100 та частоті дискретизації 8000 Гц це відповідає тривалості 12,5 мс. Часто кадри переміщуються назустріч один одному, так що інформація не втрачається на межі кадру. Фаза зсуву кадру - кількість послідовних аудіозаписів кадрів до кадру. Крок зсуву менше *N* (довжина кадру) означає, що кадри розташовані один над одним [16].

Крім того, у багатьох завданнях, таких як розпізнавання мови чи розпізнавання обличчя, кожен кадр вміщує деякі дані, які найкраще описують звук. Такі дані утворюють вектор властивостей (або вектор ознак). Математично це може бути або вектор простору *M R*, або набір функцій, або окрема функція.

Завдання розпізнавання окремих слів мови полягає в ідентифікації кожного слова, що надходить у систему, із заздалегідь визначеним класом. Існує багато різних факторів, які можуть негативно вплинути на точність системи розпізнавання - тон і стан динаміків, шум в навколишньому середовищі, швидкість вимови тощо.

Записати сигнал дуже складно, щоб він не вловлював чужий шум. На рисунках 2.6 і 2.7 показані амплітудні діаграми частоти сигналу в чистому вигляді і при тому ж сигналі, але з такими перешкодами, як білий шум. Білий шум - це шум, при якому амплітуда звукових частот різних частот рівномірно представлена, тобто середня інтенсивність звукових хвиль різних частот майже дорівнює [16].

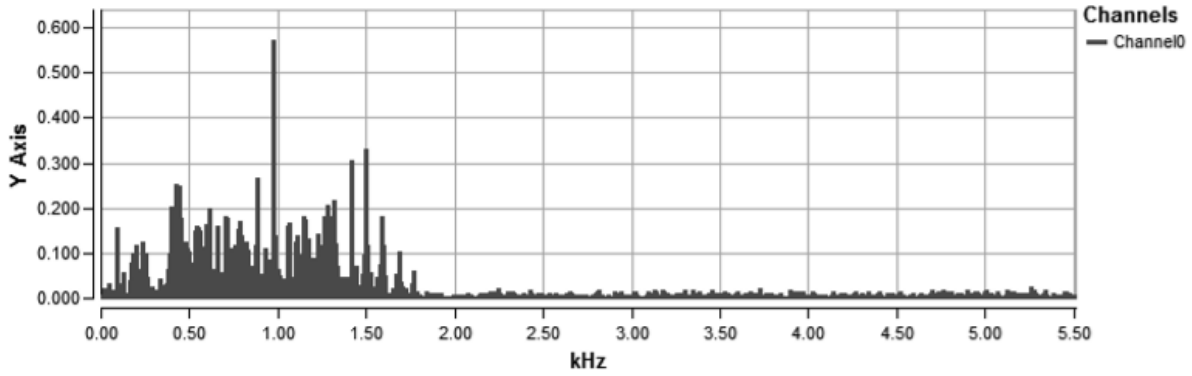


Рисунок 2.6 – Чистий сигнал

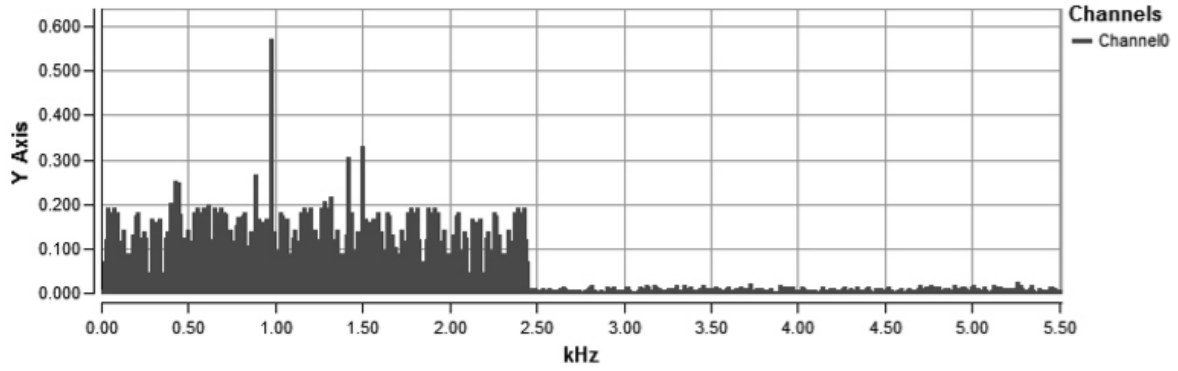


Рисунок 2.7 – Сигнал з білим шумом

Шумні сигнали сильно відрізняються від чистих. Для усунення негативного впливу шуму сигнал обробляється спеціальними частотними фільтрами. Частотний фільтр працює наступним чином: із усього набору гармонік, що складають звуковий сигнал, фільтр залишає лише ті частоти, які потрапляють у зазначену смугу пропускання.

Висновки за розділом 2

1. Підводячи підсумки результатів для різних методів ідентифікації, можна сказати, що сканування райдужки ока повинна використовуватися як метод біометрії, визнаний для середніх та великих об'єктів, а також для об'єктів з найвищими вимогами безпеки. Для закладів, де працює персонал до сотні людей, доступ зі скануванням відбитків пальців буде оптимальним. Системи розпізнавання 3D-зображень можуть знадобитися в тих випадках, коли для розпізнавання не потрібен фізичний контакт або неможливо встановити систему управління райдужкою.

2. При оцінці точності ідентифікації біометричних даних персоналу було виявлено, що якщо використовується надлишкова або мультимодальна система в організації з невеликою кількістю персоналу: система, що використовує сканування голос, отримає 48% (FRR) відмови доступу, сканування обличчя - 6,5% (FRR), мультимодальна - 3% (FRR), а якщо організація: мультимодальна система набагато надійніша, ніж унімодальні системи: сканування голосу - 38% (FAR) , обличчя - 42% (FAR), мультимодальне (голос та обличчя) - 1,2% (FAR) [16].

3. Використання методу опорного вектора (SVM) дозволяє функцію розподілу принаймні з максимальною оцінкою очікуваного ризику (рівень помилки розподілу).

РОЗДІЛ 3
РОЗРОБКА АЛГОРИТМІВ ФУНКЦІОНУВАННЯ МУЛЬТИМОДАЛЬНОГО ПРИСТРОЮ ДЛЯ РОЗПІЗНАВАННЯ КОРИСТУВАЧІВ

3.1 Дослідження та реалізація різних алгоритмів та методів виділення кордонів в обробці зображень

Алгоритми та методи граничної дискримінації при обробці зображень, які будуть вивчені та застосовані в цьому розділі: Лаплас, Гаусс-Лаплас, Собель, Прутт та Кірш. Всі алгоритми та методи реалізовані за допомогою збору зображень.

Вибір меж - це назва серії математичних методів, що використовуються для визначення контурів цифрового зображення, де яскравість зображення раптово змінюється або має інші неоднорідності [17].

Контури, в яких різкість змін яскравості зображення зазвичай організовані в ряд кривих лінійних відрізків, які називаються межами. Підсвічування меж є основним інструментом у обробці та розпізнаванні зображень, особливо у сферах виявлення та вибору особливостей. Отже, використання фільтра виділення меж на зображенні може значно зменшити обсяг даних, що обробляються, оскільки відфільтрована частина зображення вважається менш значущою і отримуються найважливіші структурні властивості зображення. Однак не завжди можна розрізнити межі реальних зображень середньої складності. Межі, вибрані з таких зображень, часто мають такі дефекти, як фрагментація (межові криві не пов'язані), відсутність меж або наявність помилок.

Стиснення - це проста математична операція, яка лежить в основі багатьох операторів обробки зображень. Стиснення дозволяє множенням двох наборів чисел, як правило, різних розмірів, але однакових за довжиною, щоб

отримати третій набір чисел того самого виміру. Це може бути використано при обробці зображень для застосування операторів, значення вихідних пікселів яких є простими лінійними комбінаціями деяких значень вхідних пікселів.

В контексті обробки зображення одним із вхідних рядків є лише відтінки сірого на зображенні. Другий рядок, як правило, набагато менший, він також двовимірний (хоча може мати товщину лише в один піксель) і називається ядром [17].

Вихідний код, наведений у Додатку В, застосовує метод Collapse Filter до класу Bitmap, дозволяє використовувати визначену користувачем матрицю та додатково перетворює вхідне зображення в шкалу сірого.

Були використані горизонтальні та вертикальні матриці перекриття, які наведені у Додатку Г.

На рисунку 3.1 показано початкове зображення.

Рисунок 3.1 – Оригінал зображення

3.1.1 Виділення кордону зображення методом Лапласа

Метод Лапласа щодо вибору межі зображення вважається одним із найпоширеніших [17].

Дискретний оператор Лапласа часто використовується в обробці зображень, наприклад, у програмах виявлення меж та оцінки руху. Дискретне перетворення Лапласа визначається як сума інших похідних виразу координат Лапласа і обчислюється як сума різниць найближчих сусідів центрального пікселя.

Для одновимірних, двомірних і тривимірних сигналів дискретний лапласіан можна задати як згортку з наступними ядрами [17]:

$$1D: \vec{D}_x^{\,2} = [1 \quad -2 \quad 1]$$

$$2D: D_{xy}^{\,2} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -4 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$

Або з діагоналями:

$$\text{Фільтр } 2D: D_{xy}^{\,2} = \begin{bmatrix} 1 & 1 & 1 \\ 1 & -8 & 1 \\ 1 & 1 & 1 \end{bmatrix}$$

$$\text{Фільтр } 3D: D_{xy}^{\,3} \approx$$

$$\text{для першої площини} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}; \text{ для другої} = \begin{bmatrix} 0 & 1 & 0 \\ 1 & -6 & 1 \\ 0 & 1 & 0 \end{bmatrix}; \text{ для третьої} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Ці ядра виводяться за допомогою дискретних часткових похідних.

Багато змін матриці / ядра можуть бути застосовані з результатами в межах від невеликого до досить явного.

Нижче досліджуємо два матричних впровадження: 3 × 3 та 5 × 5 (рисунки 3.2 та 3.3).

Лапласа 3 × 3:

```
public static Bitmap
Laplacian3x3Filter(this Bitmap sourceBitmap, bool grayscale = true)
{
    Bitmap resultBitmap =
            ExtBitmap.ConvolutionFilter(sourceBitmap, Matrix.Laplacian3x3,
                                        1.0, 0, grayscale);
    return resultBitmap;
}
public static double[,] Laplacian3x3
{get
 {
    return new double[,]

      { { -1, -1, -1, },
        { -1,  8, -1, },
          { -1, -1, -1,
                  }, };
 }
}
```

Рисунок 3.2 – Метод Лапласа 3 × 3

Лапласа 5 × 5:

```
public static Bitmap
Laplacian5x5Filter(this Bitmap sourceBitmap,
                        bool grayscale = true)
{
    Bitmap resultBitmap =
            ExtBitmap.ConvolutionFilter(sourceBitmap,
                                    Matrix.Laplacian5x5,
                                      1.0, 0, grayscale);
    return resultBitmap;
}
public static double[,] Laplacian5x5
{
  get
    {
        return new double[,]
        { { -1, -1, -1, -1, -1, },
          { -1, -1, -1, -1, -1, },
          { -1, -1, 24, -1, -1, },
          { -1, -1, -1, -1, -1, },
          { -1, -1, -1, -1, -1 } };
       }
   }
```

Рисунок 3.3 – Метод Лапласа 5 × 5

Матриця Лапласа 5 × 5 створює зображення результатів з чітко вираженими відмінностями. Акцентування меж виражається у великій кількості дрібних деталей, хоча матриця Лапласа чутлива до шумів зображення.

3.1.2 Вибір межі зображення відповідно до методу Гауса-Лапласа

Метод Гаусса-Лапласа розроблений для протистояння чутливості звичайного фільтра Лапласа (рис. 3.4) [18].

Рисунок 3.4 – Метод Гауса-Лапласа

Метод Гаусса-Лапласа для вилучення шуму із зображення застосовується до згладжування гауссовим туманом. Для оптимізації продуктивності ми можемо обчислити одну матрицю, що представляє гауссову затемнення та матрицю Лапласа.

public static Bitmap

LaplacianOfGaussian(this Bitmap sourceBitmap)

```
{
    Bitmap resultBitmap =

            ExtBitmap.ConvolutionFilter(sourceBitmap,
                        Matrix.LaplacianOfGaussian,
                                1.0, 0, true);
    return resultBitmap;
}
public static double[,] LaplacianOfGaussian
{ get
    {
        return new double[,]
        { { 0, 0, -1, 0, 0 },
          { 0,-1,-2,-1, 0 },
          {-1,-2,16,-2,-1},
          { 0,-1,-2,-1, 0 },
          { 0, 0, -1, 0, 0 } };
    }
}
```

3.1.3 Виділення кордону зображення методом Собеля

Метод припинення Собеля - ще одне загальне застосування розмежування [19]. Оператор Собеля використовується при обробці зображень для підкреслення меж. Це дискретний диференціальний оператор, який обчислює значення приблизного градієнта або норми градієнта для яскравості зображення.

Оператор Собеля заснований на загасанні зображення за допомогою невеликих знімних цілочисельних фільтрів у вертикальному та горизонтальному напрямках. Хоча градієнтне наближення є досить грубим, особливо у високочастотних частинах зображення [19].

Оператор використовує ядра 3 × 3, які обертають зображення для обчислення приблизних значень часткових похідних по горизонталі та вертикалі. Якщо

A - вихідне зображення, а Gk і Gu - два зображення, де кожна точка містить часткові похідні k та i, відповідно.

Вони обчислюються наступним чином [18]:

$$G_y = \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix} * A \text{ and } G_x = \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} * A$$

де $*$ позначає двовимірну операцію згортки.

Координата x зростає «направо», а y — «вниз». Для кожної точки зображення наближене значення градієнта обчислюється через наближенні значення часткових похідних:

$$G = \sqrt{G_x^2 + G_y^2}$$

а також напрямок градієнта:

$$\Theta = arctan\left(\frac{G_y}{G_x}\right)$$

де, наприклад, кут Θ рівний нулю для вертикальної границі, в якої темна сторона зліва.

Значення функції існує лише в звичайній мережі, тому, строго кажучи, не можна знайти похідні, але за умови неперервності функції можна застосувати кінцеві різниці, а саме оператор Собеля для наближення часткових похідних.

На відміну від описаних раніше фільтрів Лапласа, результати фільтра Собеля значно різняться. Фільтр Собеля, як правило, менш чутливий до шуму зображення, ніж фільтр Лапласа. Виявлені граничні лінії не настільки деталізовані, як граничні лінії, виявлені за фільтрами Лапласа (рис. 3.5).

Рисунок 3.5 – Оператор Собеля

```
    public static Bitmap
    Sobel3x3Filter(this Bitmap sourceBitmap,
                        bool grayscale = true)
{
      Bitmap resultBitmap =
              ExtBitmap.ConvolutionFilter(sourceBitmap,
                              Matrix.Sobel3x3Horizontal,
                                Matrix.Sobel3x3Vertical,
                                        1.0, 0, grayscale);
      return resultBitmap;
}
public static double[,] Sobel3x3Horizontal
{
    get
    {

        return new double[,]
            { { -1,   0,  1, },
            {   -2,   0,  2,  },
            {   -1,   0,  1,  }, };
    }

}
public static double[,] Sobel3x3Vertical
{
    get
    {
        return new double[,]
          { {1,   2,   1, },
            { 0,  0,   0,   },
            { -1, -2,   -1,  }, };
    }
}
```

3.1.4 Виділення кордону зображення методом Прюітта

Метод границі Прутта також є досить поширеним застосуванням. Оператор Прутта - це метод вибору межі при обробці зображень, який обчислює максимальну реакцію на кілька ядер згортки, щоб знайти локальну

орієнтацію межі на кожному пікселі [19]. Його створив доктор Джудіт Првітт для позначення меж медичних зображень.

Оператор обчислює градієнт інтенсивності зображення в кожній точці, надаючи напрямок найбільшого збільшення світла темряві та рівень зміни в цьому напрямку (рис. 3.6).

Оператор Прутта, як і Собель, використовує 3 × 3 ядра інверсії зображення для обчислення приблизних значень часткових похідних по горизонталі та вертикалі. Якщо A - вихідне зображення, а Gx і Gy - два зображення, де кожна точка містить часткові похідні x і y, відповідно. Вони обчислюються наступним чином:

$$G_y = \begin{bmatrix} -1 & -1 & -1 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{bmatrix} * A \text{ and } G_x = \begin{bmatrix} -1 & 0 & 1 \\ -1 & 0 & 1 \\ -1 & 0 & 1 \end{bmatrix} * A$$

де $*$ позначає двовимірну операцію згортки.

Координата x зростає «направо», а y — «вниз». Для кожної точки зображення наближене значення градієнта обчислюється через наближенні значення часткових похідних:

$$G = \sqrt{G_x^2 + G_y^2}$$

а також напрямок градієнта:

$$\Theta = a \tan 2(G_y, G_x)$$

де, наприклад, кут Θ рівний нулю для вертикальної границі, в якої темна сторона зліва.

```
    public static Bitmap
  PrewittFilter(this Bitmap sourceBitmap,

                    bool grayscale = true)
    {

        Bitmap resultBitmap =
          ExtBitmap.ConvolutionFilter(sourceBitmap,
```

```
                                    Matrix.Prewitt3x3Horizontal,
                                      Matrix.Prewitt3x3Vertical,
                                                1.0, 0, grayscale);
        return resultBitmap;
}
public static double[,] Prewitt3x3Horizontal
{
    get
    {
        return new double[,]
            { { -1,   0,  1, },
            {   -1,   0,  1,  },
            {   -1,   0,  1,  }, };
    }

}
public static double[,] Prewitt3x3Vertical
{
    get
    {
        return new double[,]
          {{   1,   1,    1, },
           {   0,   0,   0,   },
           { -1, -1, -1,    }, };
    }
}
```

Рисунок 3.6 – Оператор Прюітт

3.1.5 Виділення кордону зображення методом Кірша

Метод визначення межі Кірша часто застосовується у формі визначення межі Компаса [18]. Нижче реалізуються лише два компоненти: горизонтальний і вертикальний. Оригінальні зображення мають високий ступінь яскравості (рисунок 3.7).

Рисунок 3.7 – Оператор Кірша

Оператор бере одноядерну маску і обертає її з кроком у 45 градусів у кожному з восьми напрямків компаса. Граничне значення оператора Кірша обчислюється як максимальне значення на адресу:

$$h_{n,m} = max_{z=1,\dots,8} \sum_{i=1,\dots,8}^{1} \sum_{i=-1}^{1} g_{ij}^{(z)} \cdot f_{n+i,m+j}$$

де z перераховує напрями компас ядра.

$$g^{(1)} = \begin{bmatrix} 5 & 5 & 5 \\ -3 & 0 & -3 \\ -3 & -3 & -3 \end{bmatrix}, g^{(2)} = \begin{bmatrix} 5 & -3 & -3 \\ 5 & 0 & -3 \\ 5 & -3 & -3 \end{bmatrix}$$

```
    public static Bitmap
KirschFilter(this Bitmap sourceBitmap,
                    bool grayscale = true)
    {
        Bitmap resultBitmap =
                ExtBitmap.ConvolutionFilter(sourceBitmap,
                        Matrix.Kirsch3x3Horizontal,
                          Matrix.Kirsch3x3Vertical,
                                    1.0, 0, grayscale);
        return resultBitmap;
    }
    public static double[,] Kirsch3x3Horizontal
    {
        get
        {
            return new double[,]
            { {   5,   5,   5, },
              { -3, 0, -3, },
              { -3, -3, -3, },
              };
        }
    }
    public static double[,] Kirsch3x3Vertical
    {
        get
        {
            return new double[,]
             { {  5, -3, -3,
                    },
            {  5,  0, -3, },
              {  5, -3, -3, }, };
        }
    }
```

Дослідивши та застосувавши методи вибору меж зображень, можна вибрати найкраще для завдання розпізнавання людей. Обрали оператор Собеля, оскільки він менш чутливий до шуму зображення, а граничні лінії не настільки точні, як інші розглянуті фільтри.

3.2 Керування мультимодальним пристроєм ідентифікації об’єкта

Мультимодальні ІТ можуть подолати багато обмежень нелінійних систем, оскільки деякі особливості компенсують недоліки, властиві іншим особливостям.

Переваги мультимодальних ІТ [19]:

1) збільшити область застосування (одна функція відсутня, використовується інша);

2) зменшити неправильні помилки розпізнавання, розширити діапазон умови навколишнього середовища, з використанням декількох методів;

3) зменшити чутливість до шуму.

Мультимодальна ІТ для розпізнавання, розпізнавання та авторизації об’єктів поєднує дві біометричні функції: голос та обличчя [11].

Спочатку був розроблений алгоритм роботи модуля з аудіо (голосом): увімкнення пристрою, вибір режиму (запис або посилання), при виборі першого - є стереозвуковий сигнал, зменшення шуму та запис посилання на спектрограму ; коли обирається інший, пристрій отримує стереозвук у режимі реального часу, зменшує шум і порівнює його зі стандартним. Якщо запис не відповідає стандарту, тоді зазначений об'єкт не буде доступний (рисунок 3.8 a).

Потім був розроблений алгоритм роботи з модулем зображення: увімкнення пристрою, вибір режиму (дотримання стандартів або ідентифікації), вибір першого - отримання 3D-відеосигналів, налаштування зображення та збереження еталонного зображення; коли обирається інший - пристрій отримує 3D-відеосигнал у режимі реального часу, покриває зображення та порівнює їх зі стандартним. Якщо зображення людини не відповідає стандарту, то ідентифікований об'єкт буде недоступним (Рисунок 3.8 b).

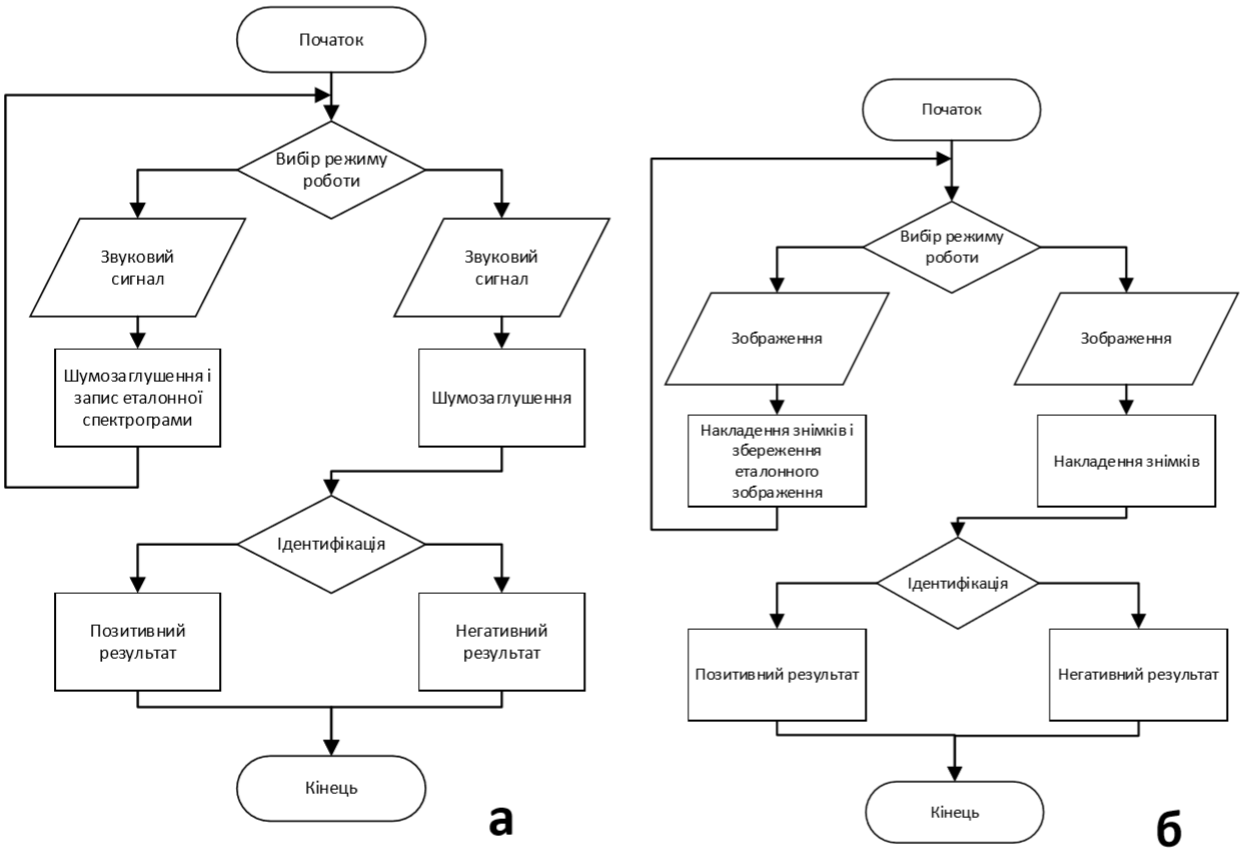


Рисунок 3.8 – Алгоритми роботи модулів звуку (а) і зображення (б)

В результаті проектування мультимодального пристрою розпізнавання об’єктів, до якого можуть бути застосовані описані вище алгоритми, пристрій отримав назву «3D комбінована камера з функцією ІЧ та стереозапису» [19] (рис. 3.9).

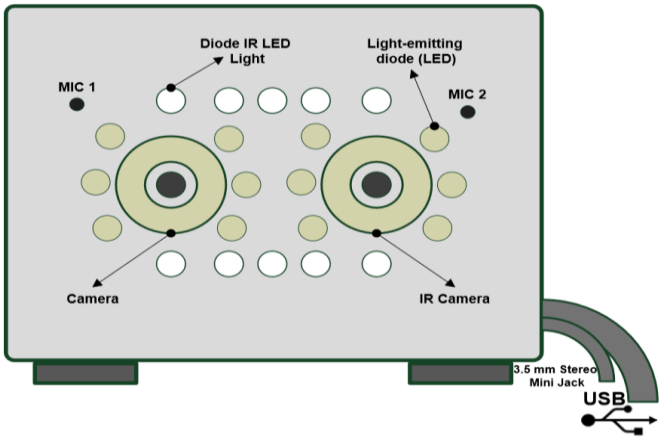


Рисунок 3.9 – Комбінована 3D камера з функцією ІЧ зйомки та записом стереозвуку

Переваги цього плану проекту:

1) отримати два зображення: звичайне та в інфрачервоному діапазоні. (При подальшій обробці зображення можна накладати зображення, які досягають розширеного динамічного діапазону зображення);

2) завдяки 2 мікрофонам можна записати стереозвук;

3) регульоване світлодіодне підсвічування для вечірньої зйомки або в місцях з низьким освітленням (включаючи 12 світлодіодів);

4) інфрачервоні ліхтарі для нічної зйомки. Завдяки 10 ІЧ-діодам та ІК-камері відстань нічної зйомки знаходиться в межах 15 метрів;

5) USB-з'єднання для фотографування та MiniJack 3,5 мм для підключення мікрофонів. Для цього не потрібно додаткове джерело живлення;

6) низька ціна.

Перший прототип мультимодального пристрою розпізнавання об'єктів складався з двох відеокамер: однієї інфрачервоної та звичайної, 12 світлодіодів з регульованою яскравістю, 2 мікрофонів та схеми для цих пристроїв. Структурна схема показана на рисунку 3.10.

Метод ідентифікації об'єктів за допомогою мультимодального пристрою, що поєднує дві функції [20]:

– звук і зображення, що зберігаються в базі даних (БД), а потім доставляються до алгоритму порівняння, що характеризується наявністю комбінованої камери, що містить нормальний та інфрачервоний (ІЧ), який використовуються для формування спрямування зразків зображень із розширеним динамічним діапазоном та додавання їх до бази даних;

– два мікрофони, що використовуються для формування стереозвукового сигналу та додавання їх до бази даних;

– регульоване світлодіодне підсвічування, що дозволяє знімати вночі або в приміщеннях без освітленого освітлення;

– інфрачервоні ліхтарі, що дозволяють знімати вночі;

– схема перемикання, яка дозволяє одночасно підключити обидві камери до одного USB і не вимагає додаткового живлення;

– один 3,5-мм стерео міні-роз'єм для підключення двох мікрофонів.

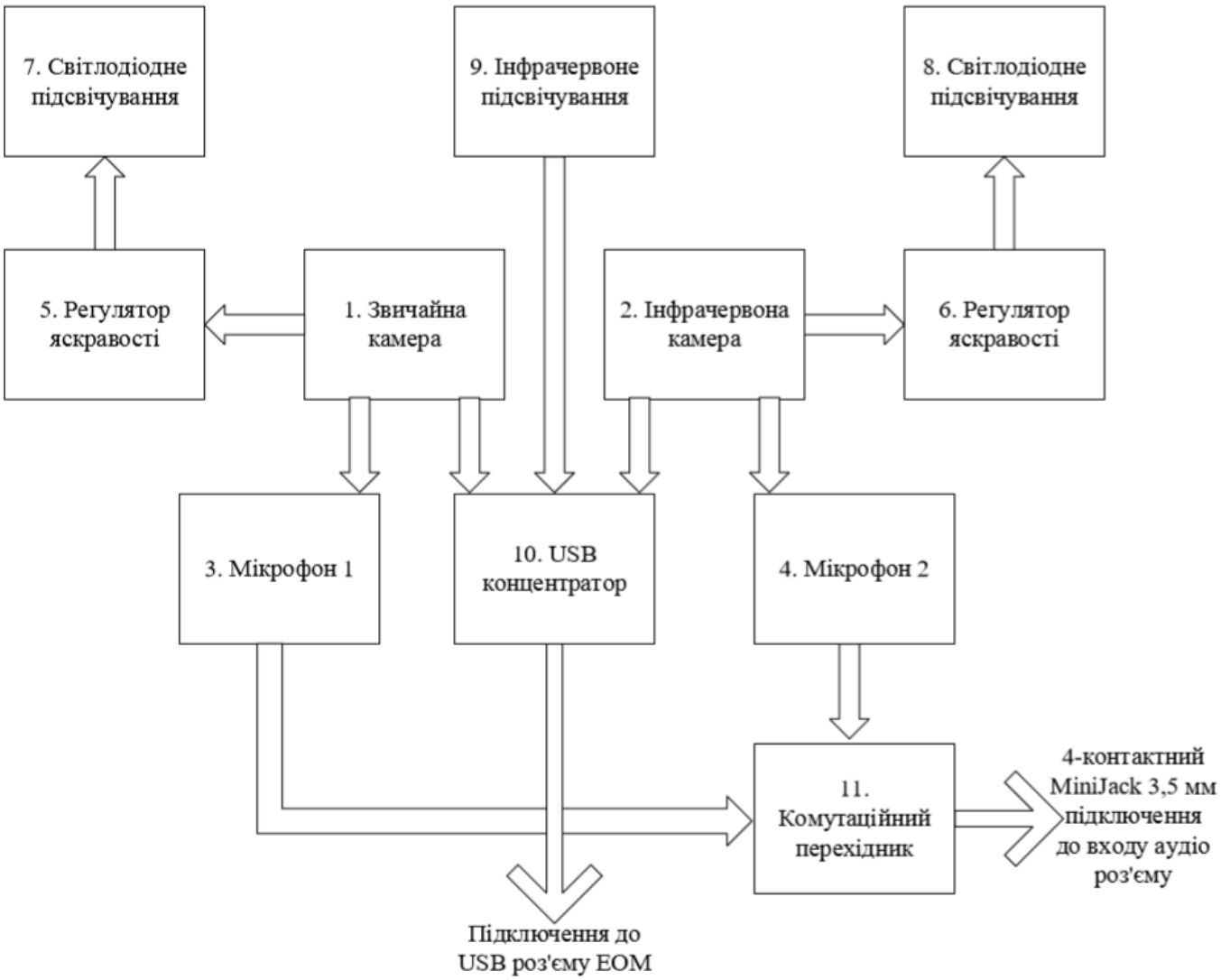


Рисунок 3.10 – Структурна схема мультимодального пристрою для розпізнавання об’єктів

Ідентифікація ІТ-об'єктів за допомогою біометричних методів має значні переваги. Використовуючи мультимодальний підхід, що враховує багато особливостей біометрії, можна зменшити кількість людей, біометрична ідентифікація яких неможлива на порядок, і значно підвищити захист інформаційних ресурсів від несанкціонованого доступу загалом.

Мультимодальний пристрій розпізнавання об’єктів знімає багато обмежень нелінійних систем, оскільки деякі параметри компенсують вади, властиві іншим параметрам, поєднуючи дві функції: розпізнавання звуку та зображення, область застосування збільшення, зменшення помилок помилкової ідентифікації та чутливість.

3.3 Реалізація розробленого алгоритму створення еталону зображення засобами мови HTML5 та JavaScript

Щоб застосувати вдосконалений алгоритм для створення стандартів зображень та подальшого шифрування біометричних зразків, використовуємо мови веб-програмування: HTML5 та JavaScript, а також спеціальну мову CSS (каскадні таблиці стилів) для візуального представлення сторінок, написаних мовами позначок.

На рисунку 3.11 показана головна сторінка створеного сайту, яка має таку структуру: головна сторінка, база даних, публікації та шифрування. Структура кожної окремої сторінки включає: заголовок (верх сторінки), навігацію (меню навігації), меню (меню правого розділу), пункт (основна частина сторінки) та нижній колонтитул (унизу сторінки).

Загалом сайт використовує 14 різних стилів, які перелічені в розділі <chairs> ... </chairs> та мають регульований дизайн.

Рисунок 3.11 – Головна сторінка створеного сайту Bondarenko Biometry

Першим кроком у роботі зі сторінкою є додавання біометричної функції для цієї операції, потрібно натиснути на «Додати», і завантажити нову - «Видалити» (рис. 3.12). Після того, як біо-функція відображається у браузері, можна переходити до наступних кроків.

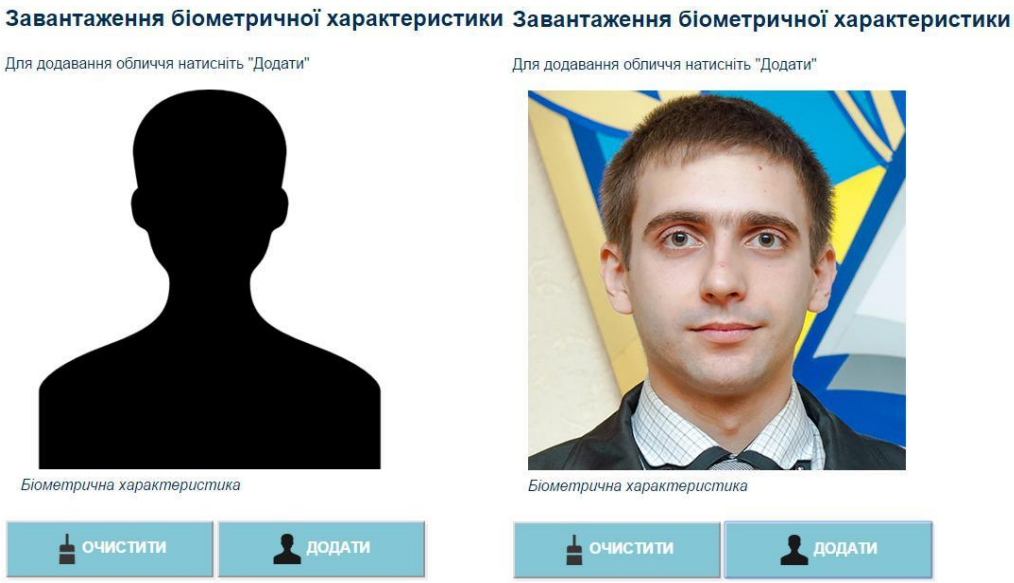


Рисунок 3.12 – Завантаження біометричної характеристики

Другий та третій кроки – це знебарвлення та виділення області ідентифікації (рисунок 3.13).

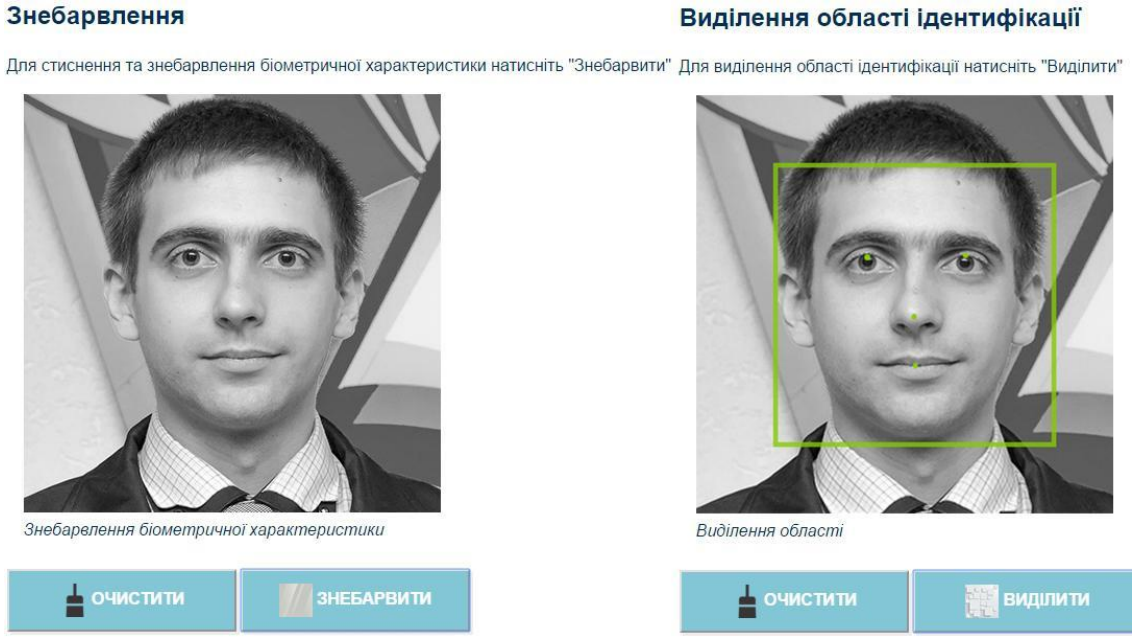


Рисунок 3.13 – Попередня обробка біометричного зразка

Четвертий крок – це виділення кордонів та додавання еталону до БД (рисунок 3.14).

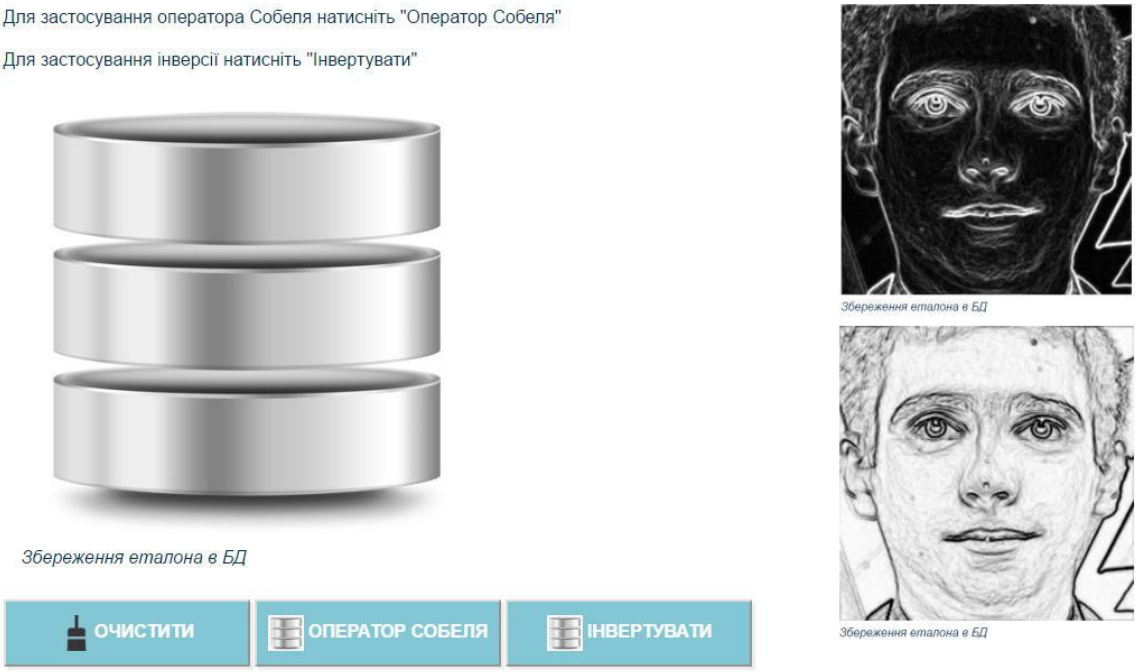


Рисунок 3.14 – Виділення кордонів та додавання еталону до БД

П’ятий, останній крок, реалізує шифрування еталона засобами CryptoJS (рисунок 3.15). Більш докладний опис наведено у додатку 3.

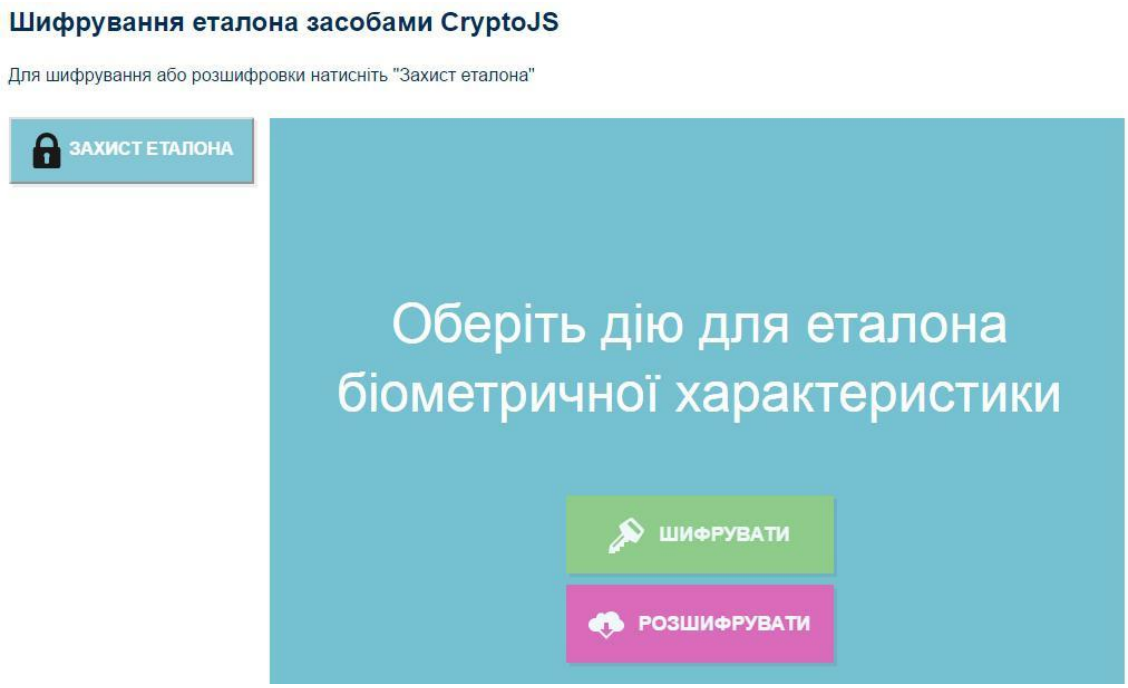


Рисунок 3.15 – Шифрування та розшифровка еталона засобами CryptoJS

Висновки за розділом 3

1. Алгоритми та методи, досліджені та застосовані для граничної дискримінації при обробці зображень: Лаплас, Гаусс-Лаплас, Собель, Пруйт та Кірш шляхом згинання зображення. Був обраний оператор Собеля, що найкраще підходить для нашого завдання розпізнавання людини, оскільки він менш чутливий до шуму зображення, а граничні лінії не округлені настільки детально, як у інших розглянутих фільтрах.

2. Розроблений, експлуатований та випробуваний мультимодальний пристрій розпізнавання об’єктів: «Комбінована 3D-камера з ІЧ-записом та стереозаписом», що складається із звичайної та ІЧ-камери, що утворюють еталонний зразок зображення з розширеним динамічним діапазоном.

3. Алгоритм створення, шифрування та подальшого зберігання стандартів біометричних характеристик із використанням сучасних мов веб-

програмування: HTML5 та JavaScript, а також спеціальної мови CSS (каскад таблиць стилів) для подання сторінок, написаних мовами, що візуально позначають.

ВИСНОВКИ

У дипломній роботі вирішено актуальну науково-технічну задачу розробки інформаційної технології для ідентифікації персоналу на основі комплексу біометричних параметрів з використанням поєднання статично-динамічних методів розпізнавання та удосконаленням методів створення еталонних зразків.

Ідентифікація персоналу, із застосуванням мультимодальних біометричних методів, має суттєві переваги. Завдяки поєднання методів, що враховують відразу кілька біометричних характеристик, можна підвищити захищеність інформаційних ресурсів від несанкціонованого доступу загалом.

Основні результати дипломної роботи:

1. Проведено аналіз сучасних ІТ та методів ідентифікації персоналу за біометричними параметрами. Виявлено їх переваги та недоліки. Запропоновано комплексний підхід на основі даних Acuity Market Intelligence, який включає комбінацію голосу та обличчя – мультимодальний метод.

2. Розглянуто та класифіковано існуючі характеристики статичних біометричних систем, пов’язаних з помилками ідентифікації, для визначення доцільності використання біометричної технології в залежності від початкових умов, а також визначено переваги мультимодальних ІТ перед унімодальними системами.

3. Досліджено та реалізовано алгоритми та методи для виділення кордонів в обробці зображень: Лапласа, Гауса-Лапласа, Собеля, Прюітта та Кірша за допомогою згортання зображення. Обрано оператор Собеля, найкращий для задачі розпізнавання людини, тому що він менш чутливий до шуму зображення та лінії кордону не так точно гранульовані, як у інших розглянутих фільтрів.

4. Спроектовано, реалізовано та випробувано мультимодальний пристрій для розпізнавання об’єктів: «Комбінована 3D камера з функцією ІЧ зйомки та

записом стереозвуку», яка складається зі звичайної та ІЧ камери, за допомогою яких формується еталонний зразок зображення з розширеним динамічним діапазоном.

5. Реалізовано розроблений алгоритм створення еталону біометричної характеристики, подальше її шифрування та зберігання шляхом використання сучасних мов Web-програмування: HTML5 та JavaScript, а також спеціальну мову CSS (каскадні таблиці стилів), щоб візуально представити сторінки, написаних мовами розмітки даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Горбійчук М. І. Комп'ютерна система контролю доступу з використанням авторизації за голосом / М. І. Горбійчук, Р. Р. Соловій. // Методи та прилади контролю якості. – 2014. – №2. – С. 98–105.

2. Газин А. И. Особенности голосовой аутентификации личности [Електронний ресурс] / А. И. Газин. – 2010. – Режим доступу до ресурсу: cyberleninka.ru/article/n/osobennosti-golosovoy-autentifikatsii-lichnosti.pdf.

3. Прудник А. М. Биометрические методы защиты информации / А. М. Прудник, Г. А. Власова, Я. В. Рощупкин. – Минк: БГУИР, 2014. – 123 с.

4. Acuity Market Intelligence [Електронний ресурс]. – Режим доступу до ресурсу: http://www.acuity-mi.com.

5. Задорожный В. Обзор биометрических технологий / В. Задорожный. // Конфидент. – 2003. – №5.

6. Моржаков В. Современные биометрические методы идентификации / В. Моржаков, А. Мальцев. // БДИ. – 2009. – №2.

7. Кумченко Ю. О. Аналіз основних характеристик біометричних систем розпізнавання на основі поширених помилок ідентифікації / Ю. О. Кумченко, А. І. Купін // Сучасні інформаційні технології 2013: Матеріали третьої Міжнародної конференції студентів і молодих науковців (25–26 квітня 2013 р.). – Одеса, 2013. – С. 112–113.

8. Кумченко Ю. О. Оцінка точності роботи та переваги мультимодальної біометричної інформаційної технології ідентифікації персоналу / Ю. О. Кумченко // IX Всеукраїнська науково-практична WEB конференція аспірантів, студентів та молодих вчених «Комп'ютерні інтелектуальні системи та мережі»: 22–24 березня 2016 р.: матер. – Кривий Ріг, 2016. – С. 92–94.

9. Брюхомицкий Ю. А. Метод обучения нейросетевых биометрических систем на основе копирования областей / Ю. А. Брюхомицкий, М. Н. Казарин //

Перспективные информационные технологии и интеллектуальные системы. Электронный журнал. – 2003. – №3. – С. 17–23.

10. Kumchenko У. Multimodal Biometric System Using Face and Speech / У. Kumchenko // Advanced Computer Systems and Networks: Design and Application: Proceedings of the 6-th International Conference ACSN 2013 (September 16 18, 2013). – Lviv, 2013. – P. 163–164.

11. Абдуллаева Ф. Д. Классификационная модель биометрической идентификации граждан / Ф. Д. Абдуллаева // Институт информационных технологий НАНА, Баку, Азербайджан. – 2006.

12. Граничин О. Н. Рандомизированный алгоритм стохастической аппроксимации в задаче самообучения / О. Н. Граничин, О. А. Измакова // Автоматика и телемеханика. – 2005. – №8. – С. 52–63.

13. Dan Tran, Michael Wagner and Tongtao Zheng, “A Fuzzy approach to Statistical Models in Speech and Speaker Recognition”, IEEE International Fuzzy Systems Conference Proceedings, Korea. pp. 1275-1280, 1999.

14. Christopher J. C. Burges, “A Tutorial on Support Vector Machines for Pattern Recognition”, Kluwer Academic Publishers, Boston, 1998.

15. Шалымов Д. С. Рандомизированный алгоритм стохастической аппроксимации в задаче распознавания отдельных слов речи / Д. С. Шалымов. // Санкт-Петербургский государственный университет. – 2006. – С. 207–218.

16. Сергиенко А. Б. Цифровая обработка сигналов / А. Б. Сергиенко. – СПб: Питер, 2006. – 751 с.

17. Аверченко А. П., Преобразование Фурье и преобразование Хартли / А. П. Аверченко, В. К. Воропаев, Б. Д. Женатов // Технические науки в России и за рубежом: материалы III междунар. науч. конф. (г. Москва, июль 2014 г.). – М.: БукиВеди, 2014. – С. 22–24.

18. P. Viola and M.J. Jones, «Rapid Object Detection using a Boosted Cascade of Simple Features», proceedings IEEE Conf. on Computer Vision and Pattern Recognition (CVPR 2001), 2001.

19. P. Viola and M.J. Jones, «Robust real-time face detection», International Journal of Computer Vision, vol. 57, no. 2, 2004., pp.137–154.

20. Шмаглит Л. Применение методов машинного обучения к задаче автоматического распознавания пола и возраста людей по изображению лица [Електронний ресурс] / Л. Шмаглит, В. Хрящев // Ярославский Государственный Университет имени П.Г.Демидова. – 2011. – Режим доступу до ресурсу: http://graphicon.ru/html/2011/conference/gc2011shmaglit.pdf.

21. Kumchenko У. О. Improved Algorithm for Creating a Template for the Information Technology of Biometric Identification / У. О. Kumchenko, A. I. Kupin // Metallurgical and Mining Industry. – 2015. – № 4. – P. 7–10.

ДОДАТКИ

ДОДАТОК А

Таблиця 1.1

Сучасні біометричні системи ідентифікації персоналу

Назва	Виробник	Біоознака	Примітки
SACcat	SAC Technologies	Рисунок шкіри пальця	Приставка до комп'ютера
TouchLock, TouchSafe, TouchNet	Identix	Рисунок шкіри пальця	СКУД об'єкта
Eye Dentification System 7,5	Eyedentify	Рисунок сітківки ока	СКУД об'єкта (моноблок)
Ibex 10	Eyedentify	Рисунок сітківки ока	СКУД об'єкта (порт, камера)
eriprint 2000	Biometric Identification	Рисунок шкіри пальця	СКУД універсал
ID3D-R Handkey	Recognition Systems	Рисунок долоні руки	СКУД універсал
HandKey	Escape	Рисунок долоні руки	СКУД універсал
ICAM 2001	Eyedentify	Рисунок сітківки ока	СКУД універсал
Secure Touch	Biometric Access Corp.	Рисунок шкіри пальця	Приставка до комп'ютера
BioMouse	American Biometric Corp	Рисунок шкіри пальця	Приставка до комп'ютера
Fingerprint Identification Unit	Sony	Рисунок шкіри пальця	Приставка до комп'ютера
Secure Keyboard Scanner	National Registry Inc.	Рисунок шкіри пальця	Приставка до комп'ютера
Рубеж	НПФ «Кристалл»	Динаміка підпису, спектр голосу	Приставка до комп'ютера
Дакточип Delsy	Элсис, НПП Электрон (Россия), Опак (Белоруссия), P&P (Германия)	Рисунок шкіри пальця	Приставка до комп'ютера
BioLink U-Match Mouse, SFM-2000A	BioLink Technologies	Рисунок шкіри пальця	Стандартна миша з вбудованим сканером відбитка пальця
Біометрична система захисту комп'ютерної інформації Дакто	ОАО «Черниговский завод радиоприборов»	Біологічно активні точки та капілярні лінії шкіри	Окремий блок

Таблиця 1.2

Технічні характеристики деяких сучасних біометричних систем

Модель	Принцип дії	Ймовірність помилкової відмови, %	Ймовірність помилкового допуску, %	Час ідентифікації, с
Eye Dentify	Параметри ока	0,001	0,4	1,5-4
Iriscan	Параметри зіниці	0,00078	0,00068	2
Identix	Відбиток пальця	0,0001	1,0	0,5
Startek BioMet	Відбиток пальця	0,0001	1,0	1
Partners Recognition	Геометрія руки	0,1	0,1	1
Systems	Геометрія руки	0,1	0,1	1
«Кордон»	Відбиток пальця	0,0001	1,0	1
DS-100	Відбиток пальця	0,001	-	1-3
TouchSafe Personal(8)	Відбиток пальця	2	0,001	1
Eyedentify ICAM 2001 (Eyedentify)	Параметри сітківки ока	0,4	0,0001	1,5-4
Iriscan (Iriscan)	Параметри райдужної оболонки ока		0,00078	2
FingerScan (Identix)	Відбиток пальця	1,0	0,0001	0,5
TouchSafe (Identix)	Відбиток пальця	2,0	0,001	1
TouchNet (Identix)	Відбиток пальця	1,0	0,001	3
Startek	Відбиток пальця	1,0	0,0001	1
1D3D-R NDKEY (Recognition Systems)	Геометрія руки	0,1	0,1	1
U.areU. (Digital Persona)	Відбиток пальця	3,0	0,01	1
Fill (Sony, I/O Software)	Відбиток пальця	0,1	1,0	0,3
BioMause (ABC)	Відбиток пальця	-	0,2	1
Кордон (Росія)	Відбиток пальця	1,0	0,0001	1

ДОДАТОК Б

Таблиця 2.1

Загальна таблиця стабільності роботи системи ідентифікації персоналу

№	Біометрична характеристика (ознака)	FAR, %	Кількість персоналу, N≈
1.	Відбиток пальця	0.001	300
2.	Райдужна оболонка ока	0.00001	3000
3.	3-D розпізнавання особи	0.0047	145
4.	Вени руки	0,0008	350

Таблиця 2.2

Залежність між помилками FRR і FAR унімодальних біометричних систем та розробленої мультимодально

№	Біометрична характеристика (ознака)					
	Унімодальна				Мультимодальна	
	Голос		Обличчя		Голос та обличчя	
	FRR, %	FAR, %	FRR, %	FAR, %	FRR, %	FAR, %
1.	48	0.01	6.5	0.01	3	0.01
2.	46	0.02	5.1	0.02	1.9	0.02
3.	42	0.05	5	0.05	1.8	0.03
4.	35	0.1	4.8	0.1	1	0.05
5.	30	0.2	4	0.2	0.9	0.07
6.	20	0.4	3	0.4	0.8	0.1
7.	18	0.5	2.2	0.5	0.8	0.2
8.	10	1	2	1	0.7	0.3
9.	7.5	2	1.5	2	0.6	0.4
10.	4	5	1	5	0.5	0.45
11.	3	10	0.48	10	0.35	0.5
12.	1.5	15	0.48	15	0.3	0.8
13.	0.9	20	0.48	20	0.25	1
14.	0.2	37	0.3	30	0.15	1.1
15.	0.02	38	0.02	42	0.02	1.2

Таблиця 2.3

Залежність між помилками FRR і FAR унімодальних біометричних систем та розробленої мультимодальної (розширена)

FAR, %	0	0,01	0,02	0,05	0,08	0,1	0,15	0,2	0,3	0,4	0,5	0,7	1	1,5	2	2,5	5	6	7	10	15	20	25	30	42
Голос (унімодальна) FRR, %	49	48	46	42	38	35	32	30	25	20	18	12	10	8,5	7,5	5,1	4	3,7	3,5	3	1,5	0,9	0,7	0,4	0
Обличчя (унімодальна) FRR, %	6,5	6	5,1	5	4,9	4,8	4,1	4	3,5	3	2,2	2,1	2	1,7	1,5	1,2	1	1	1	0,48	0,48	0,48	0,25	0,3	0,02
Голос та обличчя (мультимодальна) FRR, %	4	3	1,9	1	0,9	0,8	0,8	0,8	0,7	0,6	0,35	0,3	0,25	0	0	0	0	0	0	0	0	0	0	0	0

ДОДАТОК В

Частина коду CryptoJS AES:

FileREader API:

```
/*
CryptoJS v3.1.2
code.google.com/p/crypto-js
(c) 2009-2013 by Jeff Mott. All rights reserved.
code.google.com/p/crypto-js/wiki/License
*/
var CryptoJS=CryptoJS||function(u,p){var d={},l=d.lib={},s=function(){},t=l.Base
={extend:function(a){s.prototype=this;var c=new s;a&&c.mixIn(a);c.hasOwnProperty
("init")||(c.init=function(){c.$super.init.apply(this,arguments)});c.init.
prototype=c;c.$super=this;return c},create:function(){var a=this.extend();a.init
.apply(a,arguments);return a},init:function(){},mixIn:function(a){for(var c in a
)a.hasOwnProperty(c)&&(this[c]=a[c]);a.hasOwnProperty("toString")&&(this.
toString=a.toString)},clone:function(){return this.init.prototype.extend(this)}},
r=l.WordArray=t.extend({init:function(a,c){a=this.words=a||[];this.sigBytes=c!=p
?c:4*a.length},toString:function(a){return(a||v).stringify(this)},concat:
function(a){var c=this.words,e=a.words,j=this.sigBytes;a=a.sigBytes;this.clamp
();if(j%4)for(var k=0;k<a;k++)c[j+k>>>2]|=(e[k>>>2]>>>24-8*(k%4)&255)<<24-8*((j+
k)%4);else if(65535<e.length)for(k=0;k<a;k+=4)c[j+k>>>2]=e[k>>>2];else c.push.
apply(c,e);this.sigBytes+=a;return this},clamp:function(){var a=this.words,c=
this.sigBytes;a[c>>>2]&=4294967295<<
32-8*(c%4);a.length=u.ceil(c/4)},clone:function(){var a=t.clone.call(this);a.
words=this.words.slice(0);return a},random:function(a){for(var c=[],e=0;e<a;e+=4
)c.push(4294967296*u.random()|0);return new r.init(c,a)}}),w=d.enc={},v=w.Hex={
stringify:function(a){var c=a.words;a=a.sigBytes;for(var e=[],j=0;j<a;j++){var k
=c[j>>>2]>>>24-8*(j%4)&255;e.push((k>>>4).toString(16));e.push((k&15).toString(
16))}return e.join("")},parse:function(a){for(var c=a.length,e=[],j=0;j<c;j+=2)e
[j>>>3]|=parseInt(a.substr(j,
2),16)<<24-4*(j%8);return new r.init(e,c/2)}},b=w.Latin1={stringify:function(a){
var c=a.words;a=a.sigBytes;for(var e=[],j=0;j<a;j++)e.push(String.fromCharCode(c
[j>>>2]>>>24-8*(j%4)&255));return e.join("")},parse:function(a){for(var c=a.
length,e=[],j=0;j<c;j++)e[j>>>2]|=(a.charCodeAt(j)&255)<<24-8*(j%4);return new r
.init(e,c)}},x=w.Utf8={stringify:function(a){try{return decodeURIComponent(
escape(b.stringify(a)))}catch(c){throw Error("Malformed UTF-8 data");}},parse:
function(a){return b.parse(unescape(encodeURIComponent(a)))}},
```

```
[Constructor, Exposed=Window,Worker]
  interface FileReader: EventTarget {
    // async read methods
    void readAsArrayBuffer(Blob blob);
    void readAsText(Blob blob, optional DOMString label);
    void readAsDataURL(Blob blob);
    void abort();
    // states
    const unsigned short EMPTY = 0;
    const unsigned short LOADING = 1;
    const unsigned short DONE = 2;
    readonly attribute unsigned short readyState;
    // File or Blob data
    readonly attribute (DOMString or ArrayBuffer)? result;
    readonly attribute DOMError? error;
    // event handler attributes
    attribute EventHandler onloadstart;
    attribute EventHandler onprogress;
    attribute EventHandler onload;
    attribute EventHandler onabort;
    attribute EventHandler onerror;
    attribute EventHandler onloadend;
  };
```

ДОДАТОК Г

Реалізація методу згортаючого фільтру для Bitmap класу:

```
private static Bitmap ConvolutionFilter(Bitmap sourceBitmap,

                                        double[,] filterMatrix,
                                             double factor = 1,

                                                  int bias = 0,
                                            bool grayscale = false)
{

    BitmapData sourceData =
                                    sourceBitmap.LockBits(new
                        Rectangle(0, 0, sourceBitmap.Width,
                                        sourceBitmap.Height),
                                     ImageLockMode.ReadOnly,
                                PixelFormat.Format32bppArgb);

                            byte[] pixelBuffer = new
                            byte[sourceData.Stride *
                                 sourceData.Height];

                            byte[] resultBuffer = new
                             byte[sourceData.Stride *
                                  sourceData.Height];

    Marshal.Copy(sourceData.Scan0, pixelBuffer, 0,
                                    pixelBuffer.Length
                                    );

    sourceBitmap.UnlockBits(sourceData);


    if(grayscale == true)
    {
        float rgb = 0;


        for(int k = 0; k < pixelBuffer.Length; k += 4)
        {
            rgb = pixelBuffer[k] * 0.11f;

            rgb += pixelBuffer[k + 1] * 0.59f;
            rgb += pixelBuffer[k + 2] * 0.3f;


            pixelBuffer[k] = (byte)rgb;

            pixelBuffer[k + 1] = pixelBuffer[k];
            pixelBuffer[k + 2] = pixelBuffer[k];
```

```
        pixelBuffer[k + 3] = 255;
    }
}


double blue = 0.0;
double green = 0.0;
double red = 0.0;


int filterWidth = filterMatrix.GetLength(1);
int filterHeight = filterMatrix.GetLength(0);

int filterOffset = (filterWidth-1) / 2;

int calcOffset = 0;
int byteOffset = 0;
for(int offsetY = filterOffset; offsetY <
    sourceBitmap.Height - filterOffset; offsetY++)
{
    for(int offsetX = filterOffset; offsetX <
        sourceBitmap.Width - filterOffset; offsetX++)
    {
        blue = 0;

        green = 0;
        red = 0;
        byteOffset = offsetY *

                     sourceData.Stride +
                     offsetX * 4;
        for(int filterY = -filterOffset;

            filterY <= filterOffset; filterY++)
        {
            for(int filterX = -filterOffset;

                filterX <= filterOffset; filterX++)
           {
                       calcOffset =
                         byteOffset +
                         (filter
                         X        * 4) +
                         (filter   sourceData.Stride
                         Y        * );

               blue += (double)(pixelBuffer[calcOffset]) *
                       filterMatrix[filterY +
                       filterOffset,
                                    filterX + filterOffset];


               green += (double)(pixelBuffer[calcOffset+1]) *
                        filterMatrix[filterY + filterOffset,
                                     filterX + filterOffset];
               red += (double)(pixelBuffer[calcOffset+2]) *
                      filterMatrix[filterY + filterOffset,
                                   filterX + filterOffset];
```

```
                }
            }
            blue = factor * blue + bias;
            green = factor * green + bias;
            red = factor * red + bias;
            if(blue > 255)
            { blue =
            255;} else
            if(blue < 0)
            { blue = 0;}
            if(green > 255)
            { green =
            255;} else
            if(green < 0)
            { green = 0;}
            if(red > 255)
            { red =
            255;} else
            if(red < 0)
            { red = 0;}
            resultBuffer[byteOffset] = (byte)(blue);
            resultBuffer[byteOffset + 1] = (byte)(green);
            resultBuffer[byteOffset + 2] = (byte)(red);
            resultBuffer[byteOffset + 3] = 255;
        }
    }
    Bitmap resultBitmap = new Bitmap(sourceBitmap.Width,
                                     sourceBitmap.Height
                                     );
    BitmapData resultData =
               resultBitmap.LockBits(new Rectangle(0, 0,

               resultBitmap.Width, resultBitmap.Height),
                             ImageLockMode.WriteOnly,
                          PixelFormat.Format32bppArgb);


    Marshal.Copy(resultBuffer, 0, resultData.Scan0,
                               resultBuffer.Length
                               );
    resultBitmap.UnlockBits(resultData);
    return resultBitmap;
}
```

Горизонтальне та вертикальне матричне згортання:

```
public static Bitmap ConvolutionFilter(this Bitmap sourceBitmap,

                                       double[,] xFilterMatrix,
                                       double[,] yFilterMatrix,
                                             double factor = 1,

                                                   int bias = 0,
                                            bool grayscale = false)

{
    BitmapData sourceData =
```

```
                        sourceBitmap.LockBits(new
                Rectangle(0, 0, sourceBitmap.Width,
                                sourceBitmap.Height),
                            ImageLockMode.ReadOnly,
                    PixelFormat.Format32bppArgb);
                byte[] pixelBuffer = new
                byte[sourceData.Stride *
                     sourceData.Height];
                byte[] resultBuffer = new
                 byte[sourceData.Stride *
                     sourceData.Height];
Marshal.Copy(sourceData.Scan0, pixelBuffer, 0,
                     pixelBuffer.Length
                     );
sourceBitmap.UnlockBits(sourceData);
if (grayscale == true)
{
    float rgb = 0;
    for (int k = 0; k < pixelBuffer.Length; k += 4)
    {
        rgb = pixelBuffer[k] * 0.11f;

        rgb += pixelBuffer[k + 1] * 0.59f;
        rgb += pixelBuffer[k + 2] * 0.3f;
        pixelBuffer[k] = (byte)rgb;
        pixelBuffer[k + 1] = pixelBuffer[k];
        pixelBuffer[k + 2] = pixelBuffer[k];
        pixelBuffer[k + 3] = 255;
    }
}
double blueX = 0.0;
double greenX = 0.0;
double redX = 0.0;
double blueY = 0.0;
double greenY = 0.0;
double redY = 0.0;
double blueTotal = 0.0;
double greenTotal = 0.0;
double redTotal = 0.0;
int filterOffset = 1;
int calcOffset = 0;
int byteOffset = 0;
for (int offsetY = filterOffset; offsetY <
    sourceBitmap.Height - filterOffset; offsetY++)
{
    for (int offsetX = filterOffset; offsetX <
        sourceBitmap.Width - filterOffset; offsetX++)
    {
        blueX = greenX = redX = 0;
        blueY = greenY = redY = 0;
        blueTotal = greenTotal = redTotal = 0.0;
        byteOffset = offsetY *
                     sourceData.Stride +
                     offsetX * 4;
        for (int filterY = -filterOffset;
            filterY <= filterOffset; filterY++)
        {
```

```
        for (int filterX = -filterOffset;
         filterX <= filterOffset; filterX++)
        {
                    calcOffset =
                      byteOffset +
                       (filter
                       X        * 4) +
                       (filter   sourceData.Stride
                       Y        * );

            blueX += (double)
                     (pixelBuffer[calcOffset]) *
                     xFilterMatrix[filterY +

                                   filterOffset,
                                   filterX +
                                   filterOffset];
            greenX += (double)
                  (pixelBuffer[calcOffset + 1]) *
                     xFilterMatrix[filterY +

                                   filterOffset,
                                   filterX +

                                   filterOffset];
            redX += (double)
                  (pixelBuffer[calcOffset + 2]) *

                     xFilterMatrix[filterY +
                                   filterOffset,
                                   filterX +
                                   filterOffset];
            blueY += (double)
                     (pixelBuffer[calcOffset]) *

                     yFilterMatrix[filterY +
                                   filterOffset,
                                   filterX +
                                   filterOffset];
            greenY += (double)
                  (pixelBuffer[calcOffset + 1]) *
                     yFilterMatrix[filterY +
                                   filterOffset,
                                   filterX +
                                   filterOffset];
            redY += (double)
                  (pixelBuffer[calcOffset + 2]) *
                     yFilterMatrix[filterY +
                                   filterOffset,
                                   filterX +
                                   filterOffset];

        }
    }
blueTotal = Math.Sqrt((blueX * blueX) +
                     (blueY * blueY));
```

```
                greenTotal = Math.Sqrt((greenX *
                    greenX) + (greenY * greenY));
        redTotal = Math.Sqrt((redX * redX) +
                             (redY * redY));
              if (blueTotal > 255)
              { blueTotal = 255;
              } else if
              (blueTotal < 0) {
              blueTotal = 0; }
              if (greenTotal > 255)
              { greenTotal = 255;
              } else if
              (greenTotal < 0) {
              greenTotal = 0; }
              if (redTotal > 255)
              { redTotal = 255;
              } else if
              (redTotal < 0) {
              redTotal = 0; }
              resultBuffer[byteOffset] = (byte)(blueTotal);
              resultBuffer[byteOffset + 1] = (byte)(greenTotal);
              resultBuffer[byteOffset + 2] = (byte)(redTotal);
              resultBuffer[byteOffset + 3] = 255;
          }
      }
      Bitmap resultBitmap = new Bitmap(sourceBitmap.Width,
                                       sourceBitmap.Height
                                       );
      BitmapData resultData =
                 resultBitmap.LockBits(new Rectangle(0, 0,
                 resultBitmap.Width, resultBitmap.Height),
                                  ImageLockMode.WriteOnly,
                               PixelFormat.Format32bppArgb);
      Marshal.Copy(resultBuffer, 0, resultData.Scan0,
                                  resultBuffer.Length
                                  );
      resultBitmap.UnlockBits(resultData);
      return resultBitmap;
}
```