Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
Кафедра радіотехнічних систем
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: «Метод обробки зображень для верифікації особи в телекомунікаційних системах»

Виконав(ла): студент(ка) VI курсу, групи РРм-61
спеціальності 172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

	(підпис)	Мойсей П. І. (прізвище та ініціали)
Керівник	(підпис)	Дедів І. Ю. (прізвище та ініціали)
Нормоконтроль	(підпис)	Хвостівська Л. В. (прізвище та ініціали)
Завідувач кафедри	(підпис)	Дунець В. Л. (прізвище та ініціали)
Рецензент	(підпис)	Дозорський В. Г. (прізвище та ініціали)

Тернопіль
2020

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)

Кафедра радіотехнічних систем
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Дунець В. Л.
(підпис) (прізвище та ініціали)
« » 20___ р.

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня магістр
(назва освітнього ступеня)

за спеціальністю 172 «Телекомунікації та радіотехніка»
(шифр і назва спеціальності)

студенту Мойсею Павлу Ігоровичу
(прізвище, ім'я, по батькові)

1. Тема роботи «Метод обробки зображень для верифікації особи в телекомунікаційних системах»

Керівник роботи Дедів Ірина Юріївна, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «*24*» *11* 2020 року № _____

2. Термін подання студентом завершеної роботи

3. Вихідні дані до роботи Процес та методи обробки зображень для верифікації особи в телекомунікаційних системах

4. Зміст роботи (перелік питань, які потрібно розробити)
Задача розпізнавання та верифікації особи в телекомунікаційних системах;класифікація методів верифікації та їх принцип роботи; методи верифікації особи за параметрами обличчя; алгоритм роботи методів розпізнавання особи; системи верифікації особи; методи обробки зображень; обґрунтування методу обробки зображення; еквалізація гістограми; фільтр Лапласа; реєстрація експериментальних даних; обробка зображення для верифікації особи; аналіз та оцінка зображення; охорона праці та безпека в надзвичайних ситуаціях.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Алгоритм розпізнавання особи; методи верифікації особи; відомі системи доступу верифікації; існуючі методи обробки зображень; алгоритм попередньої обробки зображень; структурна схема алгоритму функціонування системи біометричної верифікації; спрощена структурна схема системи біометричної верифікації; алгоритм роботи системи біометричної верифікації; збільшення динамічного діапазону рівня яскравостей; застосування фільтра Лапласа; перетворення кольорового зображення в напівтонове та його гістограма; напівтонове зображення після еквалізації з гістограмою; кінцеве оброблене зображення з гістограмою; оцінка рівня якості зображення.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці			
Безпека в надзвичайних			
ситуаціях			

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1	Отримання завдання	24.11.20	
2	Аналіз завдання	25.11.20	
3	Виконання розділу 1	27.11.20	
4	Виконання розділу 2	29.11.20	
5	Виконання розділу 3	01.12.20	
6	Виконання розділу 4	04.12.20	
7	Оформлення пояснювальної записки	06.12.20	
8	Оформлення графічного та презентаційного матеріалу	14.12.20	
9	Перевірка роботи на антиплагіат	19.12.20	
10	Попередній захист	20.12.20	
11	Захист	21.12.20	

Студент _____ Мойсей П. І.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Дедів І. Ю.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Метод обробки зображень для верифікації особи в телекомунікаційних системах» // Дипломна робота // Мойсей Павло Ігорович// Тернопільський національний технічний університет імені Івана Пулюя, факультет прикладних інформаційних технологій та електроінженерії, група РРм-61 // Тернопіль, 2020 //

Ключові слова: ІДЕНТИФІКАЦІЯ, ВЕРИФІКАЦІЯ, ГІСТОГРАМА, ЕКВАЛІЗАЦІЯ, ФІЛЬТР, АНАЛІЗ, ОБРОБКА, ДОСТОВІРНІСТЬ, ШВИДКІСТЬ.

Дипломну роботу присвячено обґрунтованню методу обробки зображення для верифікації особи в телекомунікаційних системах з використанням фільтра Лапласа та еквалізації гістограми зображення. Проведено аналіз методів розпізнавання особи, представлено структурні схеми систем верифікації особи в телекомунікаційних мережах для ідентифікації особи та обґрунтовано метод обробки зображення, що дає можливість збільшити достовірність та швидкодію систем верифікації.

ABSTRACT

The topic of qualifying work is: «Methodof processing image for identity verification in telecommunication systems» - Manuscript // Diploma work // MoiseiPavloIgorovich // Ternopil Ivan Puluj National Technical University, Faculty of Applied Information Technologies and Electrical Engineering, group RRm-61 // Ternopil, 2020 //

Key words: IDENTIFICATION, VERIFICATION, HISTOGRAM, EQUALIZATION, FILTER, ANALYSIS, PROCESSING, RELIABILITY, SPEED.

The diploma work is devoted to the substantiationof methodof processing image for identity verification in telecommunication systems using the Laplace filter and the equalization of the image histogram. The analysis of face recognition methods is carried out, the structural schemes of face verification systems in telecommunication networks for face identification are presented and the method of image processing is substantiated, which gives an opportunity to increase the reliability and speed of verification systems.

СПИСОК СКОРОЧЕНЬ

FAR – FalseAcceptanceRate (рівень помилкових дозволів)

TAR – True Acceptance Rate (рівень вірних дозволів)

FRR – FalseRejectionRate (рівень помилкових відмов)

TRR – True Rejection Rate (рівень вірних відмов)

HTER – Human-targetedTranslationErrorRate(усереднений показник помилок FRRтаFAR)

FTE – FailuretoEnrollRate (помилка реєстрації)

FTA – FailuretoAcquireRate (ймовірність помилки збирання даних)

ERR – EqualErrorRate (точка рівності помилок)

ROC – Receiveroperatingcharacteristic (робоча характеристика приймача)

AUC – AreaUnderCurve (площа під кривою ROC)

СКУД – система контролю та управління доступом

БД – база даних

ПЗ – програмне забезпечення

ІТ – інформаційна технологія

ПК – персональний комп’ютер

ЗМІСТ

ВСТУП

Актуальність роботи.На сьогодні існує багато автоматизованих методів і засобів верифікації користувача для підтвердження його особи, доступу користувача до захищених баз даних тощо. В залежності від поставлених задач, всі методи верифікації використовуються в тих чи інших системах з різними способами їх втілення.

Поширеним та відомим є метод верифікації користувача за параметрами обличчя. Як правило, це комбінація верифікації за параметрами обличчя та унікальних особливостей людини (колір шкіри; вікові особливості тощо), що дає можливість однозначного ідентифікувати особу в телекомунікаційних мережах. Однак, при застосуванні даного методувиникає ряд недоліків, які пов’язані з якістю реєстрації вхідних даних та впливом зовнішніх факторів на нього, що призводить до зниження швидкодії та надійності системи. До таких недоліків відноситься- недостатняосвітленість, кути огляду, рух особи, несприятливий фон, використання реєструючого обладнання з низькою роздільною здатністю, тощо. Тому, при застосуванні даного методу верифікації потрібно здійснити попередню обробку вхідного зображення.

В залежності від задачі та зовнішніх факторів, обробка здійснюється різними методами:перетворення яскравості (підвищення яскравості; логарифмічне перетворення; прояв негативу; підвищення контрастності; покращення з використанням гістограм; еквалізація зображення; еквалізація гістограми; гістограмний підгін);просторова фільтрація (найпростіший фільтр з операцією imfilter; фільтр Лапласа; медіанна фільтрація);виділення краю об’єкта.

Тому, застосування методу обробки вхідного зображення дасть змогу підвищити швидкодію та надійність роботи системи верифікації особи в телекомунікаційних системах.

Мета і задачі дослідження.Метою дослідження є обґрунтування методу обробки зображення для верифікації особи в телекомунікаційних системах. Досягнення цієї мети вимагає розв’язання поставлених задач, а саме:

- провести аналітичний огляд літературних джерел за тематикою дослідження;

- обґрунтувати вибір методу обробки зображення для верифікації особи в телекомунікаційних системах;

- представити алгоритм методуобробки зображення для систем верифікації особи в телекомунікаційних системах;

- обґрунтувати використання методуобробки зображення длясистем верифікації користувача;

- розробити програмне забезпечення методуобробки зображення для систем верифікації особи в телекомунікаційних системах.

Об’єкт дослідження: процес обробки зображення для систем верифікації особи в телекомунікаційних системах.

Предмет дослідження: метод обробки зображення для систем верифікації особи в телекомунікаційних системах.

Методи дослідження:аналіз і синтез, математичне та імітаційне моделювання, науковий експеримент в програмному середовищі.

Наукова новизна одержаних результатів.Вперше обґрунтовано метод обробки зображення для систем верифікації особи в телекомунікаційних системах, що ґрунтується назастосуванні попередньої обробки зображення

Практичне значення одержаних результатів.Одержані результати можуть бути використані при розробленні систем автоматизованої верифікації користувача за параметрами обличчя в телекомунікаційних системах.

Структура та обсяг.

Робота складається із анотації, списку скорочень, вступу, чотирьох розділів, викладених на 85 сторінках, списку використаних джерел з 33 назв, вказаних в розділах та додатках. Загальний обсяг магістерської роботи становить 92 сторінки.

РОЗДІЛ 1.
АНАЛІТИЧНА ЧАСТИНА

1.1.Задачарозпізнавання особи в телекомунікаційних системах

На сьогоднішній день, при великій кількості мешканців світу стало необхідним виконувати розпізнавання людей для встановлення особи. При покупці товарів з віковими обмеженнями,приприйманні участі в банківських послугах або при проходженні контролю на митному кордоні, слід переконатись достовірність особи документа. Ручна перевірка не зможе дати максимальної достовірності, що документи є справжні. Тому частіше запобігають автоматизованим методам[1].

При одному з досліджень, досвідчені касири з великим стажем роботи допускали 35% фальшивих ID-карток, з підробленою зовнішністю, за справжні.При дослідженні в ідеальних умовах лабораторії, допуск помилок складає 10-20%. Сьогодні кращий алгоритм розпізнаванняоблич людей має похибку з коефіцієнтом 0,08% [1-3].

Технології розпізнавання осіб застосовуються в найрізноманітніших сферах [2]:

- при великому натовпі людей;
- в приміщеннях, що охороняються;
- для розшукування злодіїв;
- контролювання їдалень та місць для ігор;
- пошук порушників закладів;
- в банках, для ідентифікації карточок;
- купівля та продаж в інтернеті;
- для розповсюдження інформації в інтернеті;
- в поліції для виявлення даних особи;
- для телевізійних передач;
- телефонні програми;

- для верифікації людей в інтернеті на фотографіях тощо.

З початком всезагального карантину значно поширилось дистанційне навчання в інтернеті. Досить часто викладачам необхідно знати чи всі студенти знаходяться на парі чи ні. Для цього теж використовується розпізнавання особи, при цьому система збирає інформацію про кількість сторінок, що відвідав користувач (студент) за сеанс роботи; час, проведений на кожній сторінці; активовані гіперсилки на сторінці; кількість файлів, використані студентом із системи; час тестування тощо.Розпізнавання також застосовують в навчальних закладах для уникненнявикрадання дітей, вхід наркоманів, педофілів тощо. Технологія також може розпізнавати 10 видів зброї для запобігання актів насильства в школах [1-3].

В медицині використовуються додаткові програми з знаходженням генетичних порушень, що мають назву Face2Gene і DeepGestalt [3].

Для універмагів розпізнавання особи необхідне для виявлення людей з чорним списком, що порушували закон в магазині, або ж неповнолітніх осіб. Дана системапройде верифікацію зловмисника і надасть власнику приміщення, підприємства чи будь-якої організації повідомлення про порушення закону, не залежно від того, чи заходила дана особа коли-небудь в універсальний магазин до того. Проте такі системи не завжди можуть правильно розпізнати зловмисника чи простого покупця [2-3].

При виявленні людей, складним завданням постає вимірювання коректної точності роботи.Розпізнавання осіб використовується, наприклад, для детектування особи на смартфонах, ноутбуках, планшетах, на фотографії або в відеопотоці, визначення статі і віку, пошук потрібної людини серед безлічі зображень або перевірка одної людини на двох зображеннях. Для розпізнавання особи, із зображень витягуються спеціальні дескриптори, або вектори ознак. У цьому випадку завдання ідентифікації зводиться до пошуку найближчого вектора ознак, а верифікацію можна реалізувати за допомогою порогу відстаней між векторами. Комбінуючи ці дії, можна ідентифікувати людину серед набору зображень або приймати рішення про те, що його немає серед цих зображень

[1]. Така процедура (рис. 1.1) називаєтьсяідентифікацією на відкритій множині (open-setidentification).

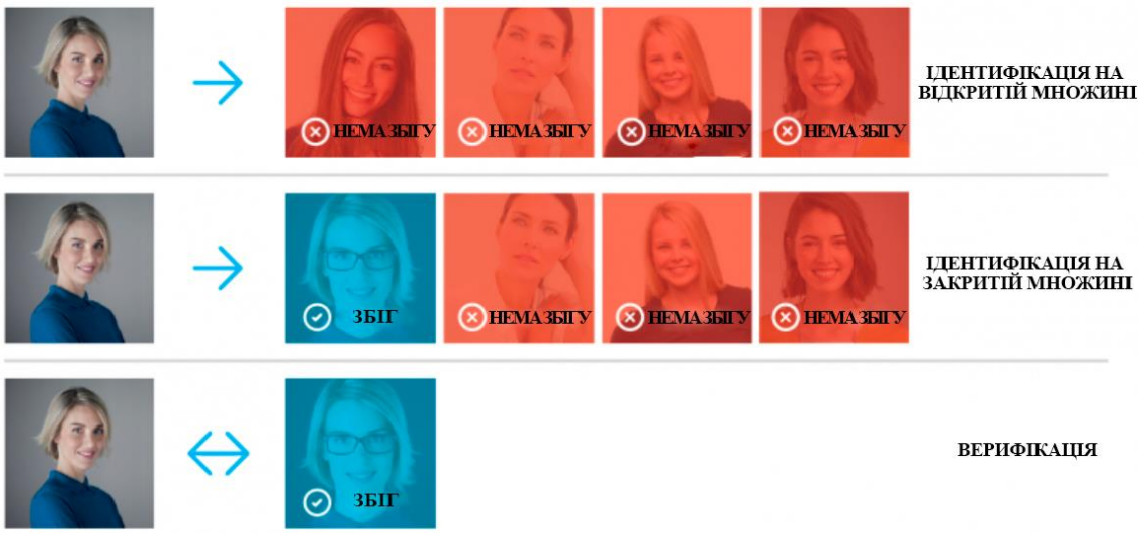


Рис. 1.1. Ідентифікація на відкритій множині

Для кількісної оцінки схожості осіб можна використовувати відстань в просторі векторів ознак. Переважно вибирається евклідово або косинусна відстань. Ідентифікація та верифікація повертають різні результати і використовуються різні метрики для оцінки якості.Окрім вибору правильної метрики, для оцінки точності алгоритму потрібен розмічений набір зображень (датасета).

Для розпізнавання осіб сучасне ПЗспроектовано на машинному навчанні. Алгоритми навчаються на великих датасета (наборах даних) з розміченими зображеннями. Правильний вибір дата сету значно впливає на точність розпізнавання. Чим краще вихідні дані, тим краще алгоритм буде справлятися з поставленим завданням.

Для виміру потрібної точності, використовують тестові датасети. В ідеальних умовах організації, необхідно мативласний набір даних, схожим на зображення, з якими система буде працювати при експлуатації. Також звертається велика увага на камеру, умови зйомки, вік, стать і національність людей, які потраплять в тестовий датасета. Чим більше схожий тестовий

датасетана реальні дані, тим більш достовірними будуть результати тестування. Окрім того, замість тестових датасетів можна скористатися публічними, наприклад, LFW і MegaFace. LFW містить тільки 6000 пар зображень облич і не підходить для багатьох реальних сценаріїв тому, що на ньому неможливо виміряти низькі рівні помилок. ДатасетаMegaFace містить набагато більше зображень і підходить для тестування алгоритмів розпізнавання осіб на великих масштабах [1-3].

Інший метод полягає у використанні результатів тестування третьою особою. Такі тестування проводяться кваліфікованими фахівцями на великих закритих датасета, і їх результатам можна довіряти. Одним із прикладів може служити NIST (FaceRecognitionVendorTestOngoing). Це тест, що проводиться Національним Інститутом Стандартів і Технологій (NIST) при Міністерстві торгівлі США.

Недоліком даного підходу полягає в датасетній організації, яка може істотно відрізнятися від даного сценарію використання.

Одним з поширених машинних навчань є перенавчання. В перенавчанні алгоритм показує хороші результати на даних, які використовувалися при навчанні, а на нових даних вони виходять поганими.

Проблемою такого методу є те, що через деякий час список людей з допуском на підприємствах, організаціях розширюються і система починає відмовляти новим людям в доступі. Алгоритм тестувався і навчався на одних данихі ніхто не проводив вимірювання точності на нових фотографіях [2].

У деяких випадках перенавчання проявляється інакше. Наприклад, алгоритм навчається на зображеннях користувачів одної етнічна група. При застосуванні такого алгоритму до осіб іншої національності, точність буде меншою. Необхідно тестувати алгоритм на нових даних, які йому потрібно буде обробляти в реальному застосуванні, а не на навчальних даних.

Після вибору датасета, потрібно обрати метрику для оцінки результатів. Метрика - це функція, яка приймає на вхід результати роботи алгоритму

(ідентифікації або верифікації), а на виході повертає число, яке відповідає якості роботи алгоритму на конкретному дата сеті [1-3].

Використання одного числа для кількісного порівняння різних алгоритмів або вендорів дозволяє стисло представляти результати тестування і полегшує процес прийняття рішень.

На рис. 1.2 показано як змінюється ринок біометричного обладнання.

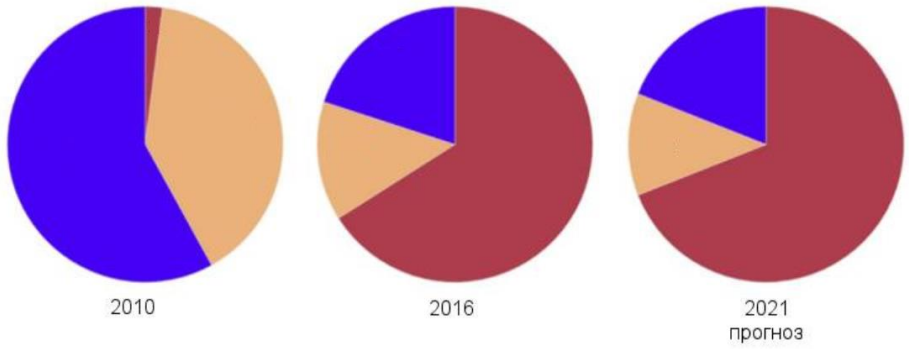


Рис. 1.2. Діаграма використання біометричного обладнання

На рис. 1.2 бордовим кольором показані пристрої споживача (смартфони, автомобілі, розумні будинки), жовтим показано комерційний сектор (банк, контроль в аеропорті), синім показано національну безпеку (служби безпеки, державна система ідентифікації). Згідно із цими даними, можна сказати, що з більшим попитом на електронні пристрої, все менше виникає необхідності в національній безпеці, оскільки все легше найти особу.

Біометричні системи розпізнавання особи стали частиною повсякденного життя людини завдяки високій точності при виявленні та перевірці особистості людини для багатьох сфер життя.

1.2.Задача верифікації особи в телекомунікаційних системах

Для того, аби розпізнати особу, необхідно пройти шлях від ідентифікації, верифікації (автентифікації) до авторизації. Для того, щоби краще зрозуміти всю систему, необхідно розрізняти ці процеси між собою.

Ідентифікація – це процес розпізнавання тотожності інформації користувача (на основі різних ознак) щодо оригінальних документів в системі для надання доступу користувачу в систему. Не слід плутати ідентифікацію із верифікацією (автентифікацією) та авторизацією [3].

Ідентифікація особи, користувача необхідна для отримання інформації про суб'єкт системи на основі наданого ним ідентифікатора. Вона слугує початковою процедурою надання доступу до системи. Після неї здійснюється автентифікація та авторизація.

Верифікація (автентифікація), згідно праць [4-7], – це процес встановлення відповідності інформації, необхідної користувачу, при його зверненні до системи різними шляхами і перевірка на надання доступу користувачу для безпеки. В інтернеті верифікація використовується, як правило, щоби підтвердити офіційну особистість користувача на різних сайтах.

На різних сайтах є два типи користувачів: верифіковані та не верифіковані. Одразу після реєстрації на сайті, користувачі отримують початковий статус як не верифікований. При цьому ніяких обмежень на використання ресурсів користувач немає [5].

Щоби отримати статус верифікованого користувача, необхідно підтвердити особисті персональні дані, які будуть приховані від інших відвідувачів сайту.

Верифікація дає нам такі переваги [4-7]:

- пропозиції верифікованих користувачів відображають вище відгуків не верифікованих;
- підтвердження персональних даних служить як додатковий гарант безпеки для замовників;
- в профілі користувача і поряд з його пропозиціями появляється спеціальний значок верифікації;
- мають змогу використовувати опції «тільки для верифікованих осіб».

Значок верифікації частіше надається лише особам, які є публічно відомі. При цьому коли надається певна інформація в інтернеті про особу, також

надають і гіперсилки осіб, як офіційність і правдивість описаних слів про особу чи від самої особи.

Загальні вимоги при наданні персональних даних в базу є те, що документи повинні представлятись в вигляді файлів, простих в відкриванні без додаткових програм, з текстом, зручним для прочитання.

Авторизація, згідно праці [7], – це процес надання або не надання доступу користувачу в захищену систему після повної перевірки ідентифікацією та автентифікацією.

Прикладом цілої системи для надання доступу користувачу може послужити ключ від будинку. Коли ми вставляєм ключ в дверний замок, то відбувається автентифікація. Якщо ж будова ключа сходиться з будовою замка, то система дасть вам доступ і двері відкриються. При цьому відбуваються три процеси:

- ідентифікація – в нашому прикладі, це розпізнавання інформації про об’єкт (ключ це чи ручка і т.п.);
- верифікація (автентифікація) – це процес перевірки інформації про об’єкт – будова ключа, його структура;
- авторизація –це перевірка прав користувача на надання доступу – чи підходить будова ключа до структури і будови дверного замка, відповідно чи зможем ми відчинити двері чи ні.

1.3.Класифікація методів верифікації особи

Для розпізнавання особи за верифікацією в різних сферах життя, користувачу необхідно надати персональні дані. Документи, що надано, повинні відповідати необхідними правилами. Вони повинні бути легко читаючими, зрозумілими, лаконічними та з офіційними печатками. Якщо ж документи видаються в файлах, то файли повинні відкриватись без додаткового програмного забезпечення. Фото повинно бути чітким, без дзеркальних ефектів [4-7].

Згідно із цими даними верифікація поділяється на різні види:

- верифікація по e-mail;
- верифікація по номеру паспортного коду;
- верифікація по смс на мобільний телефон;
- верифікація з відповідним кодом, який повинен співпадати з тим, що в базі даних;
- верифікація дзвінком;
- верифікація з фото;
- верифікація ключовим питанням;
- верифікація з номером карти;
- верифікація паролем;
- тощо.

1.4.Принципи верифікації особи

Для отримання доступу до будь-якої системи, кожен користувач повинен підтвердити свою особистість. При цьому здійснюється перевірка згідно даних, які було надано до бази даних системи. Якщо вони правильні, то відбувається безпомилковий доступ в систему. Якщо ні, то система буде просити повторити перевірку до тих пір, поки особа не надасть інформацію, що підтверджує її [4-7].

Згідно із різними сферами життя, де відбувається верифікація, особа проводить розпізнавання різними методами. Для зручнішого розуміння, при верифікації відбувається порівняння інформації особи з тою інформацією, що є в базі даних. Наприклад, якщо ви в аеропорті, то підтвердженням того, що ви не злодій, шахрай або ще хтось, відбувається сканування вашого багажу на присутність холодної зброї чи небезпечних речовин та сканування вас через спеціальну арку з детекторами. Якщо присутня зброя чи якийсь метал, то детектори почнуть сигналити та охоронці не дадуть вам сісти в літак без ретельного огляду багажу і вас [6-7].

Для простішого розуміння, алгоритму розпізнавання особи відбувається наступним чином:

- виявлення обличчя за допомогою камери;
- аналіз обличчя (кожне обличчя має 80 вузлових точок або різноманітні орієнтири);
- конверсія даних в цифровий код (дані обличчя);
- пошук збігів. Код порівнюється з базою даних в пошуку збігу, і в результаті збігу видається додаткова інформація про особу.

Камера виявляє обличчя людини. Особа найкраще розпізнається коли людина дивиться прямо в камеру або ж під певним кутом, в залежності від можливостей системи.

Потім знімається фотографія особи і починається його аналіз [5]. Більшість рішень для розпізнавання осіб використовує 2-D зображення (замість 3-D)через простіше зіставлення 2-D фото з загальнодоступними фотографіями або фотографіями, наявними в базі даних. Кожне обличчя складено з помітних орієнтирів або вузлових точок. Кожна людська особа має 80 вузлових точок. Програми для розпізнавання осіб аналізують вузлові точки (відстань між очима, форму носа).

Після цього аналіз обличчя перетворюється в математичну формулу. Риси обличчя перетворюються в числовий код - відбиток особи (faceprint), який є унікальним, як термограма вен кожної людини.

Третій етап це порівняння коду з базою даних осіб. У цій базі даних є фотографії з ідентифікаторами, які можна порівнювати.

ФБР має доступ до більш ніж 641 мільйону фотографій, включаючи 21 державну базу даних, такі як DMV. Інший приклад бази даних - це фотографії в Facebook. Будь-які фотографії, помічені ім'ям людини, стають частиною бази даних Facebook.

Останній етап це визначення відповідності точних даних з тими, що в базі даних. Результатом цього стає ідентифікація людини з наданням додаткової інформації (ПІБ, адрес і т.п.).

1.5. Висновки до розділу 1

В розділірозглянуто загальні поняття розпізнавання, точність, використання в різних сферах життя, загальні поняття верифікації, ідентифікації та авторизації, переваги та недоліки систем, проблеми верифікації та найпростіші принципи роботи.

Крім того,представлено види систем ідентифікацій на основі даних особи, загальні принципи системи ідентифікації з послідовними процесами та наведено найпростіші приклади використання цих систем в різних галузях.

РОЗДІЛ 2.
ОСНОВНА ЧАСТИНА

2.1.Методиверифікації особи за параметрами обличчя

Верифікація за параметрами обличчя є один із найшвидше розвиваючих методів верифікації користувача. Розвиток цього методу пов'язаний зі швидким зростанням мультимедійних відео-технологій, завдяки яким можна побачити все більше відеокамер, встановлених майже на кожному кроці [8-10].

Найпростіший метод верифікації обличчя це верифікація по зображенню людини, яка тримає в руках паспорт. Проте цей метод застосовується лише при дистанційній ідентифікації фізичного обличчя. В різних організаціях, підприємствах тощо використовуються більш складні методи верифікації.

Існують два загальні методи верифікації людини за параметрами обличчям [8-9]:

- верифікація за геометрією обличчя;
- верифікація за артеріями.

В методіверифікації за геометрією обличчяпроектується3-D зображення обличчя. Основу цього способу складає спеціальне програмне забезпечення, яке отримує зображення обличчя через фотокамери й здійснює аналіз його. Дана програма виділяє лініїгуб, носа та інших частин обличчя користувача, після чого аналізуєтьсявідстань контурів та формується алгоритм порівняння з тими, що є в базі даних.

Тривимірний образ обличчя людини необхідний приверифікації під невеликимикутами обличчя особи.

Перевага даного методу верифікації це низька ціна.

Недоліки ідентифікації – низька точність.

Метод верифікації за артеріями обличчя.

Термограма аналізує тепло обличчя людини. Отримання зображення здійснюється через інфрачервону камеру, після чого система отримує область розташування артерій. В всіхкористувачів вона унікальна.

Переваги даного методу це достатньо великадостовірність.

Недоліком - новизна ідентифікації, тому поки не має досить чітких алгоритмів роботи.

Існують також декілька детальніших методів верифікації за обличчям. Вони виконують аналіз зображень з встановленням відмінностей різних характеристик обличчя [10]:

- метод емпіричного підходу – верифікація за ключовими точками, 3-Dшаблоном;
- метод відмінних геометричних характеристик обличчя;
- метод порівняння еталонів;
- метод гнучких контурних моделей користувача – верифікація з порівнюванням контурів особи;
- лінійний дискримінантний метод – верифікація з лінійним розділенням попіксельних областей обличчя осіб;
- метод порівняння еластичних графів – верифікація осіб за графом обличчя;
- метод головних компонент – верифікація з перетворенням зображення в головні компоненти для порівняння з базою даних.

2.2. Алгоритм роботи методів розпізнавання особи

Верифікація організована як порівняння цільових функцій (функція правдоподібності), побудованої за верифікованоюмоделлю для тестового зображення [15]:

- максимальною цільовою функцією серед всіх цільових функцій, спроектованихдля текстового зображення за моделями, що вже є присутні;

- середнім значенням за всіма цільовими функціями, спроектованими для тестових зображень замоделями, що вже є присутні;

- цільовою функцією, спроектованоюдля тестового зображення за загальною моделлю.

Верифікація особи- це процес приймання бінарного рішення:

- так (одна людина на двох зображеннях);
- ні (різні люди на двох зображеннях).

В загальному є 2 можливі стани алгоритму і 2 варіанти справжнього стану речей (рис. 2.1), тобто 4 варіанти класифікації помилки [15].

Рис. 2.1. Класифікація помилки

Згідно рис. 2.1, колір фону кодує істинневідношення між картинками (синій - це прийняти; жовтий - відкинути), колір рамки відповідає прогнозу алгоритму (синій - прийняти, жовтий – відкинути).

В табл. 2.1, вищі стовпці відповідають рішенням алгоритму (синій - прийняти, жовтий - відкинути), рядки відповідають істинним значенням (кодуються такими ж кольорами). Правильні відповіді алгоритму відзначені зеленим фоном, помилкові - червоним.

Таблиця 2.1

Алгоритм усунення помилки

	Прийняти	Відхилити
Відхилити	Тип 1 помилки (невірно прийнято)	Вірно (правильно відхилено)
Прийняти	Вірно (правильно прийнято)	Тип 2 помилки (не вірно відхилено)

З цих результатів два відповідають правильним відповідям алгоритму, а два - помилок першого і другого роду відповідно. Помилки першого роду називають falseaccept, falsepositive або falsematch (невірно прийнято), а помилки другого роду - falsereject, falsenegative або falsenon-match (невірно відкинуто) [15].

Про якість верифікації можна судити за такими показниками як FAR - ймовірність прийняти помилкове припущення, FRR - ймовірність відкинути справжнє припущення. HTER - усереднений показник помилок FRR і FAR. Якщо кількість помилок різного роду серед пар зображень в датасеті підсумувати і поділити їх на кількість пар, ми отримаємо falseacceptrate (FAR) і falserejectrate (FRR).

Параметрами, якими ми можемо впливати на якість верифікації, є M - кількість кластерів на які розподіляються спостереження, t - допустима різниця при порівнянні цільових функцій. Дослідження першого способу показали, що залежність якості верифікації прямо залежить від кількості кластерів і починає мало змінюватися після M = 6 (рис. 2.2). Оптимальне значення порогу t = 20 для 6 кластерів, при якому FAR = 1.66, FRR = 1.73, HTER = 1.66.

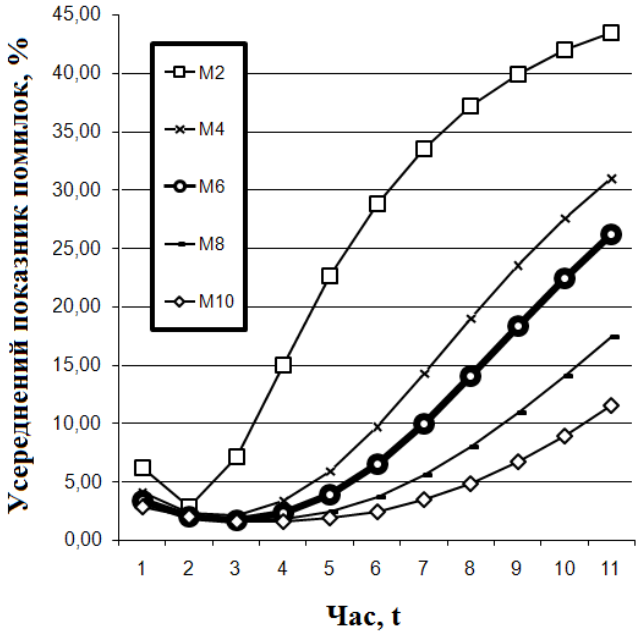


Рис. 2.2. Залежність HTER від кількості кластерів M

Другий спосіб AVG є менш якісним в плані верифікації, тому що в середнє значення закладаються цільові функції різних моделей, які погано підходять під тестове зображення, так і погано описують це зображення (рис.2.3).

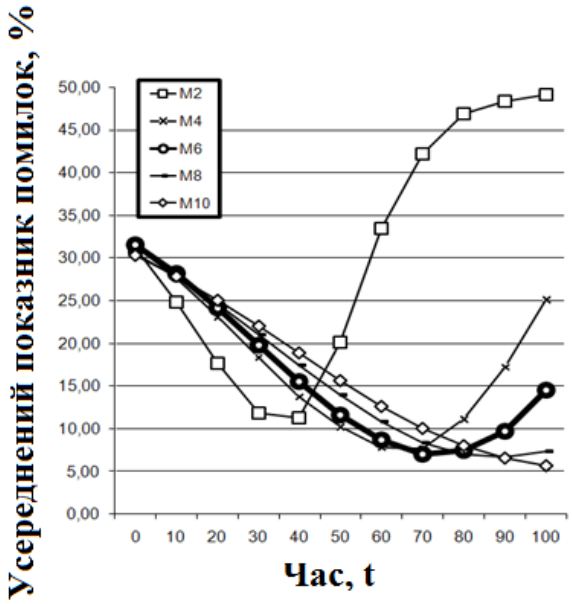


Рис. 2.3. Залежність HTER від кількості кластерів M

Починаючи з M = 6, спостерігається зменшення зміни якості верифікації від кількості кластерів. Оптимальні значення при M = 6: t = 70, FAR = 9.64, FRR = 4.44, HTER = 7.04.

При дослідженні третього способу, на будь-якій кількості кластерів, збільшення параметра t негативно позначається на якості верифікації. Тому при t = 0 оптимальна кількість кластерів M = 6 (рис. 2.4) при зменшенні залежності HTER від M. На виході такі результати: FAR = 2.07, FRR = 7.00, HTER = 4.53.

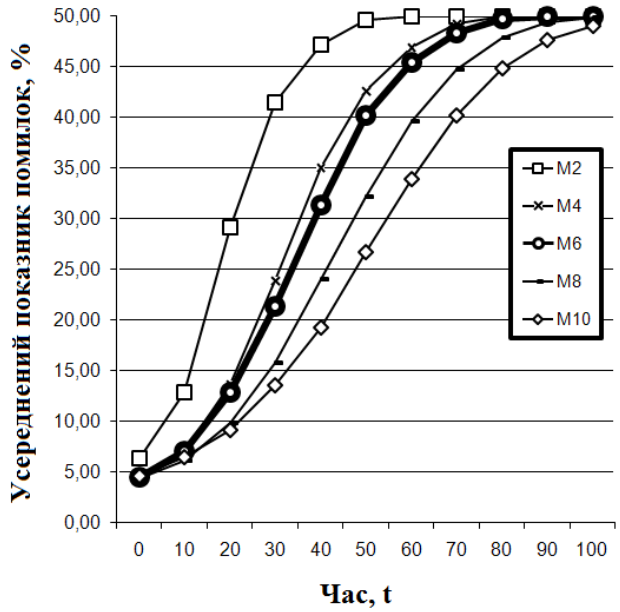


Рис. 2.4. Залежність HTER від кількості кластерів M

Відповідно отриманих даних, оптимальним способом верифікації за критеріями якості верифікації є перший спосіб. Це пояснюється тим, що саме на своїй моделі отримана цільова функція для тестової фотографії є максимальною. Другий спосіб являєтьсянайгіршим. Час розпізнавання для кожного з методів не перевищує 10^{-3} секунди.

Система контролю доступу falsepositive надає доступу людині, для якої цей доступ не передбачений, а falsenegative система помилково відмовляє в доступі авторизованого користувача. Система з контролем доступу falsenegativeвимагає співробітнику служби безпеки перевірити два рази пропуск

співробітника. Надання несанкціонованого доступу потенційному порушнику (falsepositive) може привести до набагато гірших наслідків.

Розробники ПЗ для розпізнавання осіб часто дають можливість налаштувати алгоритми щоб мінімізувати один з типів помилок. Для цього алгоритм повертає не бінарне значення, а дійсне число, що відображає впевненість алгоритму в своєму рішенні. Користувач таким чиномсамостійно вибирає рівень помилок на певних значеннях [15].

Для прикладу, надане зображення 1 і 2 належать одній і тій же людині, а зображення 3 невідомій особі. Далі програма оцінює своєрішення верифікації для кожного зображення (табл. 2.2).

Таблиця 2.2

Програмне оцінювання верифікації

	1	2	3
1		0.85	0.6
2	0.85		0.9
3	0.6	0.9	

Значення виставленні так, щоб жоден поріг не класифікував всізображення правильно. Значення порогу нижче 0.6 призведе до двох falseaccept (для пар 2-3 і 1-3). Даний результат можна покращити.

Вибір порога з діапазону від 0.6 до 0.85 призведе до того, що пара 1-3 буде відкинута, пара 1-2 і раніше буде прийматися, а 2-3 буде помилково прийматися. Якщо збільшити поріг до 0.85-0.9, то пара 1-2 стане помилково відхилятися. Значення порога вище 0.9 приведуть до двох truereject (пари 1-3 і 2-3) і одному falsereject (1-2). Значить кращимрезультатомє значення порогу в діапазоні 0.6-0.85 (один falseaccept 2-3) і значення порогу, що є вищим 0.9 (призводить до falsereject 1-2). Вибір значення порогу залежить від вартості помилок різних типів. В даному прикладі поріг варіюється в широких діапазонах через малі розміридатасета і через те, як ми вибрали значення

рішучості алгоритму для верифікації. Для великихдатасетівбули б більш точні значення порога. Найчастіше вендори ПЗ для розпізнавання осіб постачають значення порога за замовчуванням для різних FAR.

З зменшенням FAR необхідно все більше позитивних пар для точнішого обчислення значення порога. Так, для FAR = 0.001 потрібно щонайменше 1000 пар, а для FAR = 10^{-6} буде потрібно вже 1 мільйон пар. Складність розробки такого датасета з низьким значенням FAR провокує звернутись допублічнихбенчмарок(NIST FaceRecognitionVendorTest;MegaFace).

Типи помилок відрізняються за вартістю, і користувач може віддаватиперевагу в сторону тих чи інших помилок. Для цього треба розглянути широкий діапазон значень порога. Зручний спосіб візуалізації точності алгоритму при різних значеннях FAR полягає в побудові ROC-кривих (Receiveroperatingcharacteristic - робоча характеристика приймача).

Рішучістьпорогу та алгоритму приймають значення з фіксованого інтервалу. Іншими словами, ці величини обмежені зверху і знизу. Наприклад, це інтервал від 0 до 1. Тоді вимірювання кількості помилок варіюються значенням порога від 0 до 1 з невеликим кроком. Відповідно, для кожного значення порога отримується значення FAR і TAR (trueacceptrate). Далі проектується кожна точка (рис. 2.5) таким чином, щоби FAR відповідав осі абсцис (x), а TAR - осі ординат (y).

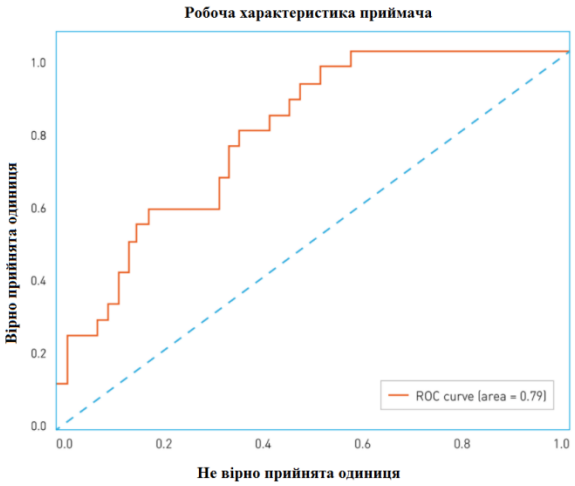


Рис. 2.5. Приклад ROC-кривої

Перша точка буде мати координати 1.1. З порогом, рівному 0, приймаютьсяі не відкидаються всі зображення. Остання точка буде з координатами 0.0.3 порогом, рівному 1,не приймається жоднезображення і відкидаються всі зображення. В інших точках крива є опукла. Найгірша крива простягається на діагоналі графіка і відповідає випадковому вгадуванню результату. Найкраща можлива крива утворюється трикутником з вершинами (0,0) (0,1) і (1,1) Проте датасети з такими потрібними розмірами дуже рідко зустрічаються.

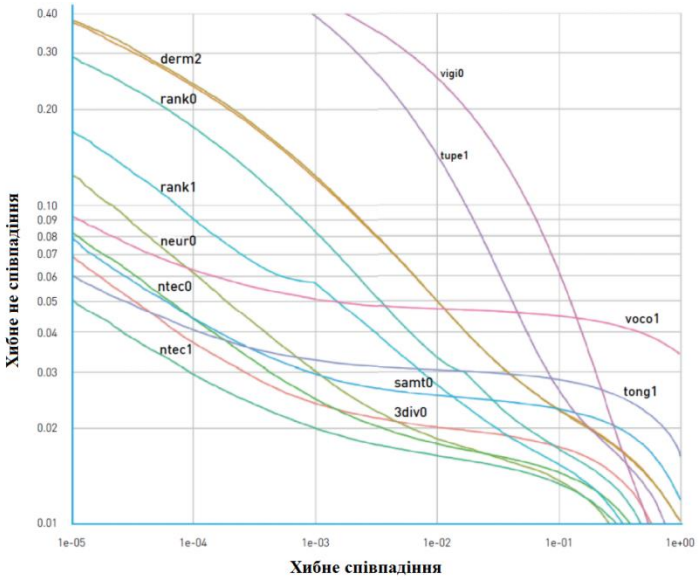


Рис. 2.6. ROC-криві NISTFRVT

На рис. 2.6 видно, що організатори NIST FRVT по осі Y намалювали FRR (на малюнку - Falsenon-matchrate), а по осі X - FAR (на малюнку - Falsematchrate). В даному прикладі кращі результати досягнуті нижчимикривими, і які зміщені вліво, що дає потрібні низькі показники FRR і FAR. Через це необхідно дивитись які величини відкладені по осях.

Достатньо знайти точку на кривій з координатою X рівній потрібного FAR і відповідне значення TAR для оцінювання точності алгоритму з заданим FAR. Якість ROC-кривої можна оцінити одним числом порахувавши під нею площу. Тоді краще можливе значення буде 1, а значення 0.5 - випадкове

вгадування. Таке число називають ROC AUC (AreaUnderCurve). Проте ROC AUC передбачає, що помилки першого і другого роду однозначні, але це не завжди так. При відмінностях вартості помилок, необхіднопридивитись на форму кривої і ті області, де FAR відповідає вимогам [15].

2.3. Системи верифікації особи в телекомунікаційних мережах

Систем розпізнавання особи вимагають обчислювальні ресурси. Всі отримані з камер зображенняобробляються в максимально швидкі терміни. Однак для видачі людині доступу система повинна зіставити зображення з відеокамери з наявною базою даних.Організації з великою кількістю співробітників мають безліч камер, що спричиняє велику потужність споживання [11-14].

Обробка одного кадру відбувається близько двохсотмілісекунд, одне ядро обробляє п'ять кадрів щосекунди. Згідно обчислень, для чотирьох каналів потрібно комп'ютер з процесором 4.2 ГГц і вище (оптимальний буде процесор 7-го покоління Nvidia) та оперативною пам'яттю від восьми гігабайт.

Розпізнавання осіб не дає 100% результату, тому вона має деякі обмеження. В режимі верифікації коректна робота гарантується тільки при обмеженій кількості осіб в базі СКУД - до 1000. Також на роботу системи впливають [11-14]:

- орієнтація особи щодо камери;
- якість фотографій і відео потоку;
- якість освітлення в зоні розпізнавання;
- розмір особи в кадрі (мінімально допустимий розмір - 100px).

Існують багато систем верифікації особи, серед яких [11-14]:

- системи, які контролюють доступ корпоративного масштабу NODER (ITV Group);
- система Sigur;
- система RusGuard;

- система Neurocore;
- програмний комплекс Візир (група компаній ЦРТ);
- система Concept;
- система NtechLab.

Програмне забезпечення СКУД NODER (рис. 2.7) з інтелект - платформою безпеки надає доступ до даних бібліотек ідентифікації осіб від відомих виробників. Їх особливість полягає в використанні штучних нейронних мереж і liveness-технологій (відрізняють реальне обличчя від використовуваної картинки), саме вони гарантують високоточне розпізнавання особистості.

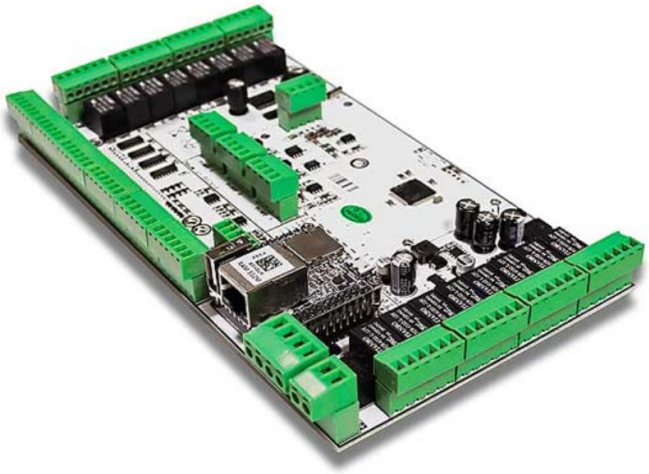


Рис. 2.7. Системи, які контролюють доступ корпоративного масштабу NODER (ITV Group)

СКУД NODER дає можливість:

- створити точки проходу із забезпеченням доступу ідентифікованого користувачеві;
- провести двухфакторную систему розпізнавання по пропуску та особі.

Функції ПЗ можна зробити кращими або змінити. Наприклад, доступ співробітникам або іншим особам може видаватися при схожості з зображенням з бази даних на певну кількість відсотків. Припустимо, мінімальний поріг - 80%. Співробітнику з нижче 80-ти відсотком схожості не надається доступ до об'єкта і зобов'язаний звернутися до охоронця або

оператору. Здійснюється і попередження оператора світлозвуковим сигналом про використання чужої картки доступу.

Всі події, що відбуваються, записується на відео. Дані систем розпізнавання осіб може бути використана для обліку робочого часу.

Використання системи розпізнавання осіб Sigurвідбувається без додаткове ПЗ або дорогого обладнання. В систему вбудовані необхідні алгоритми, а для роботи Sigur необхідні звичайні IP-камери. Технологія заснована на згорткахнейро-мережах, які дають можливість розпізнатиосіб при поворотах і розмитті зображення. Також дана система використовує алгоритмиверифікації для систем відеоспостереження. Серед них відомі Macroscop, Connection, Форпост.

Sigur дозволяє впроваджувати верифікацію осіб з використанням сторонніх схем дій, як,наприклад, компанія NtechLab.

Функція розпізнавання осіб використовується в Sigur для автоматичної ідентифікації співробітників в точках проходу. Процес розпізнавання включає в себе захоплення особи співробітника на відео і порівняння даного зображення з уже наявною базою фотографій персоналу в СКУД (рис. 2.8). Відеопотокотримується як з IP-камер, підключених до системи безпосередньо, так і камер з інтегрованих в Sigur систем відеоспостереження.

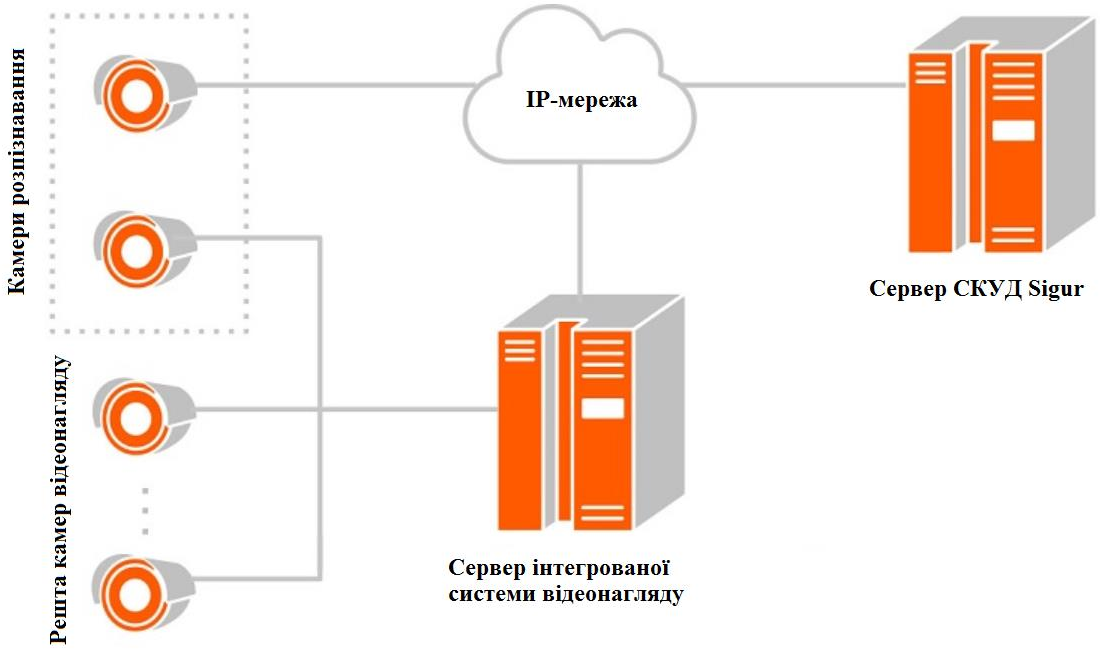


Рис. 2.8. Процес розпізнавання Sigur

В даній системі біометрична ознака є додатковою. Основна ознака- будь-який інший ідентифікатор, наприклад, безконтактна картка. Режим верифікації може бути:

- жорстким - після ідентифікації за основною ознакою система виробляє порівняння зображення, отриманого з камери з фотографією співробітника. У разі, якщо особу не розпізнано або працівник не з'явився в кадрі протягом 5 сек, система забороняє доступ.
- м'яким - система надає доступ в будь-якому випадку, проте якщо особу так і не було розпізнано, буде виведено відповідне поле в інтерфейсі спостереження.

Дана технологія є нова.Перевага - миттєво і безпомилково здійснює діяльність на нових комп'ютерах.

Рис. 2.9. СистемаRusGuard

Відмінною особливістю рішення компанії RusGuard (рис. 2.9) - використання власних терміналів розпізнавання, які легко можна інтегрувати в існуючу СКУД. В рамках використання даних пристроїв можна налаштувати роботу за кількома логіками - прохід тільки по обличчю чи по карті та обличчі.

В системі Neurocore контроль за доступом здійснюється через СКУД Octagram. Вона надає дані методів і засобів, що дозволяють взаємодіяти базі

даних працівників, їх зображень, бібліотеці подій, ПЛК, а також доступам до контрольних пунктах.Також можлива експлуатація інших СКУД.

СКУД Octagram записує нових працівників в систему через графічний інтерфейс, де зберігаються всі дані працівників організації. Списки осіб, яким було видано доступ, є в GUI. Управління камерами виконується за допомогою протоколів HTTP / HTTPS або RTSP (залежить від характеристик камер), що дає можливість підключити до системи звичайні IP-камери. Частина системи, що відповідає за розпізнавання осіб, являє собою окремий сервер, розташований безпосередньо в самій організації або у віддаленому місці, що знижує ризик перевантаження сервера СКУД. Даний алгоритм розпізнавання осіб простий і швидкий в реалізації та налаштуванні.

Комплекс Візир (рис. 2.10) був створений центром мовних технологій. Він здійснює фази біометричних функцій, включаючи механічну фіксацію зображень осіб з аналізом якості, верифікацію користувачів, трансляцію керуючих сигналів в бази СКУД. Унікальність даного комплексу полягає в відкритій платформі, що підтримує протокол інтеграції, завдяки чому відеоідентифікація впроваджується в різні системи відеоспостережень і контролю доступу.

Використання комплексу Візир проводиться в спортивних спорудах, де технології розпізнавання осіб взаємодіють з квитково-касовими системами.

Перевага – висока надійність системи - на 10 тисяч проходів тільки 1 випадок неправильної ідентифікації особи; потоковий режим розпізнавання осіб, що забезпечує швидку перевірку осіб і відсутність черг.

Ядро системи розпізнавання Concept дозволяє виконувати верифікацію як по фотографії, так і відеопотоку. При відеопотоці система об'єднує результати верифікації для різних кадрів і по системі голосування приймає рішення, що підвищує вірогідність результату порівняння.

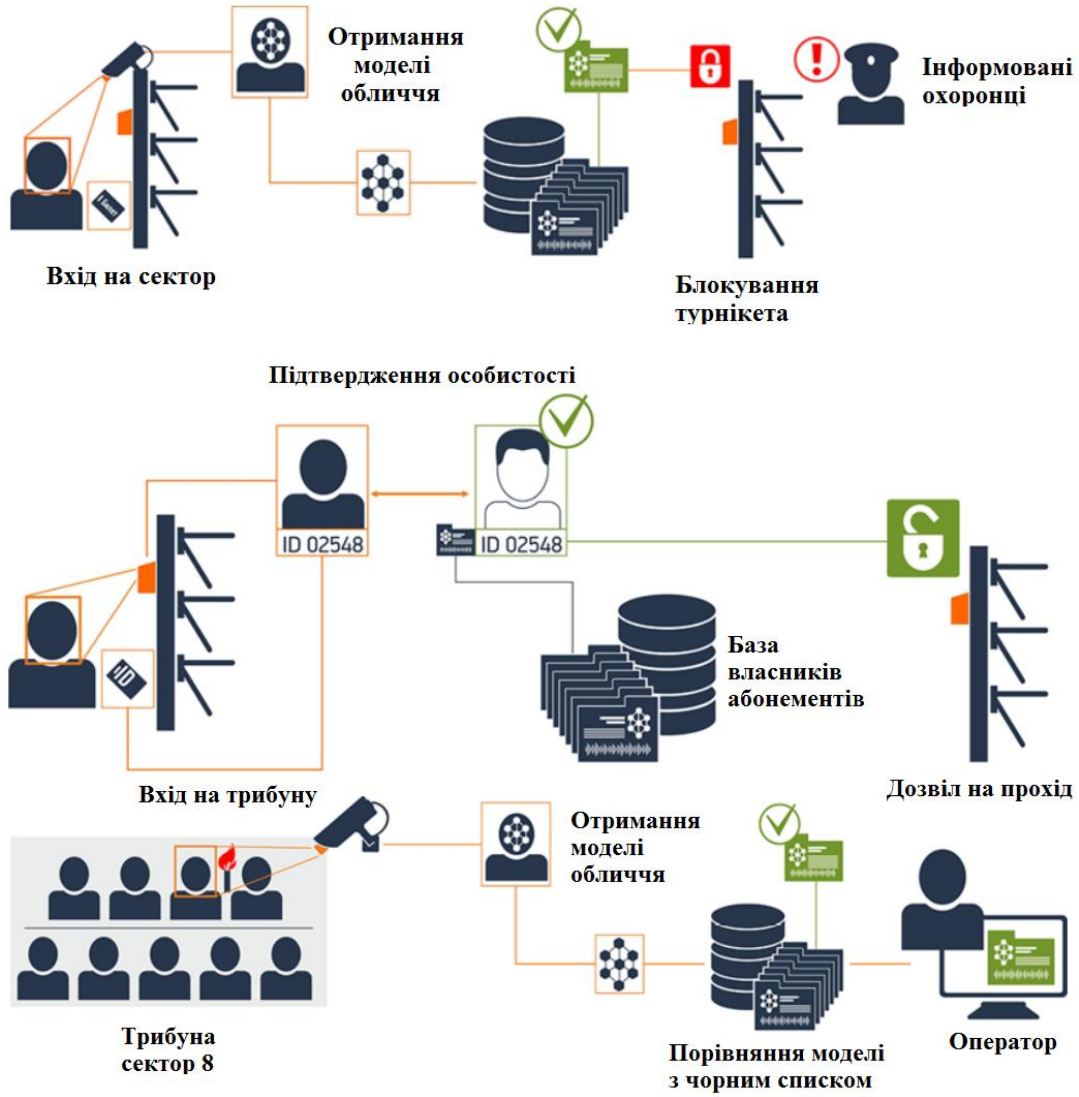


Рис. 2.10. Комплекс Візир

В якості вхідних зображень використовуються зображення з web-камер і сканування паспортів.

Алгоритми верифікації оптимізовані для роботи з фотографіями і сканами засвідчених документів із присутніми проблемами відображення голографічних відблисків від елементів захисту. При проектуванні шаблону ці відблиски виявляються, позначаються як елементи маскування і при зіставленні шаблонів не враховуються, що підвищує точність розпізнавання при відблисках.

Алгоритм NtechLab (рис. 2.11) здатний розпізнавати необмежену кількість осіб в кадрі, що робить його ідеальним рішенням для забезпечення

безпеки в місцях масового скупчення людей. Алгоритм NtechLab використовує кілька нейронних мереж для пошуку та ідентифікації по зображенню особи. Одна з мереж розпізнає особу на фото або відео потоці, друга витягує біометричний шаблон, інші працюють з атрибутами (стать, вік, окуляри, борода тощо).

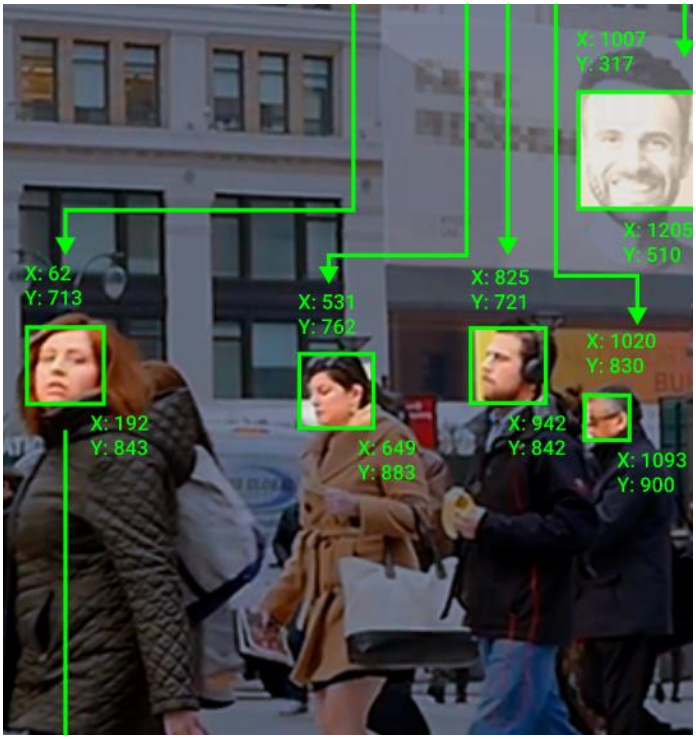


Рис. 2.11. Система NtechLab

Головні завдання, які ефективно вирішує розпізнавання за силуетом - миттєвий і точний підрахунок величезної кількості людей в відеопотоці, а також міжкамернийтрекінг силуетів.Швидкість роботи детектора не залежить від кількості осіб в кадрі.

NtechLab використовує власну технологію визначення Liveness. Технологія спроектована на пасивному методі детектування, для вирішення завдань управління доступом і авторизації в мобільних додатках.

Дані системи і методи розпізнавання особи відрізняються між собою різними характеристиками та способами здійснення верифікації, проте в всіх них присутні недоліки. Дані недоліки пов’язані із освітленістю, кутом огляду,

рухом, не якісним обладнанням, через що можливі помилки в подальших процесах із зображенням.

2.4. Методи обробки зображення

Для забезпечення високої достовірності інформації та швидкодії самої ідентифікації, в системах верифікації важливе місце має попередня обробка зображення. Дані процеси мають ключову роль в початкових етапах верифікації, оскільки дають в кінцевому результаті якісніше зображення, ніж при поступленні, що спрощує подальші етапи систем [16-26].

Цифроваобробка зображень - це зміна даних, представлених у вигляді цифрових фотографій. Результатом обробки також є цифрове зображення. Мета обробки - покращенняфото для кращого сприйняття людиною (підвищення якості, корекція кольору і контрасту, усуненняшумів зображення) і їх подальший автоматизований аналіз (наприклад, фільтрація, математична морфологія, сегментація, виділення об'єктів тощо) [16].

Візуальне оцінювання якості зображення - це суб'єктивний процес, який не можливо оцінити чисельно. Коли метою є обробка зображення для комп'ютерного аналізу, завдання оцінювання простіше. Наприклад, при вирішенні задачі розпізнавання символів кращим буде той метод обробки зображення, завдяки якому будуть отримані більш точні результати машинного розпізнавання [17].

При відновленні зображення також виконується покращення, проте не в всіх випадках воно є коректним.Відновлення зображення оцінюється більш об'єктивно.

Методи обробки зображень при виправленні дефектів зображень спричиняються [16-26]:

- шумом (випадковими похибками кольору в окремих пікселях зображення);

- недостатньою (надлишковою) яскравістю;
- недостатньою контрастністю або вузьким динамічним діапазоном зображення;
- неправильним колірним тоном;
- недостатньою різкістю (розфокусуванням);
- спотвореннями через пил, подряпин на сканованому документі;
- дісторсією (викривленням);
- необхідністю ретуші фотопортретів – це виявлення і видалення або зменшення програмношкірних пошкоджень з порізами, забіями, гематомами, усунення ознак старіння тощо. Тобто, це програмні операції з метою удосконалення візуальної зовнішності особи при різних її недоліках чи тимчасових порушеннях.

Згідно обчислювальної складності з урахуванням кількості пікселів, що беруть участь в обчисленні значення яскравості одного пікселя нового зображення, методи ділять на три класи [18-22]:

- точкові (в обчисленнях використовується значення одного пікселя вихідного зображення);
- локальні (в обчисленнях використовуються значення декількох сусідніх пікселів в заданій околиці);
- глобальні (при обчисленні значення пікселя використовуються всі пікселі вихідного зображення).

Існують такі рівні процесівкомп’ютерного зору[19-24]:

- низького - це найпростіші операції над зображеннями, як зниженнязавад, збільшення контрастності або чіткості. Вони характеризуються тим, що на початок і кінець систем надходять зображення;
- середнього - це сегментація, доданняданим зручної форми з виділенням при подальшій комп'ютерній обробці;
- усередненого рівня мають на вході фото, а на виході –параметри та характеристики цих фото;
- високого рівня - це аналіз розпізнаних об'єктів.

Для усунення спотворень, внесених в процесі реєстраціїзображень, часто використовуються методи геометричної корекції і корекції яскравості. При обробці космічних знімків застосовують атмосферну корекцію зображень [16,21,26].

Для покращення зображення буде використовуватись програмаMatLab. Вона дає змогу виконувати різні наукові і технічні дослідження. Поставлені задачі можуть здійснюватись через різні складні та прості програмні операції, що представлені в простому, математичному виді [24-26].

Існують такі відомі методи покращення зображень [16-26]:

- сегментація;
- градаційні перетворення (рис. 2.12);
- поелементні перетворення;
- гістограмні перетворення;
- просторова фільтрація;
- виділення краю об’єкта.

Сегментація.

При даному методі обробки розглядаються такі основні види покращення [16-26]:

- метод нарощування;
- метод злиття-розщеплення;
- метод водорозділів;
- центроїдне зв’язування;
- метод деформованих шаблонів;
- ієрархічна кластеризація;
- нейронна мережа.

Метод нарощування проводить відбір початкових точок і наступним аналізом сусідніх ділянок з певним критерієм однорідності. Ці вибрані ділянки потрапляють в відбірні групи.

Метод злиття-розщеплення здійснює попередній вибір однорідних областей з поступовим нарощуванням.

Метод водорозділів полягає в виборі однорідних областей на основі градієнта інтенсивності зображення.

Метод центроїдного зв’язування проводить аналіз початкових областей зображення.

Метод деформованих шаблонів проводить вибір шаблонів з мінімізованою цільовою функцією по параметрам, що характеризує геометричну форму зображення.

Метод ієрархічної кластеризації полягає в поетапному об’єднанні (або роз’єднанні) кластерів зображення відносно дальності один до одного. Об’єднані чи роз’єднанні кластери вміщують в собі характеристики кольорів.

Метод нейронних мереж вміщує в собі самоорганізовані карти Кохонена, що здійснює автоматичне навчання та проводить візуалізацію і кластеризаціюфотографій. Для цього проектується широкий простір зображення в простір з меншою розмірністю фотографії.

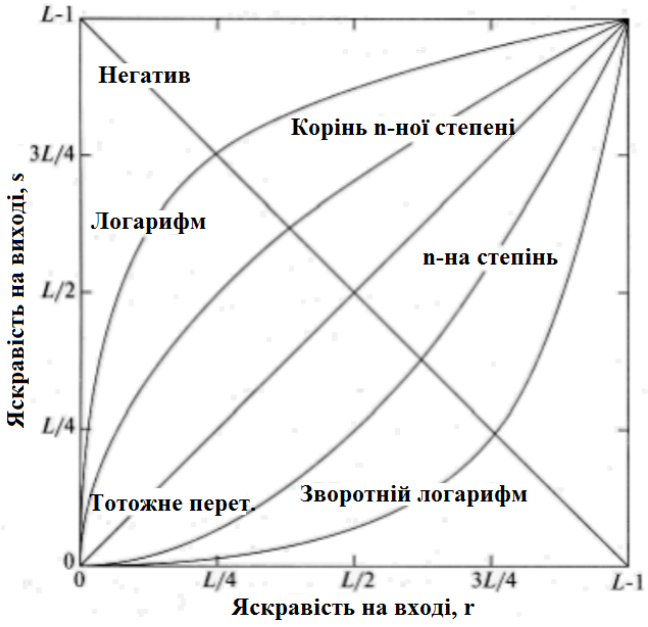


Рис. 2.12. Методи градаційних перетворень

Просторові градаційні перетворення.

В даному методі це процедури, які керують кожною деталею зображення.Вони описуються рівнянням:

$$s(x, y) = T[r(x, y)], \quad (2.1)$$

де s і r –це рівень яскравості початкового і результуючого зображення (x,y); T -цефункція перетворення кінцевого зображення (максимум 256 елементів).

Змінні s(x,y) залежать від змінних яскравості r(x,y)результуючого зображення; T - функція відображенняабо функція перетворення інтенсивностей.

В даному методі обробки, результат обробки кожного елемента зображення залежить лише від яскравості одного і того самого елемента.

Існують такі види градаційного перетворення:

- лінійного типу (негативне);
- логарифмічного;
- статичного(n-я ступінь і корінь n-го ступеня).

Негативне перетворення.

Для виконання певних дій з яскравостями, часто використовують частинно-лінійні функції перетворення зображення. При цьому методі через операцію incomplementпроектується негатив з зображень для різних задач користувача (рис. 2.13).

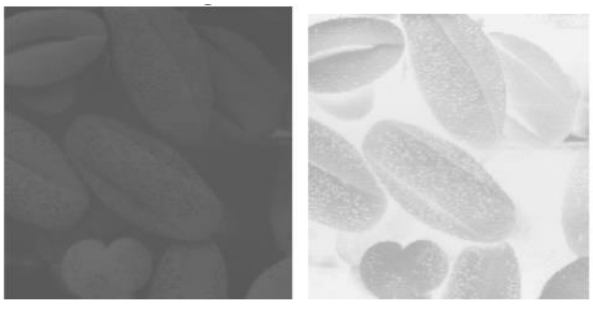


Рис. 2.13. Прояв негативу через операцію incomplement

Також через операцію polyline2 та imadjust відбувається підвищення контрастності зображення (рис. 2.14).

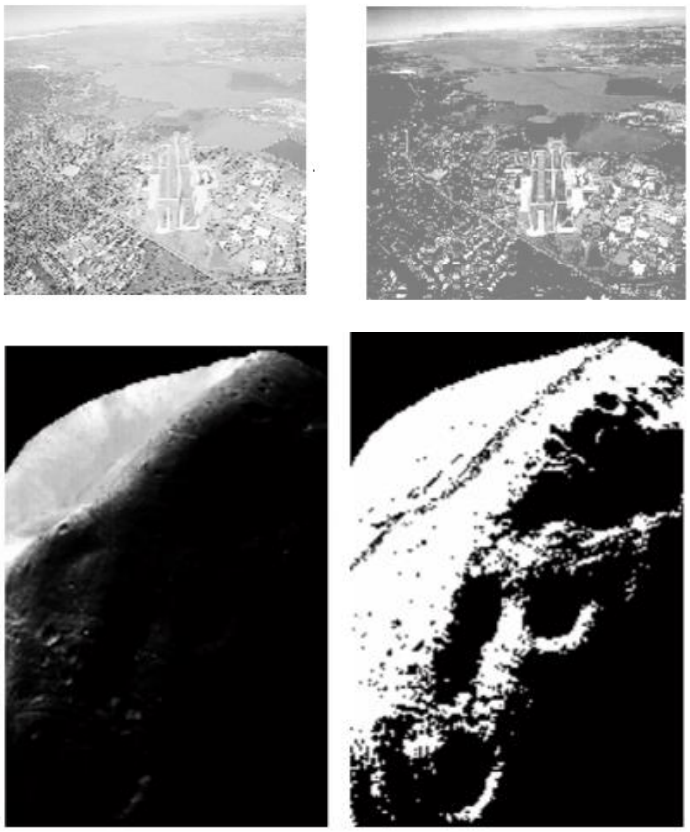


Рис. 2.14. Підвищення контрастності зображеннячерез операцію polyline2 та imadjust

Операція imadjust (f, [0 1], [1 0]) є цифровим еквівалентом отримання фотонегативів і використовується дляпідсилення білих або сірих ділянок, що оточенітемнимиділянками.

Логарифмічне перетворення.

Серед методів обробки зображень, часто використовують логарифмічне перетворення (рис. 2.15).

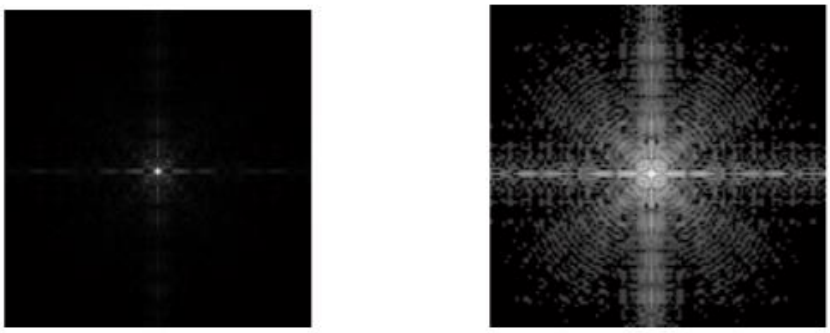


Рис. 2.15. Логарифмічне перетворення

В даному методі для того, аби побачити ціле зображення, з всіма його яскравостями, проведено виклик спектру яскравостей. Після цього здійснено операцію перетворення - розтягнення зображення по контрастності. При цьому, до попередньої операції double, додається epsдля уникнення помилок переповнення, тобто певний поріг:

$$g = 1./(1 + 0.5./ (f + eps)).\hat{}20) \quad (2.2)$$

Зворотнє логарифмічне перетворення.

Загальний вигляд зворотнього логарифмічного перетворення має вигляд:

$$s = clg(1 + r), \quad (2.3)$$

де c - константа (умова константи r> 0).

Даний метод здійснює зворотнє логарифмічне перетворенняз збільшенням діапазону світлих областей і зжимання діапазону з темними областями зображення, тим самим покращуючи зображення.

Статичне перетворення.

Даний метод обробки має такий вигляд:

$$s = cr^{\gamma}, \quad (2.4)$$

де c та γ – позитивні константи.

При малих значеннях константиγ здійснюється перетворення малого діапазону початкових значень зображення в широкий діапазон значень результуючої фотографії.Даний метод перетворення відрізняється від логарифмічного отриманням сімейства кривих перетворення, які регулюються зміною параметра γ.

Гамма-корекція.

Дана функція необхідна для правильного (природного) відтворення кольорів абиточніше відтворити зображення в цифровому вигляді.

Кусково-лінійні функції перетворення.

Даний метод обробки здатний виконувати більш складні перетворення зображень з використанням додаткових параметра мів та кусково-лінійних функцій.

Підвищення контрастності.

Якщо помітна частка пікселів займає значну частину всього діапазону рівнів сірого, то ми говоримо, що фото має високий контраст.

Зображення з малим динамічним діапазоном зазвичай виглядає тьмяним, розмитим і сірим. Збільшення динамічного діапазону зображення робить його більш контрастним.

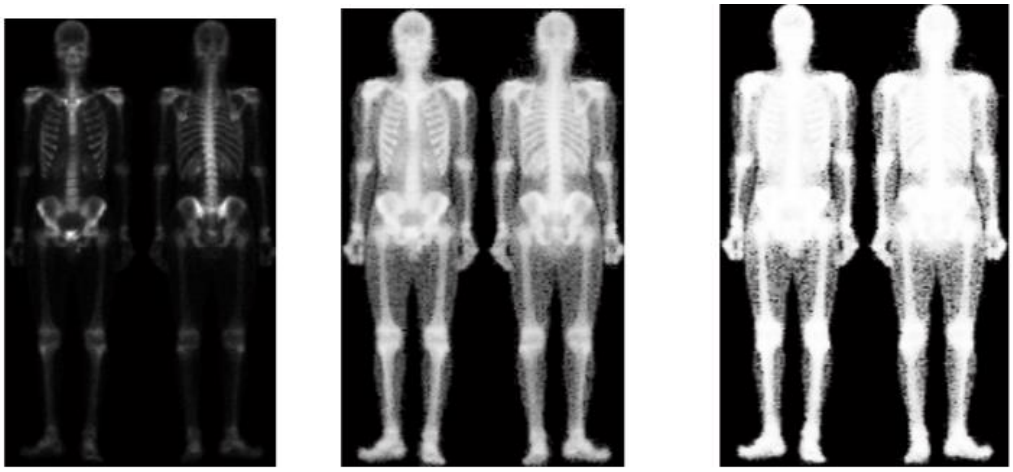


Рис. 2.16. Підвищення контрастності

На рис. 2.16 показано вхідне зображення, зображення із розтягненою контрастністю і підвищеною контрасністюз використанням операції double:

$$g = double(image)./(double(f + 10), \text{де} \qquad (2.5)$$

double (image) – операція підвищення контрастності вхідного зображення;

double(f+10) – саме значення контрастності, яке корегується.

Вирізання діапазону яскравостей.

В цьому методі покращенні зображення здійснюється відображення лише тих рівнів яскравості, які нам необхідні. Тобто, виникає певна фіксація області. Потрібна область буде мати один рівень яскравості, а не потрібна – інший.

Вирізання бітових площин.

Цей метод дуже похожий до попереднього з вирізанням діапазону яскравостей, проте виділяється область з інформацією бітів зображення. При цьому, початкова фотографія повинна бути закодована 8-ма бітами. Старші біти (7-4) вміщують в собі найважливішу інформацію про об’єкт. Рівні зображення даного методу можуть представлятись від 0 до 255.

Поелементні перетворення.

Даний лінійний метод є найпростішим, що здійснюєфункціональне перетворення для кожного елемента матриці в кожній точні на зображенні. Даний метод має наступний вигляд:

$$g = g(f), \tag{2.6}$$

де значення кожного елемента f перетворюється в нове значення g.

Соляризація.

В цьому методі обробки фотографій (рис. 2.17) світлі ділянки початкових експериментних даних в результаті мають рівні чорного з збереженням чорних ділянок та фону.

Рис. 2.17. Соляризація зображення

Порогова обробка.

Даний метод обробки поділяє всі елементи зображення по класах яскравості з по елементним перетворенням. При цьому важливим є вибір порогового значення обробки, від якого залежить плавність перепаду яскравості.

Препарування.

Метод препарування (рис. 2.18) – це обробка зображення до такого виду, щоби краще сприймалось користувачеві, але яке може буде далеке від природного виду. Одною із таких обробок є порогова, де виділяється потрібна інформація з збереженням фону.

Рис. 2.18. Препарування зображення з пороговою обробкою та пилкоподібним контрастуванням

Наступний різновид такого методу є контрастне масштабування, яке ідентичне лінійному контрастуванню або ж в ньому застосовуються функції, що приводять зображення в негатив.

Пилкоподібна контрастне масштабування полягає в плавній (практично не замітній) зміні яскравості, що дозволяє покращити чіткість.

Гістограмні перетворення.

Наступний метод полягає в пошуку гістограм з їх графіками для визначення областей з недостачею яскравості або перебільшенням для покращення зображення (рис.2.19).

Гістограма зображення показує найбільше інформативних характеристик. При аналізі гістограми можна побачитичи зображення є затемненим або засвіченим. В ідеальних умовах гістограма зображення повинна бути рівномірною.

Рис.2.19. Покращення зображення з використанням гістограм

Якщо на гістограмі чи графіку є згруповані області, то для підвищення контрастності зображення необхідно розширити діапазон яскравості, що відповідає цій області.Виведення гістограм виконується операцією imhist.

Метод еквалізації (рис. 2.20) збільшує динамічний діапазон рівня яскравостей, збільшуючи контрастність зображення на виході операцією histeq (image, 256).Число 256 – число рівнів інтенсивності, вибрані для вихідного зображення.

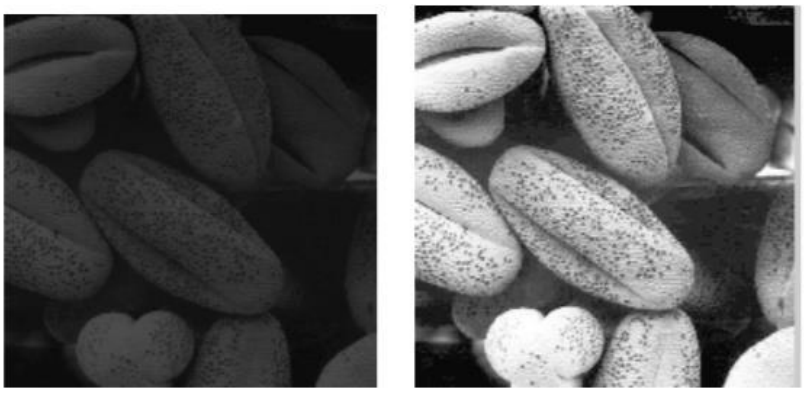


Рис. 2.20. Еквалізація зображення

При обробці зображення також використовується з заданою гістограмою через функцію histeq (image, hspec)– гістограмний підгін (рис. 2.21). Операція hspec – задана гістограма для вихідного зображення.

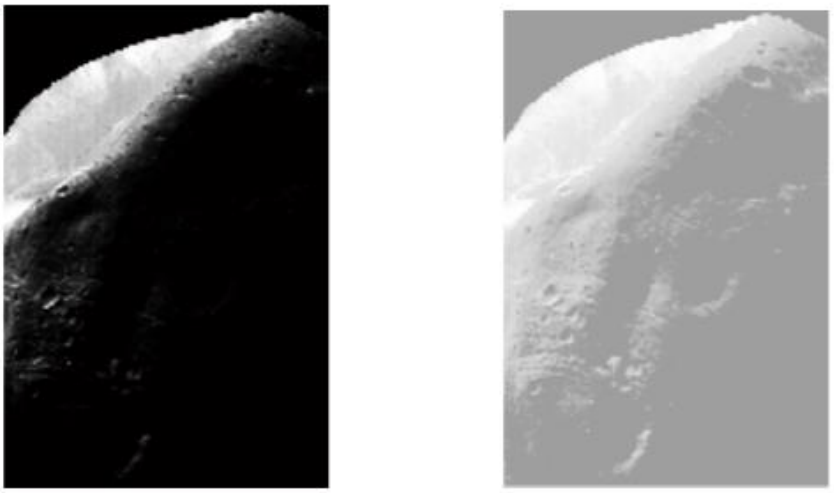


Рис. 2.21. Гістограмний підгін

Локальне покращення.

Даний метод покращення полягає в роз приділенні рівнів яскравостей (або інших параметрів) по ділянці кожного елементу зображення. При цьому задається квадратна чи прямокутна форма навкруги всіх елементів зображення, які обробляються. Далі центр кожної з таких областей рухається від точки до точки, тим самим підраховуючи гістограму і видаючи функцію перетворення еквалізації чи проведення гістограми. Ця функція відображає рівень яскравості центрального елемента, після чого центральні частини рухаються до сусідніх. Даний процес повторюється.

Просторова фільтрація.

Даний тип фільтрації тісно пов’язаний із застосуванням перетворення Фур’є і обробці сигналів в частотній області.

При перетворенні Фур’єзначна увага приділяється проекції початкового та кінцевого зображення, що дозволяє краще проаналізувати чіткість результуючого зображення.

Просторова фільтрація основана на застосуванні матриць коефіцієнтів фільтру (масок), що присутні на початковому зображенні та для кожної точки зображення здійснюєпевну операції,яка використовує лише значення яскравості пікселів у фіксованій ділянці навколо цієї точки.

Перший метод використовує операцію imfilter (рис. 2.22).

Рис. 2.22. Покращення зображення через imfilter

На рис. 2.22 видно розгалуження чорних деталей. Щоб цього позбутися, необхідно використовувати нормування коефіцієнтів фільтрації.

Метод зворотної проекції.

Даний метод оцінює щільність пікселів зображення в кожній точці шляхом проектування сукупність променів, які проходять через дану точку. Після цього отримується приближена апроксимація початкового зображення.

Метод зворотної проекції з фільтруванням згортки.

Цей метод обробки такий самий, як і попередній але є більш точним за рахунок фільтрації променів, що є зворотніми. Це дозволяє усунути ефект затемнення фотографії.

Ітераціонний метод.

В даному методі наперед вибираються зображення і розраховуються для них проекції. Далі до зображення додаються певні корекції для покращення збігу експериментальних проекцій з тими, що є. Даний процес повторюється до необхідного збігання проекцій.

Лінійні згладжуючи фільтри.

Згладжуючі фільтри використовуються для розфукусовки зображення та подавлення шуму. При даному методі обробки здійснюється заміна початкових значень елементів зображення на середні значення (одинакові коефіцієнти) по масці фільтру для більш плавного переходу рівня яскравостей. Таким чином зменшується рівень шуму. Лінійний згладжуючий фільтр має за основу подавлення деталей фотографії, які нам не потрібні.

Застосування фільтра Вінера (рис. 2.23) вимагає використання спектральної щільності потужності зображення. Отримання цього здійснюється через зміну певних параметрів чи характеристик початкового зображення. Технічно фільтр Вінера реалізується через дискретне перетворення Фур'є та з використанням рівнянь Вінера-Хопфа.

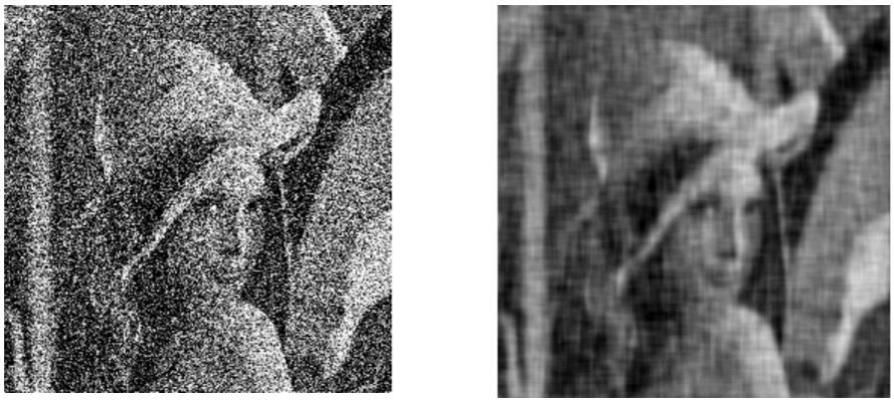


Рис. 2.23. Обробка зображення фільтром Вінера

Байесовська фільтрація має дуже високі вимоги до об'єму та характеру експериментальних даних з сигналами та шумами та застосовує складні математичні розрахунки.

В якості фільтрації також застосовуються Марківські фільтри (рис. 2.24). В даному методі застосовується оцінка зображення, після чого здійснюється сама фільтрація.

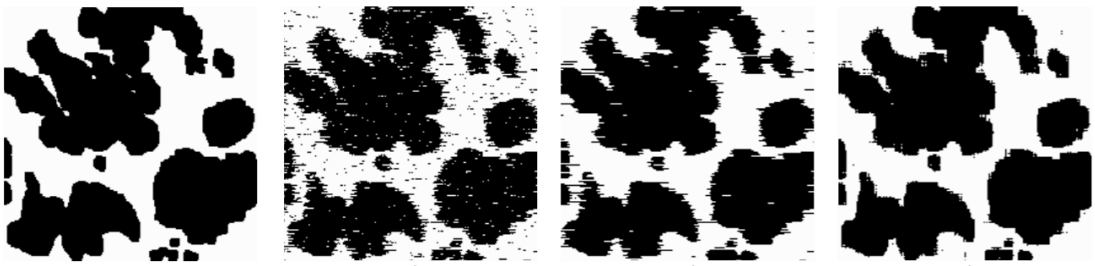


Рис. 2.24. Марківський фільтр

На рис. 2.24 показано Марківський фільтр з одномірною казуальною фільтрацією, одномірною не каузальною фільтрацією та двохмірною не каузальною фільтрацією.

Часто для покращення зображення використовується фільтр Лапласа (рис. 2.25). При цьому методі використовується операція imfilter та проектування самого фільтру операцією fspecial (‘laplacian’, 0).

Рис. 2.25. Обробка зображення фільтром Лапласа

На рис. 2.25 видно, що даний фільтр підкреслює області з значними змінами рівнів яскравості та подавляє решту деталей.

Не різке маскування та фільтрація з підніманням високих частот.

Для отримання більш чіткої фотографії, на негативне початкове зображення накладається розфокусований позитив, що спричиняє до експозиції з двохшаровим оригіналом.

Покращення з використанням градієнту.

В цьому методі обробки експериментальних даних, початкове зображення перетворюється в модуль градієнта. Спочатку визначаються дискретні величини для початкового зображення, після чого по них формуються маски фільтрів (наприклад, маскиСобеля, маски Прюїтта, маски Шарра, Робертса, Канні тощо).

Метод Собеля (метод Шарра, Канні тощо) використовує спеціальні ядра (оператори Собеля), що застосовуються до кожної точки зображення.

Значення градієнта визначається як квадратний корінь з суми квадратів значень вертикальних та горизонтальнихскладових з отриманням даних, що характеризують зміни яскравості в певнихділянкахфотографії.

Градієнт часто використовується для виявлення дефектів деталей, що не помітні для людського ока, підкреслюючи малі деталі.

При фільтрації з підняттям високих частот необхідно ретельно підбирати коефіцієнт підсилення частот, що збільшує рівень яскравості. Чим більший цей коефіцієнт, тим світліша стає результуюча фотографія.

Медіанна фільтрація (рис. 2.26) дуже ефективна при видаленні ззображень імпульсних шумів. Даний метод здійснюється через операцію medfilt2(image).

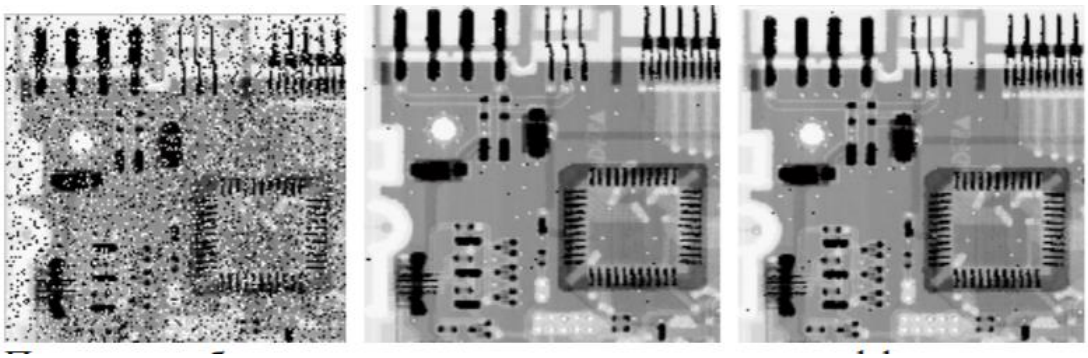


Рис. 2.26. Обробка зображення медіанною фільтрацією

Такі фільтри здійснюють попереднє впорядкування значень пікселів зображення і наступним вибором значень, що знаходяться на певній позиції. Таким чином фільтрація здійснює заміну початкових значень пікселів

фотографії (в центрі маски) на отримані значення фільтру (медіани). В результаті отримується заміна відмінного від фону значення пікселя на інше значення, що є ближчим до сусідів.

Просторові фільтри підвищеної різкості.

Даний метод збільшує чіткість розфокусованих або малих деталей зображення та використовується в електронному друці, медицинській інтроскопії, системах автоматичного наведення тощо. Дані операції здійснюються через просторове диференціювання, що дозволяє підсилити перепади яскравості та шуми без зачіпання областей з плавними перепадами яскравостей.

Локально-адаптивна фільтрація.

Даний метод обробки зменшує шуми на однорідних ділянках з збереженням контурних деталей та текстури зображення. Для фільтрації ретельно підбирається коефіцієнт дискретно-конусного перетворення k так, щоби не спричиняти перефільтрацію або недостатню чіткість.

До цього методу також додають індикатор негаусівських розподілів з введенням коефіцієнта, яких дозволяє розпізнавати активні ділянки зображення.

Виділення краю об’єкта.

Краї областей зображення - це криві на зображенні, вздовж яких відбувається різка зміна яскравості або її похідних по просторових змінних. Найбільш потрібні такі зміни яскравості, де відображаються важливі особливості зображуваної області. Цеділянки, де орієнтація поверхні змінюється стрибкоподібно;перегородження об’єктів;межа відкинутої тіні; відсутність безперервності у відбивних властивостях поверхні тощо. Томунеобхідно локалізувати місця розривів яскравості або її похідних для отримання кращого фото необхідного об’єкта.

Зашумленість вимірювань яскравості обмежує можливість виділити інформацію про краях. Коротші краї зображення повинні мати більшу контрастність, ніж довгі для їх кращого розпізнавання. Виділення країв - це як

доповнення до сегментації зображення, оскільки межінеобхідно використовувати для розбиття фото на області.

При покращенні зображення часто також відбувається поєднання різних методів обробки фотографій. При цьому одна обробка може не дати суттєвого покращення, як при комбінації двох різних.

Для усунення проблем із системами верифікації в даному випадку найкраще підійде поєднання двох методів покращення зображення, а саме гістограмнаеквалізація та фільтр Лапласа. Дані методи є дешеві та прості в реалізації, а тому з легкістю можуть усунути недоліки з освітленістю, розмиттям зображення, поганим кутом огляду. Така попередня обробка зображення використовує зручне для розуміння програмне середовище MatLab та зможе підвищити надійність та швидкість системи верифікації.

2.5. Висновки до розділу 2

В розділі розглянуті відомі методи ідентифікації за параметрами обличчя, загальні характеристики методів розпізнавання особи, на основі яких побудовані системи верифікації, характеристики систем розпізнавання з їхніми алгоритмами, оцінками та графіками залежностей різних параметрів, основні складності та проблеми при верифікації, відомі системи ідентифікації з їхніми особливостями, які використовуються в різних підприємствах, виробництвах. Крім того, наведенізагальні поняття, завдання та оцінювання обробки та проаналізовано відомі методи покращення фотографій при різних задачах та умовах з їхнім описом роботи та спільними проблемами та обрано два методи попередньої обробки зображення.

РОЗДІЛ 3.
НАУКОВО-ДОСЛІДНА ЧАСТИНА

3.1.Обгрунтування методу обробки зображення

Попередня обробка зображення – це початкова форма обробки інформації у вигляді зображень, представлені відео- та фотокамерами.

Мета попередньої обробки – це отримати в результаті кращу чіткість зображення для спрощення процесів наступних етапів взаємодії із експериментними даними.

В системі верифікації основну увагу необхідно приділити саме попередньому покращенні зображення. Це дасть змогу отримати кращу достовірність експериментних даних, а також швидкодію системи верифікації при впливаючих на них завадах.

Для кращого розуміння процесу попередньої обробки, на рис. 3.1 представлено алгоритми дій в системах верифікації.

Рис. 3.1. Алгоритм попередньої обробки зображення

Сьогодні існує безліч методів обробки, основні з яких можна поділити на такі групи [16-26]:

- сегментація;
- градаційні перетворення;
- поелементні перетворення;
- гістограмні перетворення;
- просторова фільтрація;
- виділення краю об’єкта.

Кожен із методів обробки по-своєму якісно покращує зображення, проте в даному науковому дослідженні основним об’єктом є параметри лиця. При виявленні обличчя людини, на зображення часто впливають завади в вигляді поганої яскравості та чіткості зображення. Тому для цього завдання обрано комбінацію методів гістограм них перетворень та просторової фільтрації.

Обробка зображень для верифікації особи буде проводитись в два етапи:

- еквалізація гістограми зображення;
- використання фільтру Лапласа.

Метод обробки з застосуванням еквалізації гістограми та фільтру Лапласа частково або повністю усуває завади в вигляді поганої яскравості та чіткості зображення.Дані методи обробки зображень були вибрані через простоту реалізації та ефективність дії.

3.1.1.Еквалізація гістограми. При створенні зображень часто виникає необхідність їхньої обробки для кращого бачення. При цьому в більшості зображень рівні яскравостей розподілені не рівномірно і не на всьому діапазоні. Процес еквалізації гістограми якраз виконує рівномірне розподілення яскравості на всьому діапазоні. Іншими словами, здійснюється збільшення динамічного діапазону рівня яскравостей (рис. 3.2). При цьому збільшується контрастність зображення [16-26].

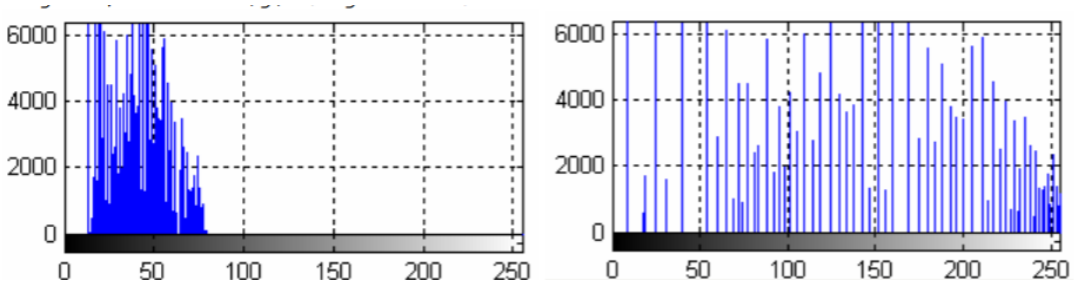


Рис. 3.2. Збільшення динамічного діапазону рівня яскравостей

Маючи справу з дискретними величинами, ми працюємо з гістограмами. Проте, сама гістограма не зможе бути ідеально рівномірною через саму природу дискретних величин. Величини нормованої гістограми є приближеними вірогідностями появлення кожного рівня яскравостей на зображенні. Для дискретних величин відбувається сумування.

Еквалізація гістограм реалізована в пакеті IPT операцією histeq:

$$g = histeq(f, nlev), \tag{3.1}$$

де f – вхідне зображення;

nlev – число рівнів інтенсивності, встановленого для вихідного зображення (по замовчуванням число 64; максимум 256).

Для еквалізації можна застосувати також операцію cumsum, що сумує величини нормованої гістограми.

3.1.2. Фільтр Лапласа. Покращення зображення через фільтр Лапласа полягає в підкресленні перепадів рівнів яскравості на зображенні при збереженні областей постійної тональності (рис. 3.3) [16-26].

Рис. 3.3. Застосування фільтру Лапласа

Фільтр w створений у вигляді квадратної матриці. Для виконання операцій фільтрації в MatLab є операціяfspecial, яка генерує маску фільтра w при виконанні команди w =fspecial ('type', parameters). 'type' позначає тип фільтра, а parameters задають параметри обраного фільтра. Цей параметр може приймати значення:

- 'Average' - прямокутний усереднюючий фільтр;
- 'disk' - круговий усереднюючий фільтр;
- 'laplacian' - фільтр Лапласа 3 x 3.

Одним із стандартних є фільтр Лапласа.Оператор Лапласа зображення f (x, y) позначається $\Delta f(x, y) = \nabla^2 f(x, y)$ і здійснюється за формулою:

$$\nabla^2 f(x,y) = \frac{\partial^2 f(x,y)}{\partial x^2} + \frac{\partial^2 f(x,y)}{\partial y^2} \tag{3.2}$$

В якості дискретних приближень похідних (3.3-3.4),використовуються вираження:

$$\frac{\partial^2 f}{\partial x^2} = f(x+1,y) + f(x-1,y) - 2f(x,y) \tag{3.3}$$

$$\frac{\partial^2 f}{\partial y^2} = f(x,y+1) + f(x,y-1) - 2f(x,y) \tag{3.4}$$

Тому, вираз 3.2 має кінцевий вигляд:

$$\nabla^2 f = [f(x+1,y) + f(x-1,y) + f(x,y+1) + f(x,y-1) - 4f(x,y) \quad (3.5)$$

Дане вираження (див. 3.5) можна застосувати в будь-якій точці (x, y) зображення, зробивши згортку з просторової маскою. Друге наближення похідних враховує значення діагональних елементів і дає маску в вигляді матриці.

Похідні часто утворюються з протилежним знаком, що приводить до зміни знаків в наведених формулах. Поліпшення зображень за допомогою фільтра Лапласа здійснюється за формулою 3.6:

$$g(x,y) = f(x,y) + c\nabla^2 f(x,y), \text{ де} \quad (3.6)$$

f (x, y) - це вихідне зображення;

g(x, y) - покращене зображення;

параметр c дорівнює 1, якщо центральний коефіцієнт маски позитивний, і c = -1 в протилежномувипадку. Оскільки оператор Лапласа є диференціальним, він підвищує різкість зображення, але переводить області з постійними значеннями яскравості в 0. Додавання вихідного зображення відновлює тональність рівнів в всьому діапазоні зображення.

Функція fspecial ('laplacian', alpha) реалізує більш складнумаску Лапласа. За допомогою неїможна точніше підстрояти результат. Це можливо здійснити через ручний підбір параметрів фільтра.

3.2. Реєстрація експериментальних даних

Для того, щоб певна система верифікації розпочала свою роботу, необхідно мати дані біометричноговерифікатора, за допомогою якого надалі буде здійснюватися верифікація користувача. В різних типах систем може

використовуватись декілька біометричних верифікаторів. Після отримання біометричного верифікатора система перетворює його за допомогою відповідних засобів в електронний вигляд. Ця стадія роботи системи біометричної верифікації називається реєстрація, тобто система отримує первісну інформацію, необхідну для її подальшої роботи. Звичайно система верифікації не зберігає зображення біометричних особливостей людини. В ній отримується шаблон версифікатора –це декілька цифрових послідовностей, які були отримані під час оброблення біометричного ідентифікатора. Проте, система зберігає персональні дані, які необхідні для подальшого доступу особи до системи. Тобто, біометричний верифікатор, який надав користувач, перетворюється в електронний вид, який потім проходить декілька стадій оброблення за різними алгоритмами, внаслідок чого отримується шаблон, за допомогою якого потім здійснюється безпосередньо процедура верифікації користувача [1-14].

У будь-якому випадку незалежно від типу біометричного верифікатора, який застосовується системою, загальний алгоритм функціонування системи біометричної верифікаціїпредставляється вигляді, показаному на рис. 3.4, а спрощена структурна схема системи біометричної верифікації показана на рис. 3.5 [6-15].

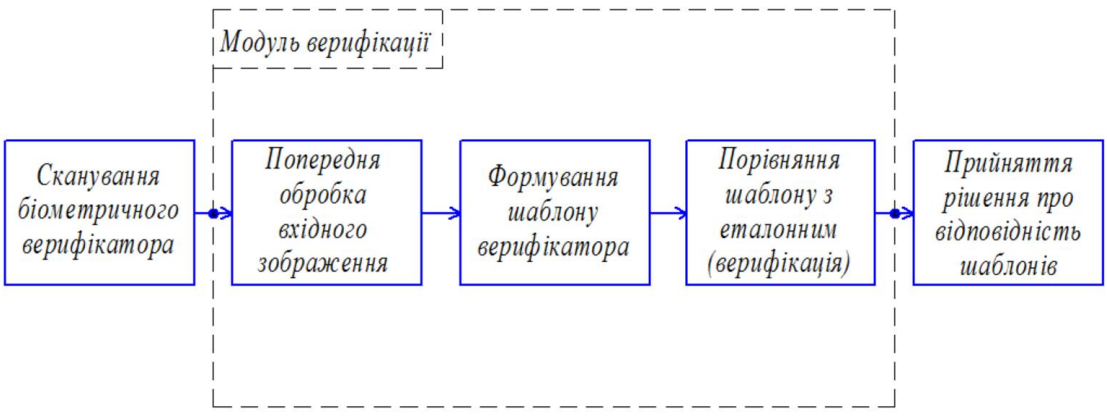


Рис.3.4. Загальний алгоритм функціонування системи біометричної верифікації

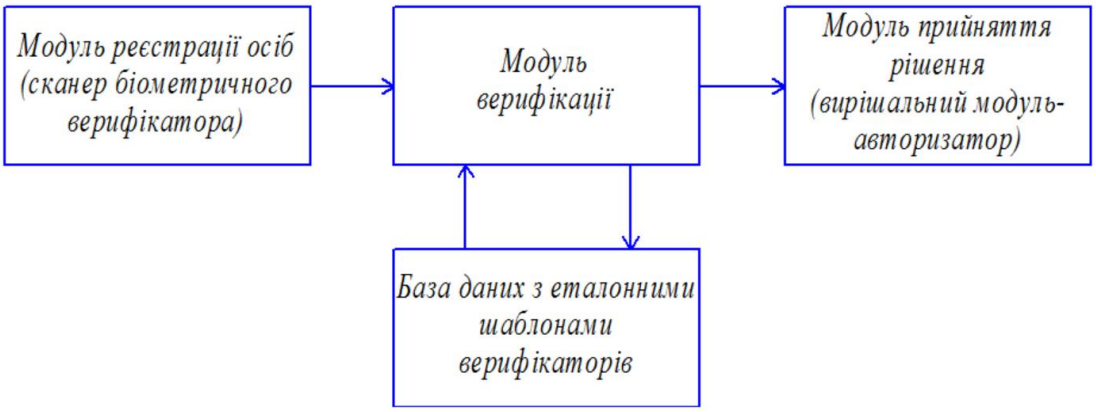


Рис. 3.5. Спрощена структурна схема системи біометричної верифікації

Після поступлення і запису вхідних експериментальних даних система здійснює процес обробки зображення та подальшу верифікацію, тобто встановлення відповідності особи та визначення її прав на інші дій.

На рис. 3.6 зображено загальний алгоритм роботи системи біометричної верифікації.

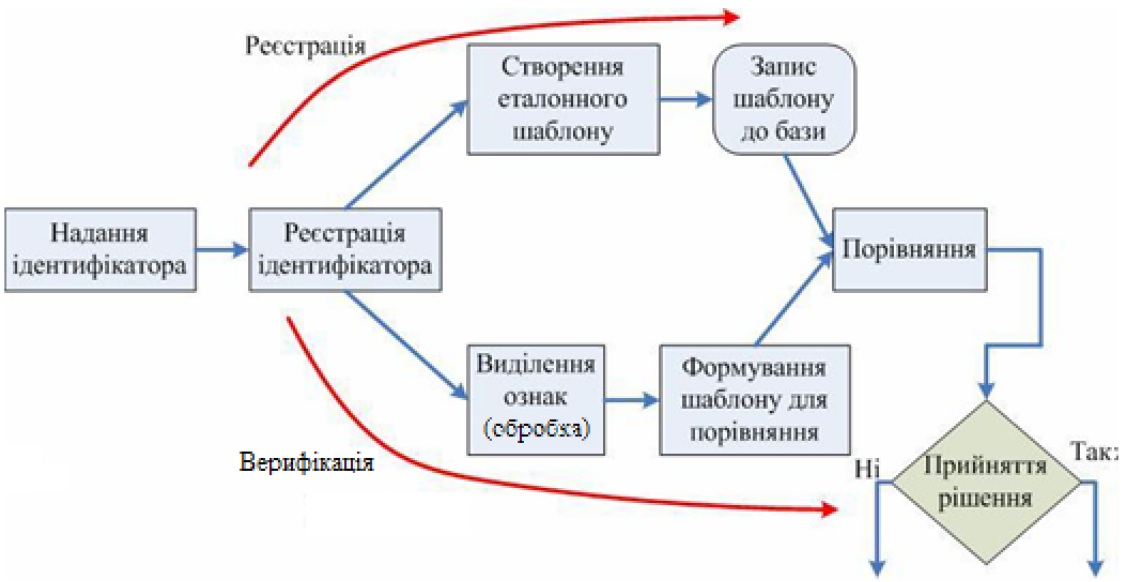


Рис. 3.6. Загальний алгоритм роботи системи біометричної верифікації

Процес верифікації користувача умовно можна поділити на дві фази – отримання зображення особи та подальша обробка для швидшої і надійнішої

верифікації. У загальному випадку, верифікація за обличчям складається з декількох етапів:

- отримання зображення та перетворення його у напівтонове зображення;
- обробка зображення (зменшення шумів, покращення якості);
- отримання результатів покращення зображень та їх порівняння з еталонними зображеннями з бази.

Процесфото сканування та відео сканування обличчя засновано на створеннішаблона в реальному часі та порівняннійого з файлом шаблона-зразка.Ступіньвідповідностіоб'єктівзображення, щопотребуютьперевіркиможе бути не однаковим для різних задач в різних системах, або ж бути залежнимвідкористувача, ПК, освітлення, модуля реєстрації зображення (фото-відео камера) та інших факторів.

Основні проблеми при верифікації, які суттєво впливають на ефективність роботи, є зміна освітлення, різні кути огляду обличчя під час руху, складність виділення інформативної частини обличчя та несприятливий фон, який визначає особу важче.

Проблеми верифікації частково, або ж повністю можна усунути через покращення зображення, що збільшить шанс достовірності та швидкодії верифікації особи.

3.3. Обробка зображення для верифікації особи

В попередньому розділі було вирішено обрати метод еквалізації гістограми та застосувати фільтр Лапласа.

Кожне зображення, яке поступає, потрібно проаналізувати в якому воно стані. В даному методі використовується гістограма, яка дасть змогу побачити розподілення рівнів яскравостей зображення. Еквалізація ж розподілить яскравість рівномірно по всьому діапазоні, а фільтр Лапласа зробить зображення більш чітким.

При виконанні операції еквалізаціїhisteq, для початку необхідно перевести зображення з RGBв напівтонове, тобто з кольорового в чорно-біле, для зменшення інформаційної надмірності. Для цього в програміMatLab використовується операція rgb2gray(рис. 3.7). Після перетворення викличемо гістограму зображення (рис. 3.8).

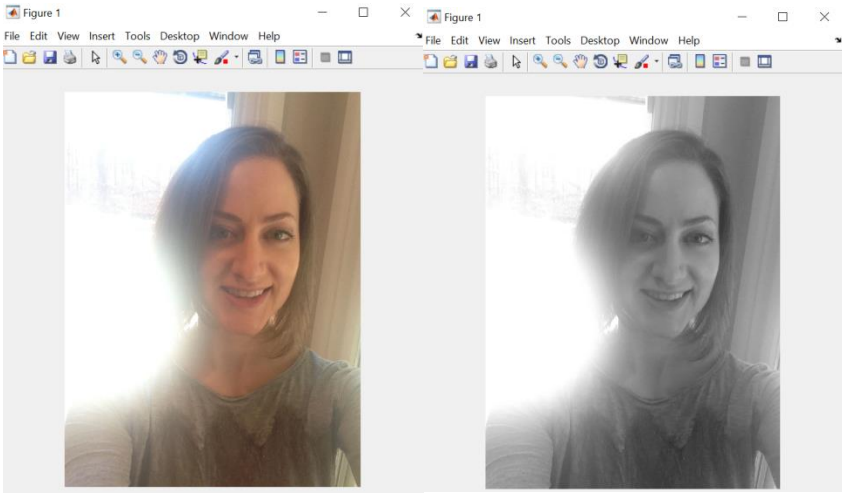


Рис. 3.7. Перетворення кольорового зображення в напівтонове

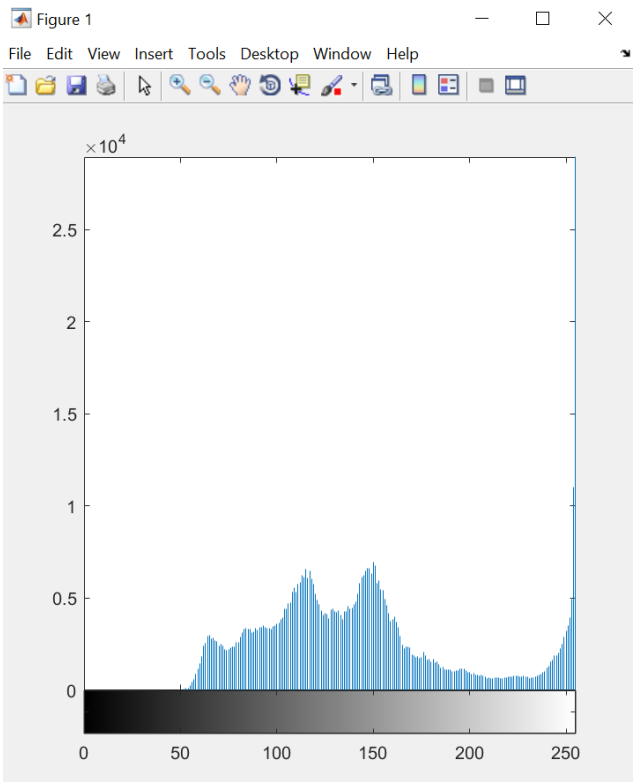


Рис. 3.8. Гістограма напівтонового зображення

Наступний крок – це обробка зображення – гістограмнаеквалізація та виведення зображення і його гістограму на екран (рисунок 3.9-3.10).

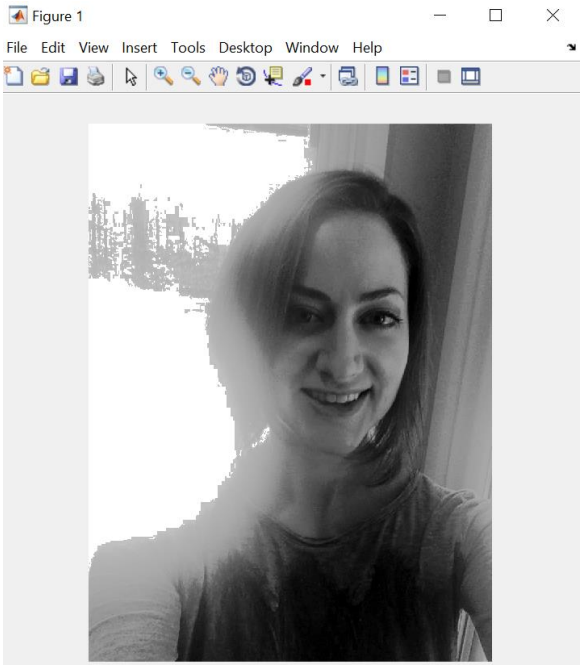


Рис. 3.9. Напівтонове зображення після еквалізації

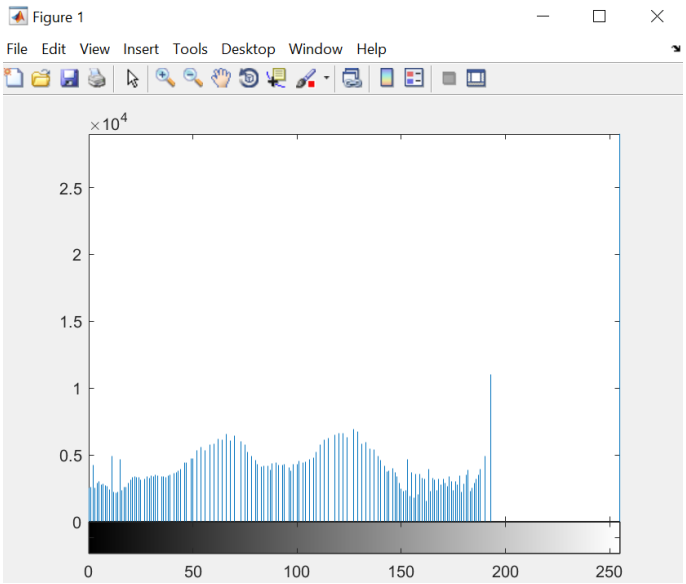


Рис. 3.10. Гістограма напівтонового зображення з еквалізацією

Згідно рис. 3.7-3.10 можна зробити висновки, що обробка зображення здійснила рівномірний розподіл яскравостей, нібито перенесла важливу інформацію з яскравих областей в темніші області, вирівнявши напівтоновефото.

Наступні дії будуть відбуватись для здійснення кращої чіткості зображення.Для початку вводяться параметри фільтру Лапласа, а далі застосовується вже сам фільтр на зображення (рис. 3.11).

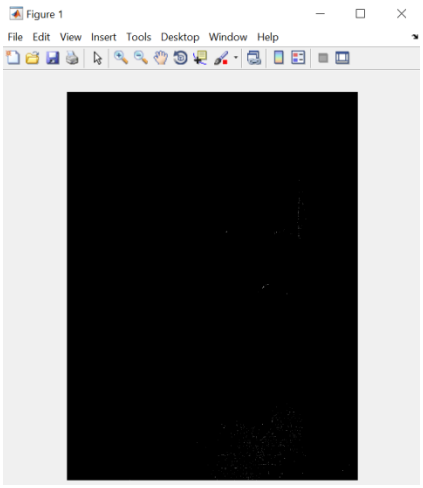


Рис. 3.11. Зображення після застосування фільтра Лапласа

Через від’ємний центральний коефіцієнт фільтру, фільтрація зображення буде з ефектом від’ємних значень пікселів, тобто саме зображення буде майже повністю чорним. Для цього виконується перетворення зображення в відповідний клас – з того, що в нас був (uint8) в кластdouble і подальше відновлення тонів (рис. 3.12-3.14). Це необхідно робити тому, що фільтрація операцією imfilterстворює на виході зображення того ж класу, що було на вході, і через це від’ємні величини будуть обрізані.

В результаті отримується кінцеве оброблене зображення (рис. 3.13) та спостерігається його гістограма (рис. 3.14).

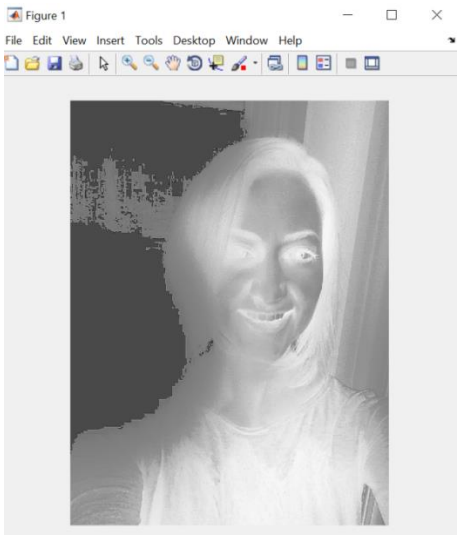


Рис. 3.12. Перетворення зображення в клас double

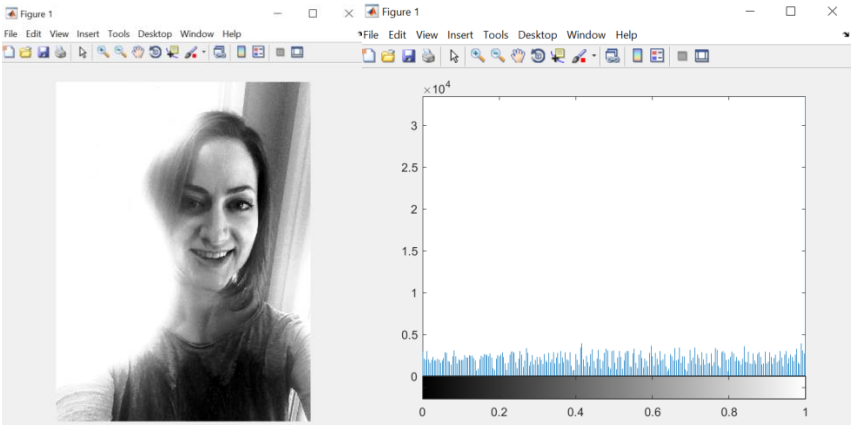


Рис. 3.13. Кінцеве оброблене зображення з відновленими тонами та його гістограма

3.4.Аналіз та оцінка зображення

Для того, аби краще помітити покращення зображення, необхідно порівняти зображення до і після обробки (рис.3.15-3.16).

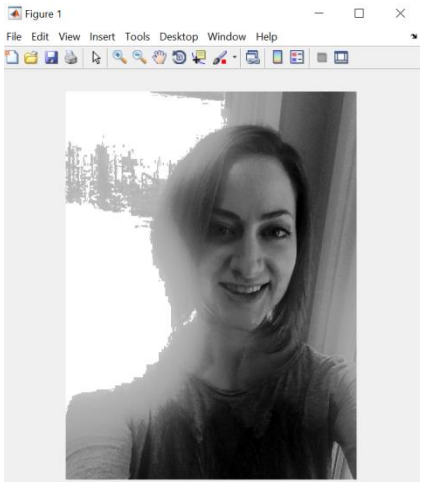


Рис.3.15. Зображення після еквалізації гістограми

На рис. 3.15 видно, що після еквалізації зображення охопило задній фон, якого майже не було видно, а також воно є трохи розмитим. Якщо ж при реєстрації зображення має погану початкову деталізацію, то фільтр Лапласа значно краще показує свої функції. А якщо початкове зображення було з нормальною деталізацією, тоді дію фільтра замітно лише візуально (рис. 3.16).

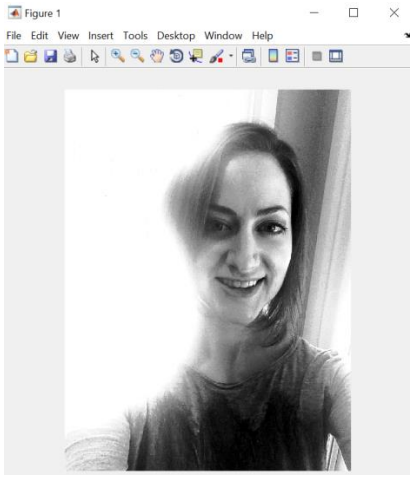


Рис.3.16. Кінцеве оброблене зображення

При застосуванні фільтра потрібно ретельно підбирати його параметри, аби зображення на виході було не надто різким.

Кінцеве зображення, згідно рис. 3.16, має рівномірно розподілену по всьому діапазоні яскравість, хорошу контрастність та кращу деталізацію. Проте

при застосуванні фільтра частина зображення обрізалась. Це пов’язано із дуже великим засвітленням, з якого фільтр просто не зміг добитись кращої чіткості, сфокусувавши увагу на більш темніших деталей (обличчя та одяг).

В якості ефективності обробок зображення порівняємо гістограми зображення до і після (рис. 3.17).

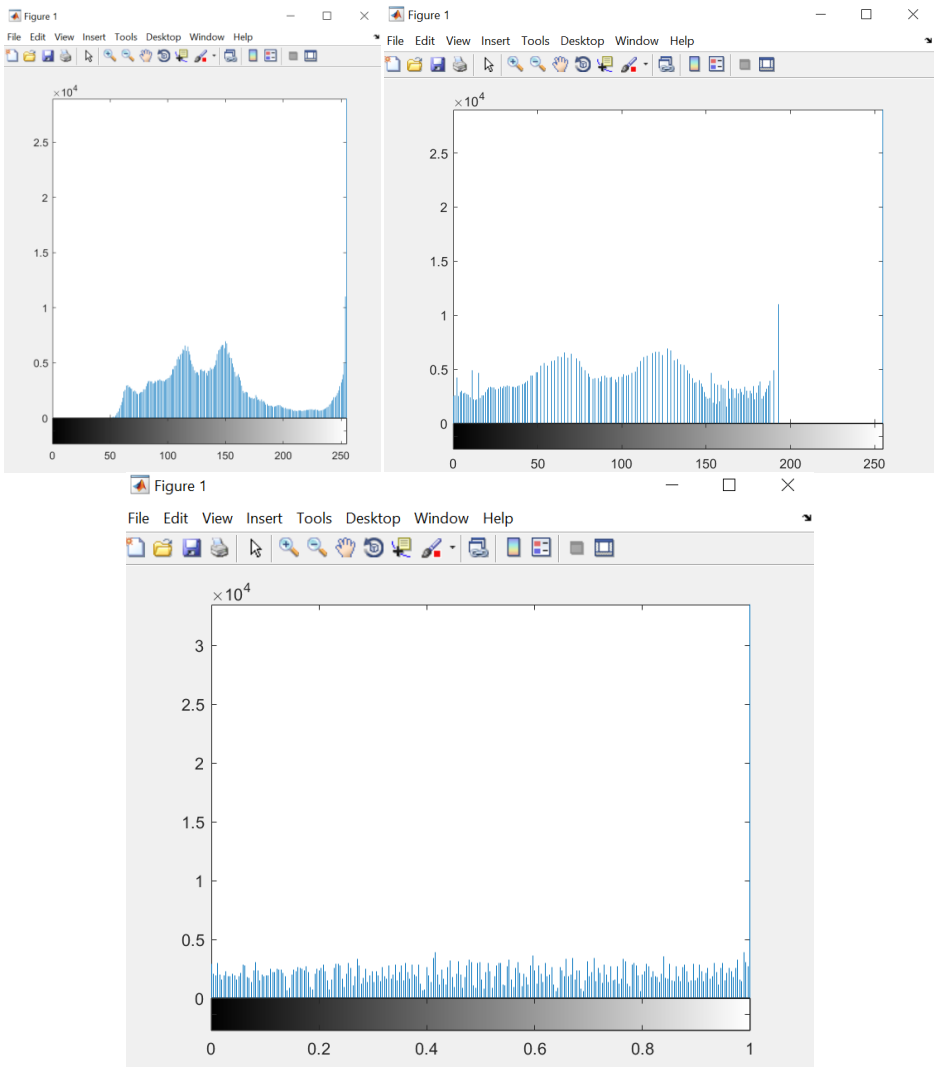


Рис. 3.17. Гістограми початкового зображення та обробленого

На рис. 3.17 видно, що рівень контрастності початкового зображення при найменших рівнях яскравості (225 кд/м^2) має значення приблизно 200:1. Після процесу еквалізації, сама форма гістограми не змінилась, вона наче посунулась в лівий бік добавивши темних відтінків, тим самим збільшивши мінімальний рівень яскравості на 17 кд/м^2 при мінімальній контрастності 225:1. Останній

етап покращення зображення через фільтр Лапласа здійснив рівномірний розподіл контрастності до рівня 225:1 у всьому діапазоні яскравості, що значно покращило якість зображення (рис. 3.16).

Для того, аби побачити ефективність попередньої обробки зображень, наведемо ще декілька прикладів дії цих методів та порівняємо їх.Зверху буде початкове напівтонове зображення, а знизу – кінцеве покращене зображення (рис. 3.18 – 3.20).

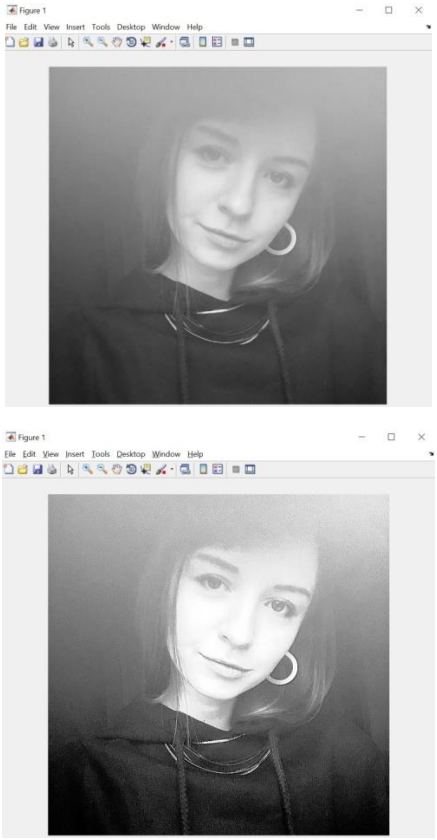


Рис. 3.18. Приклад 2 фото до і після обробки

На рисунку 3.18 початкове зображення мало більш-менш нормальну розподілену яскравість зображення, тому суттєвих змін, окрім чіткіших деталей зображення і більш освітленого обличчя в даному прикладі немає.

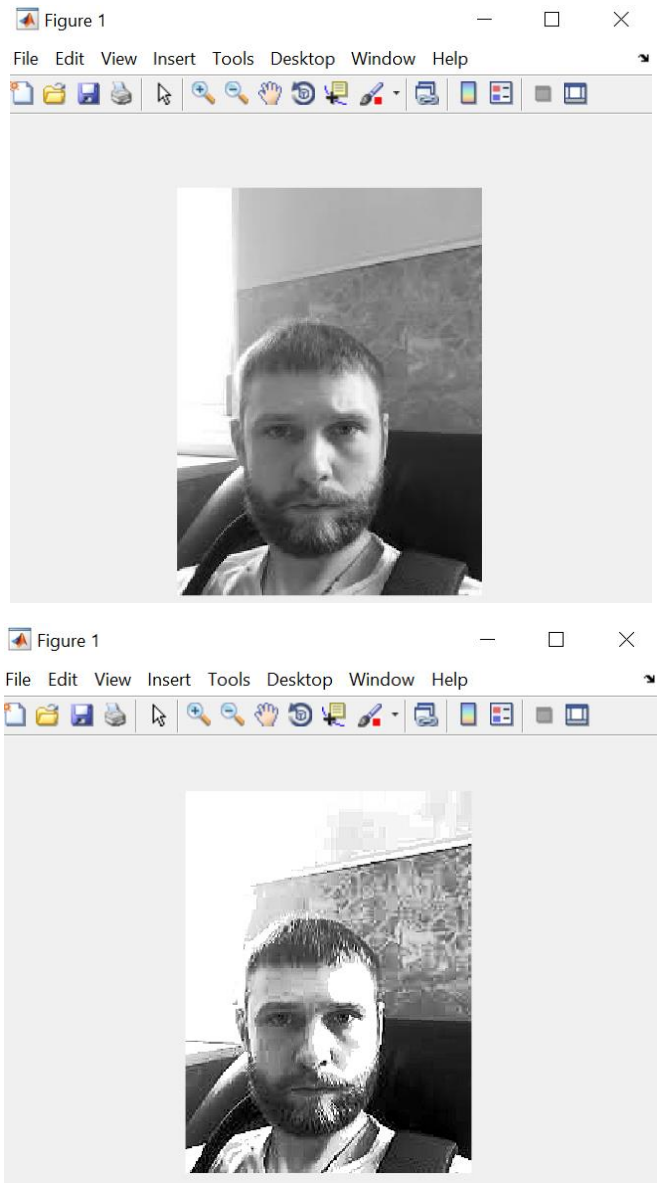


Рис. 3.19. Приклад 3 фото до і після обробки

На рисунку 3.19 видно, що початкове зображення має засвітлені області та малу чіткість. Після обробки, риси обличчя та задній фон стали більш чіткими, проте занадто освітлені області так і лишились світлими.

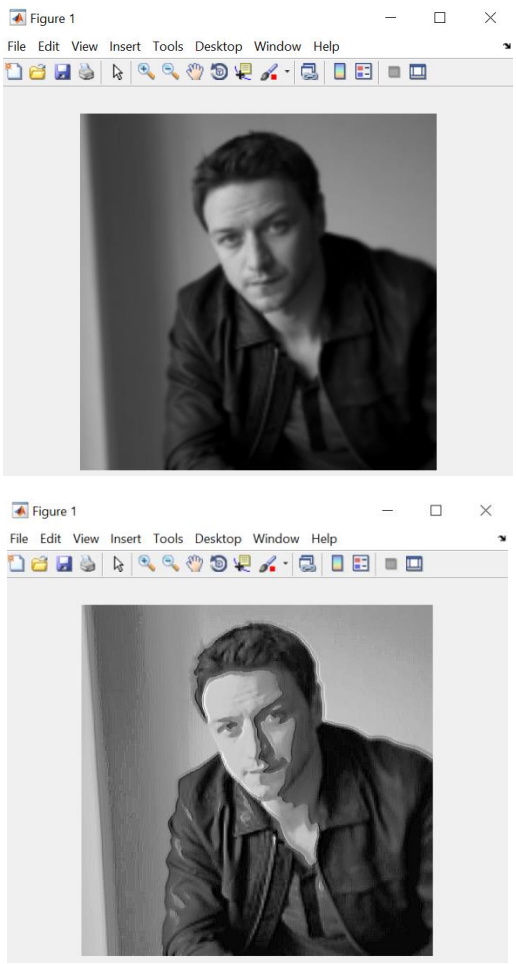


Рис. 3.20. Приклад 4 фото до і після обробки

На рисунку 3.20 показано дуже розмите зображення, і після обробки самі контури одягу стали чіткі, проте саме обличчя і одяг дуже спотворились. Це пов’язано із тим, що якщо зображення має дуже погану якість, то попередня обробка може спортити його, оскільки покращення такого зображення буде не можливим з технічної точки зору.

Для більш наглядної оцінки обробки зображень, застосуємо рівень структурної подібності, що має вигляд[27]:

$$SSIM = \left(\frac{\sigma_{xy}}{\sigma_x \sigma_y}\right)\left(\frac{2\overline{XY}}{\left(\overline{X}\right)^2+\left(\overline{Y}\right)^2}\right)\left(\frac{2\sigma_x\sigma_y}{{\sigma_x}^2+{\sigma_y}^2}\right); \quad (3.7)$$

$$\overline{X} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} x_{ij}, \overline{Y} = \frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N} y_{ij}; \quad (3.8)$$

$$\sigma^2{}_x = \frac{1}{(M-1)(N-1)} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - \overline{X})^2; \quad (3.9)$$

$$\sigma^2{}_y = \frac{1}{(M-1)(N-1)} \sum_{i=1}^{M} \sum_{j=1}^{N} (y_{ij} - \overline{Y})^2; \quad (3.10)$$

$$\sigma_{xy} = \frac{1}{(M-1)(N-1)} \sum_{i=1}^{M} \sum_{j=1}^{N} (x_{ij} - \overline{X})(y_{ij} - \overline{Y}), \quad (3.11)$$

де SSIM – значення рівня подібності (якості) зображення; хтау – початкове та кінцеве порівнювальне фото; МтаN – розміри зображення.

Вираз3.7 є коефіцієнтом кореляції між зображеннями X і Y. Другий вираз (3.8) характеризує подібність середніх значень яскравості двох порівнюваних зображень. Вираз 3.9 характеризує подібність контрастності двох порівнюваних зображень.

У загальному випадку рівеньподібності (SSIM)розраховується в непересічних областях для кожного зображення окремо. Оскільки зображення не змінювалося і не рухалось, якість можна обчислювати відразу на всьому зображенні, та чим вище це значення, тим краще виконана обробка зображення.

Результати розрахованих значень SSIMдля кожного із прикладів наведено на рис. 3.21.

На рис. 3.21 для найкращої обробки зображення значення контрастності в 300:1 повинно бути у всьому діапазоні яскравостей, і відповідно значення SSIMстановить 1. Приклад 1 показує рівень контрастності від 210:1 до 269:1 у всьому діапазоні, розраховане значення SSIM = 0.86, а приклад 2 починається із $0.3x10^3$кд/м^2 рівня яскравості. Це значить, що на даному зображенні недостатньо темних ділянок.

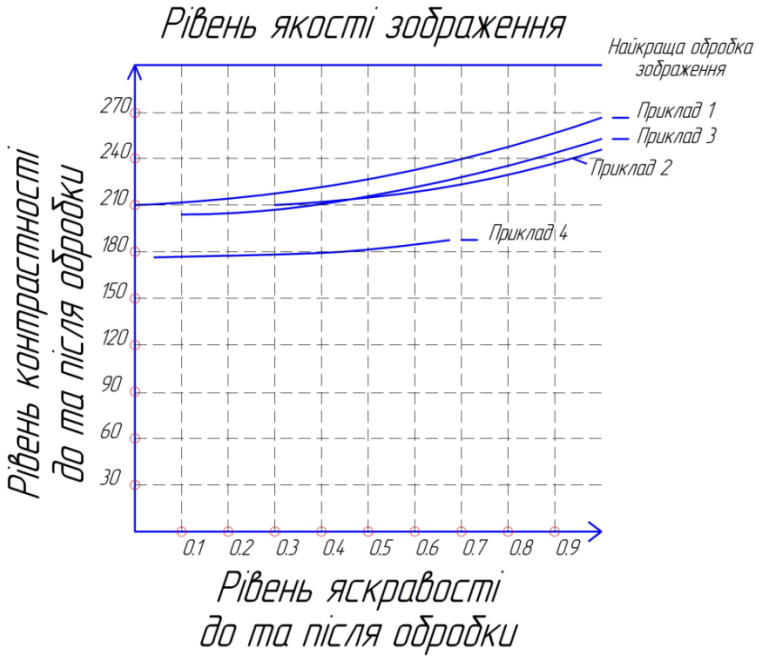


Рис. 3.21. Оцінка рівня якості зображення

Значення якості в другому прикладі становить 0.67. В прикладі 3 не на всій площині, де потрібно є темні ділянки зображення, проте вони відповідають нормі, значення якості SSIM = 0.73. В прикладі 4 окрім недостатньо світлих ділянок також є незначна недостатність темних, і рівень контрастності, що становить 190:1 на максимальних значеннях, є найгірший. Оцінка якості в даному прикладі після розрахунків становить 0.51.

3.5.Висновки до розділу 3

В підрозділі обґрунтування методу обробки зображення проаналізовано основне завдання покращення, їхніметоди та вибір. Проаналізовано загальні характеристики вибраних методів, їхні переваги та застосування на практиці. Крім того представлено реєстрацію експериментальних даних та розглянуто початковий етап до попередньої обробки зображення. Проаналізовано алгоритми та структурні схеми роботи.

В підрозділі обробка зображення для верифікації особи проведено наукове експериментальне дослідження покращення зображення та його аналіз.

Даний метод показує, що попередня обробка зображення залежить не лише від програмного покращення, а й від самого обладнання систем верифікації. З якісним обладнанням та алгоритмами попередньої обробки зображення, системи верифікації будуть мати більш високу надійність та швидкість при різних виникаючих завадах.

В підрозділі аналіз оцінки зображення проаналізовано кінцеві результати обробки зображення та порівняння покращення фотографій при різних умовах.

Розглянувши даний метод обробки зображення та перевіривши теорію в програмному середовищі, спостерігається недосконаліть попереднього покращення зображення через еквалізацію гістограми та фільтр Лапласа. Якщо зображення є критично поганої якості чи занадто розмитим, то даний метод може ще більше спортити якість, що зменшить надійність і швидкість систем верифікації. Якщо ж зображення має не критичну погану якість та розмитість, то на виході обробки воно буде більш чітким та якісним, що допоможе подальшій обробці фото.

РОЗДІЛ 4.
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці під час роботи з персональним комп'ютером при виконанні наукового дослідження

При науковому дослідженні використовується персональний комп'ютер (ПК) та різні прилади ідентифікації, призначені для верифікації осіб в організаціях, приватних підприємствах, банках тощо [30].

Дані пристрої, що застосовують, необхідно захищати кожухами струмопровідні частини. Забезпеченням електробезпеки в телекомунікаційних мережах можливе за рахунок здійснення електричного розділення через роздільний трансформатор. До електричного щитка керування потрібно підводити трьохпровідну електричну мережу та встановити рубильник аварійного вимикання.

Під час налагодження та експлуатації фото- та відео- камер з біометричними сканерами, необхідно обережно поводитися з самими пристроями, оскільки неприпустимі удари, подряпини по них, потрапляння пилу чи бруду особа не зможе достовірно пройти систему верифікації [30].

Під час роботи за ПК на виробництві, підприємстві тощо, на організм людини впливають різні небезпечні чиники, що наведені в табл. 4.1.

Таблиця 4.1

Небезпечні для організму виробничі чинники

Небезпечний фактор	Значення замірів	Нормовані значення
Рентгенівське випромінювання	17 мкР/год	75 мкР/год
Ультрафіолетове випромінювання	0.009 Вт/м2	0.01 Вт/м2
Видимий діапазон	1.4-3.8 Вт/м2	10 Вт/м2
Яскравість	86 кД/м2	>50 кД/м2
ІЧ-випромінювання	0.4-11 Вт/м2	100 Вт/м2
Електростатичне поле	15 Вт/м	20-60 кВ/м
Шум	30-45 дБА	60 дБА

Для користувача необхідно підбирати рівень освітлення таким чином, щоби при свіченні екрану не було сторонніх джерел світла та комфортночиталась інформація.

Комп'ютер випромінює рентгенівські, ультрафіолетові та інфрачервоніпромені, які частково поглинаються склом монітору. При цьому інфрачервоне випромінювання втомлює очі та порушує нормальне сприйняття кольору, рентгенівське - впливає на кісткові тканини і мозок, а електромагнітне - впливає на зорове сприйняття людини [30].

Загальні джерела електромагнітного випромінювання ПК вказані в табл. 4.2.

Таблиця 4.2

Джерела електромагнітного випромінювання ПК

Джерело випромінювання	Діапазон частот
Мережний трансформатор блока живлення	50 Гц
Статичний перетворювач напруги в імпульсному блоці живлення	20-100 кГц
Анодна напруга екрану з ЕПТ	0 Гц (електростатика)
Системний блок (процесор)	50 Гц - 1000 МГц
Джерела безперебійного живлення	50 Гц, 20-100 кГц

Відео-термінали систем верифікаціївикористовують катодну трубку і у радіодіапазоні сканують електронний промінь по монітору від15 до 35 кГц. Напруженість електричного поля при малій відстані від монітору (50 мм), має значення від одиниць до 10 В/м, а магнітна індукція - від 10^{-8} до 10^{-7}Тл.Окрім того відео-термінали здатні випромінювати змінні електричні і магнітні поля з гармоніками з частотою 50 (100) Гц.

При плануванні та організації робочого місця для наукового дослідження, модулі біометричної верифікації (сканери, відеокамери тощо) та

екраникомп’ютерів повинні розміщуватись з мінімальною кількістю блоків, та оптимальноювідстанню до очей [30].

Приміщення з розташованими відео-терміналами визначають, згідно з чинними нормативними документами з розрахунку на одне робоче місце з максимальною кількістю працюючих у зміні осіб, з площею не менше 6 $м^2$ та обсягом не менше 20 $м^2$.Самі ж термінали розміщуютьсяпід кутом 90-105° до зовнішньої стіни.

При проектуванні нових алгоритмів програм, рівень шуму для виробництва не повинен перевищувати 40 дБА, приздійсненні операторської діяльності - 65 дБА, при роботі у дисплейнихділянках - не більше 50 дБА.

Для приміщень із моніторами передбачається обов'язкове розташування на вікнах жалюзі чи шторів, а для приміщень з відео-терміналами стіни повинні бути пофарбовані у кольори пастельних тонів з коефіцієнтом відбиття від 40 до 60%. Мікрокліматцих приміщень повинну мати оптимальну температура повітря при19-21 °С, оптимальна відносна вологість – 40-60%, а оптимальна швидкість руху повітря – 0.05-0.1 м/с [30].

4.2. Забезпечення надійності роботи телекомунікаційних систем до дії уражаючих факторів надзвичайних ситуацій

Телекомунікаційні системи – це системи приймання та передавання будь-яких видів даних через телекомунікаційну мережу з одного місця в інше.

Надійність функціонуваннятелекомунікаційних систем -це комплексна властивість, щоскладається із стійкості засобів (інфраструктури) телекомунікацій до дестабілізуючихчинників, прийнятного рівня готовності телекомунікацій до надання послуг споживачам, атакож певного рівня безпеки користування телекомунікаційними послугами.

Надзвичайні ситуації у телекомунікаційних мережах –це порушення функціонування телекомунікаційних мереж внаслідок впливу чинників техногенного, природного, соціального або воєнного характеру чи інших

чинників, що призвели або можуть призвести до виходу з ладу значної частини ресурсів, засобів телекомунікацій, перевантаження телекомунікаційних мереж, втрати енергопостачання тощо.

Заходи щодо забезпечення надійності функціонування телекомунікаційних мереж спрощено представлено на рис. 4.1.

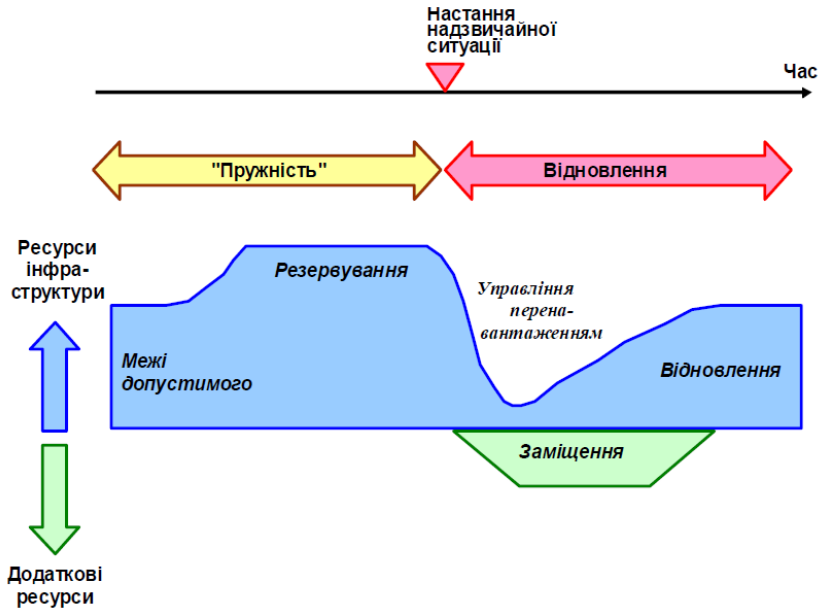


Рис.4.1. Заходи щодо забезпечення надійності функціонування телекомунікаційних мереж

Одними із основних методів підвищення ефективності роботи усіх підрозділів та апаратівуправлінь Державної служби України з надзвичайних ситуацій (ДСНС) є покращання оперативного управління за рахунокскорочення часу на виклик пожежно-рятувальної техніки, та забезпечення оптимального складу залучення сил та засобів. Ефективна робота службзабезпечується за рахунок технічного переоснащення і автоматизації основних операцій службовоїдіяльності МНС. В Україні, актуальною проблемоює узгодження всіх каналів зв’язку та об’єднання їх в єдине ціле для оптимального управліннясилами та засобами МНС[31].

Основнимицілями функціонування телекомунікаційних систем та зв'язку в інформаційній структурі підтримкиприйняття рішень будуть [31-33]:

- підвищення оперативності прийняття рішень та надання інформаційно-аналітичної підтримки на всіх рівнях управління, моніторингу та ліквідації НС;

- забезпечення посадових осіб і органів влади достовірною інформацією про НС, забезпечення сумісності інформації на всіх рівнях ієрархії управління за рахунок використання єдиних класифікаторів, стандартів, принципів побудови інформаційних структур і систем, оптимізація координації організаційної та інформаційної взаємодії функціональних систем МНС;

- оптимізація і автоматизація процесів збирання та комплексного оброблення даних, отриманих від системи моніторингу і переданих по каналах зв'язку, комп'ютерних і телекомунікаційних мережах;

- підвищення достовірності та повноти циркулюючої інформації за рахунок інтелектуального оброблення даних і засобів захисту каналів, забезпечення оперативних потоків даних визначеними маршрутами до центрів оперативного управління МНС;

- підтримка регулярного інформаційного обміну через мережі зв'язку і телекомунікаційні системи.

Інформаційна сумісність передачі пакетів даних в комп'ютерних мережах та аналоговоїінформації в каналах зв'язку забезпечується використанням сучасного єдиного лінгвістичного забезпечення,лексичного і програмного, яке включає в себе уніфіковані інформаційні структури банків данихусіх рівнів системи, а також правил і протоколів передачі даних за міжнародними стандартами та актами [32].

Організаційні заходи забезпечуютьнедоступність несанкціонованих осіб до апаратно-технічних засобів системи, магнітних носіївданих, кабельних систем зв'язку та радіоканалів. Технічні засоби мають відповідати загальноприйнятими стандартами та протоколами і забезпечити відсутністьелектромагнітних випромінювань в апаратній і кабельній системах за межами зони контролю,однозначну ідентифікацію та аутентифікацію користувачів до роботи з найбільш критичнимиелементами системи і баз

оперативної інформації, а також забезпечити безперебійне живленнякритичних компонентів структури управління центрів оперативного керування МНС [31].

У разі виникнення надзвичайних ситуацій у телекомунікаційних мережах загальне керівництво системою оперативно-технічного управління телекомунікаційними мережами здійснює постійно діюча галузева комісія з питань техногенно-екологічної безпеки та надзвичайних ситуацій, яка утворюється і діє як координуючий орган [32].

Постійно діючу комісію очолює Голова Держспецзв'язку або уповноважена ним посадова особа цього органу.До складу постійно діючої комісії входять представники Адміністрації Держспецзв'язку та інші фахівці в галузі зв'язку.Повноваження постійно діючої комісії визначаються положенням про постійно діючу комісію, яке затверджується Адміністрацією Держспецзв'язку [33].

При виникненні надзвичайної ситуації у телекомунікаційних мережах Національний центр надає Адміністрації Держспецзв'язку детальну інформацію про оперативну обстановку у мережах, вид, причини, масштаби ситуації та прогноз щодо її розвитку для аналізу і прийняття рішення про перехід до надзвичайного режиму управління в межах зони виникнення надзвичайної ситуації [33].

В умовах надзвичайних ситуацій у телекомунікаційних мережах Національний центр після отримання рішення Адміністрації Держспецзв'язку про введення надзвичайного режиму управління вживає таких заходів [31-33]:

- здійснює централізоване оперативно-технічне управління технічними засобами, лініями, трактами і каналами зв'язку мереж загального користування та інших телекомунікаційних мереж;

- організовує першочергове виділення необхідних ресурсів телекомунікаційних мереж в інтересах державної системи урядового зв'язку, національної системи конфіденційного зв'язку та спеціальних споживачів;

- відповідно до планів забезпечує організацію оперативної заміни та обходів пошкоджених ліній, трактів і каналів зв'язку, здійснює заходи щодо відновлення функціонування телекомунікаційних мереж;

- здійснює управління організацією аварійно-відновних робіт з використанням наявних ресурсів та забезпечує контроль за ходом цих робіт;

- приймає рішення про заборону або припинення профілактичних, ремонтно-налагоджувальних та інших робіт на цих мережах, інформує про прийняте рішення операторів телекомунікацій;

- повідомляє про прийняті рішення та дії Адміністрації Держспецзв'язку, центри управління мережами та спеціальних споживачів.

Для забезпечення функціонування системи оперативно-технічного управління телекомунікаційними мережами в Національному центрі формується та постійно оновлюється інформаційна база даних із застосуванням єдиної системи класифікації та ідентифікації ліній, трактів, комутаційних станцій та інших об'єктів управління системи оперативно-технічного управління телекомунікаційними мережами [31].

У разі виникнення пошкоджень технічних засобів чи руйнувань споруд магістральних та зонових телекомунікаційних мереж і неможливості передачі обхідними лініями, трактами і каналами зв'язку всього навантаження встановлюється така пріоритетність відновлення каналів [31-33]:

- канали державної системи урядового зв'язку, національної системи конфіденційного зв'язку та спеціальних споживачів;

- канали програм телебачення УТ-1 та радіомовлення УР-1;

- канали магістральних мереж телефонного зв'язку і передачі даних, у тому числі канали, які забезпечують функціонування системи оповіщення цивільної оборони;

- канали програм телебачення та радіомовлення державної телекомпанії "Крим", обласних і регіональних державних телерадіомовних організацій;

- канали програм телебачення УТ-2 та радіомовлення УР-2;

- канали програм телебачення УТ-3 та радіомовлення УР-3;

- канали зонових мереж телефонного зв'язку і передачі даних, у тому числі канали, які забезпечують функціонування системи оповіщення цивільної оборони;

- канали недержавних міжрегіональних програм телебачення і радіо;

- канали недержавних обласних програм телебачення і радіо.

З метою забезпечення функціонування системи оперативно-технічного управління телекомунікаційними мережами оператори телекомунікацій, центральні органи виконавчої влади, підприємства, установи та організації, у власності, користуванні, господарському віданні чи оперативному управлінні яких є засоби та мережі телекомунікацій, подають Національному центру інформацію про [31]:

- схеми зв'язку та зміни, що вносяться до них;

- потужність, обсяги дії та схеми включення міжнародних центрів комутації, автоматичних міжміських телефонних станцій (опорно-транзитних телефонних станцій/автоматичних міжміських телефонних станцій), центрів комутації рухомого (мобільного) зв'язку;

- кабельні та радіорелейні магістральні, зонові і місцеві (міжстанційні) лінії, типи кабелю та маршрути, типи обладнання.

Для забезпечення можливості централізованого управління мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану, а також отримання допомоги від Національного центру у розв'язанні проблем, що виникають у мережах, оператори телекомунікацій подають Національному центру інформацію про [32]:

- заходи щодо реорганізації мережі;

- планові строки відключення (переключення) трактів і каналів зв'язку;

- надання спеціальним споживачам трактів і каналів зв'язку;

- зміну стану, параметрів та характеристик станційного обладнання мережі, ліній, трактів і каналів зв'язку;

- місце, причини, тривалість подій (пошкодження, руйнування, втрату енергопостачання, синхронізації тощо), що відбуваються або можуть відбутися у мережі;

- строки відновлення трактів і каналів зв'язку, надання обходів чи заміну пошкоджених ліній, трактів і каналів зв'язку;

- перехід на резервне обладнання, у тому числі на резервне енергопостачання чи резервний опорний генератор сигналу синхронізації, роботу на останньому резервному тракті;

- динаміку змін навантаження;

- право доступу до інформації;

- спроби несанкціонованого доступу до баз даних.

Захист інформації та забезпечення безпеки системи оперативно-технічного управління телекомунікаційними мережами здійснюється на всіх етапах передачі, прийому, опрацювання, збереження даних з метою[33]:

- запобігання витоку, втраті і підробці інформації;

- запобігання несанкціонованому застосуванню, знищенню, модифікації, перекрученню, копіюванню, блокуванню інформації;

- запобігання несанкціонованому втручанню в роботу системи оперативно-технічного управління телекомунікаційними мережами;

- збереження конфіденційності документованої інформації;

- захисту від можливості впровадження будь-якими шляхами та активізації програм-вірусів, у тому числі під час з'єднання з мережею Інтернет.

Телекомунікаційні аспекти протидії і пом'якшення наслідків лиха вже досить тривалийчас досліджуються у відомому спеціалізованому органі ООН з питань ІКТ – Міжнародному союзі електрозв’язку (ITU). Три окремі його сектори ITU-T, ITU-R та ITU-D вивчаютьпитаннятелекомунікаційногозабезпеченнявидівдіяльностізвиявлення, попередження, спасіння та ліквідації наслідків надзвичайних ситуацій – ITU-T в частинізагальних питань телекомунікацій, ITU-R – в частині питань радіозв'язку, а ITU-D – вчастині питань розвитку країн [33].

4.3. Висновки до розділу 4

У підрозділі з охорони праці під час роботи з персональним комп’ютером при виконанні наукового дослідження проаналізовано негативний вплив шкідливих і небезпечних чинників під час роботи з персональним комп’ютером, описано умови роботи та заходи безпеки персоналу організацій, підприємств, виробництв тощо.

У підрозділі з забезпечення надійності роботи телекомунікаційних систем до дії уражаючих факторів надзвичайних ситуацій проаналізовано способи реалізації заходів захисту телекомунікаційних мереж у разі надзвичайної ситуації з техногенного, природного, соціального або воєнного характеру чи інших чинників, що призвели або можуть призвести до виходу з ладу значної частини ресурсів, засобів телекомунікацій, перевантаження телекомунікаційних мереж, втрати енергопостачання тощо.

ЗАГАЛЬНІ ВИСНОВКИ

В даній магістерській роботі проводилось дослідження обробки зображень дляверифікації особи в телекомунікаційних системах.

В першому розділі розглянуті загальні поняття розпізнавання особи та верифікації, їх використання в сферах життя та основний принцип роботи.

В другому розділі розглянуто відомі методи верифікації особи, їх характеристики та спроектовані в результаті системи в телекомунікаційних системах. В цьому розділі в всіх системах верифікації були спільні проблеми, при яких система має недостатню надійність і швидкість, тому було також розглянуто відомі методи обробки зображення з коротким описом роботи. Обрано два методи покращення фото.

В третьому розділі розглянуто метод обробки зображення, що застосовується в науковому дослідженні для верифікації в телекомунікаційних мережах, його алгоритм та принцип роботи. Також в даному розділі розглянуто загальний процес реєстрації зображення, його алгоритм.

Розглянувши даний метод обробки зображення та перевіривши теорію в програмному середовищі, спостерігається недосконаліть попереднього покращення зображення через еквалізацію гістограми та фільр Лапласа. Якщо зображення є критично поганої якості чи занадто розмитим, то даний метод може погіршити якість, що зменшить надійність і швидкість систем верифікації. Якщо ж зображення має не критичну погану якість та розмитість, то на виході обробки воно буде більш чітким та якісним, що допоможе подальшій обробці фото.

Даний метод показує, що попередня обробка зображення залежить не лише від програмного покращення, а й від самого обладнання систем верифікації. З якісним обладнанням та алгоритмами попередньої обробки зображення, системи верифікації будуть мати більш високу надійність та швидкість при різних виникаючих завадах.

В четвертому розділі розглянуто охорону праці та безпека в надзвичайних ситуаціях. Проаналізовано дії щодо уникнення загрози життя людей, а також умови, при яких працівник повинен комфортно себе почувати та працювати з забезпеченням надійності роботи телекомунікаційних систем.

Проблемними задачами, які технічно важко реалізувати на практиці є забезпечення верифікації високої надійності та швидкості розпізнавання особи. Для подолання цих проблем пропонуєтьсязастосувати попереднюобробку реєструючого зображення, аби в результаті мати якісне зображення.

Вирішення проблем в системах верифікації шляхом обробки зображень особи в телекомунікаційних системахпокращить надійність та швидкість розпізнавання користувачів. В якості основи для вирішення даної задачі використовуються літературні джерела та програмне середовище MatLab.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. http://masters.donntu.org/2011/frt/dyrul/library/article2.htm
2. https://evergreens.com.ua/ua/articles/digital-facial-recognition.html.
3. https://securityrussia.com/blog/face-recognition.html.
4. https://www.roboforex.ua/about/client/faq/verification/16/.
5. https://gzex.ru/legal/verification.
6. https://gzex.ru/legal/verifyDocs.
7. https://help.pikabu.ru/hc/ru/articles/360007478174-Что-такое-верификация-аккаунта.
8. https://www.tadviser.ru/index.php/Статья:Системы_распознавания_лиц_(Facial_recognition).
9. https://iidx.ru/uslugi/raspoznavanie-lits/.
10. Царьов Р.Ю. Біометричні технології: навч. посіб. [для вищих навчальних закладів] / Р.Ю. Царьов, Т. М. Лемеха. – Одеса: ОНАЗ ім. О.С. Попова, 2016. – 140 с.
11. https://www.drdoors-msc.ru/obzor_tekhnologij_i_reshenij_v_oblasti_raspoznavaniya_lic_v_skud.html.
12. https://www.bsystemspro.com/verifikaciya-lica.
13. https://findface.pro/technology/.
14. https://abakan.kiasoft.ru/verifikacija_lica.html.
15. https://habr.com/ru/company/ntechlab/blog/329412/.
16. Гонсалес Р. Цифроваяобработка зображений в средеMatLab: навч. посіб. [для вищих навчальних закладів] /Р. Гонсалес, Р. Вудс, С. Эддинс. – Москва: Техносфера, 2006. – 616с.
17. http://geometry.karazin.ua/resources/documents/20191108174923_19583744.pdf.
18. https://hub.exponenta.ru/post/kratkiy-kurs-teorii-obrabotki-izobrazheniy734.

19. https://www.researchgate.net/profile/Valery_Starovoitov/publication/272487320_Cifrovye_izobrazenia_ot_polucenia_do_obrabotki/links/5832e0a208aef19cb81c7da1/Cifrovye-izobrazenia-ot-polucenia-do-obrabotki.pdf.

20. https://cyberleninka.ru/article/n/metody-obrabotki-izobrazheniy-osnovannye-na-segmentatsii/viewer.

21. http://k504.khai.edu/index.php/iktm-2009/216-lokalno-adaptivnaya-filtratsiya-izobrazhenij-s-ispolzovaniem-robastnykh-indikatorov-negaussovykh-raspredelenij.

22. http://venec.ulstu.ru/lib/disk/2016/49.pdf.

23. http://it-visnyk.kpi.ua/wp-content/uploads/2012/08/54_30.pdf.

24. http://www.pereplet.ru/obrazovanie/stsoros/68.html.

25. https://www.eduherald.ru/ru/article/view?id=12478.

26. https://techlibrary.ru/b/2k1r1u1i1n1a1o_2q.2z._1j_1e1r._3e1j1v1r1p1c1a2g_1p1b1r1a1b1p1t1l1a_1j1i1p1b1r1a1h1f1o1j1k_1c_1j1o1v1p1r1n1a1x1j1p1o1o2c1w_1s1j1s1t1f1n1a1w._2000.pdf.

27. https://www.researchgate.net/profile/Valery_Starovoitov/publication/236593352_Ocenki_kacestva_dla_analiza_cifrovyh_izobrazenij/links/54e5dab40cf277664ff1ae6d/Ocenki-kacestva-dla-analiza-cifrovyh-izobrazenij.pdf.

28. https://exponenta.ru/matlab.

29. https://hub.exponenta.ru/post/spisok-funktsiy-image-processing-toolbox152#imread.

30. Жидецький В. Ц. Основи охорони праці: підруч. / В. Ц. Жидецький. - Львів: М-во освіти і науки України. Наук.-метод. центр вищої освіти. Укр. акад. друкарства, 2006. - 336 с.

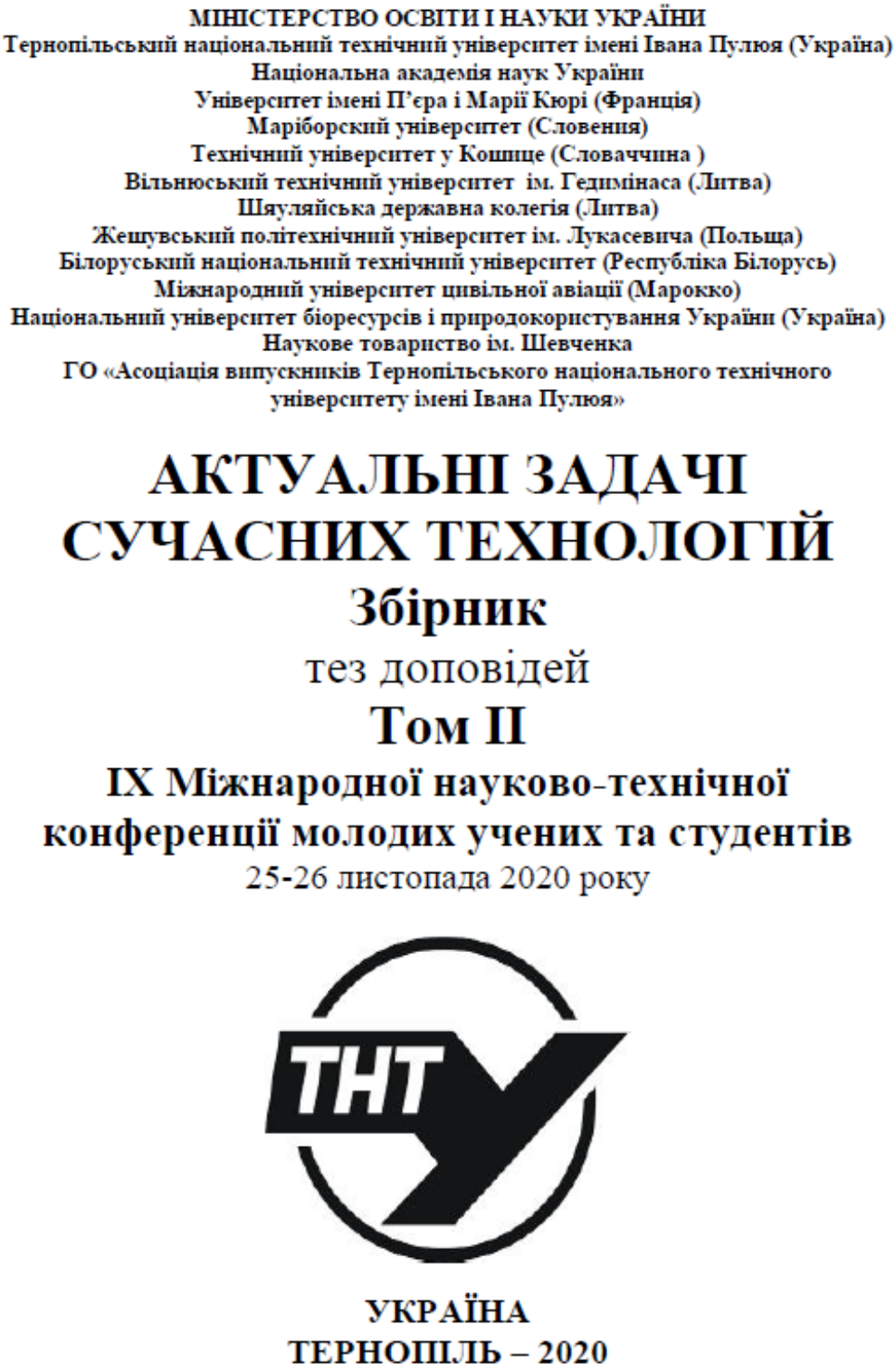
31. http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&IMAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Nzundiz_2014_5_3.pdf.

32. http://ena.lp.edu.ua:8080/bitstream/ntb/12110/1/13_РОЛЬ%20ТА%20ПРОБЛЕМИ.pdf.

33. https://ips.ligazakon.net/document/view/kp040812?an=182.

Додаток А

Копія тези конференції



МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Національна академія наук України
Університет імені П'єра і Марії Кюрі (Франція)
Маріборский університет (Словения)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Шяуляйська державна колегія (Литва)
Жешувський політехнічний університет ім. Лукасевича (Польща)
Білоруський національний технічний університет (Республіка Білорусь)
Міжнародний університет цивільної авіації (Марокко)
Національний університет біоресурсів і природокористування України (Україна)
Наукове товариство ім. Шевченка
ГО «Асоціація випускників Тернопільського національного технічного університету імені Івана Пулюя»

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник

тез доповідей

Том II

IX Міжнародної науково-технічної конференції молодих учених та студентів

25-26 листопада 2020 року

УКРАЇНА
ТЕРНОПІЛЬ – 2020

Рисунок 1.Д.А. Копія титульної сторінки збірника тез конференції

Рисунок 2.Д.А. Копія сторінки змісту збірника конференції із прізвищем автора та посиланням на тезу

Копія тексту тези із збірника конференції

УДК 004.052.42

П. І. Мойсей, студент, І. Ю.Дедів,канд.тех. наук, доцент.
Тернопільський національний технічний університет імені Івана Пулюя

МЕТОДОБРОБКИЗОБРАЖЕННЯ ДЛЯ ВЕРИФІКАЦІЇ ОСОБИ

P.I.Moisei, student, I. U.Dediv, Ph. D., Assoc. Prof.

METHOD OF PROCESSINGIMAGE FORIDENTITYVERIFICATION

Верифікація - це процес встановлення відповідності інформації, необхідної користувачу, при його зверненні до системи різними шляхами і перевірка на надання доступу користувачу для безпеки.[1-2]

Основними проблемами при верифікації є освітленість, кути огляду,рух, несприятливий фон. Вирішення даних проблем можна за допомогою покращення зображення.[2]

Для обробки зображення [3] використовується метод гістограмноїеквалізації та фільтр Лапласа.

Формула (1) гістограмноїеквалізації здійснює рівномірний розподіл яскравостей, а формула (2) фільтра Лапласа здійснює кращу деталізацію зображення:

$$g = histeq(f, nlev) \quad (1)$$

$$g = imfilter(f, w, 'replicate'), \quad (2)$$

де f – вхідне зображення;nlev – число рівнів інтенсивності для вихідного зображення (по замовчуванням число 64; максимум 256);w – фільтр Лапласа у вигляді матриці; replicate– застосування фільтра на зображення.

Рисунок 1. Зображення до обробки

Рисунок 2. Зображення після обробки

В кінцевому результаті, на виході буде зображення (рис. 2) з розподіленим рівнем яскравості та деталізацією кращою, ніж на вході (рис. 1). Це призведе до зменшення часу для верифікації осіб, а також збільшення його надійності і безпомилковості. Завади, що діють на вхідне зображення, вже не будуть так портити якість.

Література

1. https://www.roboforex.ua/about/client/faq/verification/16/.

2. https://www.tadviser.ru/index.php/Статья:Системы_распознавания_лиц_(Facial_recognition).

3. Гонсалес Р. Цифроваяобработка зображений в средеMatLab: навч. посіб. [для вищих навчальних закладів] / Р. Гонсалес, Р. Вудс, С. Эддинс. – Москва: Техносфера, 2006. – 616с.

Додаток Б

Лістинг програми обробки зображення в програмному середовищі MatLab

```
f=imread('C:\Users\Evolu\Desktop\matlab.jpg');
I=rgb2gray(f);
imshow(f)
imshow(I)
imhist(I)
g=histeq(I, 256);
imshow(g)
imhist(g)
w=[0.2 0.2 0.2; 0.1 -2 0.1; 0.2 0.2 0.2];
g1=imfilter(g,w,'replicate');
imshow(g1,[]);
g2=im2double(g);
g3=imfilter(g2,w,'replicate');
imshow(g3,[]);
d=g2-g3;
imshow(d).
```