**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

**КАФЕДРА СИСТЕМ ТА ТЕХНОЛОГІЙ КІБЕРБЕЗПЕКИ**

# КВАЛІФІКАЦІЙНА РОБОТА

на тему:

**«Технологія ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту»**

зі спеціальності *125 Кібербезпека та захист інформації*
*(код, найменування спеціальності)*

освітньо-професійної програми *Інформаційна та кібернетична безпека*
*(назва програми)*

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

_____ Олександр ВОРОНА
*(підпис)*

Виконав: здобувач вищої освіти групи БСДМ-63
ГОЛОБОРОДЬКО Владислав
*(прізвище, ім'я)*

Керівник к.т.н., доцент БОРСУКОВСЬКИЙ Юрій
*(науковий ступінь, вчене звання, прізвище, ім'я)*

Рецензент _____
*(науковий ступінь, вчене звання, прізвище, ім'я)*

Київ 2024

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ**

Кафедра Систем та технологій кібербезпеки
Ступінь вищої освіти Магістр
Спеціальність 125 Кібербезпека та захист інформації
Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри
Систем та технологій
кібербезпеки
_____ Галина ГАЙДУР
"15" жовтня 2024 року

# З А В Д А Н Н Я
## НА КВАЛІФІКАЦІЙНУ РОБОТУ

ГОЛОБОРОДЬКА Владислава Сергійовича
*(прізвище, ім'я)*

1. Тема кваліфікаційної роботи: «Технологія ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту»

керівник кваліфікаційної роботи Борсуковський Юрій Володимирович, к.т.н., доц.
*(прізвище, ім'я, науковий ступінь, вчене звання)*

затверджені наказом Державного університету інформаційно-комунікаційних технологій від «15 » жовтня 2024 року № 320.

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи 15.12.2024 р.

3. Вихідні дані до кваліфікаційної роботи
технології ідентифікації;
методи штучного інтелекту;
алгоритми машинного навчання.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1. Дослідження проблеми ідентифікації користувачів інформаційних систем організації.
2. Аналіз методів і технологій обробки зображень для ідентифікації користувачів інформаційних систем організацій.

3. Технологія ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту.

5. Перелік графічного матеріалу
Презентація PowerPoint.

6. Дата видачі завдання 01.10.2024 р.

## КАЛЕНДАРНИЙ ПЛАН

| № зп | Назва етапів кваліфікаційної роботи | Строк виконання етапів роботи | Примітка |
|---|---|---|---|
| 1. | Розробка та затвердження робочого графіка | 24.09.2024 | |
| 2. | Збір необхідної інформації | 27.09.2024 | |
| 3. | Підготовка та написання першого розділу кваліфікаційної робити. Відправка на перевірку керівнику. | 5.10.2024 | |
| 4. | Підготовка та написання другого розділу кваліфікаційної робити. Відправка на перевірку керівнику. | 15.10.2024 | |
| 5. | Розробка технології ідентифікації користувачів інформаційної системи організацій | 23.11.2024 | |
| 6. | Підготовка та написання третього розділу кваліфікаційної робити | 31.11.2024 | |
| 7. | Редагування та друк пояснювальної записки. Перевірка на антиплагіат. | 11.12.2024 | |
| 8. | Оформлення та створення презентації. | 12.12.2024 | |
| 9. | Підготовка до захисту дипломної роботи | 15.12.2024 | |

Здобувач вищої освіти _____ Владислав ГОЛОБОРОДЬКО
*(підпис)* *(ім'я, прізвище)*

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
*(підпис)* *(ім'я, прізвище)*

**ВІДГУК РЕЦЕНЗЕНТА**
на кваліфікаційну роботу

здобувача ГОЛОБОРОДЬКА Владислава

на тему: «Технологія ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту»

**Актуальність:** З огляду на стрімкий розвиток цифрових технологій та зростання кіберзагроз, ідентифікація користувачів стала ключовим елементом у забезпеченні кібербезпеки сучасних інформаційних систем. Тема роботи є надзвичайно актуальною, адже використання технологій штучного інтелекту для покращення точності та надійності ідентифікації сприяє зміцненню захисту організаційних ресурсів.

**Позитивні сторони:**

1. Проведено всебічний аналіз методів і технологій ідентифікації користувачів, завдяки яким було знайдено недоліки та переваги існуючих технологій.
2. Описано та реалізовано підхід, що поєднує переваги алгоритму SURF та згорткових нейронних мереж, що дало змогу підвищити ефективність ідентифікації користувачів.
3. Надано рекомендації щодо впровадження технології ідентифікації користувачів в системи організацій.
4. Кваліфікаційна робота містить приклади коду, побудовані моделі та схеми, які демонструють глибоке розуміння здобувачем технічної сторони питання. Текст роботи структурований, висновки логічно обґрунтовані, список використаних джерел охоплює сучасну наукову літературу.

**Недоліки:**

1. У кваліфікаційній роботі було б корисно продемонструвати використання технології ідентифікації на прикладі реальної організації, що підвищило б практичну цінність роботи.
2. Можна було б докладніше описати аспекти безпеки, пов’язані із зберіганням і обробкою біометричних даних.

Відзначені зауваження не впливають на загальну позитивну оцінку кваліфікаційної роботи.

**Висновок:** Враховуючи недоліки, кваліфікаційна робота заслуговує оцінку **“добре”**, а здобувач(ка) **ГОЛОБОРОДЬКО Владислав** – присвоєння кваліфікації магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Рецензент:

| _____ | _____ | _____ |
|---|---|---|
| *(науковий ступінь, вчене звання)* | *(підпис)* | *(ім’я, прізвище)* |

**ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ**
**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ КІБЕРБЕЗПЕКИ ТА ЗАХИСТУ ІНФОРМАЦІЇ**

**ПОДАННЯ**
**ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ**
**ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ**

Направляється здобувач ГОЛОБОРОДЬКО Владислав до захисту кваліфікаційної роботи
*(прізвище, ім'я)*
спеціальності 125 Кібербезпека та захист інформації
освітньо-професійної програми Інформаційна та кібернетична безпека
*(шифр і назва спеціальності)*
на тему: «Технологія ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту».
Кваліфікаційна робота і рецензія додаються.

Директор інституту _____ Євгенія ІВАНЧЕНКО
*(підпис)* *(ім'я, прізвище)*

**Висновок керівника кваліфікаційної роботи**

Здобувач ***ГОЛОБОРОДЬКО Владислав*** обрав тему роботи, метою якої було дослідити методи ідентифікації користувачів інформаційної системи на основі технологій штучного інтелекту, а також розробити рекомендації щодо їх впровадження. Робота демонструє здатність здобувача аналізувати сучасні підходи, визначати їх переваги та недоліки, а також пропонувати власні рекомендації для підвищення ефективності ідентифікації користувачів. В процесі виконання кваліфікаційної роботи ***ГОЛОБОРОДЬКО Владислав*** показав вміння працювати з науково-технічною літературою, самостійно вирішувати поставлені завдання, а також грамотно формулювати висновки. Робота виконана акуратно,

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача ***ГОЛОБОРОДЬКА Владислава*** на оцінку **"добре"** та присвоїти йому кваліфікації магістр з кібербезпеки за освітньо-професійною програмою інформаційна та кібернетична безпека.

Керівник кваліфікаційної роботи _____ Юрій БОРСУКОВСЬКИЙ
*(підпис)* *(ім'я, прізвище)*
"____" _____ 2024 року

**Висновок кафедри про кваліфікаційну роботу**

Кваліфікаційна робота розглянута. Здобувач **ГОЛОБОРОДЬКО Владислав** допускається до захисту
даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувач кафедри Систем та технологій кібербезпеки
*(назва)*
_____ Галина ГАЙДУР
*(підпис)* *(ім'я, прізвище)*

# РЕФЕРАТ

Текстова частина кваліфікаційної роботи: 73 сторінки, 39 рисунків, 1 таблиця, 18 джерел.

*Об'єкт дослідження* – процес ідентифікації користувачів в інформаційній системі організації.

*Предмет дослідження* – технології ідентифікації користувачів на основі штучного інтелекту та їх вплив на підвищення рівня кібербезпеки.

*Мета роботи* – розробка та дослідження методів ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту, а також розробка рекомендацій щодо їх застосування для покращення кібербезпеки.

*Методи дослідження* – аналіз наукової літератури, дослідження міжнародних стандартів у сфері кібербезпеки, аналіз існуючих систем ідентифікації, моделювання процесів біометричної ідентифікації користувачів із застосуванням ШІ, аналіз результатів і оцінка їхнього впливу на кібербезпеку

Технологія ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту забезпечує сучасний рівень захисту, автентифікації та контролю доступу. Робота демонструє практичне застосування комбінованого підходу, який поєднує можливості алгоритму SURF із глибокими нейронними мережами, що дозволило досягти високої ефективності навіть у складних умовах, таких як: обробка зображень із низькою роздільною здатністю, виявлення змін чи модифікацій обличчя, а також ідентифікація в умовах змінного чи недостатнього освітлення.

У роботі проведено детальний аналіз існуючих методів і технологій ідентифікації користувачів. Визначено основні переваги та обмеження сучасних підходів.

На основі проведених досліджень розроблено рекомендації щодо впровадження технології ідентифікації користувачів в інформаційні системи організацій. Визначено основні принципи її інтеграції, методи оптимізації та адаптації до потреб конкретних організацій.

Запропонована технологія може бути використана для захисту інформаційних ресурсів організацій, забезпечення безпеки доступу до корпоративних систем, а також у системах моніторингу й контролю доступу в режимі реального часу.

Галузь використання – кібербезпека, контроль доступу та автентифікація в інформаційних системах організацій.

АЛГОРИТМ КЛЮЧОВИХ ТОЧОК, ЗГОРТКОВА НЕЙРОННА МЕРЕЖА, МАШИННЕ НАВЧАННЯ, БІОМЕТРІЯ, ІНФОРМАЦІЙНА БЕЗПЕКА, ШТУЧНИЙ ІНТЕЛЕКТ

## ABSTRACT

Text part of the qualification work: 73 pages, 39 figures, 1 table, 18 sources.

*Object of research* – is the process of user identification in the organization's information system.

*Subject of research* –user identification technologies based on artificial intelligence and their impact on increasing the level of cybersecurity.

*The aim of research* – develop and study methods for identifying users of the organization's information system using artificial intelligence technologies, as well as to develop recommendations for their application to improve cybersecurity.

*Research methods* – analysis of scientific literature, research of international standards in the field of cybersecurity, analysis of existing identification systems, modeling of biometric user identification processes using AI, analysis of results and assessment of their impact on cybersecurity

The technology for identifying users of the organization's information system using artificial intelligence technologies provides a modern level of protection, authentication and access control. The work demonstrates the practical application of a combined approach that combines the capabilities of the SURF algorithm with deep neural networks, which made it possible to achieve high efficiency even in difficult conditions, such as: processing low-resolution images, detecting changes or modifications of the face, as well as identification in conditions of variable or insufficient lighting.

The work provides a detailed analysis of existing methods and technologies for user identification. The main advantages and limitations of modern approaches are identified.

Based on the research, recommendations have been developed for the implementation of user identification technology in information systems of organizations. The main principles of its integration, methods of optimization and adaptation to the needs of specific organizations have been identified.

The proposed technology can be used to protect information resources of organizations, ensure access security to corporate systems, as well as in real-time monitoring and access control systems.

Field of application - cybersecurity, access control and authentication in information systems of organizations.

KEYPOINT ALGORITHM, CONVULSIVE NEURAL NETWORK, MACHINE LEARNING, BIOMETRY, INFORMATION SECURITY, ARTIFICIAL INTELLIGENCE

**ЗМІСТ**

# ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

AI – Artificial Intelligence

CNN – Convolutional Neural Network

DL– Deep Neural Networks

HOG – Histogram of Oriented Gradients

HCC– Haar Cascade Classifier

Heat-Map – Heat Maps

LBP – Local Binary Patterns

MTCN – Multi-Task Cascaded Convolutional Networks

RGB – Red, Green, Blue

SIFT – Scale-Invariant Feature Transform

SURF – Speeded-Up Robust Features

VJ – Viola-Jones Algorithm

FCL – Fully Connected Layers

IL – Input Layer

CL– Convolutional Layer

PL– Pooling Layer

FCL – Fully Connected Layers

# ВСТУП

*Актуальність дослідження.* В умовах стрімкого розвитку цифрових технологій та розширення кількості користувачів, організації стикаються з новими загрозами в сфері кібербезпеки. Одним із ключових аспектів захисту інформаційних систем є ефективна ідентифікація користувачів, що забезпечує контроль доступу до конфіденційних даних і критичних ресурсів. Традиційні методи ідентифікації, такі як паролі чи смарт-карти, вже не можуть гарантувати необхідний рівень безпеки в умовах зростання обсягів кіберзагроз. У зв’язку з цим, використання технологій штучного інтелекту в процесах ідентифікації стає все більш актуальним.

Штучний інтелект дозволяє значно покращити точність і швидкість ідентифікації користувачів за допомогою аналізу біометричних даних та обробки зображень. Це дозволяє зменшити ризики, пов'язані з несанкціонованим доступом, атаками на паролі та іншими видами зловживань. Такі технології, як розпізнавання облич і поведінкова біометрія, можуть інтегруватися в інформаційні системи організацій для підвищення рівня кібербезпеки. У зв'язку з цим, дослідження та впровадження таких інноваційних підходів до ідентифікації користувачів є надзвичайно актуальними для забезпечення комплексного захисту від кіберзагроз.

Таким чином, дослідження технологій ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту є критично важливим для забезпечення кібербезпеки в сучасних умовах.

*Об’єкт дослідження* – процес ідентифікації користувачів в інформаційній системі організації.

*Предмет дослідження* – технології ідентифікації користувачів на основі штучного інтелекту та їх вплив на підвищення рівня кібербезпеки.

*Метою роботи* – створення технології ідентифікації користувачів інформаційної системи організації шляхом впровадження методів штучного інтелекту для підвищення точності, швидкості та безпеки процесу. Для досягнення поставленої мети в роботі вирішуються наступні задачі:

- дослідження сучасних проблем у сфері ідентифікації користувачів інформаційних систем організації
- аналіз методів і технології ідентифікації та обробки зображень користувач інформаційних систем організації
- створення технології ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту.

*Наукові завдання***:**

- дослідити сучасні загрози та складнощі, пов'язані з процесами ідентифікації користувачів інформаційних систем;
- проаналізувати методи обробки зображень та біометричних даних для ідентифікації користувачів;
- провести аналіз існуючих рішень ідентифікації на основі штучного інтелекту в контексті кібербезпеки;
- розробити підхід до інтеграції технологій штучного інтелекту в процес ідентифікації користувачів з акцентом на кібербезпеку;
- надати рекомендації щодо впровадження технологій ШІ в системи ідентифікації для підвищення рівня захисту інформаційних систем.

*Методи дослідження* – аналіз наукової літератури, дослідження міжнародних стандартів у сфері кібербезпеки, аналіз існуючих систем ідентифікації, моделювання процесів біометричної ідентифікації користувачів із застосуванням ШІ, аналіз результатів і оцінка їхнього впливу на кібербезпеку

*Практичне значення одержаних результатів***:** Запропоновані в дослідженні технології та методи ідентифікації користувачів на основі штучного інтелекту дозволяють підвищити ефективність та надійність кібербезпеки організації, мінімізуючи ризики несанкціонованого доступу та інших кіберзагроз. Результати роботи можуть бути використані фахівцями з

кібербезпеки для впровадження інноваційних рішень в інформаційні системи організацій.

Результати кваліфікаційної роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2024 року в Державному університеті інформаційно-комунікаційних технологій, м. Київ.

# 1 ДОСЛІДЖЕННЯ ПРОБЛЕМИ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІЗАЦІЇ

Розвиток сучасних технологій у сфері розпізнавання та виявлення образів, заснованих на штучному інтелекті та машинному навчанні, сприяє створенню більш ефективних та надійних систем ідентифікації користувачів. Раніше для ідентифікації використовувалися виключно традиційні методи, такі як паролі, PIN-коди або фізичні токени, однак вони мають ряд суттєвих недоліків, таких як низький рівень захисту, вразливість до атак на паролі та необхідність постійного оновлення.

Сучасні системи, що базуються на технологіях штучного інтелекту, забезпечують високу ефективність і швидкість роботи з великими масивами даних, надаючи велику точність у розпізнаванні обличчя, відбитків пальців та інших біометричних характеристик. Окрім того, завдяки розвитку нейронних мереж стало можливим створення систем, що адаптуються до умов реального часу, дозволяючи ідентифікувати користувачів навіть за зміненими зовнішніми ознаками.

## 1.1 Актуальність проблеми ідентифікації користувачів в інформаційних системах

Сучасні інформаційні системи організацій потребують надійних та безпечних методів ідентифікації користувачів. У зв'язку зі зростанням кількості кібератак та несанкціонованих доступів, питання ідентифікації користувачів стає ключовим у забезпеченні безпеки інформаційних ресурсів. Традиційні методи автентифікації, такі як паролі та токени, не завжди можуть забезпечити належний рівень захисту, оскільки піддаються атакам на паролі, фішингом, підробкою і крадіжкою автентифікаційних даних. Це підкреслює необхідність

впровадження новітніх технологій, здатних забезпечити більш надійні рішення для ідентифікації користувачів.

Основною проблемою традиційних методів ідентифікації користувачів є їх вразливість перед сучасними кіберзагрозами. Паролі можуть бути скомпрометовані через атаки на соціальну інженерію, а двофакторна автентифікація, хоча й підвищує рівень захисту, може бути складною в реалізації та не завжди забезпечує належний рівень безпеки в разі витоку біометричних або інших автентифікаційних даних. Особливої уваги потребують питання захисту особистих даних, оскільки використання біометричних технологій породжує нові виклики, пов’язані з конфіденційністю та етичними аспектами.

На сучасному етапі розвитку кібербезпеки найбільш актуальними є інструменти та методи ідентифікації користувачів, засновані на біометричних даних та технологіях штучного інтелекту. Ці технології дозволяють створювати динамічні системи, здатні ідентифікувати у реальному часі користувачів за різними біометричними показниками (відбитками пальців, розпізнаванням облич, сітківкою ока, голосом). При цьому такі методи можуть інтегруватися з існуючими системами безпеки для підвищення їхньої ефективності та надійності.

Незважаючи на активний розвиток технологій, існує ряд проблем, які необхідно вирішити. Сучасні підходи до ідентифікації користувачів інформаційних систем на основі біометричних даних та штучного інтелекту мають низку переваг, але також стикаються з певними проблемами. Ключовими проблемами є забезпечення високої точності та швидкості обробки значних обсягів даних, стійкість до кібератак і фальсифікації біометричних даних, а також здатність систем адаптуватися до різних умов використання.

Існуючі методи, такі як використання згорткових нейронних мереж (CNN) для розпізнавання образів, мають значні успіхи, але вони часто обмежені точністю у випадках, коли вхідні дані мають низьку якість або коли є варіації в освітленні та ракурсах. Крім того, CNN потребують великої кількості навчальних

даних, що може обмежувати їх ефективність у випадках, коли база даних є неповною або недостатньо розширеною.

Однією з існуючих проблем є вразливість до атак на біометричні системи, коли зловмисники можуть використовувати підроблені зображення або маніпулювати вхідними даними для обходу системи автентифікації. Це підкреслює необхідність вдосконалення існуючих методів для забезпечення вищого рівня захисту.

## 1.2 Методи детекції та аналізу зображень для біометричної індентифікації користувачів

Сучасні системи ідентифікації користувачів на основі аналізу зображень є складними технологіями, які використовують різноманітні методи для виявлення та розпізнавання облич, відбитків пальців та інших біометричних ознак. Ці методи можуть бути поділені на кілька категорій залежно від підходів до обробки зображень і рівня інтеграції з іншими існуючими технологіями, такими як: штучний інтелект, машинне навчання та комп'ютерний зір. У цьому підрозділі буде розглянуто основні методи детекції та аналізу зображень, які впроваджуються у сучасних системах ідентифікації користувачів.

### 1.2.1 Метод Хаара

Один із найвідоміших і найчастіше використовуваних методів для детекції облич — це метод Хаара. Він базується на застосуванні каскадних класифікаторів для виявлення облич у зображеннях за допомогою аналізу візуальних ознак, таких як зміна яскравості пікселів у конкретних областях зображення (рисунок 1.1). Метод Хаара популярний через його простоту та швидкість, але його ефективність може бути обмеженою у випадках зміни освітлення, позиції або якості зображення.

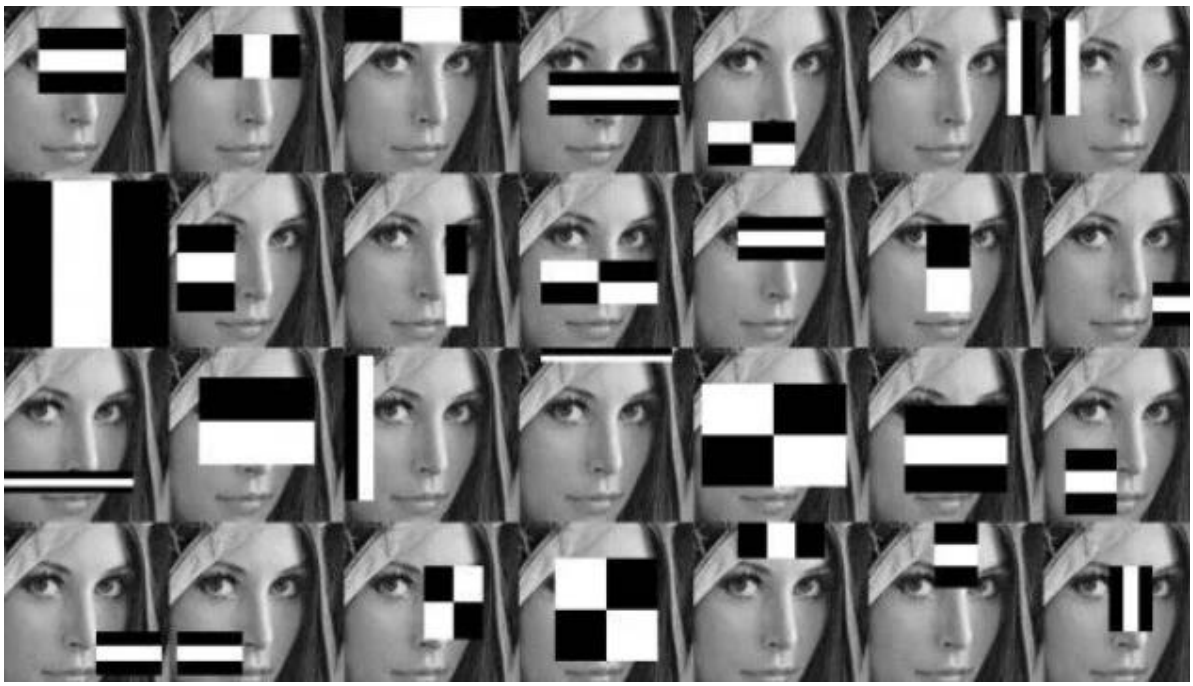


Рис. 1.1. Приклад навчання класифікатора Хаара

Переваги:

- Швидкість обробки.
- Придатний для детекції облич в умовах із постійним освітленням і чітким фоном.

Недоліки:

- Низька точність в умовах змінного освітлення.
- Обмежена здатність виявляти обличчя під різними кутами чи в умовах деформації зображення.

### 1.2.2 Метод гістограм орієнтованих градієнтів (HOG)

Метод HOG використовується для детекції облич та інших об'єктів у зображеннях. Цей підхід полягає в аналізі локальних градієнтів зображення та створенні гістограм, які відображають напрямок та інтенсивність цих градієнтів. HOG дозволяє виділяти текстури та контури об'єктів, що підвищує точність детекції (рисунок 1.2).

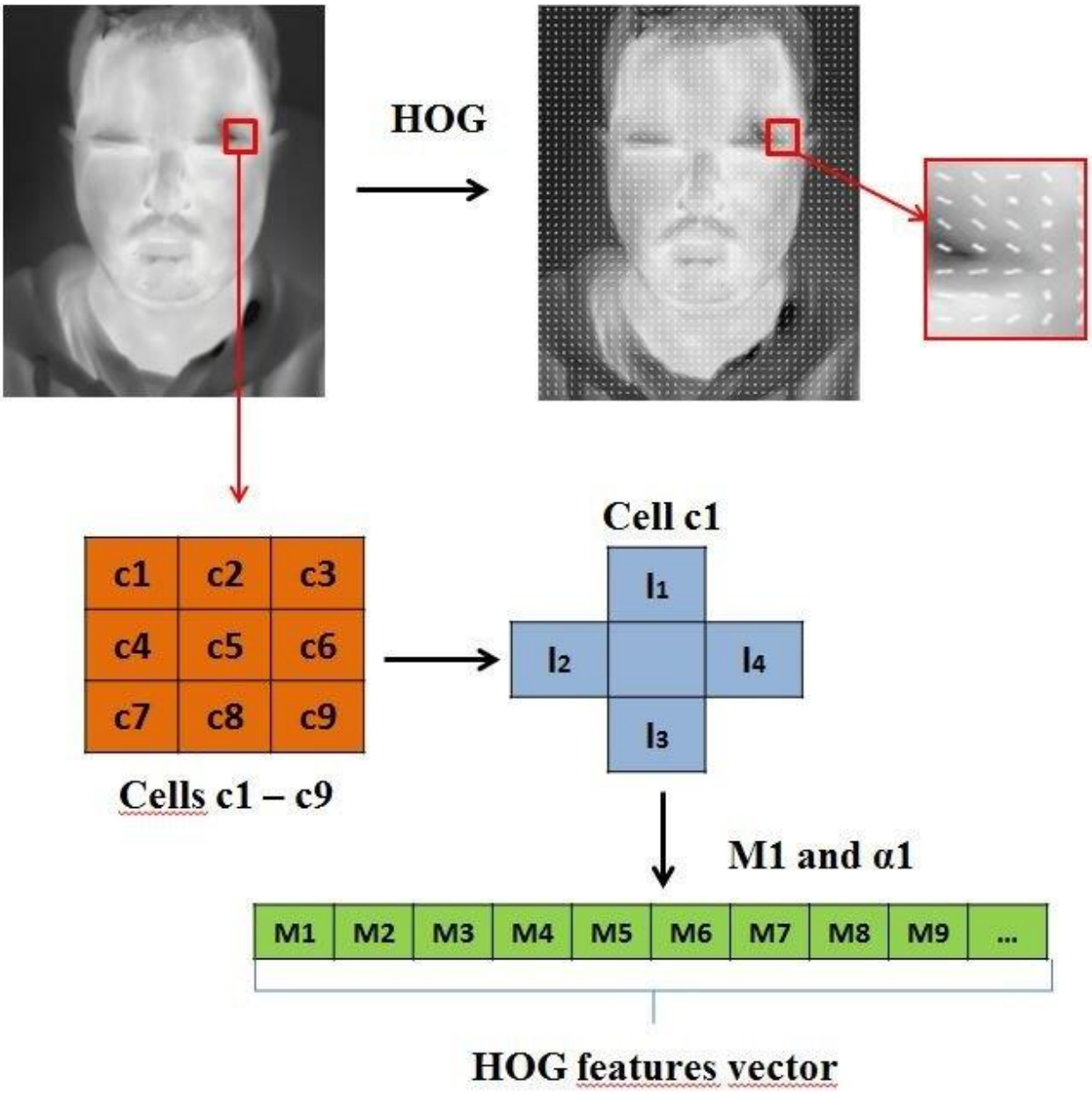



Рис. 1.2. Схема отримання ознак з використанням методу HOG

Переваги:

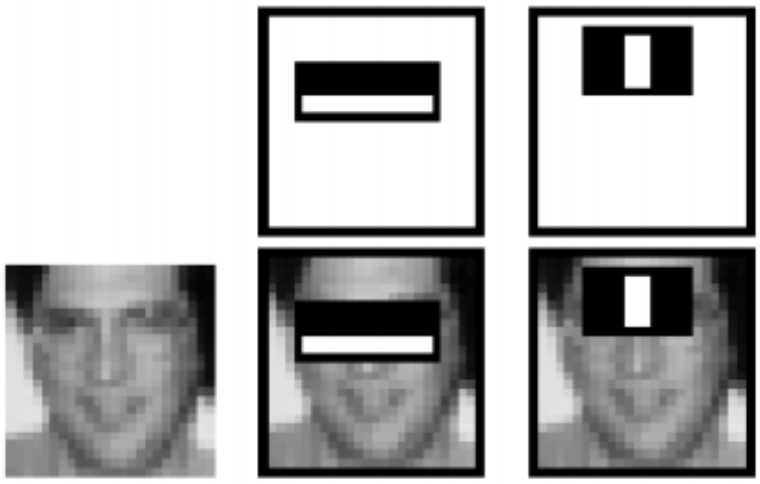
- Висока точність у стабільних умовах.
- Ефективність у виявленні різних типів об'єктів, окрім облич.

Недоліки:

- Чутливість до змін освітлення та тіні.
- Вимагає великої кількості обчислювальних ресурсів для аналізу.

### 1.2.3 Алгоритм Віоли-Джонса

Алгоритм Віоли-Джонса є класичним методом детекції облич, який використовує каскадні класифікатори та ознаки Хаара для швидкої та точної ідентифікації. Він застосовується для реального часу виявлення облич у зображеннях та відео і має добру продуктивність для таких завдань (рисунок 1.3).



$$f(x,y) = \sum_i p_b(i) - \sum_i p_w(i)$$

Рис. 1.3. Схема отримання ознак з використанням алгоритма Віоли-Джонса

Переваги:

- Висока швидкість роботи.
- Можливість роботи в реальному часі.

Недоліки:

- Схильність до помилок у випадках складного фону або змін освітлення.
- Обмежена здатність виявляти обличчя з різних кутів.

### 1.2.4 Алгоритми Canny та Sobel для детекції контурів

Методи детекції контурів, такі як алгоритми Canny та Sobel, використовуються для виявлення країв та контурів об'єктів у зображеннях. Ці методи базуються на аналізі різниці в яскравості між сусідніми пікселями і допомагають виявити границі між об'єктами. Вони є корисними для попередньої обробки зображень перед їх подальшою обробкою (рисунок 1.4).

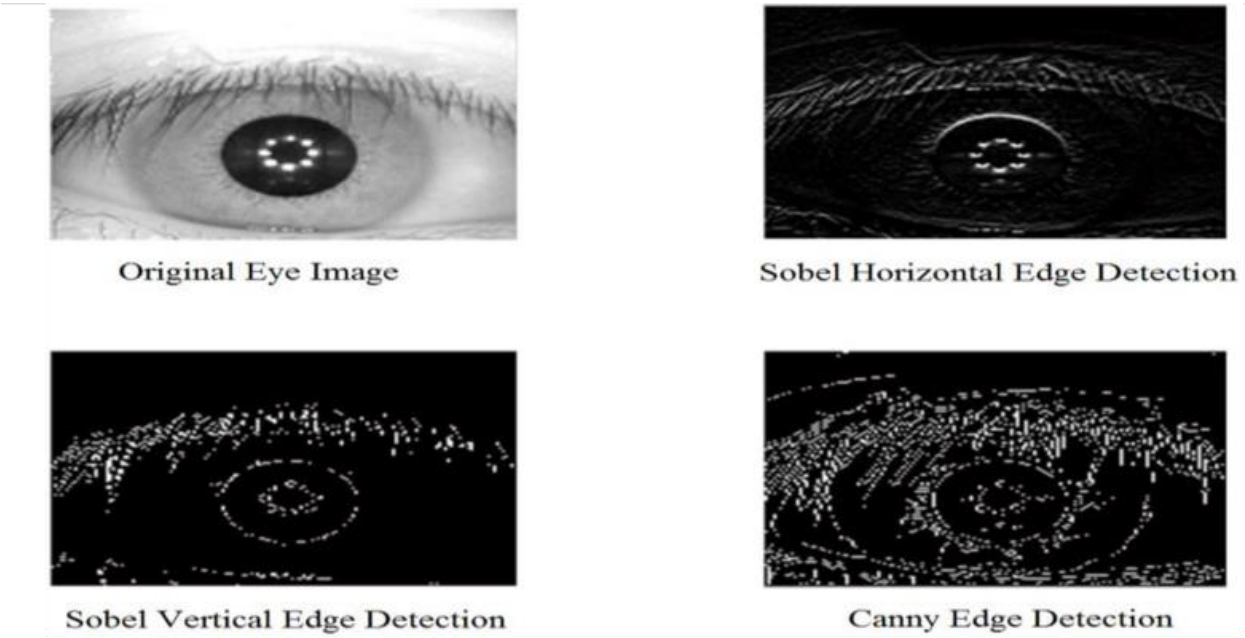



Рис. 1.4. Виявлення країв за методами Sobel і Canny

Переваги:

- Швидкість та ефективність у виявленні контурів об'єктів.
- Простота в реалізації.

Недоліки:

- Чутливість до шуму в зображеннях.
- Невисока точність при роботі з низькоякісними або сильно зашумленими зображеннями.

### 1.2.5 Локальні бінарні патерни (LBP)

Метод LBP - один із найбільш поширених підходів до аналізу текстури зображень і широко застосовується для детекції облич. LBP аналізує текстурні ознаки зображення на рівні окремих пікселів, порівнюючи значення пікселів із сусідніми та кодує цю інформацію в бінарний патерн (рисунок 1.5).

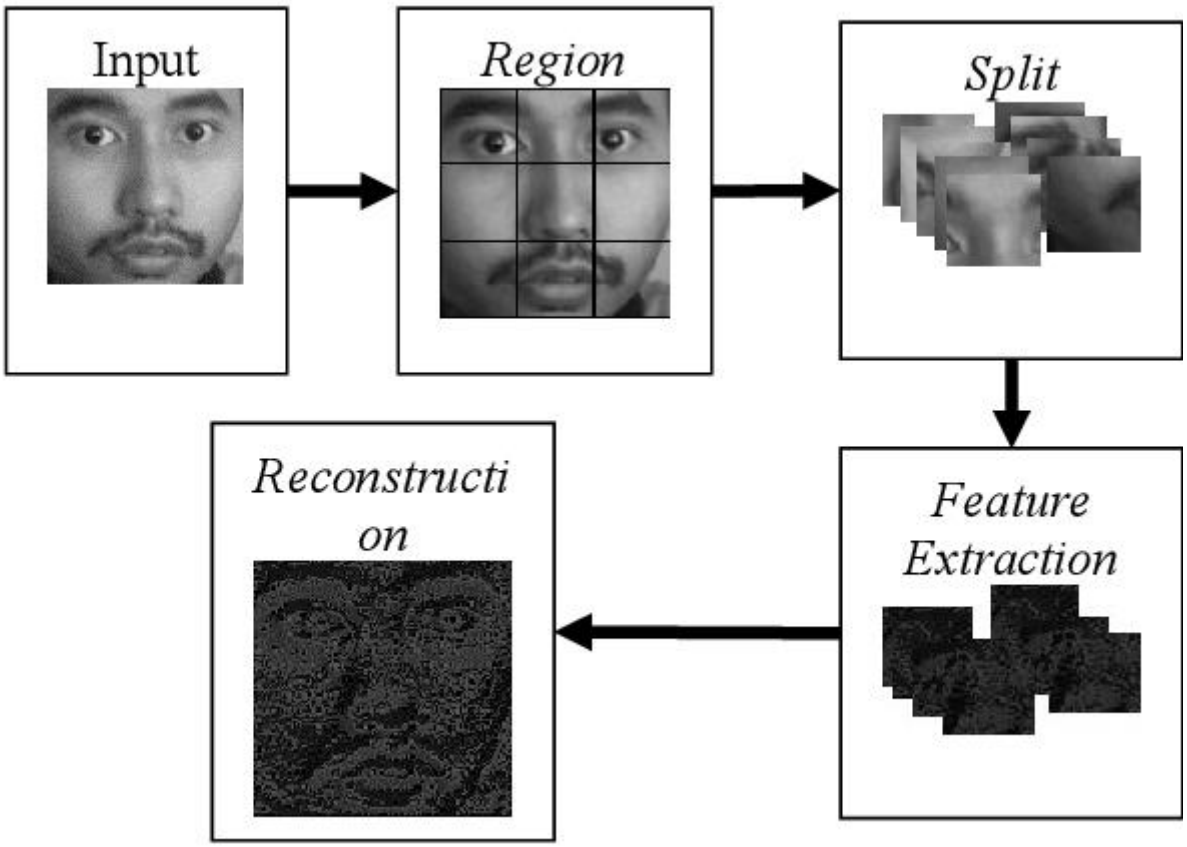



Рис. 1.5. Процес роботи LBP методу

Переваги:

- Висока стійкість до змін освітлення.
- Простота у використанні та швидкість обробки.

Недоліки:

- Обмежена здатність до детекції при змінах ракурсу обличчя.
- Не завжди забезпечує високу точність у складних умовах.

### 1.2.6 Теплові карти

Технології на основі теплових карт та зображень з глибини (3D) використовуються для підвищення точності детекції, особливо у випадках, коли звичайне 2D зображення не дає достатньо інформації. Теплові камери можуть виявляти температуру тіла користувача, що підвищує надійність ідентифікації, тоді як технології зображень з глибини дозволяють створювати тривимірні моделі об'єктів, що робить процес розпізнавання більш надійним (рисунок 1.6).

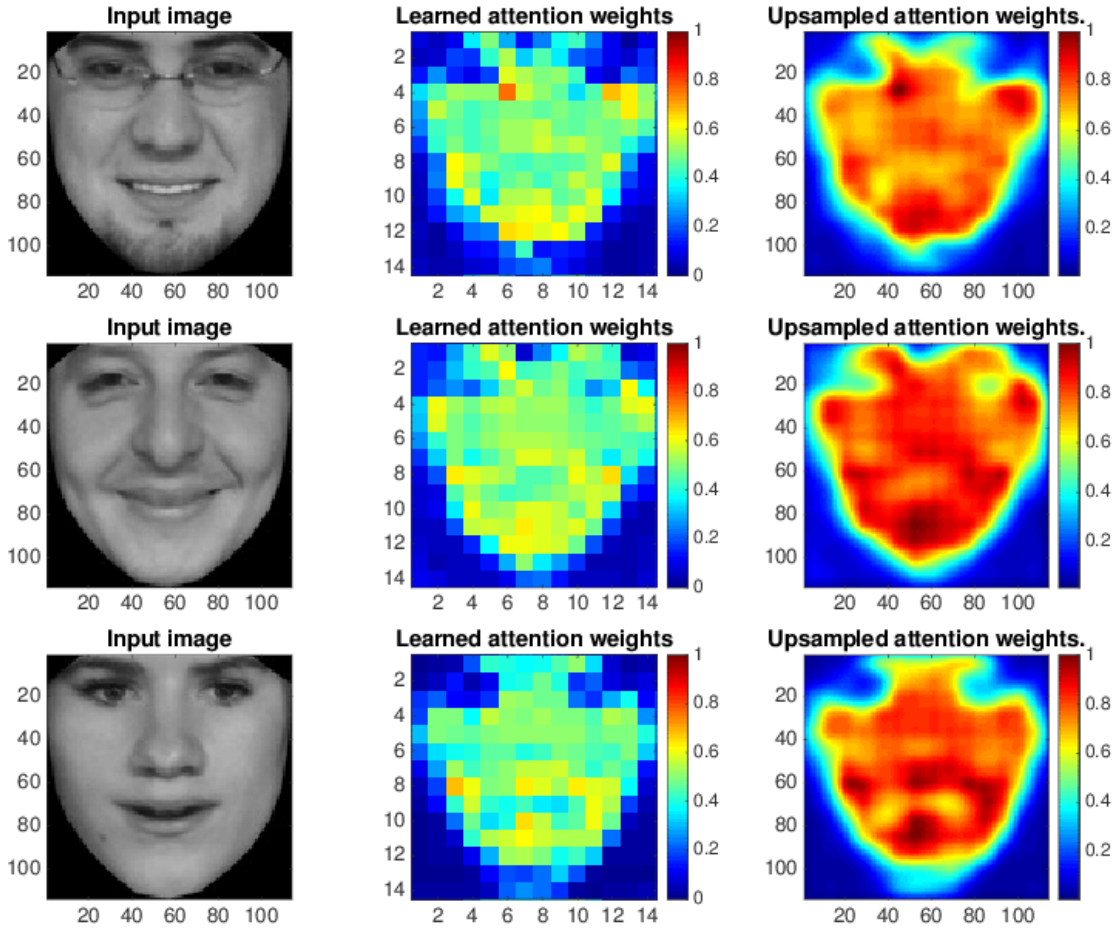



Рис. 1.6. Візуалізація роботи методу теплових карт

Переваги:

- Ідентифікація в умовах низької освітленості: Теплові камери можуть працювати навіть у повній темряві, виявляючи температуру тіла користувача

системи, та ефективно ідентифікувати особу навіть в умовах недостатнього освітлення.

- Віддалене розпізнавання: Цей метод також може бути корисним для ідентифікації на відстані, наприклад, у системах безпеки на великих відстанях, де традиційні методи не можуть надати достатньо чітких даних.

Недоліки:

- Висока вартість обладнання: Для використання цієї технології потрібні інфрачервоні камери або спеціалізовані сенсори, ціна такого обладнання не дозволяє його використовувати для широкого використання.
- Обмеження в умовах стабільного середовища: Теплові карти не завжди можуть замінити інші методи, якщо об'єкти є холодними або їх температура не значно відрізняється від оточуючого середовища.

### 1.2.7 Машинне навчання та нейронні мережі

Застосування машинного навчання та нейронних мереж у сфері ідентифікації користувачів на основі зображень є одним із найперспективніших підходів. Глибокі нейронні мережі (Deep Learning) дозволяють автоматично навчатися зображенню та створювати складні моделі, які можуть за допомогою високої точності проводити операцію ідентифікування користувачів навіть у складних умовах. Завдяки багатошаровим архітекторам (наприклад, згортковим нейронним мережам), ці методи можуть виявляти складні ознаки в зображеннях.

Переваги:

- Висока точність розпізнавання.
- Можливість навчання на великих обсягах даних.

Недоліки:

- Велика потреба в обчислювальних ресурсах.
- Складність реалізації та необхідність великих навчальних наборів даних.

## 1.3 Аналіз існуючих рішень біометричної індетифікації обличчя користувачів інформаційної систем на основі технологій штучного інтелекту

Існуючи рішення ідентифікації облич користувачів на основі штучного інтелекту використовують різні алгоритми і нейронні мережі для досягнення високої точності ідентифікації. В цьому розділі будуть розглянуті рішення від: FaceNet**,** DeepFace**,** VGG-Face. Вони займають лідируючи позиція в ідентифікації користувачів, але кожна з цих систем мають низку недоліків, які варто враховувати при їх впровадженні та використанні в безпеці інформаційних систем.

### 1.3.1 FaceNet

FaceNet — один із найпотужніших алгоритмів для ідентифікації облич, який використовує глибокі нейронні мережі для перетворення зображення обличчя в унікальний вектор ознак. Архітертура алгоритму розпізнавання FaceNet з урахуванням багатьох обмежень (рисунок 1.7).

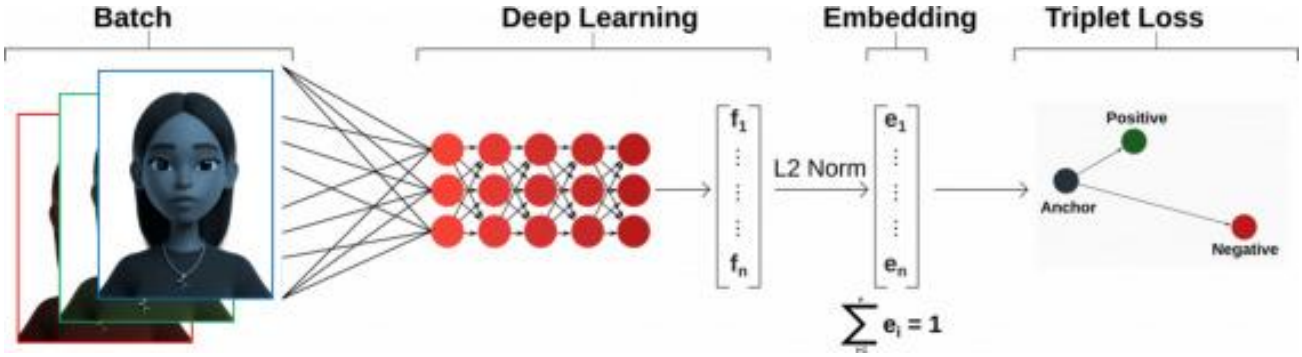



Рис. 1.7. FaceNet архітектура

Недоліки:

1. Високі вимоги до обчислювальних ресурсів: FaceNet використовує складну архітектуру нейронних мереж, що потребує значних обчислювальних

ресурсів. Це створює проблему при використанні алгоритму у реальному часі на пристроях із низькою продуктивністю або в умовах великих навантажень, наприклад, у публічних системах відеоспостереження.

2. Чутливість до змін умов. Як і більшість систем розпізнавання облич, FaceNet демонструє зниження точності при зміні умов освітлення, ракурсу або частковому закритті обличчя. Ці фактори можуть призвести до хибних результатів або неспроможності системи ідентифікувати користувача.

3. Проблеми з конфіденційністю. Використання FaceNet передбачає збереження біометричних даних у вигляді векторів ознак, що створює ризики для конфіденційності. У випадку витоку цих даних є велика загроза для інформаційної системи, оскільки біометричні ознаки неможливо змінити так, як це можна зробити з паролем або іншими ідентифікаційними даними.

4. Атаки на безпеку системи. FaceNet може бути вразливим до атак з використанням підроблених зображень або 3D-моделей. Атаки типу презентації можуть бути успішними, якщо система не використовує додаткові механізми захисту.

### 1.3.2 DeepFace

DeepFace — це алгоритм, розроблений компанією Facebook, який також використовує глибокі нейронні мережі для аналізу обличчя. Хоча DeepFace забезпечує високу точність, існує кілька суттєвих недоліків:

Неповна стійкість до варіацій зображень: Хоча DeepFace демонструє високу точність за сприятливих умов, він може давати помилки при суттєвих змінах освітлення, ракурсу або якщо обличчя частково закрите. Зокрема, система може мати труднощі з розпізнаванням осіб у випадках використання масок або окулярів.

Великі обчислювальні витрати: DeepFace потребує великих обчислювальних ресурсів для аналізу і порівняння облич, що може бути проблемою при масштабуванні системи для роботи з великою кількістю

користувачів.

DeepFace також може бути вразливим до атак з використанням підроблених зображень або спеціально створених 3D-моделей облич. Це створює додаткові ризики для систем, які використовують цей алгоритм у критичних умовах, наприклад, для контролю доступу або фінансових транзакцій. Архітектура DeepFace (рисунок 1.7).

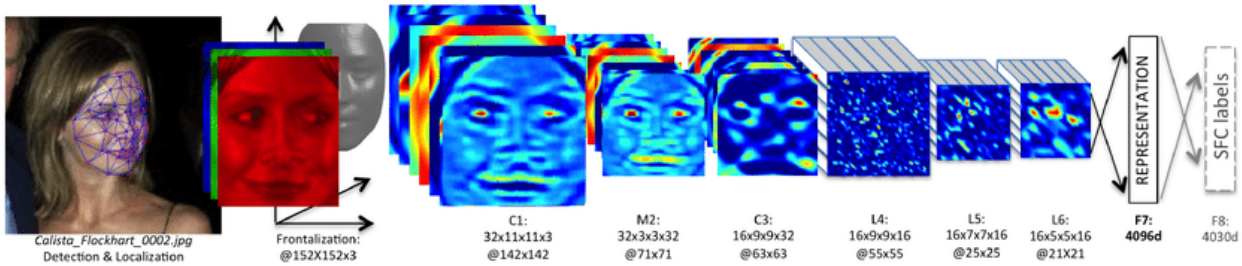



Рис. 1.7. DeepFace архітектура

Використання DeepFace для масового розпізнавання облич в соціальних мережах приводить до занепокоєння щодо приватності даних користувачів. Велика кількість зображень облич, які зберігаються і обробляються, може використовуватися без згоди користувачів, що викликає правові та етичні проблеми.

### 1.3.3 VGG-Face

VGG-Face є одним із ранніх рішень для ідентифікації облич. Вона здобула свою популярність завдяки своїй простоті та ефективності в задачах класифікації зображень. Ця система застосовує глибокі згорткові нейронні мережі для аналізу та класифікації облич. Модель VGG Face спрощує оригінальну архітектуру VGG-16, зберігаючи лише три основні блоки та видаляючи останні два згорткові блоки. Ця модифікація зменшує складність моделі, зберігаючи її продуктивність у різних завданнях розпізнавання обличчя. Показана мережева архітектура

VGGFace (рисунок 1.8).

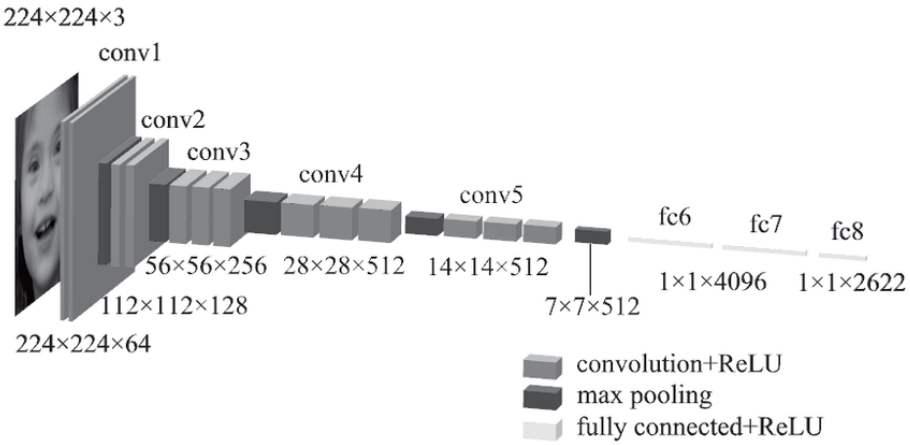



Рис. 1.7. VGGFace архітектура

Незважаючи на його успіхи, він також має недоліки:

1. Обмежена стійкість до часткових перекритів. VGG-Face демонструє зниження точності при частковому перекритті обличчя або якщо зображення є нечітким. Це може бути проблемою у випадках, коли користувачі носять маски або інші аксесуари, що змінюють вигляд обличчя.

2. Проблеми з масштабуванням. Хоча VGG-Face добре працює з відносно невеликими базами даних, його ефективність може знижуватися при обробці великої кількості користувачів у реальних умовах. Це пояснюється необхідністю значних ресурсів для навчання і використання моделі.

3. Відсутність оптимізації для реального часу. VGG-Face не був спеціально розроблений для роботи в реальному часі, що може бути перешкодою для застосування його в системах відеоспостереження або інших задачах, де потрібна миттєва реакція.

4. Надмірна залежність від навчальних даних. VGG-Face, як і інші алгоритми на основі глибокого навчання, вимагає великої кількості навчальних даних для досягнення високої точності. Якщо навчальні дані недостатньо різноманітні або не охоплюють широкий спектр варіацій облич, точність ідентифікації може суттєво знижуватися.

## Висновки до першого розділу

Перший розділ магістерської роботи присвячений аналізу сучасних методів розпізнавання та виявлення образів, зокрема технологій ідентифікації користувачів, заснованих на штучному інтелекті та машинному навчанні.

Було розглянуто сучасні системи біометричної ідентифікації, такі як: FaceNet, DeepFace та VGG-Face. Завдяки використанню глибоких нейронних мереж ці системи здатні автоматично виділяти ключові ознаки, адаптуючись до різних сценаріїв використання. Проте вони мають і недоліки, їх ефективність може знижуватися за умов змінного освітлення, варіацій ракурсів чи наявності шуму у даних. У таких ситуаціях методи, що використовують локальні ознаки, такі як HOG, LBP або алгоритм Віола-Джонса, залишаються актуальними, але поступаються у точності через обмеження у їхній адаптивності. Основні проблеми сучасних систем ідентифікації:

- необхідність забезпечення високої точності ідентифікації навіть у складних умовах, таких як змінне освітлення чи часткове перекриття обличчя;
- потребу в значних обчислювальних ресурсах для реалізації моделей та їх робота у реальному часі;
- сприятливі до підробки біометричної автентифікації;

На основі проведеного аналізу існуючих методів ідентифікації було виявлено, що для вирішення виявлених проблем доцільним є використання комбінованого підходу, який об’єднує переваги різних методів. Особливо перспективним є поєднання методу ключових точок, зокрема алгоритму SURF, із технологіями штучного інтелекту, такими як згорткові нейронні мережі. Інтеграція дозволяє поєднати швидкість і точність визначення ключових точок із потужними можливостями CNN у виділенні складних ознак та адаптації до змінних умов, що значно підвищує ефективність і надійність систем ідентифікації.

# 2 АНАЛІЗ МЕТОДІВ І ТЕХНОЛОГІЙ ОБРОБКИ ЗОБРАЖЕНЬ ДЛЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНИХ СИСТЕМ ОРГАНІЗАЦІЙ

## 2.1 Використання ключових точок та нейронних мереж для ідентифікації користувачів інформаційних систем

Метод ключових точок є одним з ключових інструментів у комп'ютерному зорі та обробці зображень, що дозволяє ідентифікувати характерні елементи об’єкта на зображенні. Цей метод полягає у виділенні унікальних точок чи ознак на зображенні, які можна використати для розпізнавання об’єктів, їх відстеження або класифікації. Одним із найбільш ефективних алгоритмів методу ключових точок є SURF. Алгоритм SURF дозволяє швидко та надійно виявляти стійкі ознаки, що робить його особливо корисним у застосуванні для ідентифікації облич або інших об'єктів.

Алгоритм SURF - був розроблений для вирішення обмежень, характерних для попереднього алгоритму SIFT. Основною особливістю SURF є його здатність забезпечувати високу швидкість обробки та точність за рахунок використання цілочисельного наближення матриці Гессе для знаходження ключових точок на обличчі людині( рисунок 2.1).

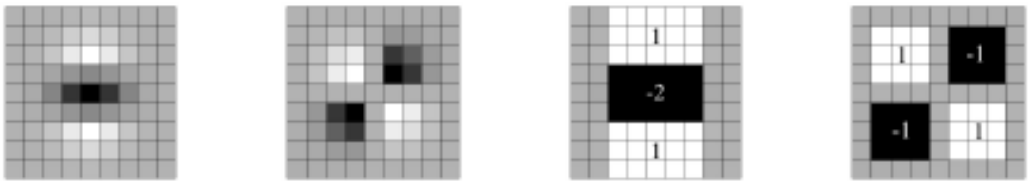



Рис. 2.1. Два приклади других похідних гаусової функції (ліворуч) і відповідні прямокутні фільтри (праворуч)

Інтегральне зображення, яке лежить в основі алгоритму, та дозволяють швидко обчислювати детектори та описувачі ознак. Перевага цього підходу є у використанні прямокутників котрі можна легко обчислювати, і розрахунки для різних масштабів можуть виконуватися одночасно

Основні кроки в алгоритмі SURF:

- Інтегральні зображення: Використовуються для швидкого обчислення суми інтенсивності пікселів у прямокутних областях, що значно підвищує швидкість обробки.
- Швидкий детектор на основі матриці Гессе: Виявляє ключові точки за допомогою визначника матриці Гессе, який оцінює локальні зміни інтенсивності на зображенні.
- Локалізація ключових точок і визначення орієнтації: Подібно до SIFT, алгоритм локалізує ключові точки та призначає їм орієнтацію на основі відповідей вейвлетів Хаара в круговій області навколо ключової точки.
- Генерація дескриптора ключових точок: Дескриптор формується, аналізуючи вейвлет-відповіді Хаара в горизонтальному та вертикальному напрямках у квадратній області навколо ключової точки, що дозволяє створити вектор ознак розмірністю 64.

Для врахування орієнтації обчислюються Гаарів вейвлет відповіді Хаара у напрямках x та y, області навколо ключової точки радіусом 6s з кроком вибірки s, де s пропорційний масштабу. Сума відповідей у скануючи області, що ковзає, використовується для визначення орієнтації.

Для виділення ознак ключової точки обирається область 20s x 20s, яка ділиться на 4x4 під області. З кожної під області витягуються вейвлет-відповіді у напрямках x та y, і ці відповіді об'єднуються, утворюючи дескриптор ознаки розмірністю 64 (рисунок 2.2).

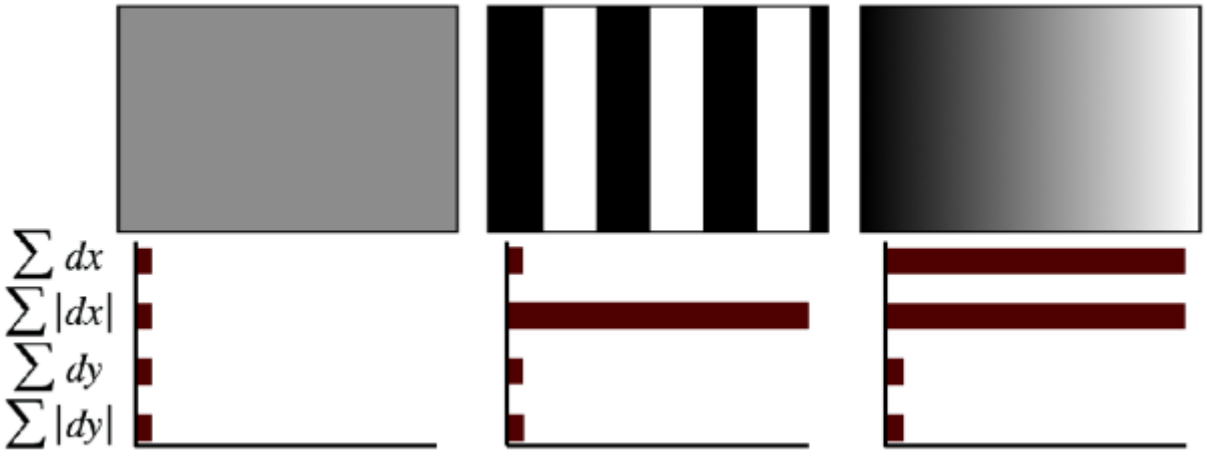



Рис. 2.2. SURF — Генерація дескриптора

Ці етапи забезпечують SURF інваріантність до поворотів і масштабування, що робить його ефективним для ідентифікації об'єктів у різних умовах.

## 2.2 Використання згорткових нейронних мереж для ідентифікації зображень людини

Згорткові нейронні мережі широко застосовуються для ідентифікації облич завдяки їхній здатності автоматично виділяти важливі ознаки на зображенні. CNN використовують шари згортки, які обробляють вхідне зображення за допомогою фільтрів, що дозволяє виділяти ключові структури об'єкта, такі як краї, контури та інші ознаки. Кожен шар CNN має здатність навчатися різним аспектам об'єкта, що сприяє підвищенню точності та гнучкості моделі (рисунок 2.3).

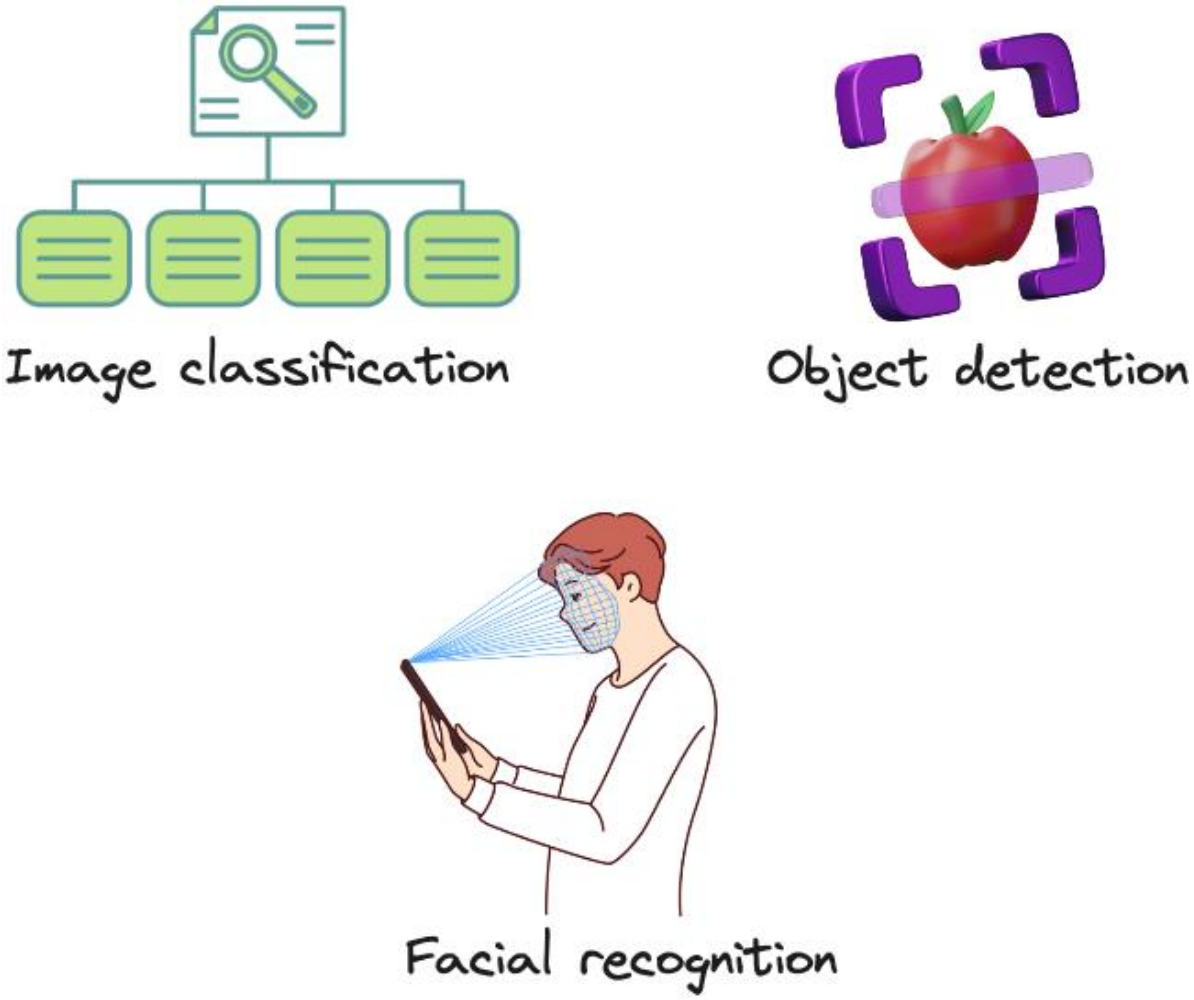



Рис. 2.3. Практичне застосування CNN

Архітектура CNN для ідентифікації зображень включає:

1. Шари згортки: Ці шари відповідають за виділення ознак зображення, використовуючи фільтри для кожної області. Це забезпечує інваріантність до зсуву об'єктів.

2. Шари об'єднання (Pooling layers): Застосовуються для скорочення розмірності даних із збереженням основних ознак, що допомагають уникнути надмірного навантаження на створену модель.

3. Повністю пов’язані шари: Вони забезпечують з'єднання виділених ознак та формують кінцевий результат, забезпечуючи класифікацію або розпізнавання зображення.

Модель CNN для виділення ознак спрямована на зменшення кількості ознак, наявних у наборі даних. Вона створює нові ознаки, які узагальнюють існуючі ознаки, що містяться в початковому наборі. Архітектура CNN зазвичай включає багато таких шарів, як показано на базовій діаграмі CNN (рисунок 2.4).

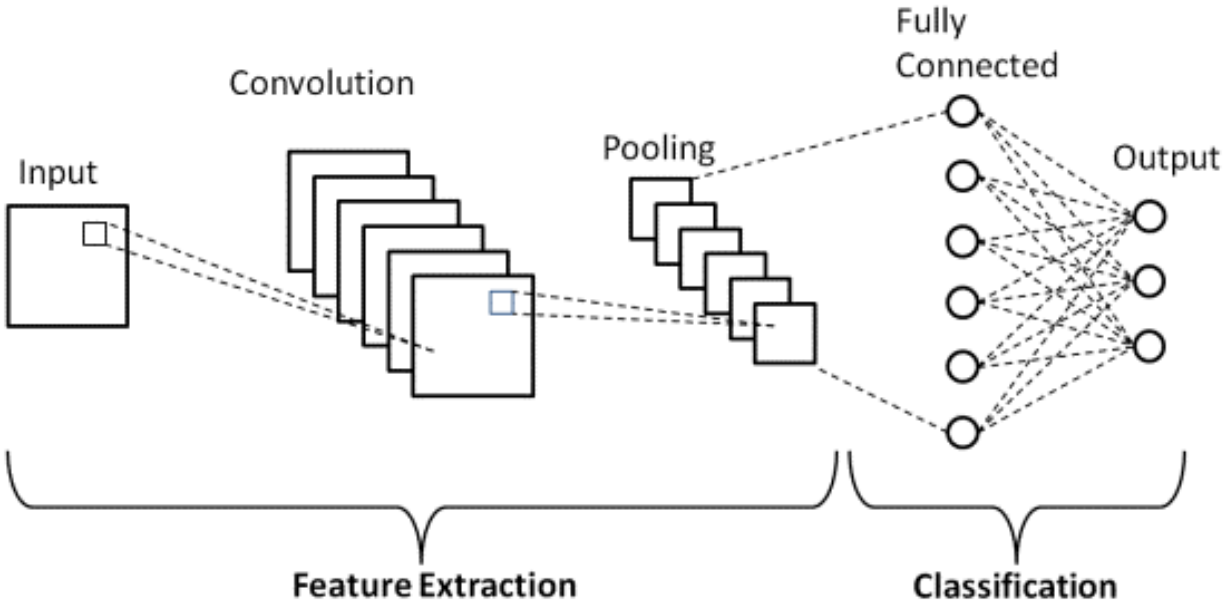



Рис. 2.4. Архітектура CNN

Згортковий шар застосовує фільтри до вхідного зображення для виділення ознак, шар об'єднання (Pooling layer) зменшує розмір зображення, знижуючи обчислювальні витрати, а повністю зв’язаний шар робить фінальну відповідь. Мережа навчається оптимальним фільтрам за допомогою зворотного поширення помилки і градієнтного спуску.

Згорткові нейронні мережі — це нейронні мережі, які розділяють свої параметри. Зображення: людини його можна представити у вигляді кубоїда з довжиною та шириною і висотою . Висота відповідає кількості каналів, оскільки зображення зазвичай мають червоний, зелений і синій канали (рисунок 2.5).

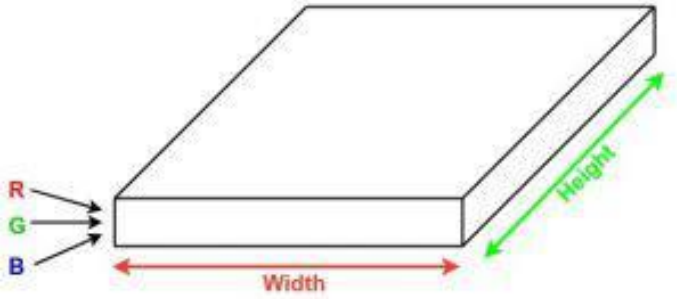



Рис. 2.5. Параметри зображення

Для цього обирається невелику ділянка зображення та запускається нейронна мережа на цій ділянці, що є фільтром або ядром. Цей фільтр має, K виходів, котрі розташовані вертикально. Наступним кроком є переміщення фільтра по всьому вхідному зображенню, обробляючи кожну ділянку послідовно. У результаті цього процесу ми отримуємо нове зображення, яке відрізняється за шириною, висотою та глибиною.

Тепер замість початкових каналів R, G і B у нас є більше каналів, але зменшені ширина та висота. Така операція називається згорткою . Якщо ж розмір вибраної ділянки відповідає розміру всього зображення, отримаємо звичайну нейронну мережу. Використання невеликої ділянки дозволяє зменшити кількість вагових коефіцієнтів, що спрощує обчислення (рисунок 2.6).

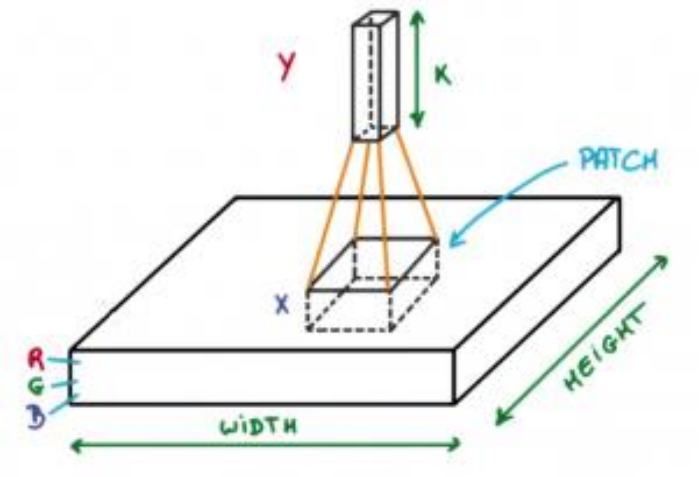



Рис. 2.6. Глибинне навчання

Шар згортки складається з набору навчальних фільтрів або ядер, які мають невеликі розміри по ширині та висоті і таку ж глибину, як і вхідний об’єм для зображень глибина дорівнює 3 через канали RGB.

Ми виконуємо згортку на зображенні розміром 34x34x3, можливий розмір фільтра може бути a×a×3, де 'a' — це невелике значення, яке значно менше від розміру зображення.

Процес згортки здійснюється під час прямого проходу, коли ми проходимо кожним фільтром по всьому вхідному об'єму. Кожен крок цього руху називається кроком згортки і може бути різним: наприклад, 2, 3 або навіть 4, особливо для зображень високої роздільної здатності. На кожному кроці обчислюється скалярний добуток між вагами ядра і відповідною частиною вхідного об’єму.

У результаті ковзання фільтра ми отримуємо двовимірний вихід для кожного фільтра. Об’єднуючи ці двовимірні результати, утворюємо вихідний об'єм із глибиною, яка відповідає кількості фільтрів. Кожен фільтр навчається окремо, оптимізуючи мережу для точного виділення ознак. Шари для побудови ConvNets.

ConvNets складаються з послідовності шарів, де кожен шар перетворює вхідний об'єм у новий об'єм за допомогою диференційованої функції. Розглянемо основні типи шарів, використовуючи приклад зображення розміром 32x32x3.

1. Вхідний шар (Input Layer)

Вхідний шар подає дані у модель. У CNN це зазвичай зображення або набір зображень. Цей шар зберігає необроблені дані зображення з шириною 32, висотою 32 та глибиною 3 (RGB-канали).

2. Згортковий шар (Convolutional Layer)

Згортковий шар призначений для виділення ознак зображення, застосовуючи набір навчальних фільтрів або ядер.

- Фільтри мають невеликий розмір, 2x2, 3x3 або 5x5, і проходять по зображенню, обчислюючи скалярний добуток між вагою ядра і відповідною ділянкою зображення.
- Вихід цього шару називається картою ознак - feature map.
- Якщо використати 12 фільтрів, вихідний об'єм матиме розмір 32x32x12.

3. Шар активації - Activation Layer

Шар активації додає нелінійність у мережу, що дозволяє моделі навчатися складнішим залежностям (рисунок 2.7).

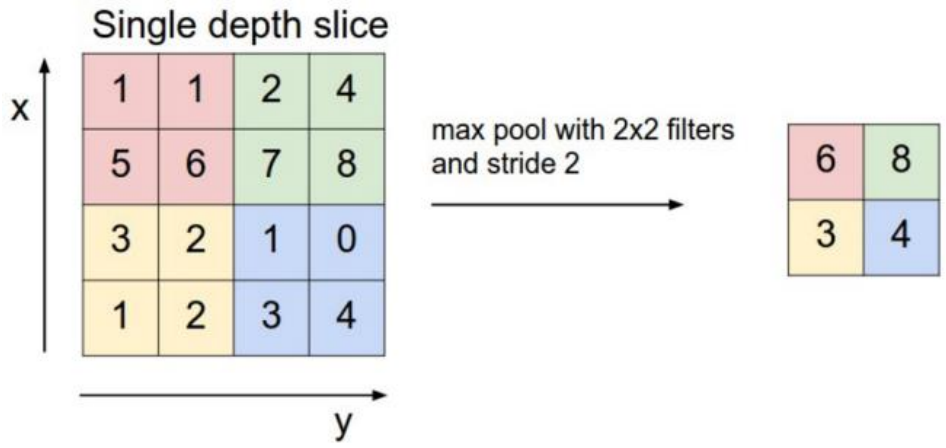



Рис. 2.7. Шар об’єднання

- Цей шар застосовує функцію активації до кожного елемента з виходу згорткового шару.
- Поширені функції активації: ReLU (max(0, x)), Tanh, Leaky ReLU.
- Розмір об'єму залишається таким самим — 32x32x12.

4. Шар об’єднання (Pooling Layer)

Шар злиття періодично додається в мережу і виконує зменшення розмірності об'єму. Це пришвидшує обчислення, знижує вимоги до пам'яті та запобігає перенавчанню.

- Найчастіше використовуються найбільше існуюче об'єднання та середнє існуюче з'єднання .
- При max pooling з фільтром 2x2 і кроком 2 вихідний об'єм зменшується до розмірів 16x16x12.

Вирівнювання (Flattening): Після проходження через згорткові та об'єднувальні шари отримані карти ознак перетворюються в одновимірний вектор. Це необхідно для того, щоб підготувати дані для подальшої обробки у повністю зв'язаних шарах, які відповідають за кінцеву класифікацію або регресію.

Повністю зв'язані шари (Fully Connected Layers): Ці шари отримують вхідні дані з попереднього вирівняного шару та виконують фінальну регресії або операцію класифікації на базі існуючих характеристик (рисунок 2.8).

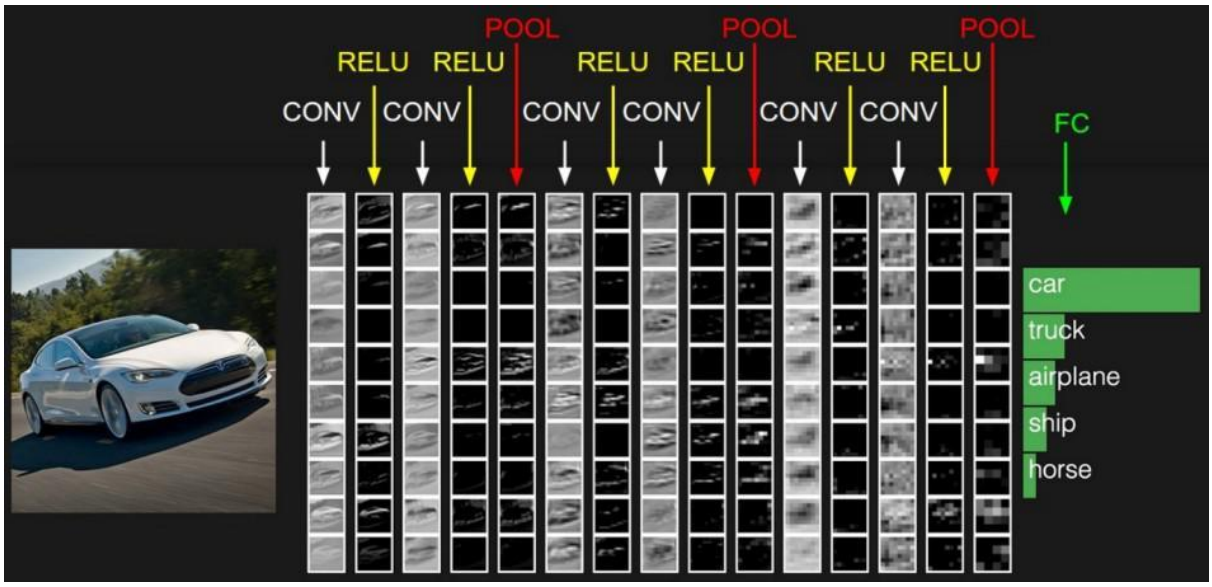



Рис. 2.8. Процес обробки зображення в згортковій нейронній мережі

Вихідний шар**:** Вихід із повністю зв'язаних шарів подається на логістичну функцію для завдань класифікації. Зазвичай використовуються функції, такі як сигмоїда або softmax, які перетворюють вихідні значення кожного класу на ймовірнісні оцінки, відображаючи ймовірність належності до кожного класу.

## 2.2. Методи попередньої обробки вхідних зображень для підвищення точності ідентифікації

Важливим етапом для підвищення точності ідентифікації є підготовка даних для згорткових нейронних мереж. Попередня обробка вхідних мереж та інших алгоритмів машинного навчання. Ефективна попередня обробка дозволяє видалити шум, збільшити якість вхідного зображення людини та зробити його більш придатним для точного виділення ознак. Основні методи попередньої обробки:

- Нормалізація. Нормалізація переводить піксельні значення зображення у визначений діапазон, зазвичай [0, 1] або [-1, 1]. Це дозволяє уникнути переваги одних ознак над іншими через високі значення яскравості, що важливо для стабільності навчання (рисунок 2.9).

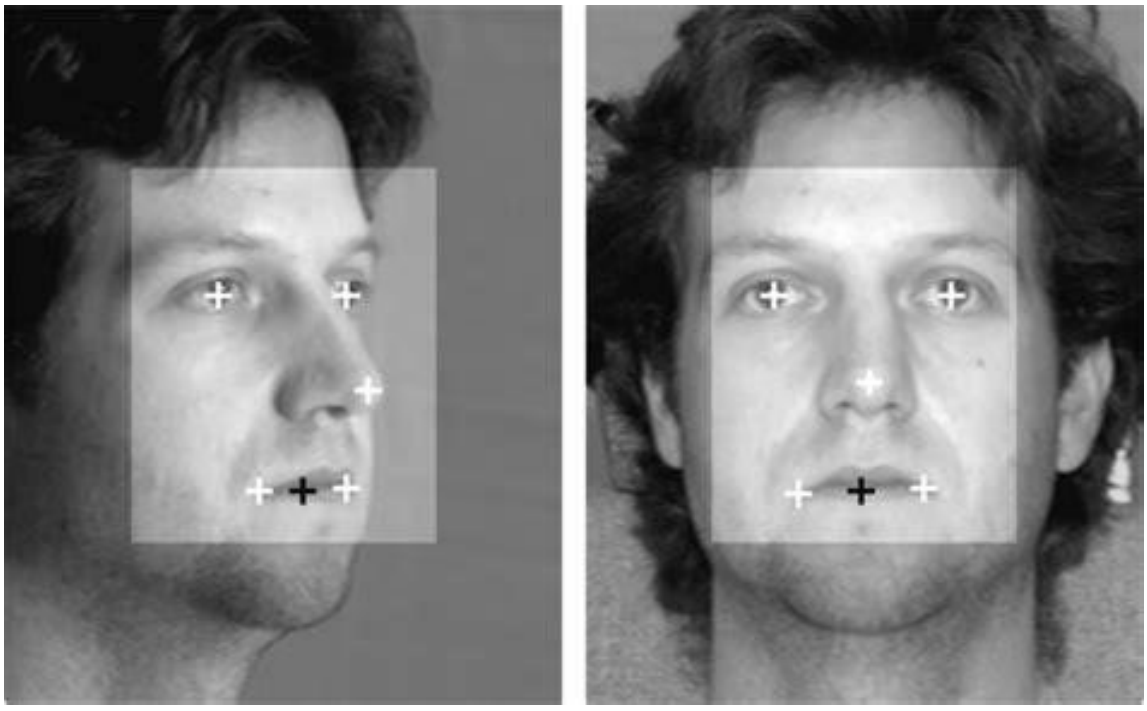


Рис. 2.9. Ілюстрація нормалізації зображення обличчя

- Масштабування зображень. Операція масштабування приводить

зображення до стандартного розміру, наприклад, 224x224 пікселі для мережі VGG. Це забезпечує уніфікацію вхідних даних і спрощує обчислення, знижуючи навантаження на модель.

- Зміна кольорового простору**.** Іноді корисно змінити кольоровий простір з RGB на сірий, HSV, LAB або YCrCb. Це може полегшити виявлення деяких ознак, наприклад, текстур чи градацій, та покращити продуктивність моделі у завданнях, де кольорова інформація не є критичною.
- Аугментація даних. Аугментація збільшує обсяг даних, використовуючи трансформації, такі як обертання, масштабування, зсув, дзеркальне відображення та зміна яскравості. Це дозволяє моделі бути стійкою до змін умов і запобігає перенавчанню.

Крім стандартних методів, існують додаткові способи попереднього редагування вхідних зображень, що помітно покращити їх якість і підвищити точність ідентифікації, до яких належить:

- Згладжування та розмивання. Розмиття допомагає виділити важливі об’єкти, зменшуючи увагу до незначних деталей. Це особливо корисно для зображень з надмірною деталізацією, яка може впливати на точність ідентифікації (рисунок 2.10).

Рис. 2.10. Розмиття зовнішніх рис

- Збільшення контрастності. Збільшення контрастності підсилює

різницю між темними і світлими областями зображення, що може покращити виявлення деталей та полегшити розпізнавання.

- Вирівнювання гістограми. Вирівнювання гістограми підвищує контрастність, перерозподіляючи значення яскравості, щоб рівномірніше заповнити весь діапазон. Це особливо корисно для зображень з поганою освітленістю (рисунок 2.11).

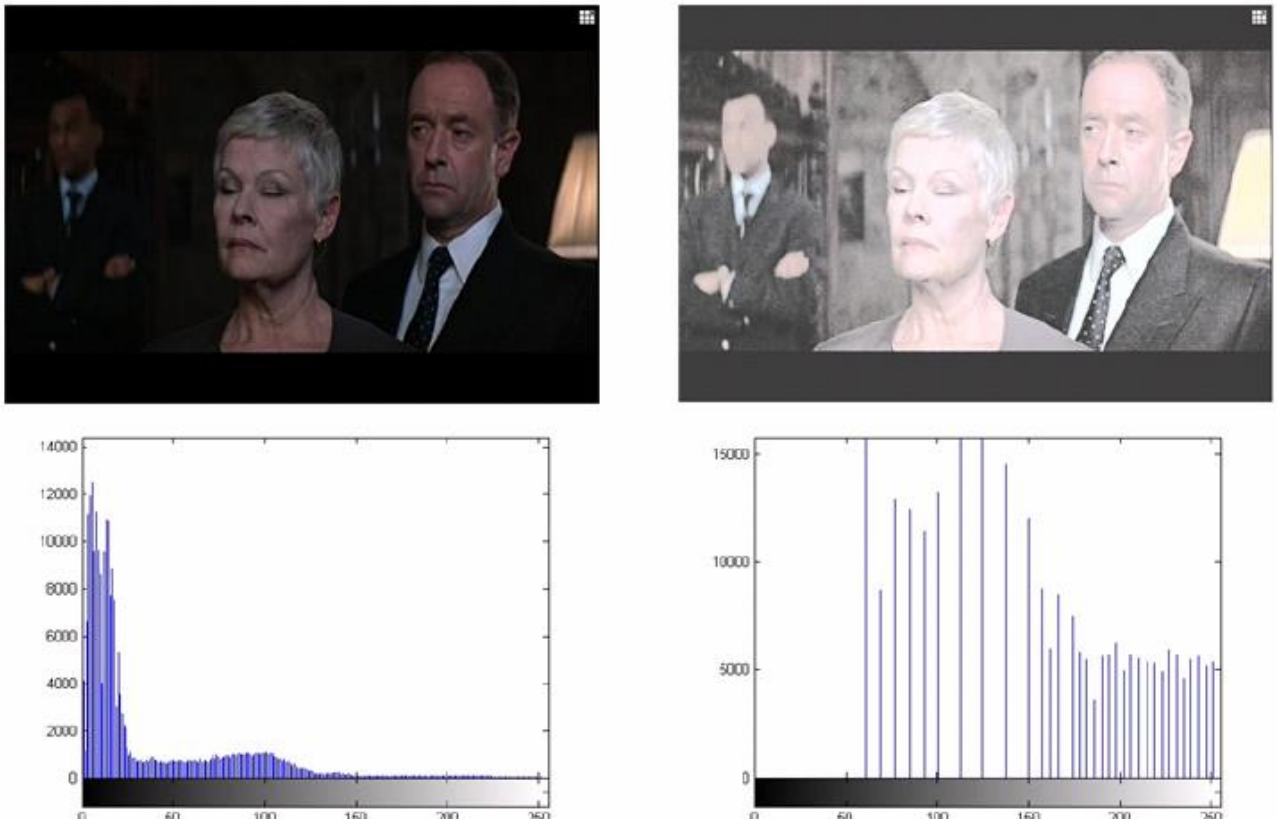



Рис. 2.11. Ефект вирівнювання гістограми

## 2.4 Вибір підходів та технологій для ідентифікації користувачів

Реалізація системи ідентифікації користувачів базується на комбінованому підході, що поєднує метод ключових точок (алгоритм SURF) та згорткову нейронну мережу (CNN). Ця комбінація об'єднує швидкість і точність алгоритмів комп'ютерного зору з можливостями нейронних мереж, що значно підвищує загальну ефективність розпізнавання. Основні етапи реалізації:

- Ідентифікація обличчя використовуючи CNN: На першому етапі CNN виявляє обличчя та може виконувати їхню класифікацію.
- Виявлення ключових точок обличчя за допомогою алгоритму SURF: Після ідентифікації обличчя людини алгоритм SURF виділяє ключові точки та обчислює їх дескриптори, що містять локальні особливості зображення. Цей спосіб обмежує обробку CNN тільки необхідними областями.
- Збереження і обробка областей ключових точок: Виділені ключові точки й області навколо них зберігаються для подальшої обробки, що дозволяє точно локалізувати важливі частини зображення.
- Аналіз через CNN: Отримана інформація від SURF передається до CNN, яка здатна розпізнавати обличчя чи інші об'єкти у зазначених областях.
- Інтеграція отриманих результатів: На фінальному етапі відбувається об'єднання даних, отриманих від згорткової нейронної мережі (CNN), та ключових точок, визначених алгоритмом SURF. Дескриптори SURF визначають позицію й орієнтацію об'єкта, тоді як CNN здійснює безпосереднє розпізнавання

Поєднання SURF та CNN забезпечує гнучкість до налаштування, швидкість та високу точність, що робить систему ідентифікації надійною і ефективною.

Для реалізації технології ідентифікації було обрано мову програмування Python та наступні бібліотеки:

- OpenCV: Це основна бібліотека для комп'ютерного зору та машинного навчання. OpenCV надає понад 2500 оптимізованих алгоритмів, що підтримують як класичні, так і сучасні методи обробки зображень. Її алгоритми впроваджуються для ідентифікації обличчя, ідентифікації об'єктів, відстеження рухомих об'єктів, створення 3D-моделей тощо, забезпечуючи точність і високу продуктивність ідентифікації.
- TensorFlow: Ця бібліотека від Google спеціалізується на глибокому навчанні та обробці великих масивів даних. TensorFlow дозволяє ефективно розподіляти обчислення на графічні процесори за допомогою графів потоку даних, що значно підвищує ефективність обробки.

- Keras: Інтерфейс для Python, який працює поверх TensorFlow і забезпечує простоту створення нейронних мереж. Keras містить структурні блоки для глибокого навчання, такі як шари, функції активації, оптимізатори, що спрощує реалізацію алгоритмів машинного навчання.

**Висновки до другого розділу**

У другому розділі магістерської роботи було проведено аналіз та обґрунтування підходів для ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту. У рамках дослідження зосереджено увагу на поєднанні методу ключових точок (алгоритму SURF) із згортковими нейронними мережами (CNN), що дозволяє ефективно вирішувати задачі ідентифікації користувачів у контексті сучасних вимог до безпеки інформаційних систем.

Було розглянуто можливості алгоритму SURF, який дозволяє швидко та точно виділяти стійкі ознаки об'єктів, що є важливим для ідентифікації користувачів у системах доступу.. Додатково CNN демонструє високий рівень точності в розпізнаванні ключових ознак об’єктів, що дозволяє значно підвищити якість ідентифікації користувачів, автоматично виділяючи та класифікуючи обличчя.

Важливою частиною ідентифікації є етап попередньої обробки вхідних зображень, оскільки якісне видалення шуму, покращення контрастності та нормалізація дозволяють підвищити ефективність розпізнавання. Методи, як: нормалізація, масштабування та вирівнювання гістограми, створюють оптимальні умови для навчання моделі та підвищують стабільність її роботи. Застосування згладжування, збільшення контрастності та інших технік обробки зображень допомагає зменшити вплив зовнішніх факторів на результативність системи.

В роботі було обґрунтовано вибір інструментів для реалізації інформаційної системи, таких як бібліотеки OpenCV, TensorFlow та Keras. Вони

надають широкий функціональний інструментарій для обробки зображень та реалізації алгоритмів глибокого навчання.

Таким чином, у результаті досліджень і реалізації розробленої технології ідентифікації користувачів на основі SURF та CNN з використанням сучасних бібліотек штучного інтелекту, вдалося створити технологію, яка забезпечує високу точність, стабільність і надійність розпізнавання, що відповідає вимогам безпеки для інформаційних систем організацій.

# 3 ТЕХНОЛОГІЯ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧІВ ІНФОРМАЦІЙНОЇ СИСТЕМИ ОРГАНІЗАЦІЇ

## 3.1 Розробка програмного інструментарію для автоматизованої ідентифікації користувачів

Для автоматизованої ідентифікації облич у інформаційних системах організацій було обрано згорткову нейронну мережу. Для виконання цього завдання застосовується згорткова нейронна мережа, яка побудована на основі багатозадачної каскадної архітектури. Це дозволило не тільки підвищити точність і швидкість ідентифікації, але й допомагає запобігати несанкціонованому доступу до критичних ресурсів інформаційної системи організацій.

Алгоритм MTCNN — це метод виявлення та вирівнювання облич на основі глибокого навчання, який використовує каскадну серію згорткових нейронних мереж (CNN) для виявлення та локалізації облич на цифрових зображеннях або відео. Алгоритм здатний виявляти обличчя різних масштабів та орієнтацій і є стійким до змін умов освітлення, виразів обличчя та перешкод.

Алгоритм MTCNN складається з трьох основних етапів: мережа пропозицій (P-Net), мережа уточнення (R-Net) та вихідна мережа (O-Net). Кожен з етапів допомагає в ідентифікації та в уточненні позиції обличчя, що є критично важливим для захисту інформаційних ресурсів від фальсифікацій і зловмисних атак. Розглянемо роботу кожного з цих етапів:

1. Мережа пропозицій (P-Net):

Перший етап алгоритму MTCNN - це P-Net, яка виконує початкове виявлення облич на зображенні. Мережа обробляє вхідне зображення, застосовуючи серію згорткових фільтрів, щоб створити набір карт ознак, які представляють різні елементи зображення. Ці карти ознак обробляються набором повністю зв’язаних шарів для прогнозування ймовірності наявності

обличчя в кожній області зображення. P-Net також обчислює координати обмежувальної рамки навколо виявленого обличчя. Це дозволяє виділити можливі регіони, які можуть містити обличчя. Архітектура P-Net (рисунок 3.1).

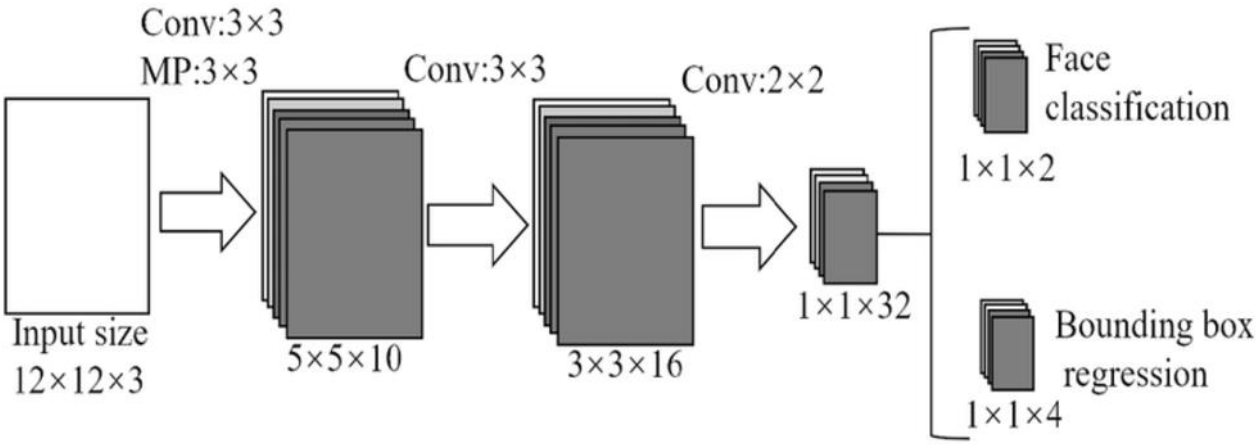



Рис. 3.1. Архітектура P-Net

2. Мережа уточнення (R-Net):

Другий етап алгоритму MTCNN - це R-Net, яка виконує подальшу обробку кандидатських обмежувальних рамок, отриманих на попередньому етапі. R-Net бере ці рамки та вирізає відповідні області з вхідного зображення. Потім ці вирізані області змінюють розмір до фіксованого значення і передають через серію згорткових та повністю зв’язаних шарів для класифікації кожної обмежувальної рамки як обличчя або не обличчя. R-Net також уточнює координати обмежувальної рамки, щоб покращити розташування виявленого обличчя та виявляти спроби підробки обличчя.

3. Вихідна мережа (O-Net):

Завершальний етап алгоритму MTCNN - це O-Net, , яка виконує точне визначення обличчя та виділення ключових точо. O-Net отримує обмежувальні рамки, уточнені на етапі R-Net, і вирізає відповідні області з вхідного зображення.. Ці вирізані області змінюють розмір до фіксованого значення і передають через серію згорткових та повністю зв’язаних шарів для класифікації

кожної обмежувальної рамки як обличчя або не обличчя. O-Net додатково уточнює координати обмежувальних рамок, забезпечуючи високу точність локалізації обличчя. Мережа визначає координати п’яти основних точок обличчя: двох очей, носа та куточків рота. Це дозволило адаптувати систему до змін у зовнішності користувачів, таких як носіння окулярів або головних уборів, що робить створену технологію більш стійкою до атак (рисунок 3.2).

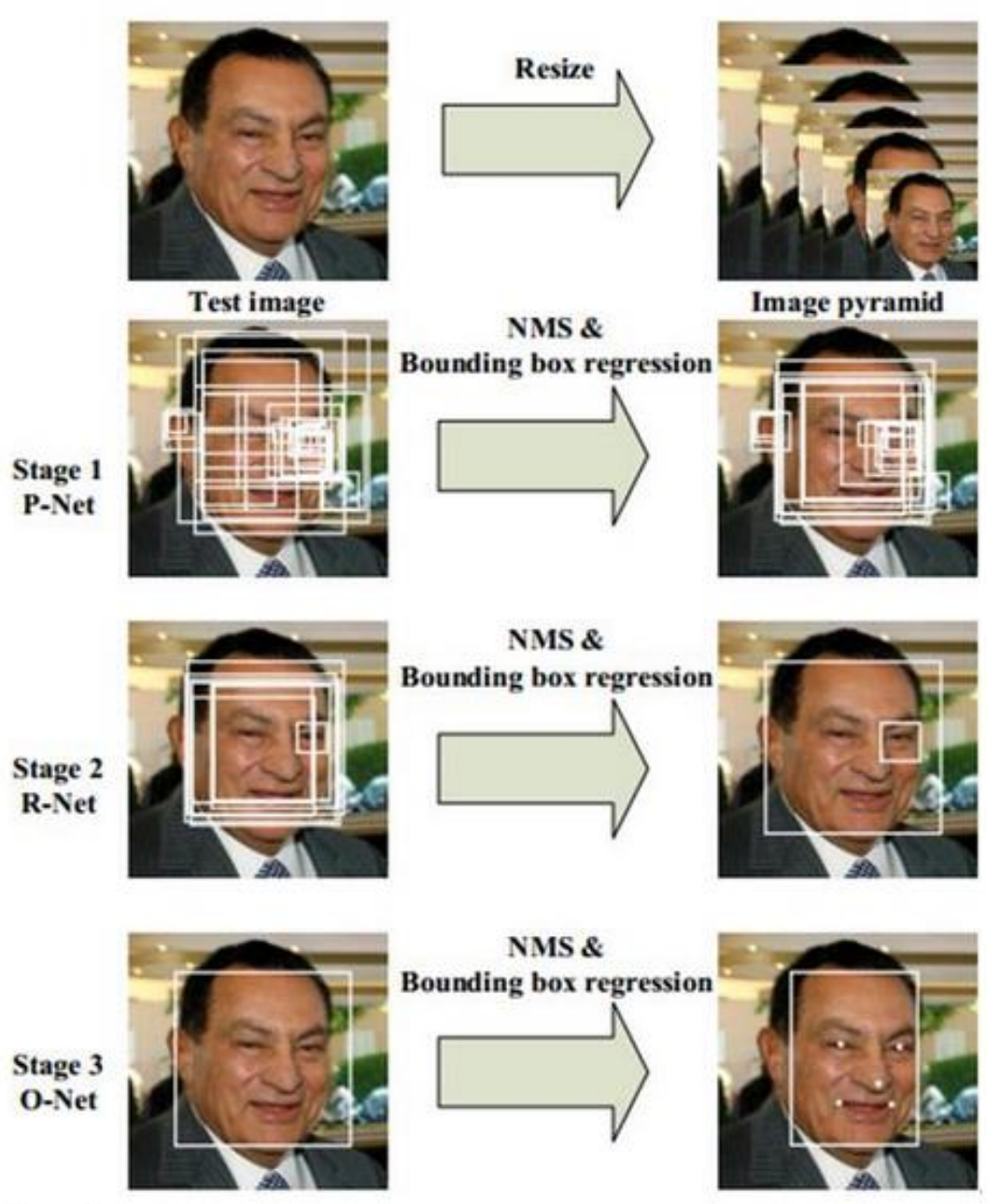



Рис. 3.2. Візуалізація роботи MTCNN

Алгоритм MTCNN був реалізований у створеній роботі за допомогою мови програмування Python із використанням бібліотеки Keras, яка забезпечує простий доступ до реалізації згорткових нейронних мереж. Реалізація включала інтеграцію всіх трьох компонентів MTCNN (P-Net, R-Net, O-Net) для ефективного виявлення та ідентифікації облич на зображеннях різної складності (рисунок 3.3).

```
def draw_image_with_boxes(filename, result_list):
    data = pyplot.imread(filename)
    pyplot.imshow(data)
    ax = pyplot.gca()
    for result in result_list:
        x, y, width, height = result['box']
        rect = Rectangle( xy: (x, y), width, height, fill=False, color='yellow')
        ax.add_patch(rect)
        pyplot.show()


filename = 'Vlad.jpg'
pixels = pyplot.imread(filename)
detector = MTCNN()
faces = detector.detect_faces(pixels)
draw_image_with_boxes(filename, faces)


resized_image=cv2.resize(img,  dsize: (601,800))
cv2.startWindowThread()
cv2.namedWindow("Test_image")
cv2.imshow( winname: "Test_image", resized_image)
cv2.waitKey(0)
```

Рисунок 3.3 Процес виявлення обличчя на зображенні за допомогою

Процес розробки включав такі етапи:

1. Попередня обробка вхідних зображень**:**

- Масштабування зображень до уніфікованого розміру. Зображення масштабується до розміру 601x800 пікселів за допомогою функції cv2.resize().
- Застосування нормалізації для приведення піксельних значень до діапазону [0, 1], для забезпечення стабільної роботи моделі.
- Усунення шумів за допомогою фільтрів.

2. Інтеграція MTCNN: Алгоритм був налаштований на отримання результатів високої точності навіть у складних умовах. Було забезпечено коректну взаємодію між P-Net, R-Net та O-Net для оптимальної роботи на тестових даних.

3. Розробка графічного інтерфейсу користувача:

- Для зручності тестування системи був створений інтерфейс, що дозволяє завантажувати зображення, запускати процес ідентифікації та візуалізувати отриманні результати. Інтерфейс відображає обмежувальні рамки та ключові точки, визначені алгоритмом та дає змогу збільшувати зображення та зберігати його.
- Функція draw_image_with_boxes() відображає зображення з нанесеними обмежувальними рамками для ідентифікованих облич.
- Функція matplotlib.pyplot()

4. Тестування та оптимізація:

- Було перевірено ефективність алгоритму на різних наборах даних, включаючи зображення зі складними умовами освітлення, обертаннями облич та частковими перекриттями.
- Завдяки інтеграції P-Net, R-Net та O-Net досягнуто оптимального балансу між швидкістю роботи та точністю.

Основні результати:

- Стійкість до зовнішніх факторів: Алгоритм продемонстрував високу точність при зміні умов освітлення, поворотах облич та часткових перекриттях.
- Гнучкість: Завдяки каскадній архітектурі MTCNN забезпечено адаптацію до облич різного розміру та розташування на зображенні.
- Ефективність: Система працює в реальному часі, що дозволяє використовувати її в інтерактивних додатках для ідентифікації користувачів.

Результати роботи цього етапу було відображено на (рисунок 3.4), який демонструє накладені обмежувальні рамки жовтого кольору на зображенні. Це наочно ілюструє ефективність алгоритму MTCNN.

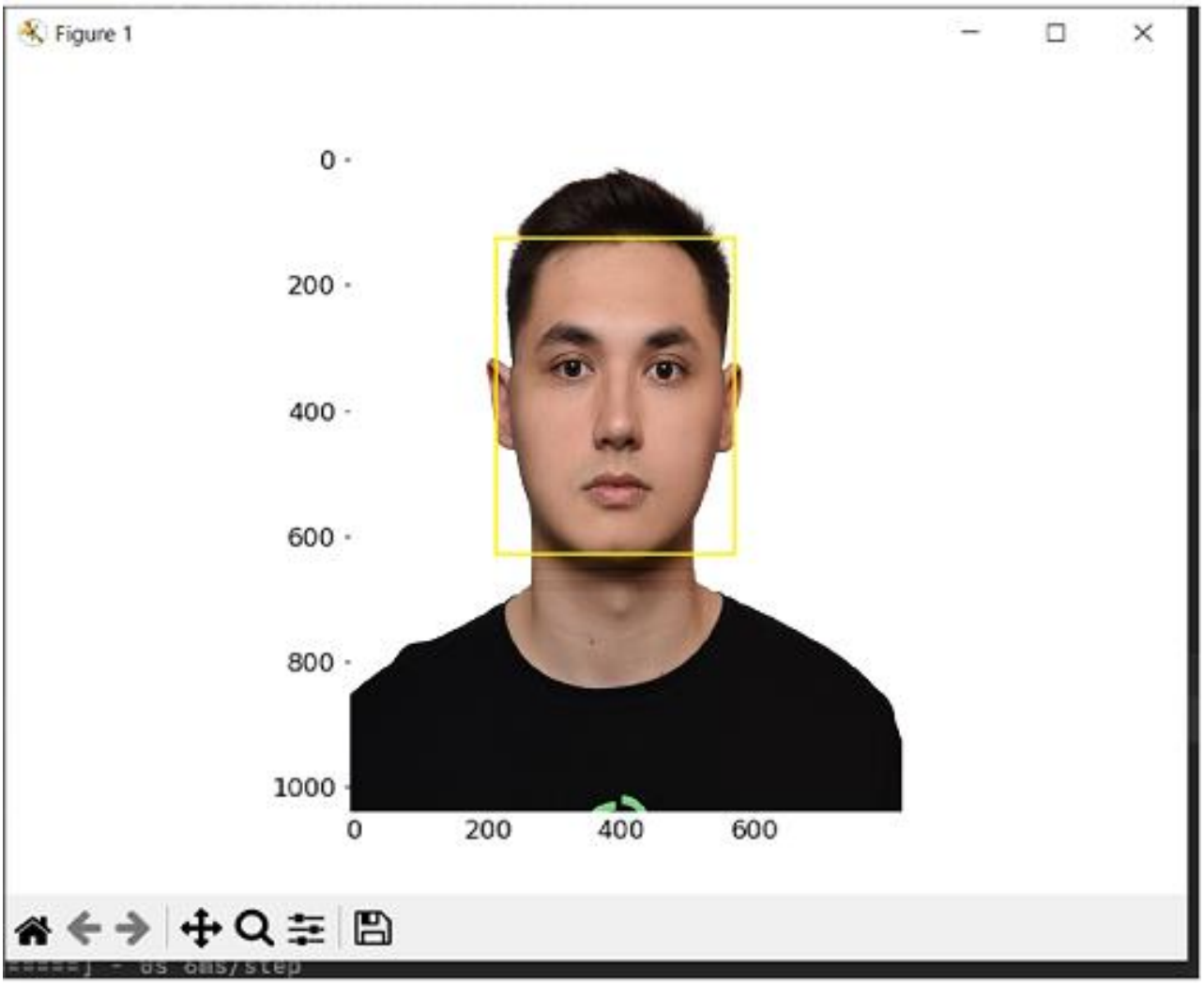



Рисунок 3.4 Виявлення обличя за допомогою алгоритму MTCNN

Після виявлення обличчя за допомогою алгоритму MTCNN, наступним кроком було обрано виявлення ключових точок на обличчі людини. Для цієї задачі використовувався алгоритм SURF. Цей метод дозволив виявити характерні точки на зображеннях і створити дескриптор, котрий зберігає характеристики зображення, та є важливим етапом у процесі ідентифікації користувачів. Це дозволило покращити точність ідентифікації облич і забезпечити стійкість до змін умов, таких як ракурси або перекриття об'єктів на зображенні.

Етапи реалізації алгоритму SURF:

1. Зображення завантажується у відтінках сірого, що спрощує обчислення.

2. Налаштовується параметр hessianThreshold, який визначає мінімальний поріг для виявлення ключових точок.

3. Виявлені ключові точки позначаються на зображенні для подальшої перевірки та використанні в майбутньому в ідентифікаційних завданнях.

4. Результат візуалізується за допомогою бібліотеки Matplotlib, що дозволяє чітко бачити ключові точки на зображенні. Функція cv.drawKeypoints(), малює кола та напрямки орієнтації ключових точок.

Використання функції SURF() демонструє, як алгоритм ідентифікує ключові точки, які можуть бути інтегровані в загальну систему ідентифікації користувачів (рисунок 3.5).

```
1 usage
def SURF():
    root = os.getcwd()
    imgPath = os.path.join(root,'images//Vlad1.jpg')
    imgGray = cv.imread(imgPath,cv.IMREAD_GRAYSCALE)
    hessianThreshold = 1000
    surf = cv.xfeatures2d.SURF_create(hessianThreshold)
    keypoints = surf.detect(imgGray,None)
    imgGray = cv.drawKeypoints(imgGray,keypoints,imgGray,flags=cv.DRAW_MATCHES_FLAGS_DRAW_RICH_KEYPOINTS)

    plt.figure()
    plt.imshow(imgGray)
    plt.show()


if __name__ == '__main__':
    SURF()
```

Рисунок 3.5 Функція SURF()

Завдяки налаштуванню параметрів алгоритм забезпечує адаптацію до зображень різної складності, підвищуючи точність розпізнавання та дозволяє створювати детектори аномалій, забезпечуючи, додатковий рівень захисту від модифікацій зображень (рисунок 3.6).

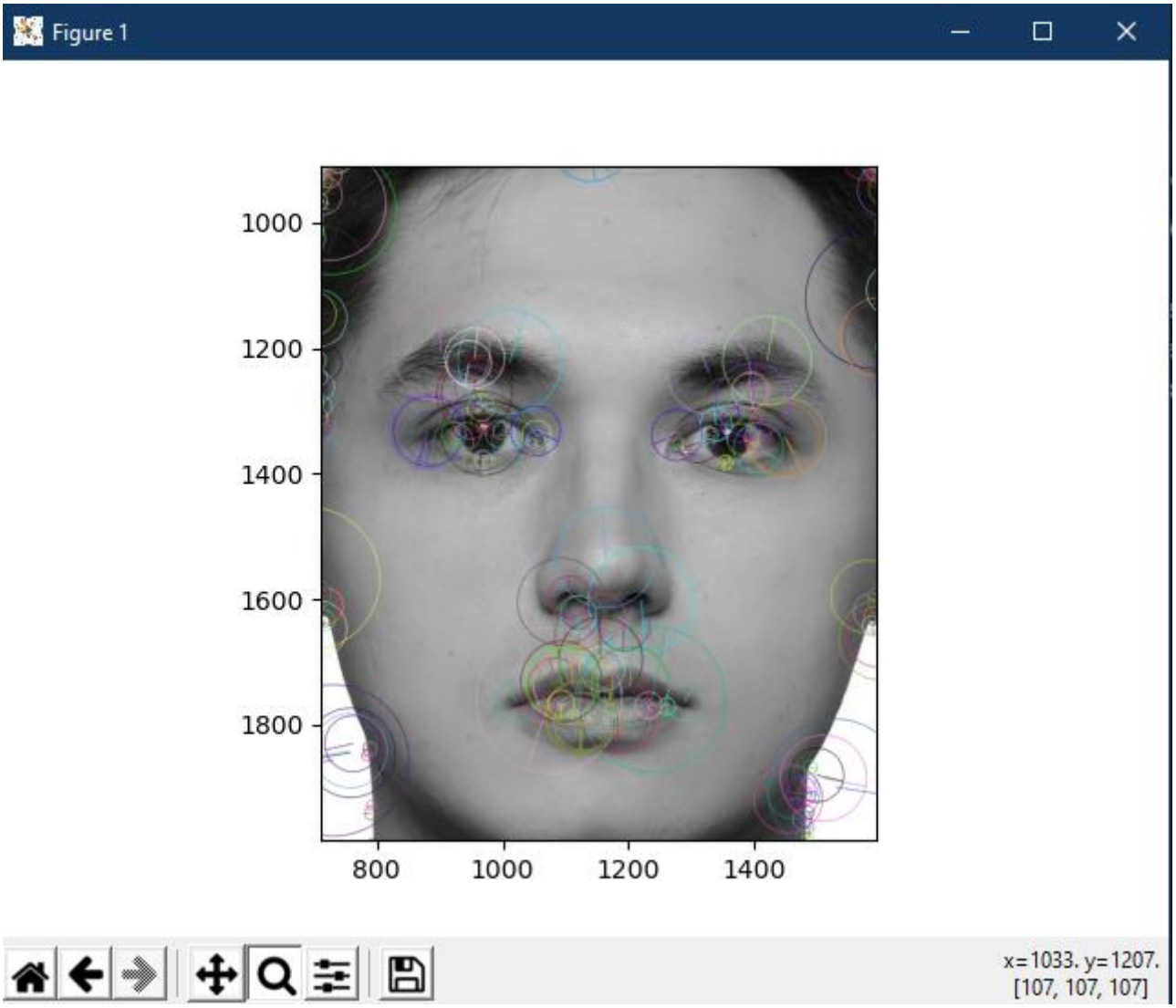



Рисунок 3.6 Застосування алгоритму SURF для пошуку ключових точок

Після знаходження ключових точок на вхідному зображенні користувача інформаційної системи за допомогою алгоритмом SURF, наступною дією є їх збереження для подальшої обробки та застосовується в рішеннях ідентифікації обличчя. Ці точки є важливими локальними особливостями, які допомагають ефективно ідентифікувати та класифікувати обличчя на основі їх унікальних характеристик.

Змінна keypoints містить дані про знайдені ключові точки. Згодом ці координати були перетворені у вектори, які слугують математичною основою для розпізнавання та порівняння об'єктів. Такий підхід забезпечив точність і швидкість при обробці зображень (рисунок 3.7).

```
surf = cv.xfeatures2d.SURF_create(hessianThreshold)
keypoints = surf.detect(imgGray,None)
imgGray = cv.drawKeypoints(imgGray,keypoints,imgGray,flags=cv.DRAW_MATCHES_FLAGS_DRAW_RICH_KEYPOINTS)

plt.figure()
plt.imshow(imgGray)
plt.show()
```

## 3.7 Перетворення ключових точок у вектори

Для забезпечення ефективного розпізнавання облич було створено спеціалізований класифікатор, який здатний ідентифікувати певну особу на основі аналізу зображень. Функція training_clasification() створює класифікатор для ідентифікації обличчя заданої особи (рисунок 3.8).

```
def training_clasification(name):

    path = os.path.join(os.getcwd()+"/data/"+name+"/")

    faces = []
    ids = []
    labels = []
    pictures = {}


    for root,dirs,files in os.walk(path):
            pictures = files


    for pic in pictures :

            imgpath = path+pic
            img = Image.open(imgpath).convert('L')
            imageNp = np.array(img, dtype: 'uint8')
            id = int(pic.split(name)[0])
            #names[name].append(id)
            faces.append(imageNp)
            ids.append(id)

    ids = np.array(ids)

    clf = cv2.face.LBPHFaceRecognizer_create()
    clf.train(faces, ids)
    clf.write("./data/classifiers/"+name+"_classifier.xml")
```

Рисунок 3.8 Процес створення класифікатора для розпізнавання обличчя

Цей класифікатор зберігається як файл name_classifier.xml, котрий застосовується для ідентифікації облич на нових зображеннях. У результаті, створений класифікатор може ефективно інтегруватися в систему кібербезпеки інформаційної системи організацій, дозволяючи ідентифікувати осіб в режимі реального часу, що стало важливим аспектом для захисту організаційних ресурсів і запобігання несанкціонованому доступу.

Зображення для тренування моделі отримуються з веб камери, в кількості 250 зображень. Процес зйомки зображення займає 2-3 секунди (рисунок 3.9).

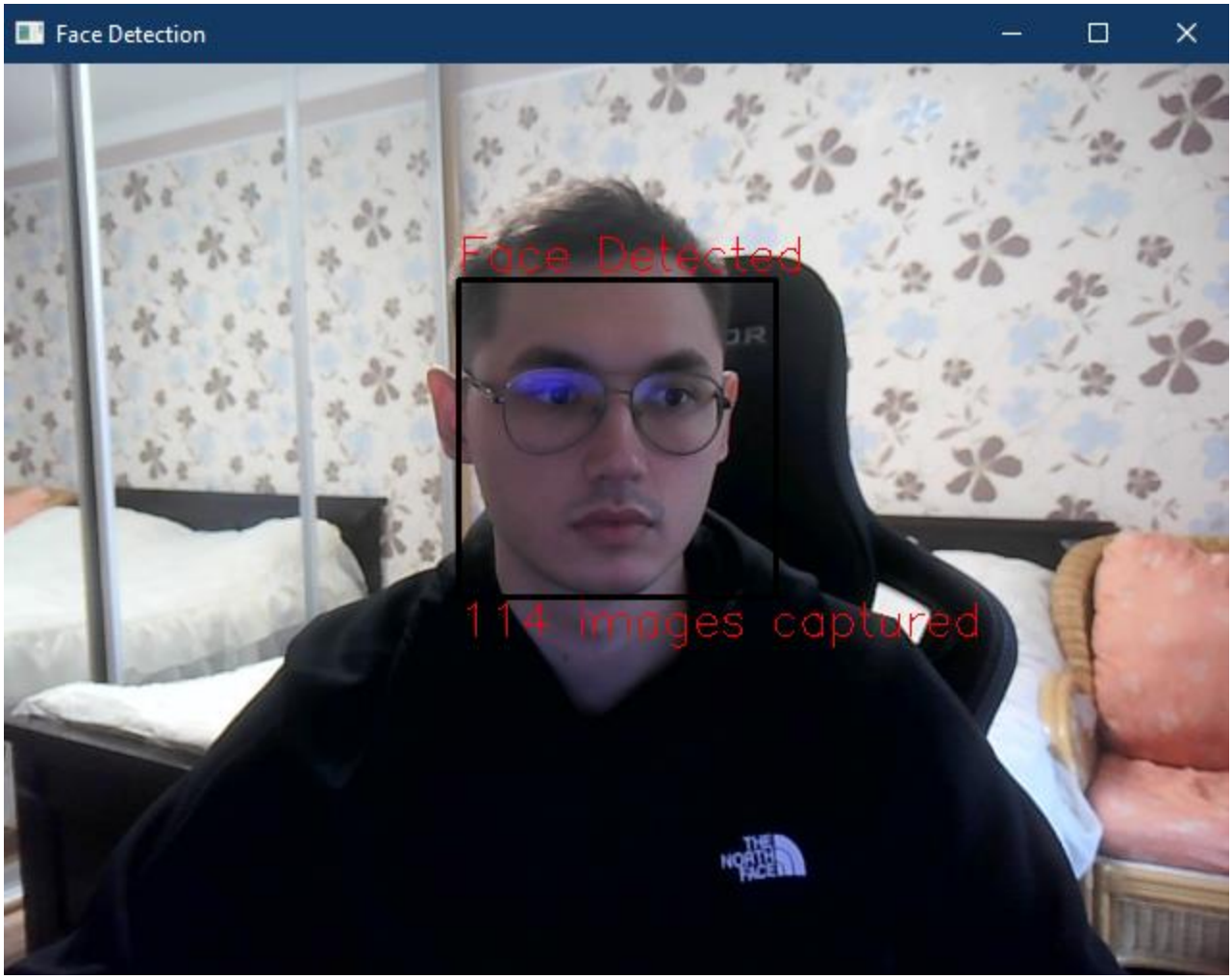



Рисунок 3.9 Формування навчального набору зображень для нейронної мережі

Усі зображення, отримані на попередніх етапах, організовуються та зберігаються в спеціально створеній директорії data. Ця папка виконує роль

сховища для навчального датасету, що використовується на етапі тренування моделі. Структура папки може включати підкаталоги, які відповідають різним категоріям чи особам, що полегшує подальшу обробку.

Збереження фотографій у впорядкованій формі є ключовим для забезпечення якості моделі. Це дозволяє уникнути плутанини та спрощує доступ до зображень під час їх попередньої обробки, вилучення ознак та навчання.

На рисунку 3.10 представлено приклад структури папки data, яка містить отримані фотографії для формування повноцінного навчального набору даних.

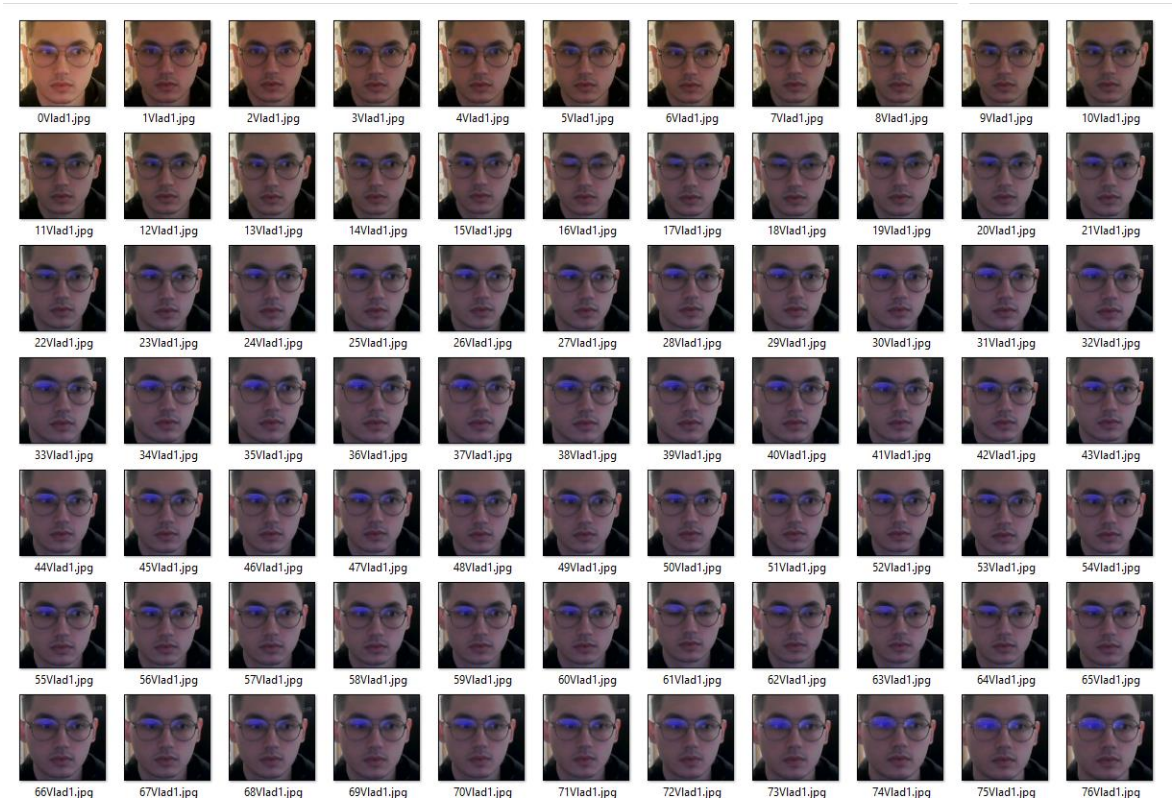



Рисунок 3.10 Збережені фотографії, для навчального датасету

Процес ідентифікації користувача інформаційної системи включає кілька послідовних етапів. Перший етап зображення обробляється через шари нейронної мережі, серед яких ключову роль відіграє згортковий шар.

Згортковий шар застосовує фільтри, які переміщуються по зображенню як у горизонтальному, так і у вертикальному напрямках, починаючи з верхньої

частини і закінчуючи нижньою. Кожна позиція фільтра обчислює значення методом скалярного добутку між фільтром і відповідною ділянкою зображення. Це дозволяє вилучити локальні ознаки зображення, які формують основу для подальшого аналізу.

Отримані значення згорткового шару передаються на шар об’єднання, який виконує:

- Зменшення розмірності зображення**.** Це дозволяє зменшити кількість обчислень та прискорити наступні етапи аналізу.
- Підвищення стійкості до зміщень**.** Зменшення дискретизації сприяє інваріантності результатів до невеликих змін положення об’єкта.

Процес обробки повторюється кілька разів: чергуються шари згортки та об’єднання для отримання найбільш релевантних ознак. У підсумку, після завершення цих етапів, об’єкт вирівнюється і передається до повністю з’єднаного рівня, де відбувається розпізнавання (рисунок 3.11).

```
face_model = Sequential()

face_model.add(KeyPoints(kp, 128))
face_model.add(Conv2D(32, kernel_size=(3, 3), activation='relu', input_shape=(48, 48, 1)))
face_model.add(Conv2D(64, kernel_size=(3, 3), activation='relu'))
face_model.add(MaxPooling2D(pool_size=(2, 2)))
face_model.add(Dropout(0.25))

face_model.add(KeyPoints(kp, 128))
face_model.add(Conv2D(128, kernel_size=(3, 3), activation='relu'))
face_model.add(MaxPooling2D(pool_size=(2, 2)))
face_model.add(Conv2D(128, kernel_size=(3, 3), activation='relu'))
face_model.add(MaxPooling2D(pool_size=(2, 2)))
face_model.add(Dropout(0.25))

face_model.add(Flatten())
face_model.add(Dense(1024, activation='relu'))
face_model.add(Dropout(0.5))
face_model.add(Dense(7, activation='softmax'))
```

Рисунок 3.11 Побудова архітектури нейронної мережі

У першому циклі виконуються наступні операції для побудови початкових шарів нейронної мережі:

- Передача ключових точок, які були визначені раніше алгоритмом SURF. Ці точки служать вхідними даними для нейронної мережі, що дозволяє фокусувати обробку лише на релевантних ділянках зображення.
- Додаються два згорткові шари з ядром розміром 3x3, які виконують вилучення локальних ознак із вхідного зображення. Завдяки невеликому розміру ядра забезпечується детальний аналіз текстур і країв зображення.
- Включається один шар об’єднання з матрицею 2x2, що виконує зменшення розмірності вхідного зображення, забезпечуючи швидкість обробки та стійкість до змін положення об'єкта.

Другий цикл створюється за аналогічною структурою, але із значними змінами в параметрах:

- Розмір фільтрів згорткових шарів збільшується до 128, що дозволяє мережі обробляти більш складні патерни та деталі зображення.
- Шар об’єднання залишається незмінним, продовжуючи виконувати функції зменшення дискретизації та підвищення стійкості до зміщень.

Фінальний цикл завершує архітектуру моделі:

- Додаються шари вирівнювання (flattening layer), які перетворюють багатовимірні матриці ознак у одновимірний вектор, що є необхідним для подальшої обробки.
- Додається повністю з’єднаний шар (fully connected layer), де виконується остаточна ідентифікація. Цей шар об’єднує вилучені ознаки для створення фінального результату розпізнавання.

Процес ідентифікації користувача базується на поєднанні ключових точок, отриманих алгоритмом SURF, і обробці через згорткову нейронну мережу. Такий підхід у тестових умовах забезпечив точність ідентифікації на рівні 93% (рисунок 3.12).

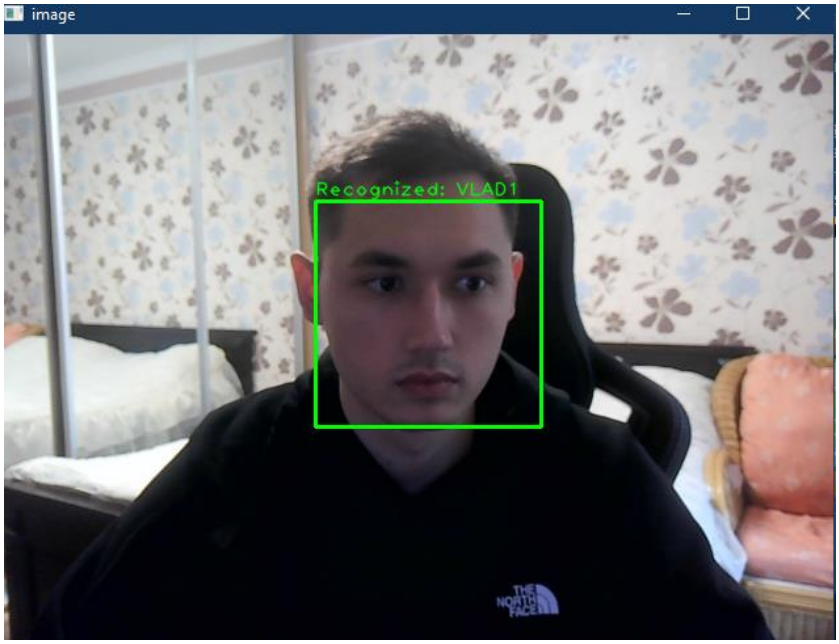



Рисунок 3.12 Результат ідентифікації

Перевага цієї технології полягає у її здатності адаптуватися до змін зовнішнього вигляду користувача, включаючи носіння окулярів, головних уборів чи інші невеликі зміни. Завдяки такій гнучкості, система стає більш універсальною та надійною в реальних умовах експлуатації (рисунок 3.13).

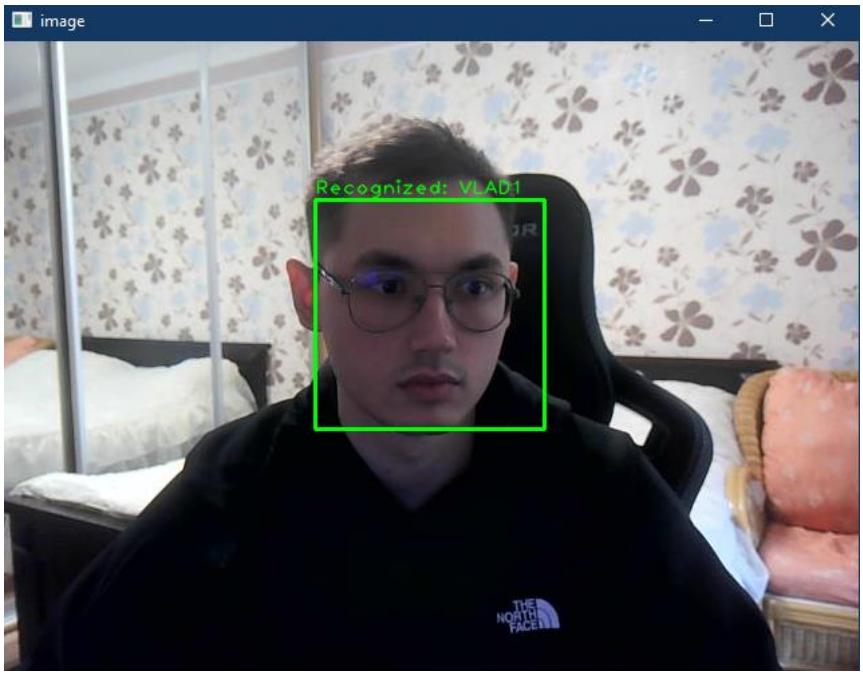



Рисунок 3.13 Результат ідентифікації користувача з окулярами

Система інтегрується із рішеннями для кібербезпеки інформаційної системи організації, що дозволяє автоматично відстежувати та реєструвати підозрілі дії. За несанкціоновані дії вважаються багаторазові спроби доступу незареєстрованих користувачів до інформаційної системи. Це дозволяє забезпечити збереження інформації та своєчасне реагування на потенційні загрози.

При ідентифікація користувача котрий не зареєстрований у системі його обличчя виділяється червоним квадратом, та написом “Unknown Face” (рисунок 3.14).

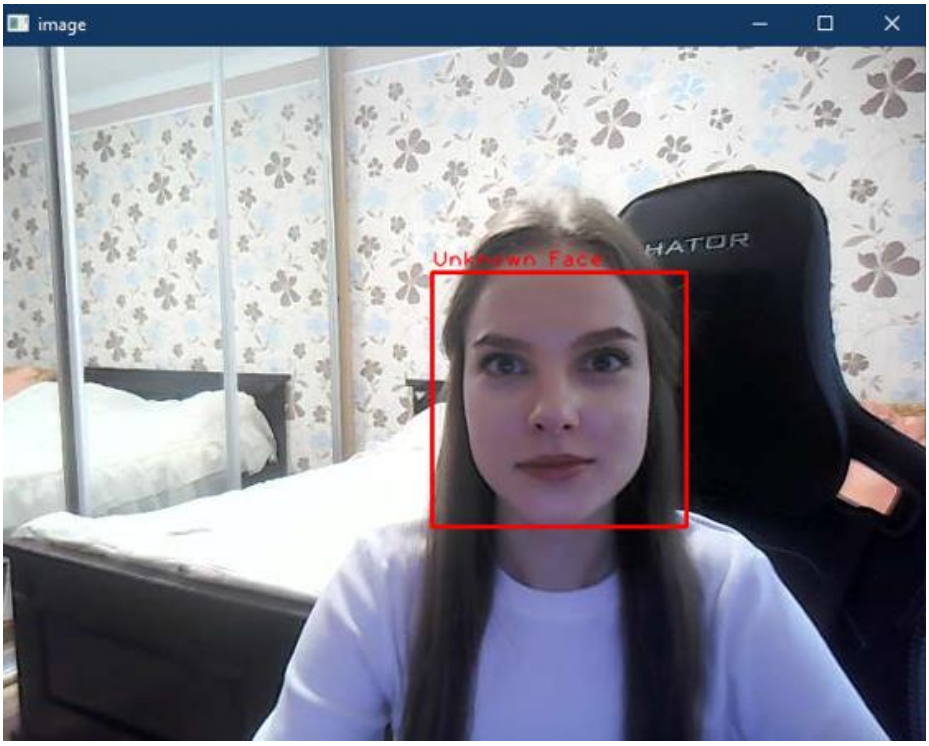



Рисунок 3.14 Результат ідентифікації користувача який незаєстрований у системі

Логи таких інцидентів зберігаються для подальшого аналізу з боку фахівців із кібербезпеки. У випадку виявлення незареєстрованого користувача система автоматично активує заходи захисту, такі як блокування доступу або вимога додаткової автентифікації. Це значно знижує ризики несанкціонованого доступу до інформаційної системи організації.

## 3.2 Редагування та перевірка вхідних зображень

Усі вхідні зображення для ідентифікації людини проходять через перевірку для збільшення точності ідентифікації користувачів, та для виявлення модифікованих зображень під час спроби несанкціонованого доступу (рисунок 3.15). Мета цієї діаграми – показати покроковий алгоритм ідентифікації обличчя. Діаграма описує процес від введення зображення до виведення результатів, враховуючи різні сценарії, такі як недостатня роздільна здатність зображення та необхідність додаткової обробки.

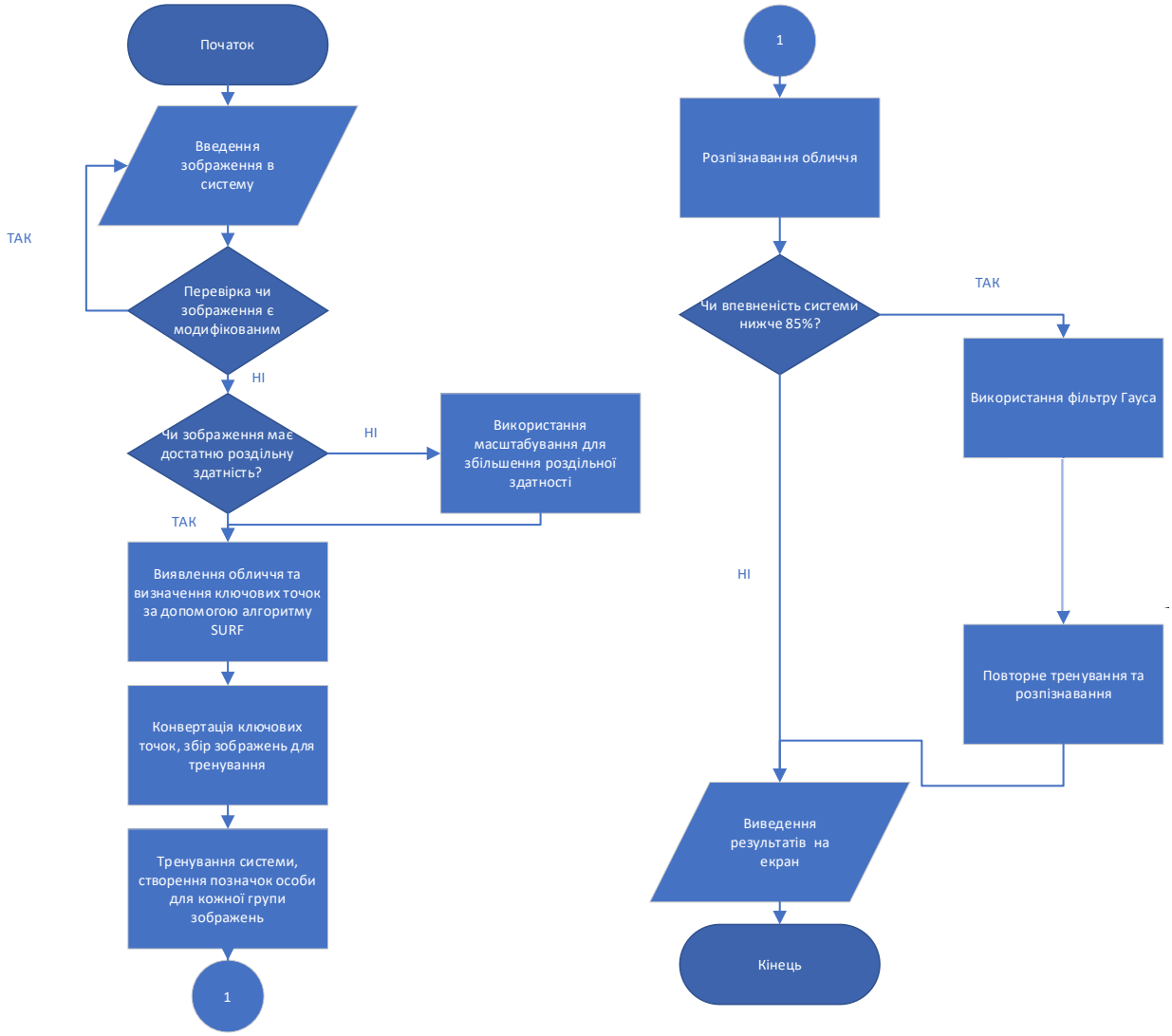



Рисунок 3.15 Діаграма роботи системи

Розроблена технологія ідентифікації інтегрована з механізмами оповіщення, що дозволяє адміністраторам негайно реагувати у разі виявлення підозрілих зображень.

Якщо вхідне зображення має малу роздільну здатність для ідентифікації людини, систем проводить масштабування зображення, котре:

- збільшує роздільну здатність зображення,
- зберігає важливі деталі обличчя для точного аналізу.

На рисунку наведений приклад порівняння якості деталей на обличчі людини до масштабування та після (рисунок 3.16).

Рисунок 3.16 Порівняння деталей ока людини

Використання технології масштабування дозволило підвищити відсоток ідентифікації та допомагає виявляти зловмисників, які використовують низькоякісні зображення для обходу системи. Завдяки захищеному зберіганню та шифруванню даних, усі вхідні зображення надійно захищені від несанкціонованого доступ. Раніше вхідне зображення поганої роздільної здатності не давало змоги ідентифікувати працівника, то зараз система виконує цю задачу (рисунок 3.17).

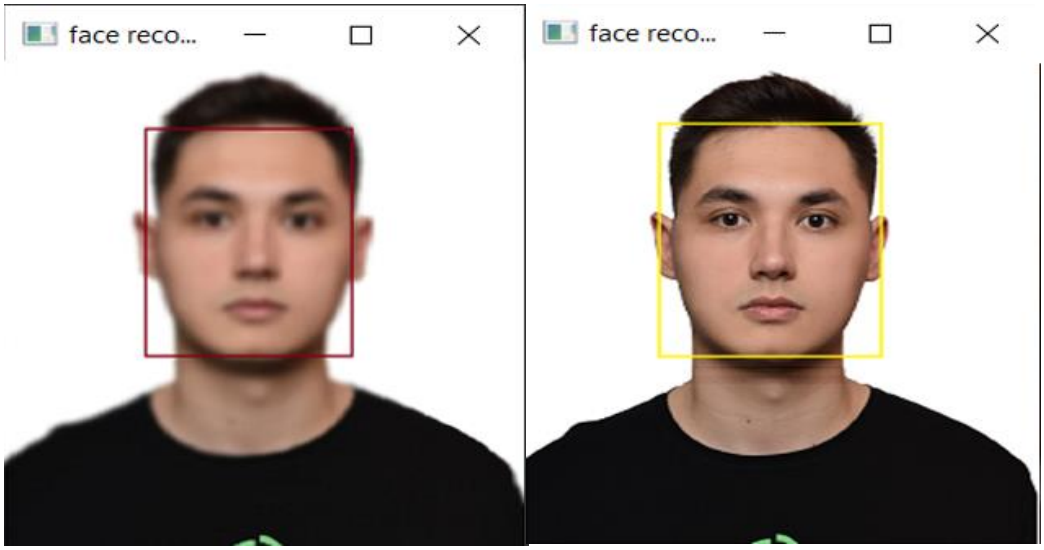



Рисунок 3.17 Порівняння результатів індентифікації обличя після масштабування

При впевненості системи під час ідентифікації нижче 85 відсотків використовується фільтр Гауса (рисунок 3.18). Цей фільтр дозволяє очищати зображення, зроблені у складних умовах, таких як слабке освітлення або цифровий шум. Фільтр допоміг зменшити вплив артефактів компресії, які можуть виникати під час передачі або зберігання зображень у форматі JPEG.

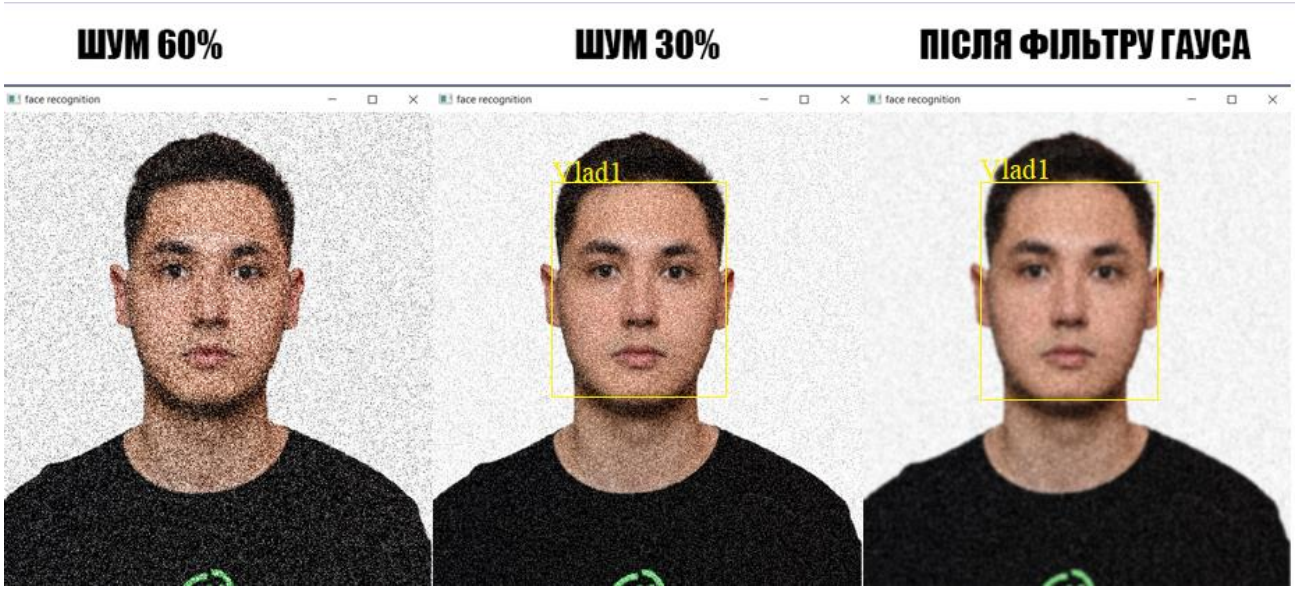



Рисунок 3.18 Порівняння результатів ідентифікації обличчя після використання фільтра Гауса

При шумі у 60% система не може ідентифікувати користувача системи, при шуму у 30% система індифікує людини з точністю 67%, після використання фільтра гауса точність ідентифікації збільшилась до 83% відсотків.

Останнім етапом є перевірка на модифікованість вхідного зображення. Для цього використовувалась перевірка на рівень помилок. Цей інструмент дозволяє порівнювати оригінальне зображення обличчя користувача з повторно стиснутою версією. Даний метод виділяє усі відредаговані частини зображення за допомогою різних підходів. Наприклад виділені частини, можуть бути темнішими або яскравішими, та відрізнятися від інших подібних областей, які не були оброблені.

До системи потрапляє модифіковане зображення зареєстрованого користувача(рисунок 3.19).

Рисунок 3.19 Вхідне модифіковане зображене з доданою маскою бороди

Процес перевірки системою вхідного модифікованого зображення на рівень помилок (рисунок 3.20).

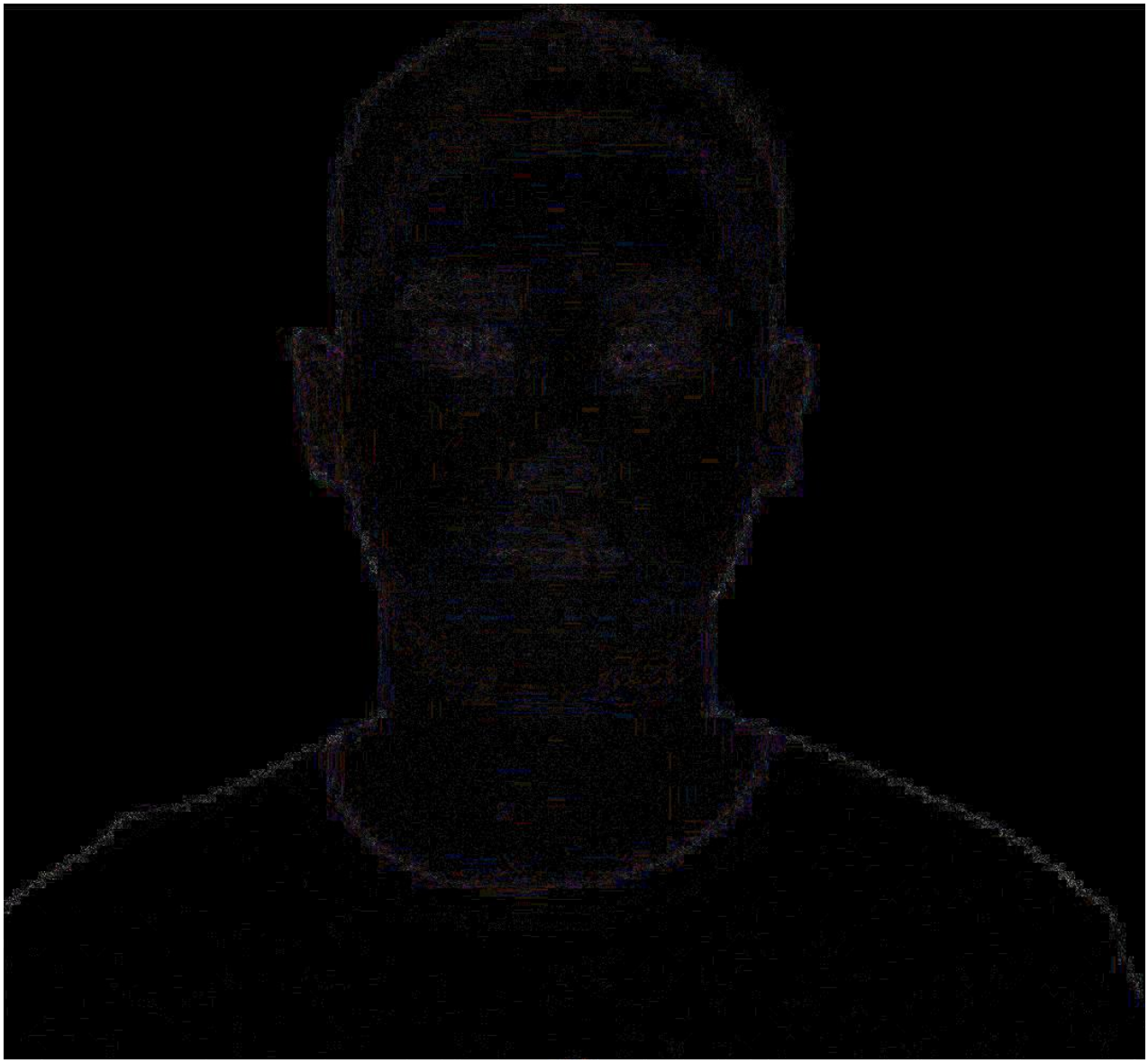


Рисунок 3.20 Перевірка модифікованого зображення на рівень помилок

Для запобігання потенційним витокам даних та несанкціонованому доступу, усі отримані результати перевірки зберігаються у захищеному форматі для подальшого аналізу.

Порівняння системою модифікованого зображення з оригінальним на рівень помилок (рисунок 3.21).

Рисунок 3.21 Перевірка оригінального зображення з модифікованим

У процесі порівняння також враховуються метадані зображення, такі як GPS-координати, час створення та деталі камери.

Аналіз модифікованості зображення дозволив виявляти спроби злому в інформаційній системі, наприклад, коли зловмисники намагаються використовувати підроблені зображення або використовувати 3д технології. Впровадження автоматичного моніторингу в інформаційну систему організацій, у режимі реального часу дозволив своєчасно запобігати несанкціонованому доступу до системи.

## 3.3 Рекомендації щодо застосування технології ідентифікації користувачів інформаційної системи організації

Для сучасних інформаційних систем організації забезпечення безпеки є одним із ключових завдань. Технології ідентифікації користувачів відіграє важливу роль, забезпечуючи надійну автентифікацію та контроль доступу. Важливим завданням є правильне впровадження та адаптація технології до умов конкретної організації. Нижче наведений приклад щодо застосування технології ідентифікації користувачів інформаційної системи організації.

- Технологія може замінити, такі методи: як ключ-картка або PIN-коди. Дозволяючи авторизованим особам входити, просто скануючи їх обличчя.
- Інтеграція з системами спостереження та моніторингу. На пунктах пропуску в організації, включаючи пропускні системи з високою інтенсивністю руху та у місцях із суворими умовами ідентифікації. Камери безпеки, можуть ідентифікувати та відстежувати людей у режимі реального часу та фіксувати інформацію про несанкціонований доступ. У разі виявлення несанкціонованого доступу система може активувати аварійні протоколи, наприклад, заблокувати двері або повідомити службу безпеки.
- Багатофакторна автентифікація. Додавання технології розпізнавання обличчя як одного з факторів, поряд із паролями чи токенами. Поєднання зі скануванням відбитків пальців або райдужної оболонки ока.
- Використання для ідентифікації віддалених користувачів, які отримують доступ до корпоративних систем або мобільних додатків через Інтернет.

Для забезпечення надійного зберігання і обробки біометричних даних необхідно:

- Використовувати шифрування біометричних шаблонів під час їхнього зберігання та передачі.
- Впровадження журналів запису вхідних зображень із зазначенням рівня впевненості системи та результатів перевірки на модифікованість

- Забезпечити сегментацію баз даних, щоб у разі компрометації одна частина системи не відкривала доступ до всієї інформації.

Оптимізація роботи через регулярне навчання моделі. Технологія ідентифікації повинна враховувати можливі зміни у зовнішності користувача Для цього необхідно:

- Регулярно оновлювати навчальні набори даних.
- Проводити повторне навчання моделі з використанням нових фотографій користувачів.
- Використовувати техніки від Transfer Learning, Online Learning котрі дозволяють навчати модель в реальному часі.
- Застосовувати алгоритми для аналізу рівня шуму та покращення зображень, отриманих із камер спостереження в умовах слабкого освітлення.

Навчання персоналу:

- Забезпечення навчання співробітників безпеки та IT-служб для роботи з новою технологією.
- Проведення семінарів для користувачів з метою пояснення процесу ідентифікації.

**Висновки до третього розділу**

У третьому розділі роботи було розглянуто розроблену технологію ідентифікації користувачів інформаційної системи організації, програмний інструментарій для автоматизованої ідентифікації та сформульовано рекомендації щодо впровадження розробленої технології. Також була приділена увага редагуванню вхідних даних, перевірці їх на фальсифікацію та покращенні їх якості.

Технологія продемонструвала високу ефективність і точність у ідентифікації користувачів навіть у складних умовах, таких як змінне освітлення,

носіння окулярів або головних уборів. Результати ефективності роботи технології ідентифікації наведено в табл.3.1

Таблиця 3.1

Результати ефективності технології ідентифікації

| Метод | Точність розпізнавання (%) | Час розпізнавання (сек) | Кількість зображень для навчання |
|---|---|---|---|
| Алгоритм Віола-Джонса | ~70 | ~0.08 | Не потребує навчання |
| Мій метод (CNN + SURF) | ~92-93 | ~1.11 | ~250-300 зображень на особу |
| Алгоритми Канні та Собела | ~50-60 | ~0.05 | Не потребує навчання |
| SURF | ~70-80 | ~0.09 | ~50-100 |
| CNN | ~70-80 | ~1.87 | >1000 зображень на особу |

Ці дані були отримані на основі досліджень та бенчмарків, які порівнювали витрати обчислювальних ресурсів та час обробки різних алгоритмів для задач ідентифікації облич людини.

Розроблену технологію рекомендовано інтегрувати в існуючі інформаційні системи для забезпечення надійного контролю доступу, моніторингу та автентифікації. Особливу увагу приділено можливостям її адаптації до специфіки різних організаційних середовищ та різних сценаріїв використання.

# ВИСНОВКИ

У результаті виконання кваліфікаційної роботи було:

1. Досліджено проблеми ідентифікації користувачів інформаційних систем організації, що підтвердило необхідність у створення надійних методів ідентифікації користувачі.

2. Проаналізовано методи і технології обробки зображень для ідентифікації користувачів інформаційних систем організацій. Було розглянуто класичні та сучасні підходи до обробки зображень. Виявлено їх переваги, недоліки та застосовність до задач ідентифікації користувачів в інформаційних системах організацій.

3. Створено технологію ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту. Для її розробки використовувались алгоритми MTCNN та технологія згорткових нейронних. Для реалізації застосовано мову Python та бібліотеки OpenCV, TensorFlow, Keras. Було впроваджено графічний інтерфейс користувача.

Технологія ідентифікації користувачів інформаційної системи організації з використанням технологій штучного інтелекту продемонструвала високу точність до 93% у розпізнаванні облич навіть у складних умовах. Її можна інтегрувати в системи контролю доступу, спостереження, багатофакторної автентифікації, а також для віддаленої ідентифікації користувачів. Подальший розвиток може бути спрямований на оптимізацію ресурсів системи покращення роботи в реальному часі, та впровадження додаткових факторів для багатофакторної автентифікації.

Поставлені в роботі завдання успішно виконано, а отримані результати мають високу практичну значущість для підвищення рівня кібербезпеки у інформаційної системи організації.

# ПЕРЕЛІК ПОСИЛАНЬ


1. Andresini G., Appice A. Editorial: AI meets cybersecurity. Journal of Intelligent Information Systems. 2022. URL: https://doi.org/10.1007/s10844-022-00767-9 (date of access: 29.11.2024).
2. Biederman I., Kalocsai P. Neural and Psychophysical Analysis of Object and Face Recognition. Face Recognition. Berlin, Heidelberg, 1998. P. 3–25. URL: https://doi.org/10.1007/978-3-642-72201-1_1 (date of access: 30.11.2024).
3. Das R. Machine Learning. Practical AI for Cybersecurity. 2020. P. 33–108. URL: https://doi.org/10.1201/9781003005230-2 (date of access: 29.11.2024).
4. Das R. Practical AI for Cybersecurity / ed. by R. Das. Auerbach Publications, 2020. URL: https://doi.org/10.1201/9781003005230 (date of access: 29.11.2024).
5. Das R. The High Level Overview into Neural Networks. Practical AI for Cybersecurity. 2020. P. 109–192. URL: https://doi.org/10.1201/9781003005230-3 (date of access: 29.11.2024).
6. Detection and Classification of Road Damage Using R-CNN and Faster R-CNN: A Deep Learning Approach / M. S. Arman et al. Cyber Security and Computer Science. Cham, 2020. P. 730–741. URL: https://doi.org/10.1007/978-3-030-52856-0_58 (date of access: 30.11.2024).
7. Dimov D. T., Cantoni V. Appearance-Based 3D Object Approach to Human Ears Recognition. Biometric Authentication. Cham, 2014. P. 121–135. URL: https://doi.org/10.1007/978-3-319-13386-7_10 (date of access: 30.11.2024).
8. Furnell S. User authentication. Human-Computer Interaction and Cybersecurity Handbook. 2018. P. 3–28. URL: https://doi.org/10.1201/b22142-1 (date of access: 30.11.2024).
9. Jøsang A. AI and Cybersecurity. Cybersecurity. Cham, 2024. P. 321–335. URL: https://doi.org/10.1007/978-3-031-68483-8_15 (date of access: 30.11.2024).

10. Jøsang A. AI and Cybersecurity. Cybersecurity. Cham, 2024. P. 321–335. URL: https://doi.org/10.1007/978-3-031-68483-8_15 (date of access: 30.11.2024).
11. Mohan J., Kanagasabai A., Pandu V. Advances in Biometrics for Secure Human Authentication System. Biometrics. 2017. P. 1834–1852. URL: https://doi.org/10.4018/978-1-5225-0983-7.ch077 (date of access: 30.11.2024).
12. Muñoz-González L., Lupu E. C. The Security of Machine Learning Systems. AI in Cybersecurity. Cham, 2018. P. 47–79. URL: https://doi.org/10.1007/978-3-319-98842-9_3 (date of access: 30.11.2024).
13. Muñoz-González L., Lupu E. C. The Security of Machine Learning Systems. AI in Cybersecurity. Cham, 2018. P. 47–79. URL: https://doi.org/10.1007/978-3-319-98842-9_3 (date of access: 30.11.2024).
14. Publications C. Password Book Disguised As a Log Book Nobody Will Want to Open: Unhackable Password Organizer. Independently Published, 2021.
15. Reddy M., Chisty N. M. A., Bodepudi A. A Review of Cybersecurity and Biometric Authentication in Cloud Network. Engineering International. 2022. Vol. 10, no. 1. P. 9–18. URL: https://doi.org/10.18034/ei.v10i1.652 (date of access: 29.11.2024).
16. Secure Biometrics: Concepts, Authentication Architectures, and Challenges / S. Rane et al. IEEE Signal Processing Magazine. 2013. Vol. 30, no. 5. P. 51–64. URL: https://doi.org/10.1109/msp.2013.2261691 (date of access: 30.11.2024).
17. Sikos L. F. AI in Cybersecurity. Springer, 2018. 205 p.
18. Teichmann F., Boticiu S., Sergi B. S. Cybersecurity Trends in 2023. Jusletter-IT. 2022. No. 20-Dezember-2022. URL: https://doi.org/10.38023/8e17cdc3-b9b9-463c-b993-685bf6cc12ad (date of access: 30.11.2024).

# ДОДАТОК А

```
class UserInterface(tk.Tk):
    def __init__(self, *args, **kwargs):
        super().__init__(*args, **kwargs)
        # Глобальна змінна для збереження користувачів
        global users
        users = set()
        try:
            with open("userinformationeslist.txt", "r") as file:
                content = file.read().strip()
                users.update(content.split())
        except FileNotFoundError:
            pass  # Якщо файл не знайдено, просто продовжуємо
        self.title("User Identification")
        self.geometry("500x250")
        self.resizable(False, False)
        self.protocol("WM_DELETE_WINDOW", self.handle_exit)
        # Контейнер для сторінок
        container = tk.Frame(self)
        container.grid(sticky="nsew")
        self.frames = {}
        # Ініціалізація сторінок
        for Page in (HomePage, PageOne, PageTwo, PageThree, PageFour):
            page_name = Page.__name__
```

```
            frame = Page(parent=container, controller=self)
            self.frames[page_name] = frame
            frame.grid(row=0, column=0, sticky="nsew")
        self.show_page("HomePage")
    def show_page(self, page_name):
        """Показати вказану сторінку."""
        frame = self.frames[page_name]
        frame.tkraise()
    def handle_exit(self):
        """Дії при закритті програми."""
        if messagebox.askokcancel("Exit", "Do you really want to quit?"):
            global users
            with open("userinformationeslist.txt", "w") as file:
                file.write(" ".join(users))
            self.destroy()
class HomePage(tk.Frame):
    def __init__(self, parent, controller):
        super().__init__(parent)
        self.controller = controller
        # Завантаження зображення
        try:
            img_load = Image.open("homepagepic.png")
            img_load = img_load.resize((250, 250), Image.ANTIALIAS)
            render = ImageTk.PhotoImage(img_load)
```

```
            img_label = tk.Label(self, image=render)
            img_label.image = render
            img_label.grid(row=0, column=1, rowspan=4, sticky="nsew")
        except FileNotFoundError:
            tk.Label(self, text="Image not found").grid(row=0, column=1,
         rowspan=4, sticky="nsew")
        # Текстовий заголовок
        label = tk.Label(self, text="        Home Page        ",
         font=controller.title_font, fg="#")
        label.grid(row=0, sticky="ew")
                            command=lambda: controller.show_page("PageOne"))
        btn_another_action = tk.Button(self, text="Other Action", fg="#fafa",
         bg="#263942",
                                   command=lambda:
         controller.show_page("PageTwo"))
        btn_exit = tk.Button(self, text="Quit", fg="#", bg="#ffffff",
         command=controller.handle_exit)


        btn_sign_up.grid(row=1, column=0, ipady=3, ipadx=7)
        btn_another_action.grid(row=2, column=0, ipady=3, ipadx=2)
btn_exit.grid(row=3, column=0, ipady=3, ipadx=32)
```