Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра комп'ютерних систем та мереж
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістра
(освітній ступінь))

на тему: **Методи та засоби ідентифікації ID-карток на основі технологій комп'ютерного зору**

Виконав: студент (ка) 6 курсу, групи СІм-61
спеціальності 123 «Комп'ютерна інженерія»
(шифр і назва спеціальності)

	(підпис)	Лова М.Р. (прізвище та ініціали)
Керівник	(підпис)	Жаровський Р.О. (прізвище та ініціали)
Нормоконтроль	(підпис)	Луцик Н.С. (прізвище та ініціали)
Завідувач кафедри	(підпис)	Осухівська Г.М. (прізвище та ініціали)
Рецензент	(підпис)	Бойко І.В. (прізвище та ініціали)

Тернопіль
2021

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
Кафедра комп'ютерних систем та мереж

ЗАТВЕРДЖУЮ
Завідувач кафедри *Осухівська Г.М.*
«_____» _____ 2021 р.

З А В Д А Н Н Я

НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня *магістр*
(назва освітнього ступеня)

за спеціальністю *123 «Комп'ютерна інженерія»*
(шифр і назва спеціальності)

студенту *Лові Максиму Руслановичу*
(прізвище, ім'я, по-батькові)

1. Тема проекту (роботи) *Методи та засоби ідентифікації ID-карток на основі технологій комп'ютерного зору*
Керівник проекту (роботи) *Жаровський Руслан Олегович, к.т.н..*
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
Затверджені наказом ректора від «*28*» *жовтня* 2021 року №*4/7-916*
2. Термін подання студентом завершеної роботи
3. Вихідні дані до роботи *Зображення ID-карток, методи комп'ютерного зору, методи виявлення шахраїв, засоби побудови алгоритмів машинного навчання*
4. Зміст роботи (перелік питань, які потрібно розробити)
Вступ. 1. Аналіз сучасних підходів у сфері автоматизованого виявлення шахрайства 2. Принципи виявлення шахрайства та побудова моделі ідентифікації справжності ID-картки користувачів 3. Програмна реалізація індексу подібності зображень при аналізі ID-карток користувачів 4. Охорона праці та безпека в надзвичайних ситуаціях. Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
1. Актуальність і мета дослідження. 2. Задачі дослідження, , об'єкт і предмет, наукова новизна і практична цінність дослідження. 3. Принципи і методи виявлення шахрайства. 4. Навчальні набори зображень. 5,6. Метод порівняння зображень на основі структурного індексу 7. Архітектура комп'ютерної системи ідентифікації ID-картки. 8. Висновки

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та	*Осухівська Г.М.*		
безпека в надзвичайних	*Стадник І.Я.*		
ситуаціях			

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	*Аналіз сучасних підходів у сфері автоматизованого*	*28.10.2021-*	*виконано*
	виявлення шахрайства	*11.11.2021*	
2.	*Принципи виявлення шахрайства та побудова моделі*	*15.11.2021 –*	*виконано*
	ідентифікації справжності ID-картки користувачів	*25.11.2021*	
3.	*Програмна реалізація індексу подібності зображень при*	*26.11.2021 –*	*виконано*
	аналізі ID-карток	*05.12.2021*	
4.	*Охорона праці та безпека в надзвичайних ситуаціях*	*05.12.2021 – 10.12.2021*	*виконано*
5.	*Оформлення пояснювальної записки*	*10.12.2021- 12.12.2021*	*виконано*
6.	*Оформлення графічного матеріалу*	*12.12.2021- 14.12.2021*	*виконано*
7.	*Попередній захист кваліфікаційної роботи магістра*	*15.12.2021*	*виконано*
8.	*Захист кваліфікаційної роботи магістра*		

Студент _____ *Лова М.Р.*
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ *Жаровський Р.О.*
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Тема кваліфікаційної роботи: “ Методи та засоби ідентифікації ID-карток на основі технологій комп’ютерного зору ” // Кваліфікаційна робота // Лова Максим Русланович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем та програмної інженерії, група СІм-61 // Тернопіль, 2021 // с. – 84, рис. – 28, табл. – 11, аркушів А1 – 8, додат. – 1, бібліогр. – 30.

Ключові слова: метод, засіб, ідентифікація, шахрайство, ID-картка, комп’ютерний зір.

Метою роботи є дослідження методів і засобів виявлення справжності ID-карток з використанням технологій комп’ютерного зору.

У дипломній роботі запропоновано архітектурне рішення для авторизації працівників на основі ID-карт, що включає в себе апаратну складову з використанням міні-комп’ютера на базі Raspberry PI та камери з роздільною здатністю 2 Мп, а також програмну модель виявлення справжності ідентифікаційного документу працівника, що дають змогу забезпечити продуктивність та функціональну зручність при його аутентифікації до приміщень з обмеженим доступом.

Запропоновано метод ідентифікації справжності ID-карток, який базується на визначенні індексу структурної подібності зображень і враховує комплекс із трьох властивостей: яскравості, контрастності та структурних елементів графічного представлення ID-карток і дає змогу підвищити ефективність процесу виявлення шахрайства шляхом використання меншої кількості апаратних ресурсів та забезпечує точність ідентифікації на рівні не нижче, ніж 85%.

ABSTRACT

The theme of the thesis: " Methods and means of ID-cards identification based on computer vision technologies " /Master thesis / Lova Maksym Ruslanovych / Ternopil Ivan Pul'uj National Technical University, Faculty of Computer Information Systems and software engineering, group CIm -61 // Ternopil, 2021// p. - 84, fig. – 28, table. – 11, Sheets A1 – 8, Add – 1, Ref. – 30.

Keywords: method, tool, identification, fraud, ID-card, computer vision.

The aim of the work is to study the methods and means of authenticating ID-cards using computer vision technology.

The thesis proposes an architectural solution for authorization of employees based on ID-cards, which includes a hardware component using a mini-computer based on Raspberry PI and a camera with a resolution of 2 MP, as well as a software model for authenticating the employee's identification document, which allow to provide productivity and functional convenience at its authentication to premises with limited access.

The method of authenticating ID-cards is proposed, which is based on determining the index of structural similarity of images and takes into account a set of three properties: brightness, contrast and structural elements of graphical representation of ID-cards and allows to increase fraud detection by using less hardware identification accuracy at a level not lower than 85%

ЗМІСТ

ПЕРЕЛІК ОСНОВНИХ УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ І СКОРОЧЕНЬ

КС	Комп’ютерна система
ПЗ	Програмне забезпечення
ЗНМ	Згорткова нерйонна мережа
РНМ	Рекурентна нейронна мережа
CNN	Convolutional Neural Network
GPU	Graphics Proccesing Unit
RGB	Red Green Blue
RNN	Recurrent Neural Network
SSIM	Structural Similarity Index Measure
UXGA	Ultra Extended Graphics Array

ВСТУП

Актуальність теми. Сучасна технологічність і розвиненість методів, засобів та інструментальних комплексів дають змогу значно підвищити автоматизацію у різних сферах діяльності, починаючи від елементарних програмно-технічних засобів опрацювання інформації до комплексних систем управління космічними апаратами. Така інтенсивність впровадження і технологічний стрибок пояснюється переходом від ери інформаційних технологій до ери великих даних.

Революційність опрацювання великих об’ємів інформації пов’язана із застосуванням хмарних технологій та широким впровадженням інтелектуальних методів і засобів для виконання складних задач та бізнес-процесів. Це дає змогу знизити вплив людського фактору на прийняття рішень та підвищити ефективність результатів відповідних технологічних процесів.

Важливою областю у сфері побудови інтелектуальних комп’ютерних систем є розділ під назвою комп’ютерних зір. Методи та алгоритми комп’ютерного зору дозволяють будувати системи розумного моніторингу та управління, зокрема, транспортними потоками, виявлення злочинців, ідентифікації користувачів та ряду інших.

Комп’ютерний зір є дуже важливим у сучасному світі, де кожна галузь намагається вдосконалювати свої системи, зробити їх більш впорядкованими та ефективними. Основна мета цього розділу штучного інтелекту полягає у тому, щоб надати комп’ютерам «зір» або візуальні можливості. Це допоможе приймати кращі рішення набагато швидше, ефективніше та надійніше, у порівнянні з людьми, і виконувати їх на постійній основі. Сфера застосування комп’ютерного зору все частіше використовується для таких додатків, як виявлення крадіжок, роздрібна торгівля, системи охорони здоров’я, автономні автомобілі, виробничі сектори, оцінка якості тощо.

Одним із важливих напрямів впровадження технологій комп’ютерного зору є сфера, пов’язана з ідентифікацією особи або користувача. При цьому можуть використовуватися як біометричні дані, так і інші об’єкти, наприклад,

ідентифікаційні карти, радіочастотні мітки і т.п. Актуальною задачею при ідентифікації користувача із застосуванням методів комп'ютерного зору є перевірка справжності авторизаційного документу, яким може виступати, наприклад, карта працівника, ідентифікаційний код, виданий відповідним органом та ін. При цьому одночасно необхідно розв'язати задачі «виявлення шахраїв» та «виявлення об'єктів».

Мета і задачі дослідження. Метою роботи є дослідження методів і засобів виявлення справжності ID-карток з використанням технологій комп'ютерного зору.

Для досягнення мети роботи поставлено і розв'язано наступні **задачі**:

– аналіз наукових досліджень у сфері комп'ютерного зору та виявлення шахраїв для обґрунтування і побудови кращих програмно-апаратних рішень встановлення справжності ID-карток;

– дослідження характеристик комп'ютерних систем для досягнення мети роботи;

– побудова і формалізація моделі виявлення справжності ID-карток;

– розробка методу та обґрунтування алгоритмів комп'ютерного зору для виявлення справжності ID-карток;

– програмна реалізація та оцінка запропонованих рішень.

Об'єкт дослідження: процес виявлення шахраїв та розпізнавання графічних об'єктів.

Предмет дослідження: моделі, методи і засоби виявлення шахраїв, алгоритми розпізнавання образів.

Методи дослідження: При розв'язанні задач дипломного проектування використано наступні методи: аналіз та обґрунтування – при визначенні алгоритмів та процедур виявлення шахраїв, а також при аналізі зображень; теорія штучного інтелекту, теорія моделювання та алгоритми машинного навчання – при побудові моделі розпізнавання об'єктів та виявлення справжності ID-картки; програмування – при програмній реалізації запропонованих алгоритмів і моделей; апробація – при визначенні ефективності моделі виявлення справжності ID-карток.

Наукова новизна отриманих результатів. Наукова новизна результатів дослідження полягає в наступному:

– уперше запропоновано архітектурне рішення для авторизації працівників на основі ID-карт, що включає в себе апаратну складову з використанням міні-комп’ютера на базі Raspberry PI та камери з роздільною здатністю 2 Мп, а також програмну модель виявлення справжності ідентифікаційного документу працівника, що дають змогу забезпечити продуктивність та функціональну зручність при аутентифікації до приміщень з обмеженим доступом.

– набув подальшого розвитку метод ідентифікації справжності ID-карток, який базується на визначенні індексу структурної подібності зображень і враховує комплекс із трьох властивостей: яскравості, контрастності та структурних елементів графічного представлення ID-карток і дає змогу підвищити ефективність процесу виявлення шахрайства шляхом використання меншої кількості апаратних ресурсів та забезпечує точність ідентифікації на рівні не нижче, ніж 85%.

Практичне значення одержаних результатів. Практичне значення одержаних результатів полягає у програмній реалізації методу ідентифікації та виявлення справжності ID-картки на основі технологій комп’ютерного зору із забезпеченням високої ефективності цього процесу.

Публікації. Результати кваліфікаційної роботи апробовані на X міжнародній науково - технічній конференції молодих учених і студентів «Актуальні задачі сучасних технологій» (24-25 листопада 2021 р.) Тернопільського національного технічного університету імені Івана Пулюя та на IX науково-технічній конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (8-9 грудня 2021 року) як тези конференцій.

1. Яцишин В.В., Щербаков О.О., Лова М.Р. Аналіз баз даних зображень у галузі комп’ютерного зору. Матеріали X міжнародної науково - технічної конференції молодих учених і студентів «Актуальні задачі сучасних технологій» (24-25 листопада 2021 р.) Тернопільського національного технічного університету імені Івана Пулюя. Тернопіль: ТНТУ. 2021. С. 144.

2. Жаровський Р.О., Лова М.Р., Щербаков О.О. Застосування індексу структурної подібності зображень при їх аналізі. Матеріали IX науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (8-9 грудня 2021 року). Тернопіль: ТНТУ. 2021. С. 114.

Структура роботи. Кваліфікаційна робота містить розрахунково-пояснювальну записку та графічний матеріал. До складу записки входить вступу, 4 розділи, загальні висновки, список використаних джерел і додатки. Обсяг роботи: розрахунково-пояснювальна записка – 84 арк. формату А4, графічна частина – 8 аркушів формату А1.

РОЗДІЛ 1
АНАЛІЗ СУЧАСНИХ ПІДХОДІВ У СФЕРІ АВТОМАТИЗОВАНОГО ВИЯВЛЕННЯ ШАХРАЙСТВА

1.1. Аналіз основних понять та особливостей методів виявлення шахрайства у комп'ютерних системах

У загальному випадку, під поняттям «виявлення шахрайства» у фінансовому секторі розуміють процес, який дає змогу виявити і запобігти шахраям отримати гроші або майно із застосуванням фальшивих засобів доступу. Принципи виявлення шахрайства показано на рис. 1.1

Рис. 1.1. Принцип виявлення шахрайства

У більш широкому розумінні – це комплекс заходів, які здійснюються для виявлення та блокування спроби шахраїв одержати доступ до певних послуг, інформації, грошей, майна і т.п. із застосуванням інструментів різного призначення, які емулюють нативні властивості справжніх елементів доступу.

Шахрайська діяльність включає відмивання грошей, кібератаки, шахрайські банківські транзакції, підроблені банківські чеки, доступ до приміщень з обмеженим доступом, крадіжку особистих даних і багато подібних незаконних дій.

Як наслідок існування такого явища, організації впроваджують сучасні технології виявлення та запобігання шахрайству, а також стратегії управління ризиками для боротьби зі зростанням шахрайських транзакцій на різних платформах. Ці методи використовують адаптивну та прогнозну аналітику (тобто машинне навчання) для створення оцінки ризику шахрайства разом із моніторингом шахрайських подій у реальному часі. Виявлення шахрайства зазвичай включає в себе методику на основі аналізу даних. Ці методи часто класифікують як методи статистичного аналізу даних і методи машинного навчання чи штучного інтелекту. Класифікацію видів виявлення шахрайства показано на рис. 1.2.

Рис. 1.2. Методи виявлення шахрайства

Сукупність таких заходів дозволяє безперервно відстежувати транзакції та злочини в режимі реального часу, а також допомагає розшифрувати нові та складні профілактичні заходи за допомогою використання засобів автоматизації.

Аналіз статистичних даних для виявлення шахрайства виконує різні статистичні операції, такі як збір даних про шахрайство, виявлення шахрайства та перевірка шахрайства шляхом проведення детальних розслідувань. Ці методи ще поділяються на такі види:

1. Розрахунок статистичних параметрів – стосується розрахунку різних статистичних критеріїв, таких як середні значення (математичне сподівання), квантилі, показники ефективності та розподіли ймовірності для даних, пов’язаних із шахрайством і зібраних під час процесу їх накопичення.

2. Регресійний аналіз – дозволяє визначити зв'язок між двома або більше змінними, що становлять зацікавленість користувача. Даний вид аналізу дає змогу оцінити кореляцію між незалежними і залежними змінними. Це допомагає зрозуміти та визначити залежність між кількома змінними, що вважаються шахрайством. Це дозволяє передбачити майбутні дії шахраїв. Ці прогнози будуються на моделях використання змінних про шахрайство в потенційному випадку використання.

3. Моделі розподілу ймовірностей – особливістю цього підходу є те, що в їх основі лежить техніка порівняння представлення моделі об’єкту та розподіли ймовірностей різних шахрайських дій у бізнесі за різними критеріями чи розподілами ймовірностей.

4. Узгодженість (відповідність) даних – реалізовується шляхом зіставлення сукупності 2 наборів даних (тобто інформації про шахрайство). Як правило даний алгоритм повторюється циклічно при появі нових даних. Крім того, такий підхід дозволяє забезпечувати унікальність записів шляхом видалення дублікатів та виявлення залежностей між обома фреймами даних в цілях маркетингої, безпекової та інших видів політики.

Застосування елементів штучного інтелекту для запобігання шахрайству допомогло компаніям підвищити внутрішню безпеку та оптимізувати бізнес-

процеси. Завдяки підвищенню ефективності ШІ став важливою технологією для запобігання шахрайству у фінансових установах.

До методів fraud detection, які базуються на підходах штучного інтелекту належать такі методи:

1. Інтелектуальний аналіз даних – застосовується для виявлення та запобігання шахрайству шляхом виконання над даними процедур кластеризації, відношення до класу з визначеною міткою, а також сегментації даних, що дозволяє автоматично формувати і знаходити асоціації й залежності між даними, які дозволяють встановлювати певні закономірності.

2. Нейронні мережі – забезпечують виявлення викидів або нетипових даних з використанням алгоритмів кластеризації, узагальнення, прогнозування та класифікації значень, пов’язаних із шахрайством, які можна порівняти з результатами внутрішнього аудиту або іншої установленої документації.

3. Машинне навчання – можливе завдяки здатності алгоритмів ML вчитися на історичних моделях шахрайства та розпізнавати їх у майбутніх транзакціях. Машинне навчання використовує як контрольовані, так і неконтрольовані методи навчання. У контрольованому навчанні випадкова підвибірка всіх записів вручну класифікується як «шахрайська» або «не шахрайська». У неконтрольованому навчанні, з іншого боку, методи шукають загальні закономірності (тобто шахрайські) і кореляції в неопрацьованих даних, а прогнози будуються без додаткового маркування.

4. Розпізнавання образів (шаблонів) – алгоритми розпізнавання патернів виявляють приблизні класи, кластери або моделі атипової поведінки автоматичним шляхом або вручну. Інші методи, такі як аналіз каналів, байєсівські мережі, теорія прийняття рішень та узгодження послідовностей, також використовуються для виявлення шахрайства.

1.2. Сфери використання підходів «fraud detection»

«Fraud detection» має першочергове значення для банків та інших компаній, які займаються великою кількістю фінансових транзакцій і тому піддаються підвищеному ризику постраждати від такого виду шахрайства.

Однак інші сектори, такі як компанії електронної комерції, компанії кредитних карток, платформи електронних платежів і B2C фінтех-компанії, компанії та організації з обмеженим доступом до інформації також повинні використовувати підходи для виявлення атипових об’єктів чи поведінки з метою передбачення або обмеження негативного впливу шахрайства. Найпоширеніші застосування fraud detection включають шахрайство, пов’язане з обліковими записами, шахрайство з платежами і транзакціями.

Шахрайство з обліковими записами поділяється на шахрайство з новими обліковими записами та шахрайство з поглинанням облікового запису. При шахрайстві з новими обліковими записами, нові аккаунти створюються з використанням підробленої особи. Такі шахрайства можна ідентифікувати за допомогою шаблонів різних пристроїв та індикаторів сесії для виявлення підроблених ідентифікаційних даних.

Шахрайство з обліковими записами відбувається, коли хакер отримує продукти та послуги, використовуючи наявний обліковий запис іншої особи. Щоб запобігти цьому, для підтвердження облікового запису можна обчислити й оцінити біометричні дані сеансу, пристрою та поведінки користувача. Крім того, аналіз подорожей користувачів на основі поведінкових моделей може допомогти виявити поглинання облікових записів, перш ніж вони завдадуть якоїсь шкоди.

Шахрайство з оплатою – це будь-яка неправдива або незаконна операція, яку здійснює кіберзлочинець. Зловмисник обманює жертву шляхом одержання доступу до грошей, особистого майна, інтересів або конфіденційної інформації. Ця категорія також включає шахрайство з несанкціонованими транзакціями, шахрайство з викраденими товарами та неправдиві запити про шахрайство з відшкодуванням.

Оскільки цифрова тенденція набирає обертів у всьому світі, кількість шахрайств збільшується зі зростанням кількості онлайн-транзакцій та транзакцій у банкоматах. Найпоширенішими видами банківського шахрайства є:

Шахрайство з API – директива про платіжні послуги 2 (PSD2) зобов'язує певні європейські фінансові установи відкривати свої послуги через інтерфейси програмного забезпечення (API). Це створює нову хвилю атаки.

Шахрайство з викраденими/підробленими кредитними картками: підроблена картка створюється на основі інформації про картку користувача, до якої вдається отримати доступ шахраям. Для цього шахраї використовують багато способів, найпоширенішим є скімінг карт. Скімінг кредитної картки – це техніка, при якій шахрай приєднує невеликий пристрій до транзакційної машини, який неможливо легко помітити.

Клонування веб-сайтів є одним із найпопулярніших методів серед шахраїв, щоб позбавити людей їхніх грошей. Як випливає з назви, кіберзлочинці спочатку створюють «клон» оригінального веб-сайту. Далі вони формують пастку, призначену для того, щоб жертви нічого не підозрюючи відвідували клонований сайт. Зазвичай це робиться за допомогою посилань, які надсилаються в електронних листах, текстових повідомленнях або публікаціях у соціальних мережах, з проханням нічого не підозрюючих користувачів натиснути на них.

Шахрайство в банкоматах описується як шахрайська діяльність, коли злочинці використовують кредитну картку іншої особи, щоб миттєво зняти гроші з цього рахунку. Різні типи шахрайства в банкоматах включають підбір карток, скімінг карток, захоплення карток та заклинювання клавіатури.

Оскільки сектор електронної комерції процвітає на тлі пандемії COVID-19, націленність шахрайства на користувачів через канали електронної комерції стало частішим, ніж будь-коли.

Найпоширеніші методи включають:

Зловживання промо-акціями або шахрайство з купонами – відбувається, коли окремий клієнт, постачальник або агентство-партнер використовує рекламну акцію, зловживаючи політикою купонів. Шахраї можуть отримати вигоду,

викупивши купони кілька разів або просто використавши їх для отримання грошей та інших цінних предметів або послуг.

Шахрайство з оплатою – є однією з найпоширеніших шахрайських дій в електронній комерції, тобто будь-яка незаконна транзакція в Інтернеті, яку здійснює кіберзлочинець. Жертвою, як правило, є онлайн-користувач, якого позбавляють грошей, відсотків, конфіденційної інформації чи особистого майна.

Шахрайство з доставкою – два типи шахрайства з доставкою включають крадіжку особистих даних і дружнє шахрайство. Під час крадіжки особистих даних шахраї намагаються отримати особисті дані користувача за допомогою шкідливих програм, підроблених веб-сайтів, електронних листів або коротких повідомлень. Кіберзлочинець використовує їх, щоб придбати товари за рахунком-фактурою та надіслати їх на іншу адресу доставки, не маючи наміру платити за товари.

Дружне шахрайство – це коли клієнт сам не має наміру оплачувати замовлений товар і стверджує, що він так і не прийшов.

Торгові майданчики та онлайн-реклама – цей вид шахрайства зазвичай здійснюється через зловживання рекомендаціями та просуванням, а також підроблені огляди.

Фальшиві відгуки: багато споживачів покладаються на огляди в Інтернеті, коли роблять покупку, реєструються в послугах або спілкуються з конкретними компаніями. Підроблені відгуки поширюються, щоб дискредитувати бренди, підірвати довіру та навести приклади поганого досвіду, якого насправді ніколи не було.

Зловживання рекомендаціями та рекламними акціями – реферальні програми є одним із найкращих способів посилити перенаправлення з «уст в уста» для інтернет-магазинів. Однак багато клієнтів намагаються скористатися перевагами цих програм, щоб отримати кращі пропозиції та знижки, ніж ті, на які вони заслуговують, залишаючи бізнес в напруженому стані з додатковими прихованими витратами. У 2017 році Tesla Motors виявила, що люди купують рекламу Google на основі ключових слів для просування своїх реферальних кодів. Це змусило зацікавлених клієнтів несвідомо натиснути на рекламне оголошення. Це порушило

положення Тесли про добросовісність. Потім Tesla залишила за собою право визнати недійсними реферали, які були зроблені зловживаючими або шахрайськими засобами.

4. IT та телекомунікації

Ці шахрайства здійснюються за допомогою телефонних дзвінків та інших методів за допомогою телефонів.

Телефонне шахрайство, яке зазвичай називають комунікаційним, використовує телекомунікаційні продукти або послуги з метою незаконного отримання грошей від телекомунікаційної компанії або навіть її клієнтів або несплати її.

Шахрайство з переадресацією дзвінків – злом переадресації викликів є поширеною формою шахрайства VoIP-телекомунікацій. У такому випадку зловмисники отримують несанкціонований доступ до корпоративної приватної системи обміну повідомленнями (АТС) або системи голосової пошти IVR. Завдяки цьому вони можуть налаштувати переадресацію дзвінків на дорогі міжміські місця призначення та отримати прибуток від угоди про розподіл прибутку.

Шахрайство з кількома переадресаціями – у цьому шахрайському сценарії дзвінок передається з джерела виклику відразу після того, як адресат відповідає на виклик. Коли виклик переведено, шахрайський дзвінок виконується з двома дорогими адресатами, а джерело дзвінка кладе трубку. Після передачі цих викликів вони продовжуються до тих пір, поки оператор не вимкне їх. Деякі клієнти повідомили, що дзвінки залишаються на зв’язку більше 24 годин.

Шахрайство з одним дзвінком і відрізанням – на японській мові означає «один і відрізати», що просто означає дати телефону дзвонити лише один раз, а потім відключити дзвінок. Схема такого телефонного шахрайства працює за методом одного дзвінка, щоб швидко заробити гроші. Шахрай налаштовує комп’ютер для випадкового набору великої кількості телефонів. Кожен дзвінок дзвонить лише один раз, а потім розривається. Це залишає номер як пропущений дзвінок на телефонах багатьох одержувачів. Багато людей інстинктивно відповідають на пропущений дзвінок, навіть якщо він з таємничого міжнародного

номера. Щойно особа передзвонить, дзвінок перенаправляється на дорогий номер з преміальним тарифом. Тоді абонента змушують залишатися на лінії якомога довше. Чим довше триває занятість лінії, тим більше грошей заробляють шахраї.

1.3. Аналіз популярних наборів зображень об’єктів реального світу

Динамічність розвитку у різних галузях штучного інтелекту не оминули й найбільш популярного розділу computer vision. Зважаючи на те, що такі гіганти як Google, Facebook, IBM та ряд ін. мають можливість проводити глобальні дослідження у даній галузі, то для формування більшого ринку Data Science вони надали відкритий доступ до різних наборів, розкрили архітектуру та моделі для навчання для проектування різного типу інтелектуальних комп’ютерних систем.

Одним з потужних фреймів даних, що використовуються при розпізнаванні образів є сховище даних, що містить набір рукописних цифр. Дана колекція сформована MNIST і включає близько сімдесяти тисяч графічних примітивів написання арабських цифр в діапазоні від 0 до 9. Ці зображення представляються у вигляді зображень з відтінками сірого розміром 28×28 пікселів. Набір даних умовно поділено у відношенні 6:7 – тренувальний набір, та 1:7 – тестова вибірка.. Графічне представлення цифр поміщено посередині зображення. Застосування даного набору даних є базовим при реалізації систем оцифрування інформації, представленої у вигляді рукопису (рис. 1.4.).

Ще один набір даних від MNIST пов’язаний зі сферою моди і має назву «MNIST Fashion». Він сформований із зображень у вигляді та форматі подібному до базової версії з цифрами, з тими ж розмірами пікселів та відтінками сірого. Характерною особливістю даного дата фрейму є те, що він містить елементи одягу починаючи від футболок і штанів, закінчуючи взуттям та верхнім одягом. Кількість міток класів за якими проведено класифікацію становить 10.

Спонсорами збирання та формування даної колекції виступила компанія та науково-дослідницька група у сфері роздрібного рітейлу Zalando. Представлення деяких екземплярів з колекції «MNIST Fashion» наведено на рис. 1.5.

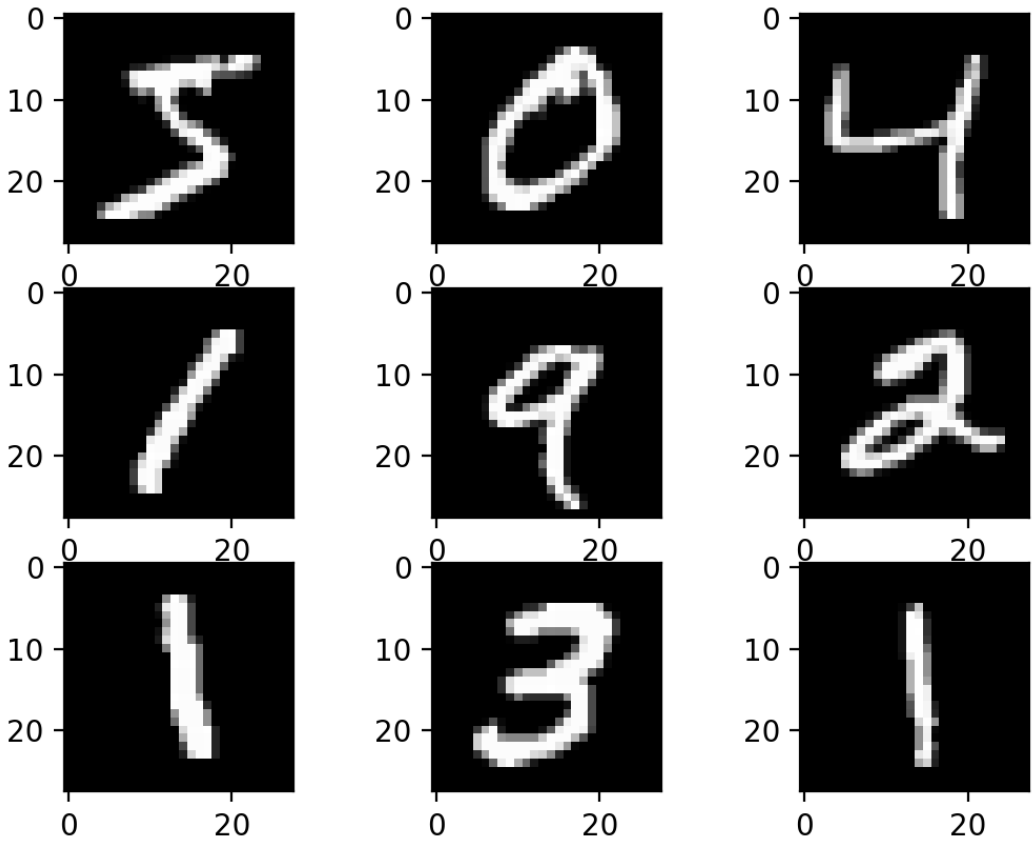

Рис. 1.4. Рукописні цифри набору MNIST

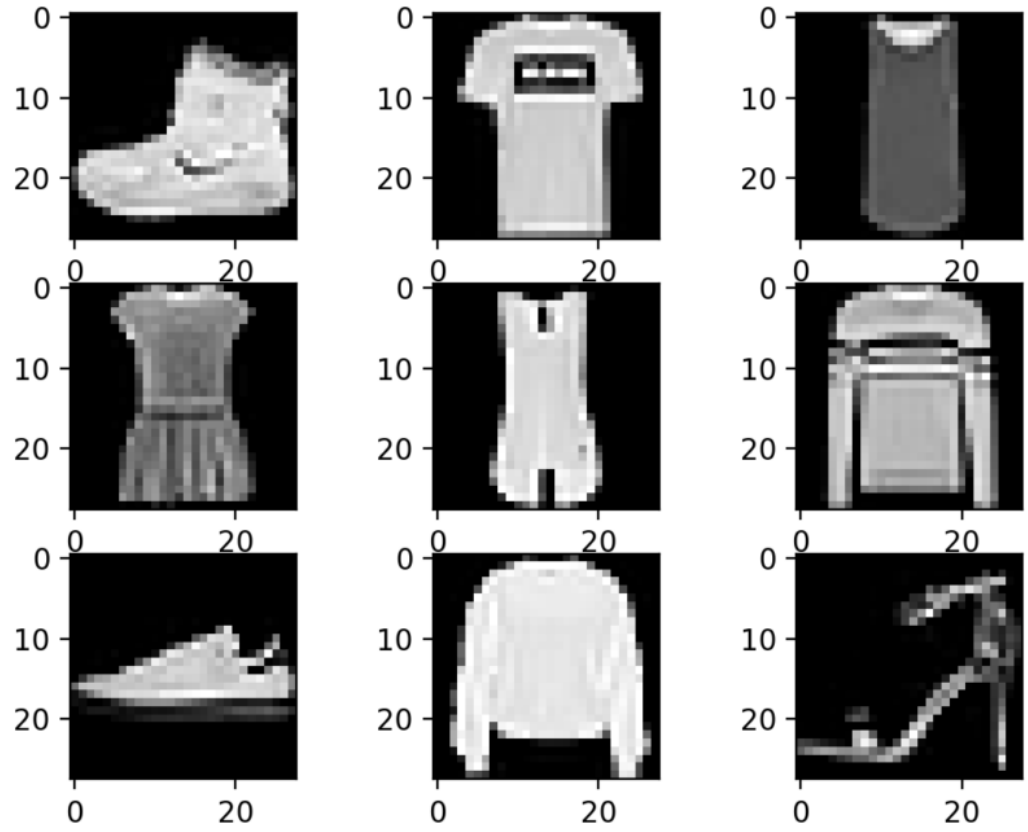

Рис. 1.5. Екземпляри з набору даних «MNIST Fashion»

У результаті досліджень Канадського інституту перспективних досліджень сформовано множину зображень, які утворили фрейми даних «CIFAR-10» та «CIFAR-100».

Менший набір містить шістдесят тисяч графічних елементів, які поділені на десять класів. Основними елементами цього набору даних є транспортні засоби, зокрема, авто різного типу, літаки і кораблі, а також множина екземплярів живої природи: домашні тварини і тварини дикої природи.

Розширений фрейм даних під назвою «CIFAR-100» доволі подібний до попереднього. Він містить таку ж кількість даних, однак кількість міток класів складає вже 100 і вони є рівномірно розподіленими за всіма класами, що складає шістсот екземплярів на кожний клас.

Обидві колекції даних є досить зручними при проектуванні та навчанні моделей. Кожне зображення має розмір «32x32» px. Розмір навчальної вибірки становить 50 тис. зображень, а тестової – 10 тис. з рівномірним розподілом за 100 мітками класів. Деякі екземпляри цих наборів представлено на рис. 1.6.

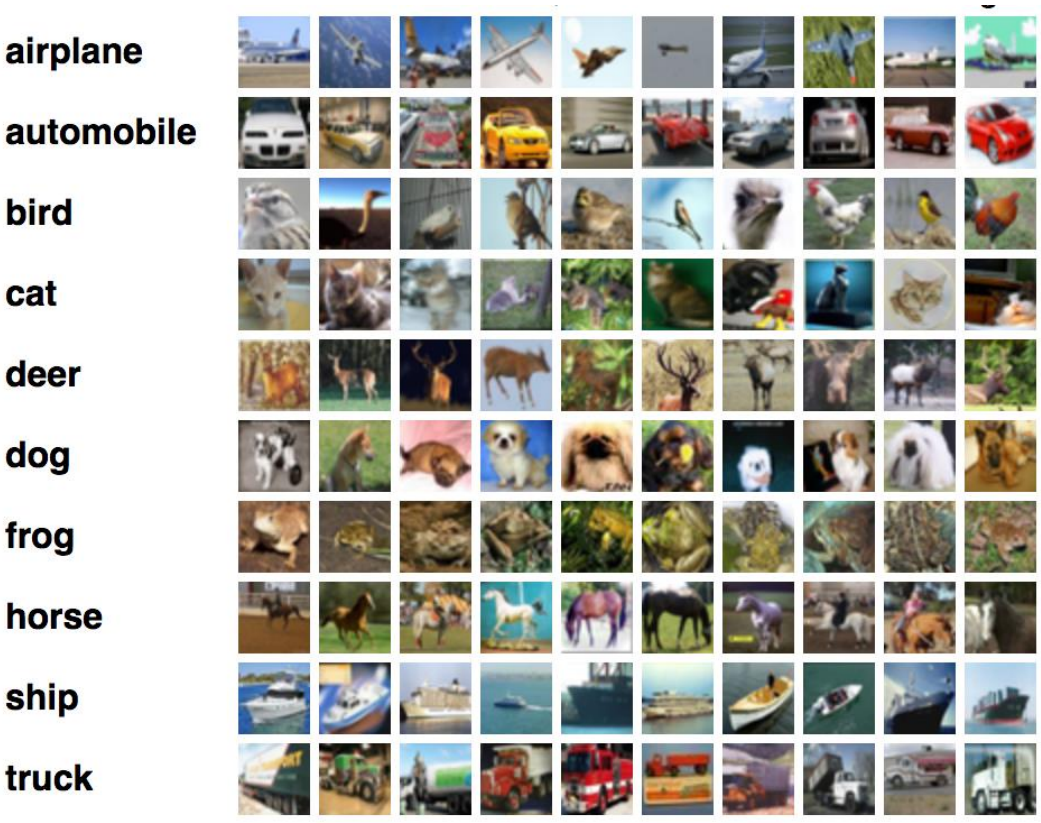

Рис. 1.6. Екземпляри колекції даних «CIFAR-10» та «CIFAR-100»

Ще одна колекція зображень, яку можна використовувати при розпізнаванні обличчя, прогнозуванні віку і статі людини включає близько півмільйона екземплярів графічних прототипів – «IMDB-Wiki». Особливістю цього набору даних є те, що самі дані включають додатковий метаопис для детектування об’єктів. На рис. 1.7 показано приклад екземплярів зображень цієї колекції.

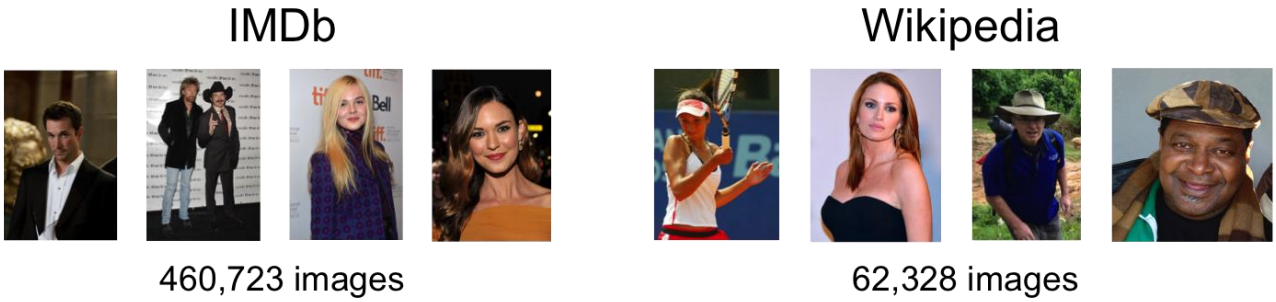

Рис. 1.7. Екземпляри зображень набору даних «IMDB-Wiki»

Інтенсивність розвитку методів і засобів комп’ютерного зору доводить згенерована колекція даних ImageNet, що є результатом спільної роботи двох університетів: Стендфорда та Прінстона. Ця колекція зображень ефективно використовується при проведенні змагання ILSVRC («ImageNet Large Scale Visual Recognition Challenge»).

Таке змагання передбачає розв’язання 5 типових задач з використанням колекції ImageNet:

– визначення мітки класу до якого належить об’єкт;
– детектування об’єктів;
– визначення положення об’єкта на зображені;
– виявлення об’єктів у відеопотоці;
– розпізнавання об’єктів на відео.

Колекція зображень ImageNet сформована на основі ієрархічного дерева WordNet, яке представляє собою сховище даних англомовних іменників. Щодо кількості екземплярів даних ImageNet, то можна сказати, що кожна вершина ієрархії містить більше п’яти ста зображень. В загальному випадку, потужність цієї

колекції вимірюються майже півтори мільйоном графічних зображень, які можна класифікувати за понад двісті двадцятьма тисячами класів. На сьогодні ImageNet є найбільшою, загальнодоступною та відкритою колекцією даних. На рис. 1.8 показано екземпляри цієї колекції.

Рис. 1.8. Приклад зображень колекції ImageNet

На противагу дослідженням комп’ютерного зору, які проводяться у США та Канаді, у Європі також інтенсивно впроваджують і розвивають даний напрям. Доказом цього є колекція зображень створена науково-дослідним інститутом Паскаля, яка носить назву PASCAL VOC.

За допомогою зображень з набору даних PASCAL VOC можна проводити дослідження щодо, наприклад, їхньої класифікації за чотирма глобальними категоріями, які містять в собі 20 підкласів. Основними категоріями є зображення транспортних засобів, об’єктів живої природи, людей та домашнього господарства. На відміну, наприклад від ImageNet, дана колекція не є настільки великою, однак може ефективно використовуватись для прототипування моделей машинного навчання на ранніх стадіях детектування і сегментування об’єктів за захначеними категоріями. Приклад екземплярів зображень набору даних PASCAL VOC показано на рис. 1.9.

Рис. 1.9. Приклад екземплярів зображень у PASCAL VOC

Для забезпечення можливості виявлення контурів об’єктів, Масачусетським інститутом створено колекцію даних під назвою LabelMe за допомогою одноіменного засобу. Цей інструмент дозволяє задавати межі об’єкту на зображенні і додавати до нього короткі текстові анотації. Як показує практика, це є ефективним інструментом при формуванні колекцій зображень та проведенні досліджень у сфері комп’ютерного зору, зокрема сегментації зображень. Приклад застосування LabelMe показано на рис. 1.10.

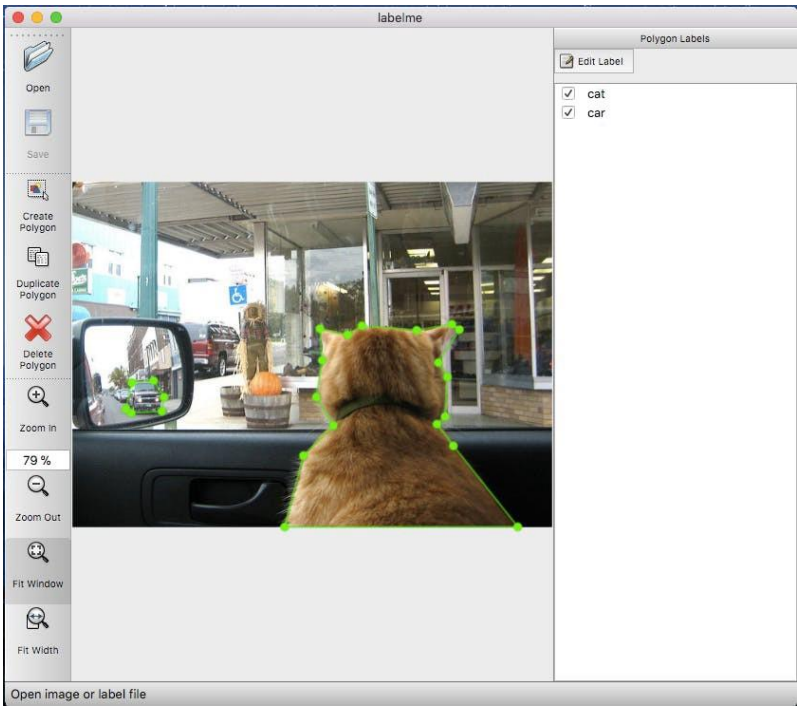

Рис. 1.10. Приклад застосування інструменту LabelMe

Ще однією розробкою MIT є колекція зображень Places2, що включає в себе близько десяти мільйонів екземплярів та понад півтисячі сцен. Цей набір застосовувся при проведенні змагань в галузі комп'ютерного зору у 2015 та 2016 роках для розв'язання задач класифікації та аналізу об'єктів на цих сценах. На рис. 1.11 показано сцени з Places2.

Рис. 1.11. Сцени набору даних Places2

Не пасе задніх у розвитку методів і засобів штучного інтелекту й компанія Microsoft і як проявив інтересу до досліджень комп'ютерного зору є створений нею набір зображень MS COCO Dataset. Потужність цієї колекції зображень характеризується наявністю більше 120 тис екземплярів та близько 880 тис. тегів-маркерів, які в сукупності формують 91 категорію зображень. На основі наборів зображень цієї колекції можна проводити аналіз з визначення представлених на них об'єктів, встановлення ключових точок, сегментації і генерації підписів. На відміну від ImageNet, колекція MS COCO Dataset володіє меншою кількістю об'єктів, але більшою кількістю зображень для кожного класу, що забезпечує можливість опрацювання більш детальних властивостей об'єктів (рис. 1.12).

Рис. 1.12. Представлення зображень у наборі даних MS COCO Dataset

При дослідженні методів і засобів виявлення справжності ID-карток доцільним є скористатися одним з таких наборів даних, або використати існуючі архітектури при застосуванні нейромережевого підходу .

1.4. Висновки до розділу

У даному розділі одержано основні наукові і практичні результати:

1. Проаналізовано основні поняття у сфері виявлення шахрайства, методи ідентифікації підозрілих об’єктів та поведінки користувачів, що дало змогу визначити потенційні шляхи та принципи ідентифікації ID-карток з використанням технологій комп’ютерного зору, які передбачають виконання п’яти стадій: формування сховища еталонних даних, формування асоціативних правил, аналіз шаблонів зображень, авторизацію користувацьких даних та формування сповіщень про загрозу.

2. Проведено аналіз сфер застосування підходів «fraud detection» і виявлено специфіку його організації у банківській галузі, сфері інформаційних технологій та інших прикладних областях, що дало змогу визначити сукупність комплексу апаратних і програмних засобів для ефективного їх впровадження.

3. Проаналізовано відкриті набори даних зображень, накопичених компаніями, що займаються інженерією даних і впровадженням елементів комп’ютерного зору, що дало змогу обґрунтувати доцільність їхнього застосування при виявленні справжності ID-карток користувачів у віртуальному просторі та ідентифікаційних документів при авторизації працівників для доступу у приміщення з обмеженими правами доступом.

РОЗДІЛ 2
ПРИНЦИПИ ВИЯВЛЕННЯ ШАХРАЙСТВА ТА ПОБУДОВА МОДЕЛІ ІДЕНТИФІКАЦІЇ СПРАВЖНОСТІ ID-КАРТКИ КОРИСТУВАЧІВ

2.1. Процес впровадження заходів та етапи виявлення справжності ID-карток

У загальному випадку, для встановлення справжності ID-карток, можна скористатись алгоритмом боротьби з шахрайством, показаним на рис. 2.1.

Рис. 2.1. Процес визначення справжності ID-картки

Аналізуючи рис. 2.1, можна визначити наступні етапи впровадження заходів щодо виявлення нетипових об’єктів та поведінки, які класифікуються як шахрайські дії.

1. Створення профілю потенційного ризику шахрайства – використовується підхід зверху вниз для оцінки ризику із вказанням сфер, у яких імовірно трапляється шахрайство, і визначаються їхні типи. Після цього виконується класифікація потенційних ризиків на основі більш комплексного загального ризику, з яким може зіткнутися організація. Далі проектуються профілі ризику

шахрайства щодо справжності ID-карток, які є частиною загальної оцінки ризиків і включають в процес усі зацікавлені сторони та осіб, які приймають рішення.

2. Визначення можливих ознак підроблених об’єктів (даних) – передбачає 100% перевірку даних підприємства, а не лише випадкових вибірок. Хоча часткова вибірка може бути ефективною для виявлення проблем, які є відносно послідовними в сукупності даних, це не завжди стосується шахрайства. Шахрайські операції за своєю природою відбуваються не випадково. Транзакції можуть входити в рамки певного стандартного тестування і все одно не позначатися.

3. Запровадження постійного спостереження та аудиту – запроваджується для перевірки та підтвердження ефективності контролю над авторизаційними транзакціями. Безперервний аналіз можна використовувати, створюючи сценарії для виявлення аномалій у міру їх виникнення протягом певного періоду часу. Цей процес може істотно підвищити загальну ефективність, послідовність і якість процесу виявлення підробок або шахрайства.

4. Підвищення організаційної обізнаності щодо моніторингової діяльності – значний вплив щодо заходів запобігання шахрайству має розповсюдження програми по усіх підрозділах організації. Це може бути особливо корисно для уникнути шахрайства всередині бізнес-організації. Якщо всі знають про запроваджені системи виявлення аномалій, то працівники не будуть займатися шахрайством і такий захід є хорошою профілактичною діяльністю.

5. Впровадження елементів штучного інтелекту – машинне навчання є потужним засобом для підвищення точності та ефективності виявлення нетипових об’єктів та аномальної поведінки. Завдяки інтелектуальним алгоритмам системи можуть автоматично виконувати наступні завдання:

– Створювати та оновлювати правила виявлення й опрацювання сповіщень – алгоритми машинного навчання можуть досліджувати велику кількість даних, щоб допомогти встановити правила та підтримувати їх у актуальному стані. Навіть такий простий метод, як дерево прийняття рішень, може надати певні переваги (у підході сегментації) щодо створення більш точних правил.

– Обирати та будувати ефективні моделі виявлення шахрайства – комбінація методів машинного навчання, таких як градієнтний спуск, метод опорних векторів і нейронні мережі може забезпечити високу точність показників виявлення нетипової поведінки.

– Автоматизувати процеси розслідування шахрайських дій – в середньому від 60 до 70% часу розслідування витрачається на збір даних про об’єкт. Системи на основі машинного навчання можуть автоматично здійснювати пошук та отримувати дані, виконувати запити до бази даних та збирати інформацію від сторонніх постачальників даних без будь-якого втручання людини.

6. Заохочення щодо сповіщення про підозрілу діяльність проти відмивання грошей та шахрайства – метою повідомлення про підозрілу діяльність та результатів розслідування є виявлення клієнтів, причетних до відмивання грошей, шахрайства або фінансування тероризму. Це може охоплювати більшу частину діяльності, яка вважається неординарною. Діяльність може бути включена до таких заходів, якщо вона викликає підозру, що власник рахунку намагається щось приховати або здійснити незаконну операцію. Таким чином, організаціям необхідно вжити заходів щодо повідомлення про відмивання грошей та пов’язане з цим шахрайство.

7. Впровадження інтелектуального управління діяльністю – розширене інтелектуальне рішення для керування бізнес-процесами, орієнтоване на аналітику, може автоматично визначати пріоритети процесів, рекомендовані слідчі дії та прискорення застосування прямих дій для уникнення або зменшення збитків від шахрайських дій. Підвищити ефективність процесу управління діяльністю можна за рахунок:

– сповіщення деталями про клієнтів, їх облікові записи або бенефіціарів;

– розумного пошуку і опрацювання даних з внутрішньої бази даних або навіть із стороннього постачальника даних.;

– представлення інформації за допомогою засобів візуалізації;

– автоматичного заповнення та підготовки анкет для електронної подачі.

Таким чином, власники бізнесу можуть спростити розслідування шахрайства, застосувавши інтелектуальні рішення для управління бізнес-процесами та допомогти у боротьбі з кіберзлочинами.

8. Дослідження, адаптація і повторення – передбачає перегляд, переоцінку та реструктуризацію профілю шахрайства, беручи до уваги найпоширеніші схеми, а також ті, що стосуються виключно ризиків, які є унікальними для конкретного бізнесу. Слід використовувати аналітику даних, щоб дізнатися, де елементи керування не працюють або неефективні.

Таким чином, основною задачею для забезпечення ефективності та автоматизації процесів виявлення шахрайства і встановлення справжності ID-карток є впровадження елементів штучного інтелекту на різних етапах бізнес-процесів організації.

2.2. Метод виявлення справжності ID-карток на основі індексу структурної подібності зображень

Структурний індекс подібності зображень використовується як метрика для вимірювання міри схожості між двома заданими зображеннями. Оскільки ця технологія існує з 2004 року, то наявними у всесвітній мережі є доволі багато наукових і прикладних публікацій, що пояснюють дану концепцію і теорію SSIM («Structural Similarity Index Model») на загальному рівні. У дипломній роботі пропонується дещо інша інтерпретація даного індексу для його узгодження з функцією втрат через метод градієнтного спуску.

Основне завдання, яке розв’язується у даному розділі полягає в обґрунтуванні прикладного застосування структурного індексу подібності при виявленні справжності ID-картки працівника та побудови сучасної передової системи глибокого навчання на основі PyTorch.

Теорія щодо використання структурного індексу подібності вперше була представлена у статті IEEE у 2004 році. Об’єктивні методи оцінки якості перцептивного зображення традиційно намагалися кількісно визначити через

видимість помилок (відмінностей) між спотвореним зображенням та еталонним. При цьому використовувались різноманітні відомі властивості зорової системи людини.

Виходячи з припущення, що зорове сприйняття людини дуже пристосоване для добування структурної інформації зі сцени, введемо альтернативну додаткову структуру для оцінки якості, що заснована на деградації структурної інформації.

У даному випадку потрібно виділити два суттєві моменти.

Більшість методів оцінки якості зображень покладаються на кількісне визначення помилок між еталонним і дослідним зразком зображення. Загальною метрикою є кількісна оцінка різниці значень кожного з відповідних пікселів між зразком та еталонними зображеннями (за допомогою, наприклад, середньоквадратичної помилки).

Система візуального сприйняття людини здатна ідентифікувати структурну інформацію зі сцени і, отже, визначити відмінності між інформацією, добутою з еталонної та сцени зразку.

Отже, метрика, яка повторює таку поведінку, буде краще виконувати завдання, які передбачають розрізнення зразка та еталонного зображення. Показник структурної схожості виділяє з зображення 3 ключові характеристики:

– яскравість;
– контраст;
– структура.

Порівняння двох зображень здійснюється на основі цих 3 ознак. На рис. 2.2, наведеному нижче, показано розташування та алгоритм вимірювання структурної подібності. Сигнали X і Y посилають на еталонні та зображення зразків.

Ця система обчислює індекс структурної схожості між двома заданими зображеннями, значення якого належать інтервалу від -1 до +1. Значення «+1» вказує, що дані зображення дуже схожі або однакові, а значення «-1» – вказує, що вони дуже різні. Часто ці значення представляються в діапазоні [0, 1], де крайні значення мають ту саму інтерпретацію.

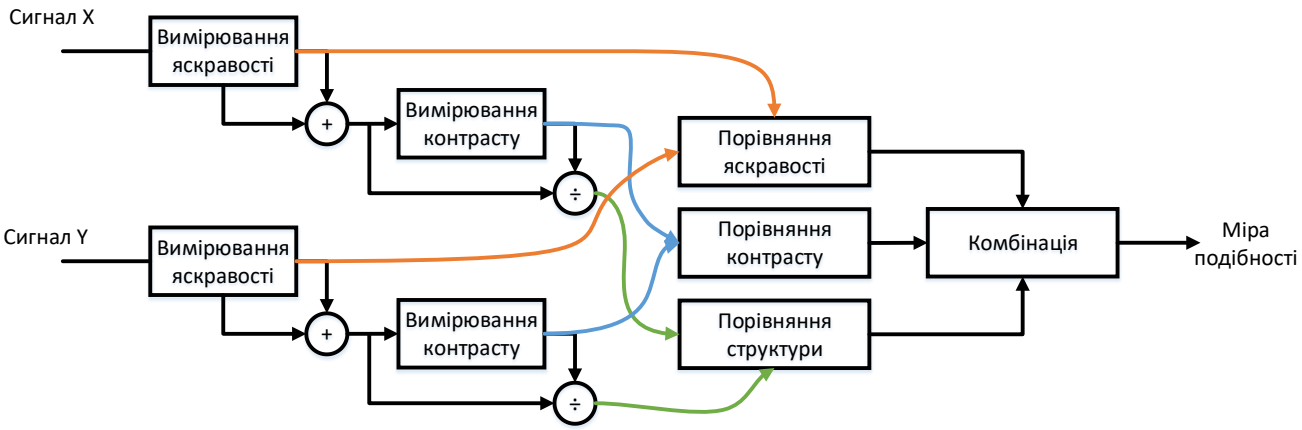

Рис. 2.2. Система вимірювання показника структурної подібності зображень

Далі перейдемо до формального представлення функцій, які дозволяють забезпечити остаточну оцінку метрики структурної подібності зображень.

Перша функція описує яскравість і вимірюється шляхом усереднення за всіма значеннями пікселів. Яскравість позначають μ, а обчислюють за наступною формулою:

$$\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{2.1}$$

де x_i – значення яскравості і-го пікселя;

N – кількість пікселів.

Виходячи з формули (2.1), функція порівняння яскравості $l(x, y)$ є функцією з двома аргументам, де замість x можна написати функцію яскравості першого зображення μ_x, а замість y – μ_y, що є функцією яскравості другого зображення.

Для вимірювання контрастності використовується функція стандартного відхилення (квадратного кореня з дисперсії) усіх значень пікселів. Цей показник позначається σ та обчислюється за такою формулою:

$$\sigma_x = \sqrt{(\frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)^2} \tag{2.2}$$

Функція порівняння контрастності $c(x,y)$ також є функцією з двома аргументам, де замість x можна вписати функцію контрастності першого зображення σ_x, а замість y – σ_y, що є функцією контрастності другого зображення. У даному випадку x та y – зображення, які необхідно порівняти, а μ_x – середнє значення кількості пікселів у зображенні.

Для порівняння структури зображень використовується консолідована формула (2.3), що по суті виконує ділення вхідного сигналу з його стандартним відхиленням для того, щоб у результаті одержати одиницю стандартного відхилення. Це нормування забезпечує більш надійне порівняння.

$$s_x = \frac{x-\mu_x}{\sigma_x} \tag{2.3}$$

де x – вхідне зображення.

Таким чином обчислюється три параметри структурного індексу подібності, однак для забезпечення повноти його представлення потрібно ще формалізувати функції порівняння зображень, які представляються трьома параметрами: яскравістю, контрастністю та структурою. Окрім цього потрібно визначити комплексну функцію, яка згортає три інші функції порівняння.

Функція порівняння яскравості зображень визначається функцією $l(x,y)$, яка подана нижче. Змінна μ представляє собою середнє значення пікселів даного зображення, а x та y – це зображення, які порівнюються:

$$l(x,y) = \frac{2\mu_x\mu_y+C_1}{\mu_x^2+\mu_y^2+C_1}, \tag{2.4}$$

де C_1 – константа для забезпечення стабільності, коли знаменник рівний 0.

Константа C_1 визначається як:

$$C_1 = (K_1L)^2, \tag{2.5}$$

де L – це динамічний діапазон для значень пікселів (наприклад, може приймати значення 255 у випадку коли опрацьовується стандартне 8-бітове зображення).

K_1 – константа-регуляризатор.

Функція порівняння контрасту визначається функцією $c(x, y)$, яка показана нижче. Змінна σ позначає стандартне відхилення (дисперсію) даного зображення, x та y є зображеннями, які порівнюються:

$$c(x, y) = \frac{2\sigma_x\sigma_y + C_2}{\sigma_x^2 + \sigma_y^2 + C_2} \quad , \tag{2.6}$$

де C_2 – константа, що є кортежем наступного вигляді:

$$C_2 = (K_2 L)^2, \tag{2.7}$$

де L і K_2 – мають інтерпретацію аналогічну до тих, що описані у формулі (2.5).

Функція порівняння структури визначається функцією $s(x, y)$, яка показана нижче. Змінна σ відображає стандартне відхилення зображення, а x та y – порівнювані зображення:

$$s(x, y) = \frac{\sigma_{xy} + C_3}{\sigma_x\sigma_y + C_3}, \tag{2.8}$$

де σ_{xy} обчислюється за формулою:

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y) \tag{2.9}$$

Нарешті, індекс структурної подібності двох зображень можна виразити наступним чином:

$$SSIM(x,y) = [l(x,y)]^{\alpha} \cdot [c(x,y)]^{\beta} \cdot [s(x,y)]^{\gamma}, \qquad (2.10)$$

де $\alpha > 0, \beta > 0, \gamma > 0$ позначають відносну важливість кожної з метрик.

Щоб спростити вираз, можна припустити, що $\alpha = \beta = \gamma = 1$ і $C_3 = \frac{C_2}{2}$, то можна одержати, що формула (2.10) набуває вигляду:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \qquad (2.11)$$

Для оцінювання якості зображення доцільно застосовувати індекс SSIM локально, а не глобально. По-перше, статистичні характеристики зображень, як правило, дуже просторово нестаціонарні.

По-друге, спотворення зображення, які можуть залежати або не залежати від локальної статистики зображення, також можуть бути проміжними.

По-третє, на типових відстанях для перегляду спостерігач-людина може одночасно сприймати з високою роздільною здатністю лише локальну область зображення (через особливості фовеації). І, нарешті, локалізоване вимірювання якості може забезпечити просторово різну карту якості ознак зображення, яка надає більше інформації про погіршення якості зображення і може бути корисною в деяких програмах.

Отже, замість того, щоб застосовувати вищенаведені показники глобально (тобто відразу по всьому зображенню), краще застосовувати показники регіонально (тобто на невеликих ділянках зображення та взяти середнє значення в цілому).

Цей метод часто називають індексом середньої структурної схожості. Через таку зміну підходу, наведені вище формули, також потрібно модифікувати для того, щоб відобразити основну концепцію підходу (слід зазначити, що цей підхід є більш поширеним).

Для реалізації індексу середньої структурної схожості використовують кругово-симетричну гауссову функцію 11x11 (по суті, матрицю 11x11, чиї значення

отримані з гауссового розподілу), яка переміщується піксель за пікселем по всьому зображенню. На кожному кроці локальна статистика та індекс SSIM обчислюються в локальному вікні.

Оскільки показники обчислюються локально, то формули (2.1), (2.2), (2.9) набувають наступного вигляду:

$$\mu_x = \sum_{i=1}^{N} \omega_i x_i \tag{2.12}$$

$$\sigma_x = \sqrt{\sum_{i=1}^{N} \omega_i (x_i - \mu_x)^2} \tag{2.13}$$

$$\sigma_{xy} = \sum_{i=1}^{N} \omega_i (x_i - \mu_x)(y_i - \mu_y) \tag{2.14}$$

Параметр ω_i представляє собою зважену функцію Гауса. По простому цей показник є множником, який використовується для обчислення шуканих значень за допомогою деяких математичних прийомів. Після виконання обчислень по всьому зображенню береться середнє значення усіх локальних значень SSIM і одержується глобальне значення:

$$MSSIM(x, y) = \frac{1}{M} \sum_{j=1}^{M} SSIM(x_j, y_j) \tag{2.15}$$

Таким чином виконано формалізацію та обґрунтування вибору метрики для виявлення справжності ID-картки, зображення якої одержується з відеопотоку.

2.3. Архітектура комп’ютерної системи розпізнавання справжності ID-карток

Комп’ютерну систему розпізнавання справжності ID-карток пропонується реалізувати на основі міні-комп’ютера Raspberry PI. Даний пристрій дає змогу

виконувати функції щодо встановлення підробок ідентифікаційних документів працівників за допомогою моделі розпізнавання, яка зберігається на носії типу SD-картки і реалізовує порівняння шаблонів справжніх ID-карток і захоплених з відеокамери. Таким чином можна забезпечити авторизацію доступу працівників до певних об’єктів. Архітектурно комп’ютерна система включає наступні програмно-апаратні модулі:

– однокристальний пристрій опрацювання даних на базі Raspberry PI;

– пристрій захоплення відеопотоку « Raspberry PI Camera Module»;

– пристрої для контролю та управління у вигляді кінцевих пристроїв типу смартфона або термінального комп’ютера;

– носій інформації у вигляді SD-карти.

Raspberry PI виконує функції керування зовнішніми периферійними пристроями. Крім того, за допомогою цього пристрою забезпечується доступ до мережі Інтернет з використанням вбудованого WiFi компоненту, що з’єднується з роутером існуючої комунікаційної інфраструктури підприємства. Передбачається, що Raspberry PI виконує запуск програмної моделі виявлення справжності ID-карток з носія інформації – SD-карти, що безпосередньо приєднана до нього.

За допомогою камери, під’єднаної до Raspberry PI, виконується захоплення зображення ID-картки. Після цього, воно передається у компонент опрацювання і виконує інтелектуальне розпізнавання шляхом порівняння на основі відомих еталонних патернів карток з вхідним зразком зображення.

Можливість зовнішнього контролю процесу перевірки справжності ID-карток і трансляції відео авторизованими користувачами забезпечуються кінцевими пристроями (смартфон або інший термінал). Доступ до камери можна одержати як зсередини підприємства через локальну комп’ютерну мережу, так і ззовні через мережу Інтернет. На найвищому концептуальному рівні архітектуру комп’ютерної системи виявлення справжності ID-карток представлено на рис. 2.3.

Реалізація комп’ютерної системи розпізнавання справжності ID-карток із застосування індексу структурної подібності передбачає реалізацію програмної моделі в основі якої лежать глибокі нейронні мережі.

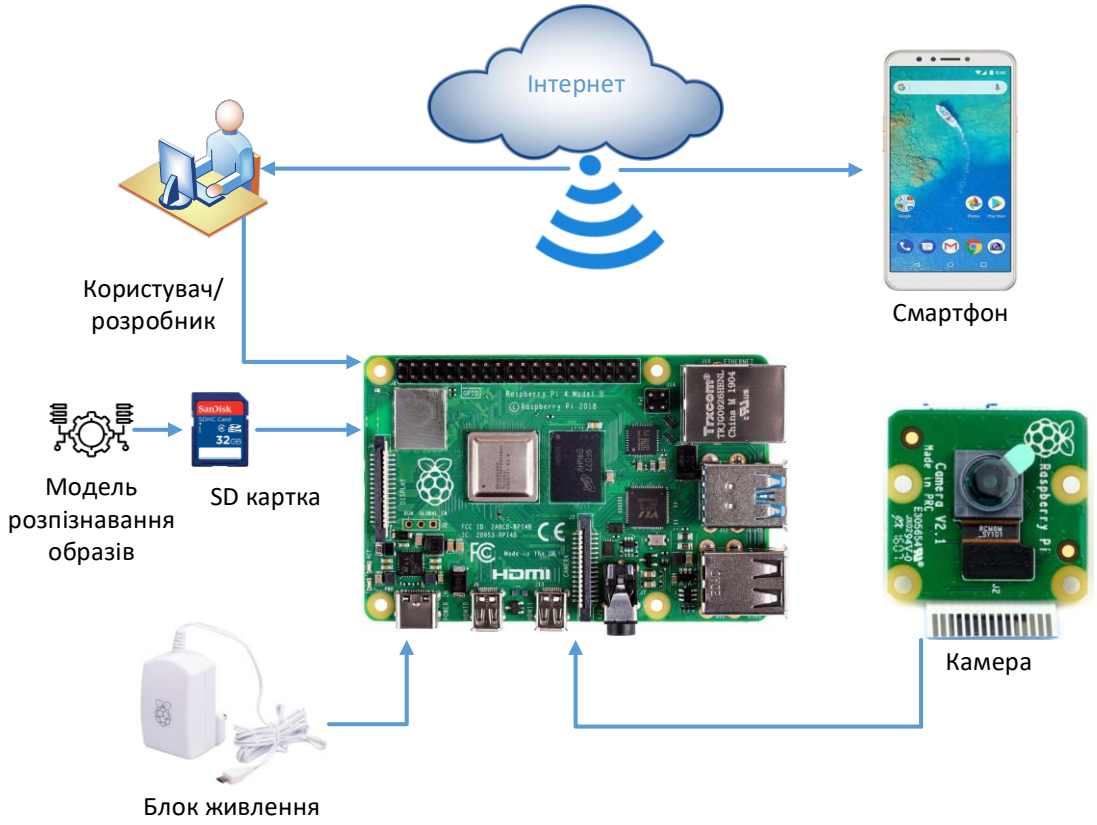

Рис. 2.3. Архітектура комп’ютерної системи виявлення справжності ID-карток

Для впровадження системи, показаної на рис. 2.3., необхідно провести навчання мережі за допомогою різних наборів даних, які були проаналізованими у першому розділі кваліфікаційної роботи. Це дозволить провести порівняння якості застосування індексу структурної подібності зображень та підходу глибоких нейронних мереж. Аналіз та обґрунтування вибору архітектури нейронної мережі проводиться нижче.

2.4. Архітектура та моделі нейронних мереж для встановлення справжності ID-карток

Характерною особливістю у сфері комп’ютерного зору є інтенсивне застосування різного типу та архітектур нейронних мереж, починаючи від примітивної реалізації на основі багатошарового перцептрону до глибоких нейромереж з великою кількістю шарів та нейронів у них. Перевагою використання

підходу Deep Learning є те, що вони здатні значно підвищити ефективність алгоритмів розпізнавання зображень подібно, або навіть краще за людський мозок.

Реалізація підходу глибокого навчання передбачає застосування різних типів моделей та архітектур з прямими і зворотними зв'язками. До них належать штучні нейромережі прямого поширення, autoencoders, мережі з рекурентними зв'язками та навчанням з підкріпленням.

Високу ефективність опрацювання зображень, одержаних з відеопотоку, показує такий клас як згорткові нейронні мережі, які є надзвичайно популярними та використовуваними при розв'язанні задач комп'ютерного зору. Вони відносяться до класу deep neural network, а сферою застосування може бути:

– класифікація та розпізнавання об'єктів на зображеннях та у відеопотоці у різних видах діяльності;

– аналіз зображень при діагностиці хвороб у медичній галузі;

– опрацювання природньої мови у вигляді тексту.

Наведений вище перелік не є повним, і використання CNN залежить від творчості та кваліфікації фахівців з інтелектуального аналізу інформації.

Під згорткою, у відповідному класі нейронних мереж, розуміють деяку лінійну математичну функцію, що інтерпретує добуток двох окремих функцій у результаті чого утворюється ще одна функція, яка описує яким чином перша змінює стан другої і навпаки.

На практиці операція згортки трактується як множення двох матриць якими представляються вхідні зображення і у результаті виконання якої одержують добуті із зображення обриси об'єктів.

Реалізація операції згортки у нейронних мереж передбачає застосування двох технік: «Padding» і «Striding». Коли вікно визначеного розміру, яке є фільтром, пересувається по зображенню (пікселях), то крайні пікселі зображення фактично не беруться до уваги. Це призводить до того, що змінюється розмір матриці ознак, наприклад матриця $5 * 5$ стає матрицею $3 * 3$. У такому випаду, пікселі, які знаходяться по краях зображення ніколи не опиняються у центрі вікна. Тому

важливо забезпечити, що розміри вхідного та вихідного представлення зображень співпадали. На рис. 2.4 показано графічну інтерпретацію операції згортки.

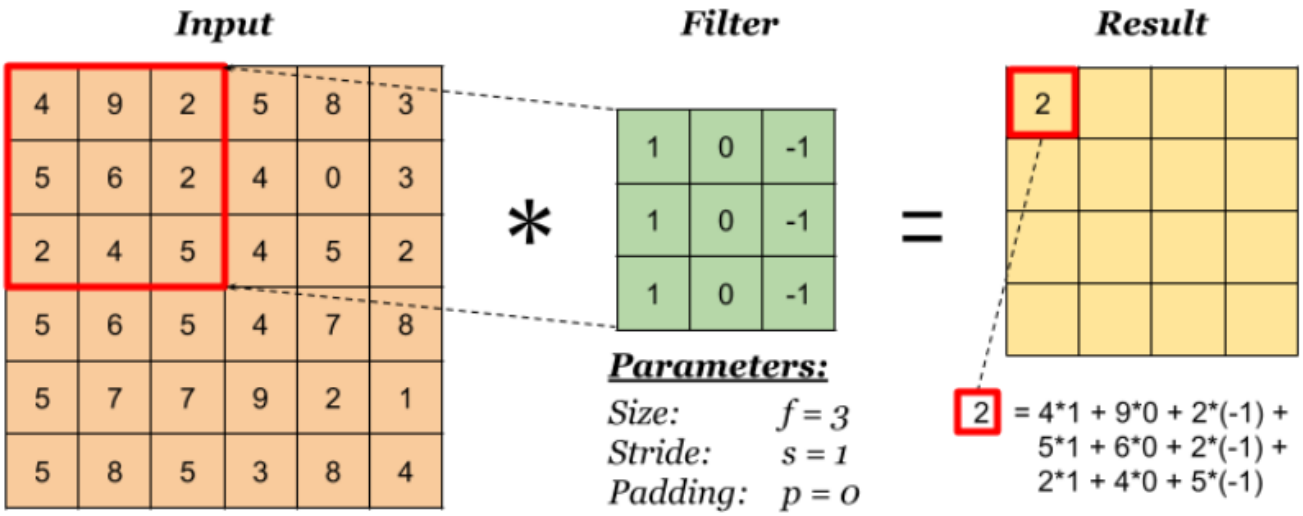

Рис. 2.4. Візуальне представлення операції згортки

Техніка «Padding» дозволяє додати до країв зображення фейкові пікселі, які в матричній інтерпретації, зазвичай, приймають нульове значення. У результаті цієї маніпуляції, фільтр рухаючись по зображенню забезпечує можливість реальним крайнім пікселям попадати в центральну область вікна, а далі пересуватись до фейкових пікселів, які фактично є поза розмірами зображеннями. Це забезпечує створення результуючої матриці, яка відповідає розмірам вхідного зображення.

Умовно, структуру ЗНМ можна представити у вигляді двох комплексних компонентів:

– структура, що визначає операцію згортки і дозволяє виявити множину ознак зображень у результаті його аналізу(«features extraction»);

– «fully connected» або повнозв’язний шар виконує прогнозування або класифікацію ознак зображення на основі попередньо виконаної операції згортки.

Структуру типової узагальненої моделі згорткової нейронної мережі показано на рис. 2.5.

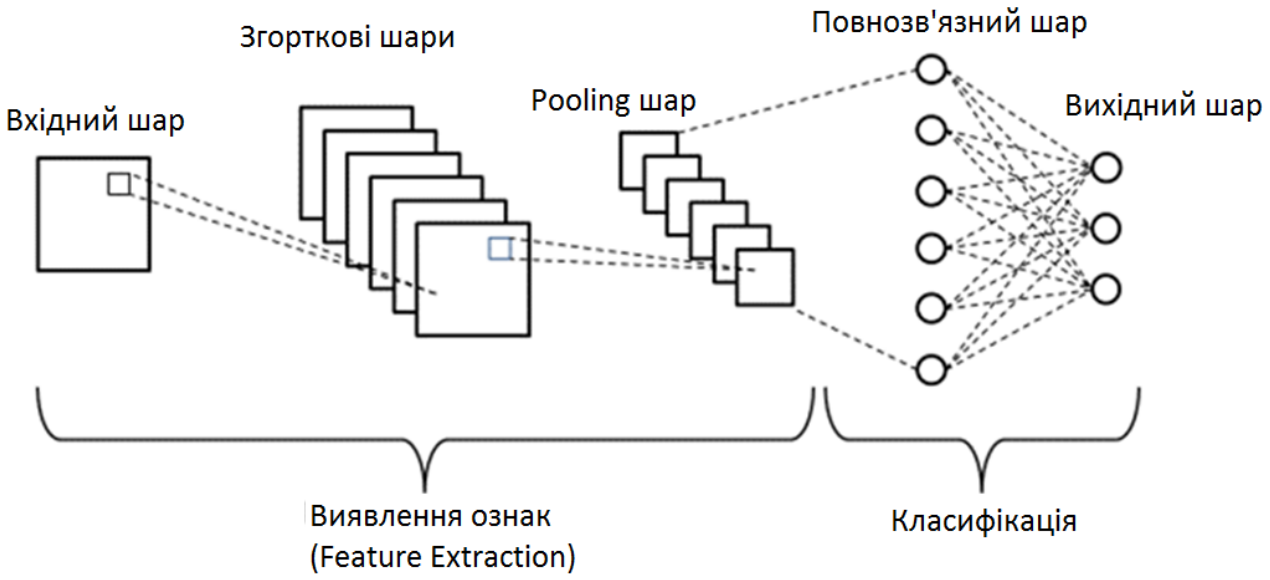

Рис. 2.5. Узагальнена структура моделі ЗНМ

Як видно з рис. 2.5, для згорткової нейронної мережі характерним є наявність основних трьох видів шарів:

– шари, що забезпечують виконання операції згортки (згорткові шари);

– шари, які виконують максимізацію або усереднення значень матриці при зменшенні її розмірності («Max Pooling», «Average Pooling layers»);

– повнозв’язний шар, усі нейрони якого формують зв’язок з нейронами вихідного шару.

В залежності від кількості та розміру описаних вище шарів будуються різні архітектури нейронних мереж, в основі яких лежить операцій згортки. Варто відміти, що до складу ЗНМ включаються функції активації нейронів та шар видалення, так званий drop out layer.

Як було зазначено раніше, основним призначенням згорткового шару є виявлення властивостей та ознак із вхідного зображення. Математично дана операція застосовується до вхідного представлення зображення та квадратного вікна-фільтра заданого розміру. Шляхом переміщення фільтра по поверхні зображення отримують сукупність відповідних пікселів, які у нього потрапляють. Результати, що одержують на виході згорткового шару представляють собою карту ознак елементів зображення, які можна інтерпретувати як, наприклад, кут чи край

зображення. Далі, визначені у цьому шарі ознаки, передаються до наступних для виявлення додаткових особливостей графічних об’єктів.

У типовій архітектурі досліджуваної нейронної мережі наступним після згорткового, іде шар «Pooling». Він забезпечує зниження розміру, визначеної на попередньому кроці, карти ознак та забезпечує економне використання апаратних ресурсів. Досягти цих цілей можна шляхом мінімізації взаємозв’язків між шарами нейронної мережі, які можуть виконувати свої функції незалежно один від одного на кожній окремій карті властивостей зображень.

У «Pooling» шарі можуть застосовуватися кілька типів операцій для зниження кількості зв’язків між шарами. Найбільш широко вживаними техніками зниження кількості зв’язків між шарами є формування карти ознак на основі знайдених максимальних значень у вікні фільтра («MaxPooling») або середніх значень («Average Pooling»). Сумарне значення елементів карти ознак формують за допомогою об’єднання локальних сум у вікні. Можна сказати, що шар зниження розмірності карти ознак виступає в якості моста між convolution layer та fully connected layer.

У повнозв’язному шарі формуються синаптичні ваги нейронів і відхилення, які показують рівень помилок. Ці дані дозволяють з’єднати нейрони двох різних шарів. Fully connected шари створюють на фронті вихідного шару, що формують завершальні рівні архітектури згорткової нейронної мережі.

Далі, представлення вхідного зображення згладжується і передається до повнозв’язного шару. Над векторним представленням графічного об’єкту виконується математичні операції у кількох повнозв’язних шарах, а після цього стартує свою роботу класифікатор або регресор.

При підключенні усіх функцій до повнозв’язного шару може відбуватись такий негативний процес як перенавчання. Це провокує виникнення ситуації, коли побудована модель видає точні і стабільні результати на тренувальній вибірці даних, але показники стають дуже поганими при застосуванні моделі до нових даних. Розв’язанням цього негативного явища займається шар «Dropout». Основною задачею цього шару є відкидання певної кількості нейронів при навчанні

згорткової нейронної мережі, що дозволяє зменшити розмір моделі та уникнути такого негативного явища як запам’ятовування. Емпірично встановлено, що застосування рівня відсіву є ефективним, коли участь в навчанні не беруть до 30% нейронів, обраних випадковим чином.

Одним з найважливіших параметрів згорткової нейронної мережі є функція активації. Її призначення полягає в тому, щоб забезпечити навчання та апроксимацію складних взаємозалежностей між параметрами моделі. По факту, функція активації встановлює правила і забезпечує нелінійну залежність при формуванні моделі та переході даних від шару до шару. До основних таких функцій належать: тангенс гіперболічний, різновиди сигмоїдної функції, функції активації SoftMax та ReLu.

При бінарній класифікації з використанням ЗНМ сигмоподібні функції та softmax показують кращі результати, ніж інші. При мультикласовій класифікації зазвичай застосовують функцію softmax.

Для забезпечення ефективності процесу виявлення графічних об’єктів різного розміру було запропоновано архітектуру «Single Shot MultiBox Detector», що використовує і базується на пірамідальній ієрархічній функції ЗНМ.

В основі піраміди зображень SSMBD лежить структура моделі VGG-16, яка вже попередньо натренована на наборі даних ImageNet. Ця базова модель використовується для виявлення корисних ознак на зображеннях. Однак на відміну від VGG16, модель SSMBD інтегрує кілька шарів, які дають можливість зменшити розмір карти ознак і представляти їх у вигляді пірамідальної форми зображень з різним масштабуванням. Перевагою такого підходу є те, що на початкових шарах нейронної мережі ефективно визначаються дрібні обриси об’єктів, що розташовані на великих за розміром і водночас дрібнозернистих картах об'єктів. З іншої сторони, невеликі за розміром, але з більшим розміром пікселів карти ознак дозволяють визначати об'єкти більшого розміру. У SSMBD добування ознак відбувається на кожному рівні піраміди з опрацюванням об’єктів, які відрізняються геометричними розмірами. Архітектура SSMBD показана на рис. 2.6.

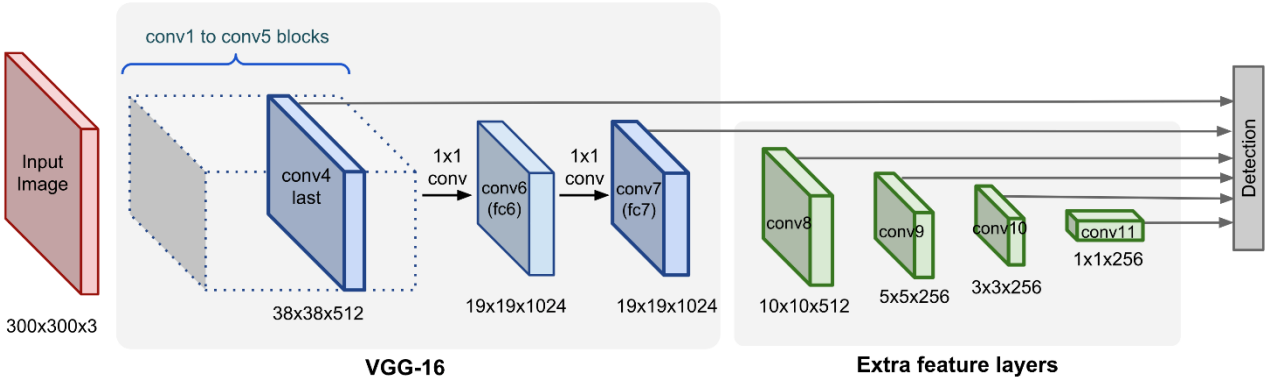

Рис. 2.6. Архітектура пірамідальної нейромережі

Якщо порівнювати архітектуру SSMBD з архітектурою YOLO, то вона не забезпечує розподілу зображення за координатною сіткою будь-якого розміру, однак здатна прогнозувати зсув попередньо виявлених опорних полів при довільному розміщенні карти ознак.

Застосування моделі згорткової нейронної мережі, що базується на архітектурі VGG16 дозволяє досягати точності при виявленні та класифікації об'єктів на зображеннях до рівня 92,7% на 5 кращих тестах набору даних ImageNet.

Основною відмінністю нейромережі на основі VGG16 від AlexNet є те, що вона використовує послідовно декілька фільтрів розміром 3×3, а не фільтри більшого розміру ядра, як в AlexNet, де розмір фільтру першого згорткового шару становить 11×11, а у другому 5×5. Графічне представлення моделі архітектури VGG-16 показано на рис. 2.7. Її можна і доцільно використовувати при розпізнаванні зображень, в тому числі і для виявлення справжності ID-карток.

Розмір зображення, що подається на вхідний шар нейронної мережі, представленої на рис. 2.7 повинен бути фіксованим і становити 224px*224px. Зображення повинно бути у форматі RGB.

Після того, як на вхідний шар подали зображення фіксованого розміру і формату, воно проходить через визначену кількість згорткових шарів з вікном фільтра 3px*3px.

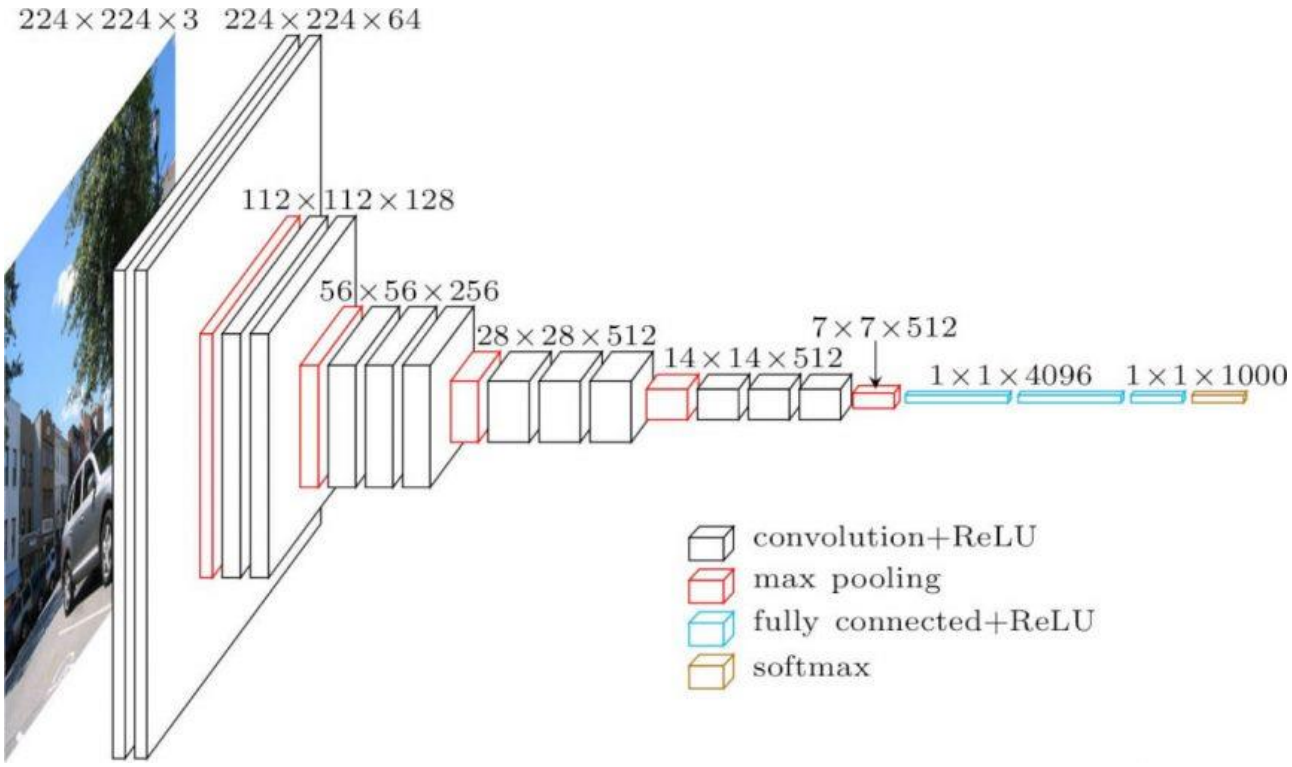

Рис. 2.7. Графічне представлення моделі VGG-16

Швидкість виконання операції згортки є фіксованою і становить 1 px, а відповідна роздільна здатність повинна зберігатись після проведення маніпуляцій у цих шарах, тобто крок переміщення по зображенню становить 1 px, а розмір вікна – 3px*3px.

П’ять шарів «Pooling» використовується при просторовому об'єднанні карт ознак. Ці шари вбудовують після згорткових і для стиснення використовується операція знаходження максимального значення («MaxPooling»). Фільтр у цьому шарі має розмір і крок кратний 2.

За множиною згорткових шарів в архітектурі VGG-16 також розташовуються 3 повнозв’язні шари. Вони можуть мати різну глибину при виконанні різних задач, однак, зазвичай, два перших рівні містять 4096 каналів, а фінальний – повнозв’язний шар, який забезпечує процес класифікації за 1000 класами. Останнім шаром VGG-16 є softmax. Характерною особливістю є те, що структура і конфігурація повнозв’язних шарів є ідентичною у всіх мережах. Рис. 2.8 відображає зв’язність і будову шарів VGG-16.

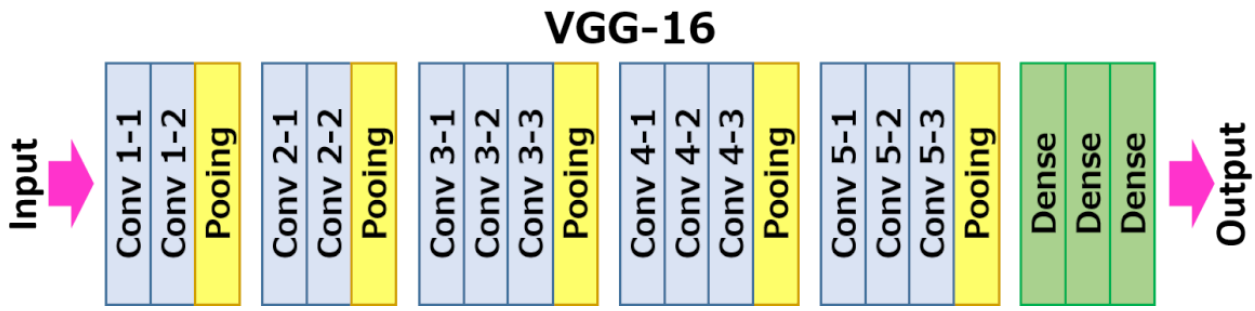

Рис. 2.8. Зв’язність і будова шарів VGG-16

Проте, застосування архітектури показаної на рис. 2.7. і рис. 2.8 володіє і недоліками, основні з них:

– неефективність процесу навчання – навчання мережі дуже повільне і тривале по часу;

– архітектура вимагає значних ресурсів дискового простору та пропускної здатності.

Враховуючи структурну складність архітектури VGG-16, її розмір становить понад 500 МБ. Тому для розв’язання прикладних задач по типу виявлення справжності ID-карток більш доцільно використовувати мобільні версії організації цієї згорткової нейронної мережі, зокрема TensoFlow, PyTorch, Keras, OpenCV та ін.

2.5. Висновки до розділу

У даному розділі одержано наступні наукові та практичні результати:

1. Запропоновано метод ідентифікації справжності ID-карток, який базується на визначенні індексу структурної подібності зображень і враховує комплекс із трьох властивостей: яскравості, контрастності та структурних елементів графічного представлення ID-карток і дає змогу підвищити ефективність процесу виявлення шахрайства шляхом використання меншої кількості апаратних ресурсів та забезпечує точність ідентифікації на рівні не нижче, ніж 85%.

2. Запропоновано архітектурне рішення для авторизації працівників на основі ID-карт, що включає в себе апаратну складову з використанням міні-комп’ютера на базі Raspberry PI та камери з роздільною здатністю 2 Мп, а також програмну модель виявлення справжності ідентифікаційного документу працівника, що дають змогу забезпечити продуктивність та функціональну зручність при аутентифікації до приміщень з обмеженим доступом.

3. Обгрунтовано застосування альтернативного підходу до виявлення шахрайства з ID-картками, який базується на основі використання глибоких нейронних мереж на основі VGG-16 і дає змогу, шляхом її донавчання, забезпечити високу точність ідентифікації користувачів на основі технологій комп’ютерного зору.

РОЗДІЛ 3
ПРОГРАМНА РЕАЛІЗАЦІЯ ІНДЕКСУ ПОДІБНОСТІ ЗОБРАЖЕНЬ ПРИ АНАЛІЗІ ID-КАРТОК КОРИСТУВАЧІВ

3.1. Розробка алгоритму виявлення справжності ID-картки

Комп'ютерний зір – це область штучного інтелекту, яка навчає комп'ютери інтерпретувати та розуміти візуальний світ. Використовуючи цифрові зображення та відео з камер і моделі глибокого навчання, машини можуть точно ідентифікувати та класифікувати об’єкти, а потім реагувати на те, що вони «бачать».

Завдання комп'ютерного зору включають методи отримання, обробки, аналізу та «розуміння» цифрових зображень Комп'ютерний зір при обробці зображень головним чином орієнтований на опрацювання вихідних і вхідних зображень для їх покращення або підготовку до виконання інших завдань. Дана сфера орієнтована на добування інформації з вхідних зображень або відео для належного розуміння їх для прогнозування за принципом людського мозку.

Метою даного розділу є імплементація програмної моделі на основі структурного індексу схожості зображень щодо ідентифікації справжності ID-карток за допомогою комп’ютерного зору.

Прикладною стороною цієї реалізації є забезпечення можливості організаціям визначити, чи є ідентифікатор, надана працівниками або клієнтам оригінальною чи ні.

Для цього пропонується обчислювати структурну подібність оригінальної ID-карти та картки, завантаженої користувачем. Подібним чином за допомогою опрацювання зображень із застосуванням прийомів комп’ютерного зору буде реалізовано можливість виявлення того, чи є зображення ID-картки оригінальним чи підробленим, тобто розв’язується задача виявлення шахрайства.

Алгоритм ідентифікації справжності ID-картки працівника пропонується реалізувати за допомогою мови програмування Python та відповідних бібліотек, які

підтримують застосування індексу структурної подібності зображень. Послідовність дій включає виконання наступних кроків:

1. Імпорт необхідних бібліотек.
2. Захоплення зображення фальсифікованої та оригінальної ID-картки.
3. Зменшення розміру і форми підробленого зображення як оригінального зображення.
4. Зчитування оригінальної та не справжньої ID-картки.
5. Перетворення кольорового зображення у зображення з відтінками сірого.
6. Застосування техніки індексу структурної подібності (SSIM) між двома зображеннями.
7. Обчислення порогу і контурів зображення.
8. Аналіз контурів та порогових значень зображень у режимі реального часу.

Імпорт необхідних для проведення дослідження бібліотек наведено у лістингу 1.1.

Лістинг 1.1. Імпорт бібліотек

```
from skimage.metrics import structural_similarity
import imutils
import cv2
from PIL import Image
import requests
```

Skimage представляє собою Python-пакет з відкритим вихідним кодом, який, у даному випадку, буде використовуватися для імплементації методів опрацювання зображень. З бібліотеки imutils можна викликати багато зручних функцій, які полегшують основні функції обробки зображень, такі як переформатування, обертання, зміна розміру та відображення зображень за допомогою OpenCV.

Бібліотека OpenCV («Open Source Computer Vision Library») – це бібліотека функцій програмування, яка у практичній частині кваліфікаційної роботи забезпечує такі основні функції, як читання та запис зображень за допомогою cv2.

Бібліотека зображень PIL – це безкоштовна додаткова бібліотека з відкритим кодом для мови програмування Python, яка додає підтримку відкриття, маніпулювання та збереження багатьох різних форматів файлів зображень.

Далі необхідно створити каталоги і підкаталоги для зберігання зображень. Це можна зробити вручну за допомогою лістингу 3.2.

Лістинг 3.2. Створення каталогів зображень

```
!mkdir pan_card_tampering
!mkdir pan_card_tampering/image
```

Для добування і завантаження оригінального та шахрайського зображення ID-картки з різних джерел виконується лістинг 3.3.

Лістинг 3.3. Завантаження оригінальної та підробленої ID-картки

```
original =
Image.open(requests.get('https://www.thestatesman.com/wp-
content/uploads/2019/07/pan-card.jpg', stream=True).raw)
tampered = Image.open(requests.get('https://assets1.cleartax-
cdn.com/s/img/20170526124335/Pan4.png', stream=True).raw)
```

У наведеному вище фрагменті коду, зображення завантажуються з різних джерел за допомогою бібліотеки запитів. Для аналізу властивостей завантажених оригінальних та наданих користувачем зображень використовується наступний програмний код (лістинг 3.3.).

Лістинг 3.3. Вивід властивостей оригінального та підробленого зображень

```
# The file format of the source file.
print("Original image format : ",original.format)
print("Tampered image format : ",tampered.format)
# Image size, in pixels. The size is given as a 2-tuple (width,
height).
print("Original image size : ",original.size)
print("Tampered image size : ",tampered.size)
```

У результаті запуску програмного коду лістингу 3.3 показано на рис. 3.1.

```
Original image format :  JPEG
Tampered image format :  PNG
Original image size :  (1200, 800)
Tampered image size :  (282, 179)
```

Рис. 3.1. Властивості зображення оригінальної та шахрайської ID-карт

З результатів показаних на рис. 3.1, можна побачити, що вихідний розмір оригінального зображення та вихідний розмір підробленого зображення різні. Це в перспективі може призвести до небажаних/хибних результатів під час опрацювання зображень. Тому доцільно застосувати техніку зменшення масштабу зображення для приведення їх до однакової форми.

Перетворення формату підробленого зображення у відповідності до оригінальної ID-картки показано у лістингу 3.4.

Лістинг 3.4. Зміна формату та розміру зображень ID-карти

```
# Resize Image
original = original.resize((250, 160))
print(original.size)
original.save('pan_card_tampering/image/original.png')
#Save image
tampered = tampered.resize((250,160))
print(tampered.size)
tampered.save('pan_card_tampering/image/tampered.png')
#Saves image
```

Результат виконання щодо приведення зображень оригінальної та фальсифікованої ID-карток показано на рис. 3.2.

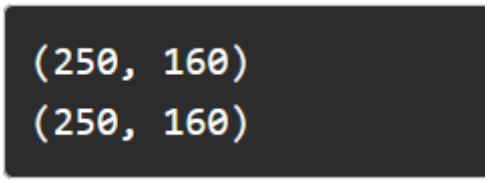

Рис. 3.2. Результат приведення зображень до однакового розміру

Тепер геометрична форма обох зображень (оригінальне зображення та підроблене) змасштабовано до однакового розміру – 250*160 пікселів. Це сприяє більш ефективному їхньому опрацюванню, ніж це було раніше. Також для забезпечення однорідності форматів зображень і виводу їх на екран виконано програмний код, наведений у лістингу 3.5.

Лістинг 3.5. Приведення зображень до однорідності формату

```
# Change image type if required from png to jpg
tampered = Image.open('pan_card_tampering/image/tampered.png')
tampered.save('pan_card_tampering/image/tampered.png')#can do
png to jpg
```

На рис. 3.3 і рис. 3.4 показано оригінальну ID-карту та зображення картки наданої працівником чи користувачем системи.

Рис. 3.3. Вигляд оригінального зображення ID-карти

Рис. 3.4. Вигляд ID-карти, наданої користувачем

Далі потрібно зчитати зображення з використанням бібліотеки OpenCV для подальшого опрацювання, як приведено у лістингу 3.6.

Лістинг 3.6. Зчитування зображень за допомогою OpenCV

```
# load the two input images
original = cv2.imread('pan_card_tampering/image/original.png')
tampered = cv2.imread('pan_card_tampering/image/tampered.png')
```

Тепер у наведеному вище коді зчитуються обидва зображення (оригінальне та підроблене) за допомогою функції imvred (cv2). Далі потрібно перетворити їх з кольорового зображення у відтінки сірого (лістинг 3.7).

Лістинг 3.7. Перетворення зображення у відтінки сірого

```
# Convert the images to grayscale
original_gray = cv2.cvtColor(original, cv2.COLOR_BGR2GRAY)
tampered_gray = cv2.cvtColor(tampered, cv2.COLOR_BGR2GRAY)
```

У наведеному вище коді виконано перетворення вихідні зображення (оригінальної ID-картки та картки, наданої користувачем) у зображення сірого кольору за допомогою функції cv2 cvtColor (), параметр якої-cv2.COLOR_BGR2GRAY.

Конвертація зображень у відтінки сірого дуже корисна функція опрацювання зображень, тому що при обробці кольорової графіки багато програм не дозволяють визначити таких важливих властивостей як контури. Окрім цього, самі кольорові зображення є складнішими у представленні і «розумінні» комп'ютерами, оскільки вони формуються трьома каналами, а відтінки сірого мають лише 1 канал.

3.2. Програмна реалізація техніки індексу структурної подібності ID-карток

Індекс структурної схожості (SSIM) – це перцептивна метрика, яка кількісно визначає деградацію якості зображення, що спричинена таким опрацюванням, як стиснення даних або втрати при передачі даних.

Застосування цієї метрики передбачає наявність двох зображень з одного знімка, що інтерпретує два графічно ідентичних зображення людського ока. Друге зображення, як правило, стиснене або має іншу якість, що зумовлює застосування такого індексу.

SSIM, зазвичай, використовується у відеоіндустрії, але також є ефективним при опрацюванні фотографій. Індекс структурної подібності фактично вимірює різницю сприйняття між двома подібними зображеннями. Він не може судити, що з двох краще: це слід зробити на основі одержаних результатів, знаючи, який з них є оригінальним і який піддався додатковій обробці, такій як стиснення або фільтр.

Для обчислення індексу структурної подібності зображень необхідно реалізувати програмний код, що представлений лістингом 3.8.

Лістинг 3.8. Програмна реалізація індексу структурної подібності

```
# Compute the Structural Similarity Index (SSIM) between the
two images,
# ensuring that the difference image is returned

(score, diff) = structural_similarity(original_gray,
tampered_gray, full=True)
diff = (diff * 255).astype("uint8")
print("SSIM Score is : {}".format(score*100))
if score >= 80:
    print ("The given pan card is original")
else:
    print("The given pan card is tampered")
```

Результат обчисленого індексу подібності двох зображень ID-карток, представлених на рис. 3.3 і рис. 3.4, показано на рис. 3.5.

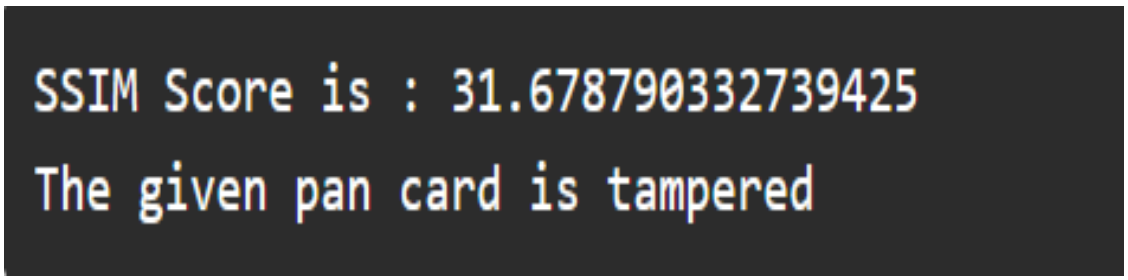

Рис. 3.5. Обчислений індекс схожості ID-карток

Індекс структурної подібності допомагає точно визначити, де з точки зору розташування координат x та y є відмінності у зображеннях. У даному випадку задача поставлена знайти подібність між оригінальним та підробленим зображенням.

Чим нижчий показник SSIM, тим нижче схожість, тобто оцінка SSIM прямо пропорційна подібності між двома зображеннями. У випадку, коли задано одне порогове значення "45", тобто, якщо будь -який показник> = 80, він буде вважатися оригінальною карткою, інакше підробленою.

Як правило, значення SSIM, що знаходиться в діапазоні 0,97-0,99 говорить про високу ефективність методів реконструкції якості.

3.3. Виявлення контурів об’єктів на зображеннях

Виявлення контурів об’єктів на зображеннях – це процес, який можна пояснити просто як криву, що з'єднує всі безперервні точки (разом з контуром), мають однаковий колір або інтенсивність. Алгоритм дійсно знаходить контури зображень, але також розміщує їх в ієрархії (лістинг 3.9).

Лістинг 3.9. Визначення порогових значень і контурів об’єктів

```
# Calculating threshold and contours
thresh = cv2.threshold(diff, 0, 255, cv2.THRESH_BINARY_INV |
cv2.THRESH_OTSU)[1]
cnts = cv2.findContours(thresh.copy(), cv2.RETR_EXTERNAL,
cv2.CHAIN_APPROX_SIMPLE)
cnts = imutils.grab_contours(cnts)
```

У даному випадку використовується порогова функція комп’ютерного зору, яка застосовує адаптивний поріг до зображення, яке зберігається у масиві форм.

Ця функція перетворює зображення у відтінках сірого в двійкове представленні за допомогою математичної формули. Пошук контурів працює над двійковим зображенням та відповідно одержує їх. Ці контури є ефективними критеріями при аналізі форми та розпізнавання об’єктів. Для створення обмежень на значення контурів реалізовано лістинг 3.10.

Лістинг 3.10. Встановлення обмежень на контури зображення

```
# loop over the contours
for c in cnts:
    # applying contours on image
    (x, y, w, h) = cv2.boundingRect(c)
    cv2.rectangle(original, (x, y), (x + w, y + h), (0, 0,
255), 2)
    cv2.rectangle(tampered, (x, y), (x + w, y + h), (0, 0,
255), 2)
```

Обмежуючий прямокутник допомагає знайти відношення ширини до висоти обмежуючого прямокутника об'єкта. Спочатку виконується обчислення параметрів обмежувальної рамки контуру, а потім власне безпосередньо вона візуалізується на обох вхідних зображеннях. Це дозволяє сформувати більш зручне представлення для порівняння зображень (лістинг 3.11).

Лістинг 3.11. Формування рамок довкола об’єктів

```
#Display original image with contour
print('Original Format Image')
original_contour = Image.fromarray(original)
original_contour.save("pan_card_tampering/image/original_conto
ur_image.png")
original_contour
#Diplay tampered image with contour
print('Tampered Image')
tampered_contour = Image.fromarray(tampered)
tampered_contour.save("pan_card_tampering/image/tampered_conto
urs_image.png")
tampered_contour
```

У результаті проведеного експерименту, одержано зображення, як показано на рис. 3.6.

Рис. 3.6. Рамки на контурах виявлених об’єктів ID-картки

У наведеному вище результаті, можна побачити, що вихідне зображення показано з контурами (обмежувальними рамками) за допомогою функції:

```
fromarray ().
```

Крім того, можна просто зберегти зображення за допомогою функції:

```
save ().
```

Наступний крок полягає у накладанні рамок на контури об’єктів ID-картки, наданої користувачем. Лістинг 3.12 демонструє формування такого контуру.

Лістинг 3.12. Формування контуру на ID-картці користувача

```
#Diplay tampered image with contour
print('Tampered Image')
tampered_contour = Image.fromarray(tampered)
tampered_contour.save("pan_card_tampering/image/tampered_conto
urs_image.png")
tampered_contour
```

У результаті, одержуємо зображення ID-картки, як показано на рис. 3.7.

Рис. 3.7. Контури користувацької ID-картки

Далі співставимо еталонний варіант ID-картки і картку, яка надана користувачем. Можна помітити, що деякі з контурів відсутні на підробленій ID-картці. На рис. 3.8 показано ілюстрацію вищезазначеного результату.

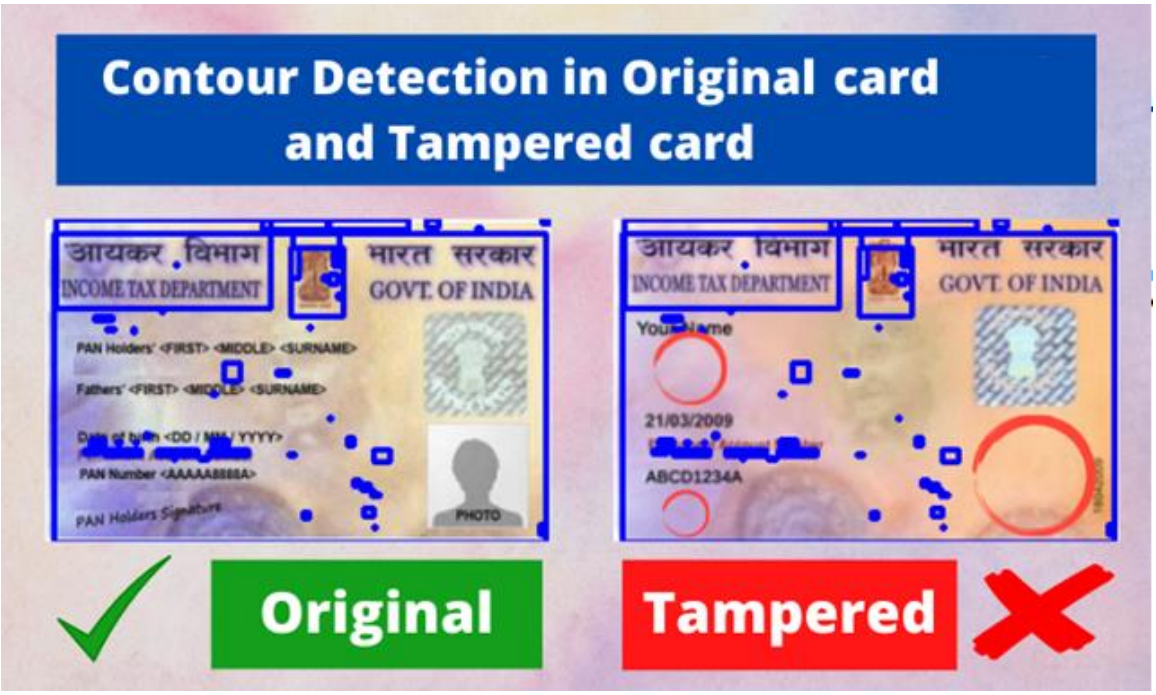

Рис. 3.8. Порівняння виявлених контурів об’єктів еталонної та підробленої ID-картки

Наступний крок полягає у приведенні еталонної (справжню) ID-картки до формату з відтінками сірого. Для цього виконаємо лістинг 3.13.

Лістинг 3.13 Представлення еталонної картки у відтінках сірого

```
# Display difference image with black

print('Different Image')
difference_image = Image.fromarray(diff)
difference_image.save("pan_card_tampering/image/difference_ima
ge.png")
difference_image
```

На рис. 3.9 показано еталонну ID-картку у форматі відтінки «сірого».

Рис. 3.9. Візуалізація ID-картки у відтінках сірого

Ще один дуже інтерактивний спосіб показати контури об’єктів із застосуванням теплової карти, тобто шляхом знаходження так званої «теплої» зони (зона тексту/зображення) та нормальної зони (без тексту/зображення).

Тепла зона, у даному випадку зона з текстом/зображеннями, буде відображатися в темній (чорній) області, а інша – як світла (свого роду біла) зона (лістинг 3.14).

Лістинг 3.14. Визначення теплових зон ID-карток

```
#Display threshold image with white

print('Threshold Image')
threshold_image = Image.fromarray(thresh)
threshold_image.save("pan_card_tampering/image/threshold_image
.png")
threshold_image
```

Результат застосування теплової карти у монохромному представлено на рис. 3.10.

Рис. 3.10. Монохромне відображення ID-картки за допомогою теплової карти

У даному випадку все однаково. Можна побачити, що це зміна ролі кольору, де білий показує нагріту зону, а чорний – нормальну зону.

Виявлення структурної подібності зображень допомагає визначити відмінності чи подібності у формі зображень. Схожим чином, визначення порогового значення та контурів об’єктів на його основі для зображень, які конвертовані у бінарний колір з відтінками сірого, також допомагає в аналізі форми та розпізнаванні аномалій.

Оскільки індекс структурної подібності SSIM становить ~ 31,2%, то можна сказати, що надане користувачем зображення ID-картки є підробленим або шахрайським.

При реалізації моделі виявлення шахрайства на основі комп’ютерного зору вдалося візуалізувати відмінності та подібності між зображеннями за відповідними контурами об’єктів, відмінностями та пороговими значеннями.

Дана модель може бути застосована у різних організаціях, де клієнтам або користувачам необхідно надати будь -який ідентифікатор, щоб пройти авторизацію. Окрім цього, за допомогою реалізованого програмного компоненту можна виявляти шахрайські дії.

3.4. Висновки до розділу

1. Розроблено алгоритм виявлення шахрайства з ID-картками, який включає в себе виконання основних 8 кроків і забезпечує можливість визначення та побудови контурів об’єктів, наявних на ID-картці.

2. Засобами мови програмування Python реалізовано програмну модель, яка на основі індексу структурної подібності зображень дозволяє виявити відмінності між еталонною ID-карткою і фальсифікованою.

3. Оптимізовано програмну реалізацію індексу структурної подібності зображень шляхом перетворення кольорового зображення у формат з відтінками сірого, що дозволяє використовувати лише один канал при аналізі контурів і теплових карт ідентифікатора користувачів.

РОЗДІЛ 4
ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

4.1. Охорона праці

Метою кваліфікаційної роботи магістра є дослідження методів і засобів ідентифікації ID-карток на основі технологій комп’ютерного зору. Оскільки, усі етапи такого дослідження передбачають використання комп’ютерної та оргтехніки, то актуальним є аналіз та дотримання вимог з охорони праці і техніки безпеки при роботі з ПК.

Для забезпечення ефективності та оптимізації роботи фахівців щодо впровадження системи ідентифікації ID-карток на основі технологій комп’ютерного зору необхідно організувати безпечні умови праці. При цьому безпосередню відповідальність за порушення нормативно-правових актів з охорони праці несуть як інженери з проектування, так і їх керівники [23, 24].

Окрім цього, на робочих місцях осіб які проектують систему ідентифікації необхідно забезпечити дотримання вимог НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями».

Згідно НПАОП 0.00-7.15-18 приміщення, де розміщені робочі місця операторів, крім серверних, мають бути оснащені системою автоматичної пожежної сигналізації відповідно до вимог:

– переліку однотипних за призначенням об'єктів, які підлягають обладнанню автоматичними установками пожежогасіння та пожежної сигналізації,;

– Державних будівельних норм "Інженерне обладнання будинків і споруд.

В інших приміщеннях допускається встановлювати теплові пожежні сповіщувачі. Приміщення, де розміщені робочі місця інженерів, мають бути оснащені вогнегасниками, кількість яких визначається згідно з вимогами Типових норм належності вогнегасників, затверджених наказом Міністерства України з питань надзвичайних ситуацій.

Приміщення, в яких розміщуються робочі місця операторів сервера загального призначення, обладнуються системою автоматичної пожежної сигналізації та засобами пожежогасіння відповідно до вимог ДБН В.1.1-7-2016, ДСТУ Б.В.1.1-36:2016, НАПБ А.01.001-2014 і вимог нормативно-технічної та експлуатаційної документації виробника. Проходи до засобів пожежогасіння мають бути вільними.

Лінія електромережі для живлення комп'ютерів та периферійних пристроїв повинні бути виконаними як окрема групова трипровідна мережа шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Нульовий захисний провідник використовується для заземлення (занулення) електроприймачів. Не допускається використовувати нульовий робочий провідник як нульовий захисний провідник. Нульовий захисний провідник прокладається від стійки групового розподільного щита, розподільного пункту до розеток електроживлення. Не допускається підключати на щиті до одного контактного затискача нульовий робочий та нульовий захисний провідники.

Площа перерізу нульового робочого та нульового захисного провідника в груповій трипровідній мережі має бути не менше площі перерізу фазового провідника. Усі провідники повинні відповідати номінальним параметрам мережі та навантаження, умовам навколишнього середовища, умовам розподілу провідників, температурному режиму та типам апаратури захисту, вимогам ДСТУ Б В.2.5-82:2016.

У приміщенні, де одночасно експлуатуються понад п'ять комп'ютерів, на помітному та доступному місці встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення.

Комп'ютери повинні підключатися до електромережі тільки за допомогою справних штепсельних з'єднань і електророзеток заводського виготовлення.

У штепсельних з'єднаннях та електророзетках, крім контактів фазового та нульового робочого провідників, мають бути спеціальні контакти для підключення нульового захисного провідника. Їхня конструкція має бути такою, щоб приєднання нульового захисного провідника відбувалося раніше, ніж приєднання

фазового та нульового робочого провідників. Порядок роз’єднання при відключенні має бути зворотним.

Не допускається підключати комп’ютери до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв.

Електромережі штепсельних з'єднань та електророзеток для живлення комп’ютерної техніки повинні бути виконаними за магістральною схемою, по 3-6 з'єднань або електророзеток в одному колі.

Штепсельні з'єднання та електророзетки для напруги 12 В та 42 В за своєю конструкцією мають відрізнятися від штепсельних з'єднань для напруги 127 В та 220 В. Штепсельні з'єднання та електророзетки, розраховані на напругу 12 В та 42 В, мають візуально (за кольором) відрізнятися від кольору штепсельних з'єднань, розрахованих на напругу 127 В та 220 В.

При системи ідентифікації ID-карток на основі технологій комп’ютерного зору, важливим, з точки зору охорони праці, є забезпечення достатньої величини природного та штучного освітлення, які визначені у ДБН В.2.5-28 : 2018. „Природне і штучне освітлення”.

Організація робочого місця оператора ПК повинна забезпечувати відповідність усіх елементів робочого місця та їх розташування ергономічним вимогам.

Відстань від екрана до ока фахівців, які працюють за комп’ютером визначається згідно з вимогами НПАОП 0.00-7.15-18.

Розміщення принтера на робочому місці має забезпечувати добру видимість екрана комп’ютера, зручність керування пристроєм введення-виведення інформації в зоні досяжності моторного поля.

Таким чином, у результаті аналізу вимог щодо охорони праці користувачів комп’ютерів, визначено особливості організації робочих місць, вимог з електробезпеки, природного та штучного освітлення для ефективної і безпечної роботи фахівців з проектування і впровадження комп’ютерної системи ідентифікації ID-карток на основі технологій комп’ютерного зору.

4.2. Особливості роботи та розлади здоров’я користувачів комп’ютерів, що формується під впливом роботи за комп’ютером.

При роботі з комп’ютером протягом тривалого періоду часу, а також при недотриманні відповідних вимог охорони праці у користувачів спостерігаються розлади, які узагальнено назвою комп’ютерний зоровий синдром.

Комп’ютерний зоровий синдром (КЗС) – комплекс порушень здоров’я, який може виникати у користувачів персональних комп’ютерів (ПК) [26]. Діагноз ставлять, якщо людина, що працює за ПК протягом двох годин, висловлює хоча б дві з десяти скарг:

- головний біль;
- сльозотеча;
- різь;
- туман;
- двоїння;
- свербіж;
- важкість в очах;
- фотофобія;
- миготіння знаків на екрані;
- нудота.

У користувачів ПК дуже поширені кон’юнктивіти і блефарити, патогенетично пов’язані з КЗС.

Синдром розвивається при умові, що робоче місце організовано неправильно – у користувача незручне крісло, відсутні пюпітри для паперів, підставки для ніг та кистей рук, не встановлена висота і нахил монітора відносно очей, відстань від очей до екрана. За таких умов тіло людини при роботі займає вимушене положення: спина статично напружена, шия витягнута, плечі жорстко фіксовані. Напружені м’язи погіршують кровотік у сонних артеріях, а недостатнє кровозабезпечення головного мозку веде до очманіння, появи головного болю. На фоні шийного

остеохондрозу з’являється відчуття випирання очних яблук, туману в очах, мушок та райдужних кіл у полі зору. Розвитку КЗС сприяє поганий мікроклімат приміщення, значна загальна іонізація та мікробне забруднення, а також куріння.

Національною радою з наукових досліджень США для стану зорового дискомфорту був уведений термін "астенопія", який означає "будь-які суб'єктивні зорові симптоми чи емоційний дискомфорт, що є результатом зорової діяльності". Симптоми астенопії були класифіковані на "очні" (біль, печія та різь в очах, почервоніння повік та очних яблук, ломота у надбрівній частині тощо) та "зорові" (пелена перед очима, мерехтіння, швидка втома під час зорової роботи та ін.).

У операторів ВДТ "очні" симптоми трапляються частіше, ніж "зорові", причому частота проявів астенопії вища у жінок, ніж у чоловіків і більше виражена в осіб середнього і старшого віку. Причиною вважається електромагнітне випромінювання від ВДТ.

При роботі з ВДТ основне навантаження припадає на всі елементи зорового аналізатора.

Робота з ВДТ може призвести до розвитку короткозорості, так як у користувачів комп'ютерів, в основному, "працює" ближній зір.

При аналізі зорової роботи операторів ВДТ, встановлено, що через дві години частота флуктуацій акомодації зменшується, а внесок низькочастотної компоненти підвищується. Це може бути причиною скарг на втому зорового аналізатора. Тривала робота на ВДТ може призвести до розвитку короткозорості, оскільки у користувачів ВДТ головним чином "працює" ближній зір.

У 100 пацієнтів із 150, які працювали на ВДТ по шість годин на день протягом чотирьох років, були виявлені проблеми з фокусуванням зору.

Робота за комп'ютером характеризується також тим, що постійний напружений погляд на екран монітора зменшує частоту моргання. При цьому погіршується зволоження поверхні очного яблука сльозовою рідиною, яка захищає рогівку ока від висихання, пилу та інших забруднень. Це може призвести до виникнення так званого синдрому Сікка: рогівка висихає і мутніє, і як наслідок розвивається сліпота.

Також при напруженій зоровій роботі за ЕОМ можуть бути не лише порушення функції зору, а й виникнення головного болю, посилення нервово-психічного напруження, зниження працездатності.

Виникнення та розвиток патології зорової функції зумовлені:

1. Умовами зорової роботи на ВДТ (зменшення вільного руху очей, зменшення функціонального поля сітківки та ін.).

В природних умовах людина розглядає предмети, які знаходяться поблизу неї і на різних відстанях включно до горизонту (розслабляючи при цьому м'язи ока). Крім того, має місце вільний рух очей у всі боки. Відтак функціонує все поле сітківки ока. Різноманітні м'язи ока і різноманітні ділянки поля сітківки функціонують поперемінно, отримуючи можливість відновлювати свій функціональний потенціал. Умови зорової роботи при використанні ВДТ набагато жорсткіші, оскільки у користувача комп'ютера "працює" лише ближній зір, тому елементи ока, що його забезпечують знаходяться у постійному напруженні.

2. Змінами умов, характерних для традиційного зорового процесу читання (темні знаки на світлому фоні при падаючому світловому потоці), а також демонстрування зображення на майже вертикальній поверхні, що випромінює світловий потік, а отже, потребує пониженого загального освітлення на робочому місці. В деяких випадках ВДТ відтворює яскраві знаки на темному фоні (зворотнє зображення затруднює адаптацію);

3. Світлотехнічною різнорідністю об'єктів зорової роботи що пов'язана з наявністю трьох об'єктів (екран, клавіатура, документація), розташованих у різних зонах спостереження, що вимагає багаторазового переведення лінії зору від одного до іншого.

Умови роботи з ВДТ ускладнюються необхідністю постійної перебудови апаратів акомодації та конвергенції, не кажучи вже про постійну необхідність переадаптації від яскравих об'єктів з позитивним контрастом на темні — з негативним. Разом узяті всі ці особливості створюють багато незручностей, а також напруження м'язового та світловідчуваючого апарату очей;

4. Робота з пульсуючим самосвітним об'єктом, який постійно перебуває у центрі поля зору, що не відповідає нормативним вимогам щодо обмеження пульсації та засліпленості. Наявність пульсації яскравості знаків викликає дискомфорт і втому, загальну й здорову;

5. Несприятливим розподілом яскравості у полі зору (стеля, стіни, меблі тощо можуть виявитися світлішими, ніж центр поля зору - темний, обмежено освітлений та іноді малозаповнений знаками екран монітора);

6. Засліплююча дія світильників, які освітлюють приміщення на робочому місці з ВДТ більша, ніж на інших, бо лінія зору користувача при роботі з екраном майже горизонтальна, що призводить до зменшення кута дії різних засліплюючих джерел (світильники, вікна і т. п.) і, відповідно, до зростання засліпленості.

Висновок.

Отже, порушення зорових функцій користувачів ВДТ пов'язані, головним чином, з чотирма групами факторів:

– параметрами освітлення робочого місця;
– характеристиками дисплея;
– специфікою роботи на ВДТ;
– неправильною організацією робочого місця.

Уникнення негативних факторів впливу на здоров’я і життя користувачів можливе лише при дотриманні вимог і норм охорони праці та правильної організації робочого розпорядку та ергономіки робочого місця.

ВИСНОВКИ

Основні наукові та практичні результати полягають в наступному.

1. Проаналізовано основні поняття у сфері виявлення шахрайства, методи ідентифікації підозрілих об’єктів та поведінки користувачів, що дало змогу визначити потенційні шляхи та принципи ідентифікації ID-карток з використанням технологій комп’ютерного зору, які передбачають виконання п’яти стадій: формування сховища еталонних даних, формування асоціативних правил, аналіз шаблонів зображень, авторизацію користувацьких даних та формування сповіщень про загрозу.

2. Проведено аналіз сфер застосування підходів «fraud detection» і виявлено специфіку його організації у банківській галузі, сфері інформаційних технологій та інших прикладних областях, що дало змогу визначити сукупність комплексу апаратних і програмних засобів для ефективного їх впровадження.

3. Проаналізовано відкриті набори даних зображень, накопичених компаніями, що займаються інженерією даних і впровадженням елементів комп’ютерного зору, що дало змогу обґрунтувати доцільність їхнього застосування при виявленні справжності ID-карток користувачів у віртуальному просторі та ідентифікаційних документів при авторизації працівників для доступу у приміщення з обмеженими правами доступом.

4. Запропоновано метод ідентифікації справжності ID-карток, який базується на визначенні індексу структурної подібності зображень і враховує комплекс із трьох властивостей: яскравості, контрастності та структурних елементів графічного представлення ID-карток і дає змогу підвищити ефективність процесу виявлення шахрайства шляхом використання меншої кількості апаратних ресурсів та забезпечує точність ідентифікації на рівні не нижче, ніж 85%.

5. Запропоновано архітектурне рішення для авторизації працівників на основі ID-карт, що включає в себе апаратну складову з використанням міні-комп’ютера на базі Raspberry PI та камери з роздільною здатністю 2 Мп, а також програмну модель виявлення справжності ідентифікаційного документу

працівника, що дають змогу забезпечити продуктивність та функціональну зручність при аутентифікації до приміщень з обмеженим доступом.

6. Обгрунтовано застосування альтернативного підходу до виявлення шахрайства з ID-картками, який базується на основі використання глибоких нейронних мереж на основі VGG-16 і дає змогу, шляхом її донавчання, забезпечити високу точність ідентифікації користувачів на основі технологій комп'ютерного зору.

7. Розроблено алгоритм виявлення шахрайства з ID-картками, який включає в себе виконання основних 8 кроків і забезпечує можливість визначення та побудови контурів об'єктів, наявних на ID-картці.

8. Засобами мови програмування Python реалізовано програмну модель, яка на основі індексу структурної подібності зображень дозволяє виявити відмінності між еталонною ID-карткою і фальсифікованою.

9. Оптимізовано програмну реалізацію індексу структурної подібності зображень шляхом перетворення кольорового зображення у формат з відтінками сірого, що дозволяє використовувати лише один канал при аналізі контурів і теплових карт ідентифікатора користувачів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Install TensorFlow. URL: https://www.tensorflow.org/install (дата звернення 17.04.2021 р.).

2. TensorFlow Datasets: a collection of ready-to-use datasets. URL: https://www.tensorflow.org/datasets (дата звернення 17.04.2021 р.)

3. Cuda. URL: https://opencv.org/platforms/cuda/ (дата звернення 21.10.2021 р.)

4. Петин В. Микрокомпьютеры Raspberry Pi: Практическое руководство. БХВ-Петербург. 2015. 240 с.

5. Магда Ю. Raspberry Pi. Руководство по настройке и применению. Litres. 2017 р. 161 с.

6. Макаров С. Arduino Uno и Raspberry Pi 3: от схемотехники к интернету вещей. Litres. 2019 р. 202 с.

7. Яцишин В.В., Щербаков О.О., Лова М.Р. Аналіз баз даних зображень у галузі комп’ютерного зору. Матеріали X міжнародної науково - технічної конференції молодих учених і студентів «Актуальні задачі сучасних технологій» (24-25 листопада 2021 р.) Тернопільського національного технічного університету імені Івана Пулюя. Тернопіль: ТНТУ. 2021. С. 144.

8. Жаровський Р.О., Лова М.Р., Щербаков О.О. Застосування індексу структурної подібності зображень при їх аналізі. Матеріали IX науково-технічної конференції Тернопільського національного технічного університету імені Івана Пулюя «Інформаційні моделі, системи та технології» (8-9 грудня 2021 року). Тернопіль: ТНТУ. 2021. С. 114.

9. Васильев В. И. Распознающие системы : справочник. К. : Наукова думка, 1983. 230 с.

10. Горелик А. Л. Методы распознавания. М. : Высшая школа, 1984. 219 с.

11. Дуда Р. Распознавание образов и анализ сцен : пер. с англ. М. : Мир, 1978. 510 с.

12. Форсайт Д. А. Компьютерное зрение. Современный подход : пер. с англ. М. : Вильямс, 2004. 928 с.

13. Шапиро Л. Компьютерное зрение : пер. с англ. БИНОМ. Лаборатория знаний, 2006. 752 с.

14. Beginner’s Guide to Object Detection Algorithms. URL: https://medium.com/analytics-vidhya/beginners-guide-to-object-detectionalgorithms-6620fb31c375 (дата звернення 01.05.2021).

15. NumPy v1.20 Manual. URL: https://numpy.org/doc/stable/ (дата звернення 25.10.2021р.).

16. Кузин Л.Т. Расчет и проектирование дискретных систем управления.-М.: ГН ТИМЛ, 2012.- 648 с.

17. Python Tutorial. URL: https://www.w3schools.com/python/default.asp (дата звернення 15.11.2021 р.).

18. Pandas documentation. URL: https://pandas.pydata.org/docs/index.html (дата звернення 28.11.2021 р.).

19. Y. Bengio, R. Ducharme, and P. Vincent. A neural probabilistic language model. In Advances in Neural Information Processing Systems 13 (NIPS 2000). 2001. p. 932–938.

20. Graves and J. Schmidhuber. Framewise phoneme classification with bidirectional LSTM networks. In 2005 International Joint Conference on Neural Networks (ICJNN’05). 2005. p. 23–43.

21. Preprocessing data. URL: https://scikit-learn.org/stable/modules/preprocessing.html#preprocessing (дата звернення 05.11.2021 р.).

22. API reference. URL: https://pandas.pydata.org/docs/reference/index.html (дата звернення 10.11.2021 р.).

23. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп’ютерні мережі. Книга 1. Львів, «Магнолія 2006». 2013. 256 с.

24. Микитишин А.Г., Митник М.М., Стухляк П.Д., Пасічник В.В. Комп’ютерні мережі. Книга 2. Львів, «Магнолія 2006», 2014. 312 с.

25. Микитишин А.Г., Митник М.М., Стухляк П.Д. Телекомунікаційні системи та мережі. Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. 384 с.

26. Микитишин А.Г., Митник М.М., Стухляк П.Д. Комплексна безпека інформаційних мережевих систем: навчальний посібник. Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. 256 с.

27. Pandas documentation. URL: https://pandas.pydata.org/docs/index.html (дата звернення 28.11.2021 р.).

28. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Київ. 2018.

29. Катренко Л.А., Катренко А.В. Охорона праці в галузі комп'ютинґу. Львів: Магнолія-2006. 2012. 544 с.

30. Желібо Е.Н. Безпека життєдіяльності: Навчальний посібник. Київ: «Каравела», Львів: «Новий світ - 2000». 2001. 320с.

Додаток А

Тези конференцій

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний технічний університет імені Івана Пулюя (Україна)
Університет імені П'єра і Марії Кюрі (Франція)
Маріборський університет (Словенія)
Технічний університет у Кошице (Словаччина)
Вільнюський технічний університет ім. Гедимінаса (Литва)
Білоруський національний технічний університет (Республіка Білорусь)
Міжнародний університет цивільної авіації (Марокко)
Наукове товариство ім. Т.Шевченка

АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ

Збірник
тез доповідей
Том І

X Міжнародної науково-практичної конференції молодих учених та студентів
24-25 листопада 2021 року

УКРАЇНА
ТЕРНОПІЛЬ – 2021

Матеріали X Міжнародної науково-практичної конференції молодих учених та студентів
«АКТУАЛЬНІ ЗАДАЧІ СУЧАСНИХ ТЕХНОЛОГІЙ» – Тернопіль 24-25 листопада 2021 року

УДК 004.89

Яцишин В.В. канд. техн. наук, доцент, Щербаков О.О., Лова М.Р.
Тернопільський національний технічний університет імені Івана Пулюя

АНАЛІЗ БАЗ ДАНИХ ЗОБРАЖЕНЬ У ГАЛУЗІ КОМП'ЮТЕРНОГО ЗОРУ

Yatsyshyn V.V. PhD, Assoc. Prof., Scherbakov O.O., Lova M.R.

ANALYSIS OF IMAGE DATA SETS IN THE AREA OF COMPUTER VISION

Комп'ютерний зір відноситься до області штучного інтелекту, який швидко розвивається. Для того, щоб полегшити роботу при проектуванні таких систем, зокрема, моделей та їхніх архітектур, деякі фірми поділились сформованими навчальними вибірками.

Одним з таких наборів даних є модифікована база даних рукописних цифр Національного інституту стандартів і технологій (MNIST). Цей набір представляє собою елементарну колекцію даних для комп'ютерного зору, що містить 70 тисяч зображень рукописних цифр для кожного числа, тобто 0 – 9, які відформатовані у форматі сірого 28x28. Дані попередньо розділені на навчальну вибірку (60 тисяч) і тестовий набір (10 тисяч). Усі цифри розміщені у центрі зображення. Даний набір є корисним для фундаментального проекту комп'ютерного зору, коли необхідно автоматично оцифрувати рукописний текст

Набори даних CIFAR-10 і CIFAR-100 підготовлені Канадським інститутом перспективних досліджень. CIFAR-10 складається з 60 тисяч зображень розподілених за 10-ма класами. Дана колекція включає зображення літаків, автомобілів, птахів, котів, оленів, собак, жаб, коней, кораблів і вантажівок. До складу CIFAR-100 входять 60 тисяч зображень, але тепер вже передбачено 100 класів, тобто 600 зображень на кожен клас. Колекції CIFAR-10 і CIFAR-100 є зручними для використання, оскільки всі вони відформатовані у форматі 32x32 пікселі та попередньо розділені на навчальний набір із 50 тисяч зображень та тестовий набір із 10 тисяч зображень з рівною часткою даних з усіх класів.

Набір даних IMDB-Wiki містить 520 тисяч зображень обличчя, виділених з IMBD та Вікіпедії. Дані містять важливу метаінформацію, наприклад розташування обличчя на зображенні, ім'я, дата народження та стать людини на фотографіях. Цей набір даних зазвичай використовується для завдань прогнозування статі та віку.

ImageNet набір даних створено спільно Стенфордським університетом та Принстонським університетом для типового змагання з комп'ютерного зору під назвою ImageNet Large Scale Visual Recognition Challenge (ILSVRC), де командам-учасникам було запропоновано 5 основних завдань, тобто класифікація об'єктів, локалізація об'єктів, виявлення об'єктів, виявлення та розпізнавання об'єктів з відео за допомогою набору даних ImageNet. Цей набір даних побудований на основі ієрархії WordNet (лексична база даних для англійської мови), де містяться лише іменники. В середньому на кожен вузол ієрархії припадає понад 500 зображень. Всього є понад 1,4 мільйона зображень понад 220 тисяч класів. Наразі це найбільший доступний набір зображень, який є відкритим і загальнодоступним.

Набір PASCAL VOC даних було відкрито дослідницьким інститутом PASCAL, що фінансується Європейським Союзом. Дана колекція містить зображення за 4-ма основними темами і включає транспортні засоби, домашнє господарство, тварин та людей.

При реалізації комп'ютеризованої системи виявлення справжності ID-картки доцільним є використання наведених наборів даних, що дозволить забезпечити виявлення об'єктів у різних предметних областях.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

IX НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ»

8–9 грудня 2021 року

ТЕРНОПІЛЬ
2021

УДК 004.89

Р.О. Жаровський канд. техн. наук, М.Р. Лова, О.О. Щербаков
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЗАСТОСУВАННЯ ІНДЕКСУ СТРУКТУРНОЇ ПОДІБНОСТІ ЗОБРАЖЕНЬ ПРИ ЇХ АНАЛІЗІ

UDC 004.89

R.O. Zharovskyy PhD, M.R. Lova, O.O. Scherbakov

APPLICATION OF THE STRUCTURAL SIMILARITY INDEX MEASURE IN THE IMAGES ANALYSIS

Структурний індекс подібності зображень використовується як метрика для вимірювання міри схожості між двома заданими зображеннями. Оскільки ця технологія існує з 2004 року, то наявними у всесвітній мережі є доволі багато наукових і прикладних публікацій, що пояснюють дану концепцію і теорію SSIM («Structural Similarity Index Model») на загальному рівні.

Система візуального сприйняття людини здатна ідентифікувати структурну інформацію зі сцени і, отже, визначити відмінності між інформацією, добутою з еталонної та сцени зразку.

Отже, метрика, яка повторює таку поведінку, буде краще виконувати завдання, які передбачають розрізнення зразка та еталонного зображення. Показник структурної схожості виділяє з зображення 3 ключові характеристики: яскравість, контраст, структура.

Порівняння двох зображень здійснюється на основі цих 3 ознак. На рис. 1, наведеному нижче, показано розташування та алгоритм вимірювання структурної подібності. Сигнали X і Y надсилають еталонні зображення та зображення, які потрібно перевірити.

Рисунок 1. Система вимірювання показника структурної подібності зображень

Ця система обчислює індекс структурної схожості між двома заданими зображеннями, значення якого належать інтервалу від -1 до +1. Значення «+1» вказує, що дані зображення дуже схожі або однакові, а значення «-1» – вказує, що вони дуже різні. Часто ці значення представляються в діапазоні [0, 1], де крайні значення мають ту саму інтерпретацію.