НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ імені ІГОРЯ СІКОРСЬКОГО»
Приладобудівний факультет

Кафедра автоматизації та систем неруйнівного контролю

До захисту допущено:
Завідувач кафедри
_____Юрій КИРИЧУК
___ _____« » 20 р.

Дипломний проєкт

на здобуття ступеня бакалавра за освітньо-професійної програмою«Комп'ютерно-інтегровані системи та технології в приладобудуванні»

спеціальності 151 «Автоматизація та комп'ютерно-інтегровані технології»

на тему: «Система інтелектуальної аутентифікації та автоматизованого керування вхідними дверима»

Виконав:
студент IV курсу, групи ПМ-з01
ФОН ДІХТЕР Ріхард Міхаель Миколайович _____

Керівник:
д.т.н., професор,
професор кафедри АСНК
ЧЕРЕПАНСЬКА Ірина Юріївна _____

Рецензент:
PhD,
асистент кафедра ІВТ
ДОРОЖИНСЬКА Ганна Василівна _____

Засвідчую, що у цьому дипломному проєкті немає запозичень з праць інших авторів без відповідних посилань. Студент: фон Діхтер Р. М.

Київ – 2024 рік

Відомість дипломного проєкту

№ з/п	Формат	Позначення	Найменування	Кількість листів	Примітка
1	А4		Завдання на дипломний проєкт	2	
2		ДПБ.ПМ-з01.03.1760.000ПЗ	Пояснювальна записка	1	
3	А3	ДПБ.ПМ-з01.03.1760.001СхЕ	Схема електрична принципова	1	
4	А4	ДПБ.ПМ-з01.03.1760.002СхС	Схема структурна	1	
5	А4	ДПБ.ПМ-з01.03.1760.003СхС	Схема структурна	1	
6	А4	ДПБ.ПМ-з01.03.1760.004СхБ	Блок-схема	1	
7	А4	ДПБ.ПМ-з01.03.1760.005СхБ	Блок-схема	1	
8	А4	ДПБ.ПМ-з01.03.1760.006СхБ	Блок-схема	1	

				ДПБ. ДП ПМ- з01.03.1760.000	
	ПІБ	Підп.	Дата		
Розробн.	Фон Діхтер Р.М.			Відомість дипломного проєкту	Лист 1 / Листів 1
Керівн.	Черепанська І.Ю.				
Консульт.					КПІ ім. Ігоря Сікорського Каф. АСНК Гр. ПМ-з01
Н/контр.					
Зав.каф.	Киричук Ю.В.				

Пояснювальна записка

до дипломного проекту

на тему «**Система інтелектуальної аутентифікації та автоматизованого керування вхідними дверима»**

Національний технічний університет України

«Київський політехнічний інститут імені Ігоря

Сікорського» Приладобудівний факультету

Кафедра автоматизації та систем неруйнівного контролю Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 151 «Автоматизація та комп'ютерно-інтегровані технології»

Освітньо-професійна програма «Комп'ютерно-інтегровані технології проектування приладів»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Юрій КИРИЧУК

__ _____ « » 2023 р.

ЗАВДАННЯ
на дипломний проєкт
студенту
фон Діхтер Ріхард Міхаель

1. Тема проєкту «Система інтелектуальної аутентифікації та автоматизованого керування вхідними дверима», керівник проєкту Черепанська Ірина Юріївна, професор, д.т.н., затверджені наказом по університету від «27» травня 2024 р. №2102-с

2. Термін подання студентом проєкту «11» червня 2024.

3. Перелік графічного матеріалу (із зазначенням обов'язкових креслеників, плакатів, презентацій тощо) структурна схема, електрична принципова схема, штучна нейронна мережа, блок схеми алгоритмічно-програмного забезпечення, презентація

4. Дата видачі завдання «10» вересня 2024 р.

Календарний план

№ з/п	Назва етапів виконання дипломного проєкту	Термін виконання етапів проєкту	Примітка
1	Аналіз сучасного стану проблеми інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима	10.09.2024	
2	Розробка структурної схеми системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима	10.10.2024	
3	Розробка штучної нейронної мережі для автоматизаної інтелектуальної аутентифікації облич	10.11.2024	
4	Проведення навчання та експериментальних досліджеень працездатності штучної нейронної мережі системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима	10.12.2024	
5	Розробка алгоритмічно-програмного забезпечення системи інтелектуальної аутентифікації облич і автоматизації процесу керування вхідними дверима	20.01.2024	
6	Схема електрична принципова системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима	20.02.2024	
7	Вступ	10.03.2024	
8	Висновки	10.04.2024	
9	Оформлення списку літератури та додатку	30.05.2024	

Студент фон Діхтер Ріхард Міхаель

Керівник д.т.н., професор,
професор кафедри АСНК
Ірина ЧЕРЕПАНСЬКА

Анотація

Метою дипломного проекту є розробка системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима, яка буде конкурентоспроможною зарубіжним аналогам.

В дипломному проєкті розроблено систему інтелектуальної аутентификації та автоматизованого керування вхідними дверима. Було проаналізовано популярні архітектури та впроваджено можливість модернізації системи для уникнення перенавчання моделі та використання на обмежених обчислювальних ресурсах. Було проведено численні експерименти для мінімізації цих проблем. Розроблена система поєднує автоматизацію процесу відкривання та закривання дверей та забезпечує аутентифікацію облич. Таким чином, було розроблено вітчизняну систему інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима, яка буде конкурентоспроможною зарубіжним аналогам.

Ключові слова: інформаційний портал, база даних, сервер, методики пошуку, проектування, керування даними, розробка порталу, програмування, нейронні мережі, розпізнавання облич, великі бази даних

.

Abstract

The goal of this diploma project is to develop a facial recognition-based intelligent authentication system and automate the management of entrance doors, making it competitive with foreign counterparts.

In this diploma project, a system for intelligent authentication and automated control of entrance doors has been developed. Popular architectures were analyzed, and the possibility of system modernization was implemented to avoid model overfitting and to be used on limited computational resources. Numerous experiments were conducted to minimize these issues. The developed system integrates the automation of the door opening and closing process and provides facial authentication. Thus, a domestic system of intelligent facial authentication and automation of entrance door management processes has been developed, which will be competitive with foreign counterparts.

Keywords: information portal, database, server, search engine, design, data management, portal development, programming, neural networks, face recognition, image databases, hpc, big data

ЗМІСТ

ПЕРЕЛІК ПРИЙНЯТИХ УМОВНИХ СКОРОЧЕНЬ

ШНМ - штучна нейронна мережа

ОК – об’єкт керування, представлений дверима

СК – система керування

ШНМ – штучна нейронна мережа

МК – мікро контролер

БД – база даних

П – перетворювач

ВМ – виконавчий механізм

ПД – підсистема датчиків (для моніторингу стану дверей)

ВСТУП

Важко уявити сучасні будівлі комерційного та житлового призначення без обладнання системами безпеки та контролю доступу до них. Окрім високотехнологічних систем на кшталт «розумний дім», в повсякденному використанні увійшли в життя та знайшли своє застосування різні види аутентифікації при автоматизації керування доступом до будівель чи приміщень. Підвищений рівень їх безпеки забезпечується різними видами аутентифікації – від застосування паролів до апаратних токенів чи зняття біометричних даних відвідувачів. Окрім збільшення рівню захисту приміщень автоматизація керування доступом до них зменшує залучення людських ресурсів для виконання завдання контролю доступу.

Водночас, такі технологічні рішення залишаються доволі вартісними і водночас мають певні обмеження функціональності, зокрема через проблему фрагментованості даних.

Розглядаючи можливості наявних технічних розробок щодо автоматизованого керування доступом за допомогою систем інтелектуальної аутентифікації людських облич, цим дипломним проектом ставиться мета запропонувати конкурентоспроможну систему інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

Невід'ємною частиною житлових та комерційних приміщень є сучасні системи безпеки та контролю доступу. Одним з ключових компонентів таких систем є інтелектуальна аутентифікація облич та автоматизація процесів керування вхідними дверима. Аутентифікація зазвичай здійснюється за допомогою паролів, апаратних токенів або біометричних даних користувачів. Ці методи забезпечують підвищений рівень безпеки, зручність використання та ефективність управління доступом.

Актуальність теми дипломного проекту полягає у тому, що сучасні системи інтелектуальної аутентифікації та автоматизованого керування вхідними дверима здатні підвищувати рівень безпеки без значного залучення

людських ресурсів. На сучасному ринку існує обмежена кількість повністю доступних рішень у сфері інтелектуальної аутентифікації облич та автоматизації процесів керування вхідними дверима. Розробники таких систем зіштовхуються з проблемою фрагментованості даних, що стримує їх розвиток та широке застосування. Більшість наявних систем пропонують лише часткові рішення або мають обмежену функціональність.

З огляду на вказане, **метою** дипломного проекту є розробка системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима, яка буде конкурентоспроможною зарубіжним аналогам.

У дипломному проекті вирішено наступні задачі:

1. Проаналізовано сучасний стан проблеми інтелектуальної аутентифікації людських облич та відомі технічні розробки щодо автоматизованого керування вхідними дверями, визначити їх переваги та недоліки.

2. Розроблено структурну схему системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

3. Розроблено інтелектуальні моделі (штучні нейронні мережі) системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

4. Проведено навчання та експериментальні дослідження працездатності штучних нейронних мереж системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

5. Розроблено схему електричну принципову системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

6. Розроблено алгоритмічно-програмне забезпечення системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

1. АНАЛІЗ СУЧАСНОГО СТАНУ ПРОБЛЕМИ ІНТЕЛЕКТУАЛЬНОЇ АУТЕНТИФІКАЦІЇ ОБЛИЧ І АВТОМАТИЗАЦІЇ ПРОЦЕСІВ КЕРУВАННЯ ВХІДНИМИ ДВЕРИМА

1.1. Сутність та зміст задачі інтелектуальної аутентифікації облич

Сучасні системи безпеки та контролю доступу є невід'ємною частиною як житлових, так і комерційних приміщень. Одним з ключових компонентів таких систем є інтелектуальна аутентифікація облич або їх (облич) автоматизоване розпізнавання та автоматизація процесів керування вхідними дверима. Системи аутентифікації відіграють важливу роль у забезпеченні безпеки та запобіганні несанкціонованому доступу до комп'ютерних систем, мереж та приміщень. Аутентифікація зазвичай здійснюється за допомогою паролів, апаратних токенів або біометричних даних користувачів. Ці методи забезпечують підвищений рівень безпеки, зручність використання та ефективність управління доступом.

Існують три основні типи систем аутентифікації: парольний, апаратний та біометричний. Парольний метод базується на використанні секретних комбінацій символів, апаратний - на фізичних пристроях, таких як смарт-карти або токени, а біометричний - на унікальних фізіологічних або поведінкових характеристиках користувачів, таких як відбитки пальців, розпізнавання облич або голосу.

Парольна аутентифікація. Це найпоширеніший тип, який базується на використанні паролів або пін-кодів, відомих лише легітимному користувачеві.

Найпростішим способом аутентифікації є текстовий цифро-буквений пароль. Користувача комп'ютерної системи просять ввести ім'я облікового запису та пароль. Систему цього типу легко реалізувати і тому отримала повсюдне поширення. Метод аутентифікації по паролю є найстарішим і простим [1].

Апаратна аутентифікація. У цьому випадку аутентифікація здійснюється за допомогою фізичних пристроїв, таких як смарт-картки, USB-ключі або інші апаратні токени.

Біометрична аутентифікація. Цей метод ґрунтується на унікальних біологічних характеристиках людини, таких як відбитки пальців, розпізнавання обличчя, сканування райдужної оболонки ока, тощо.

Основна мета інтелектуальної аутентифікації облич полягає у точному та швидкому розпізнаванні осіб на основі їх біометричних даних. Це дозволяє уникнути використання традиційних методів аутентифікації, таких як паролі або картки доступу, які можуть бути втрачені або викрадені. Автоматизація процесів керування вхідними дверима забезпечує безперебійний та безпечний доступ до приміщень, знижуючи ризики несанкціонованого проникнення.

Біометричні методи, які базуються на унікальних біологічних характеристиках, таких як відбитки пальців, розпізнавання обличчя або сканування райдужної оболонки ока, представляють більшу надійність і стійкість до злому. Реалізація біометричної аутентифікації може бути дещо складнішою, але вона значно зменшує кількість випадків витоку даних через несанкціонований доступ до них та в цілому є набагато більш безпечною. У сучасному світі інтелектуальна аутентифікація облич стає все більш важливою технологією у забезпеченні безпеки та ідентифікації осіб. Завдяки розвитку машинного навчання і комп'ютерного зору, системи розпізнавання облич набувають нових можливостей.

1.2. Аналіз сучасних засобів та методів інтелектуальної аутентифікації облич

1.2.1. Традиційні методи розпізнавання облич

Традиційні методи розпізнавання облич включають використання різних алгоритмів та технік комп'ютерного зору для аналізу та порівняння зображень облич. Основні методи включають такі методи.

Метод Eigenfaces (рис. 1.1). Використовує аналіз головних компонентів (PCA) для зменшення розмірності зображень облич та виділення основних характеристик. Цей метод є одним з перших, що був застосований для розпізнавання облич. Він дозволяє зменшити розмірність даних, що значно

спрощує процес розпізнавання. Eigenfaces базується на ідеї, що будь-яке обличчя може бути представлене як лінійна комбінація деяких базових зображень облич, які називаються eigenfaces [2, 3].

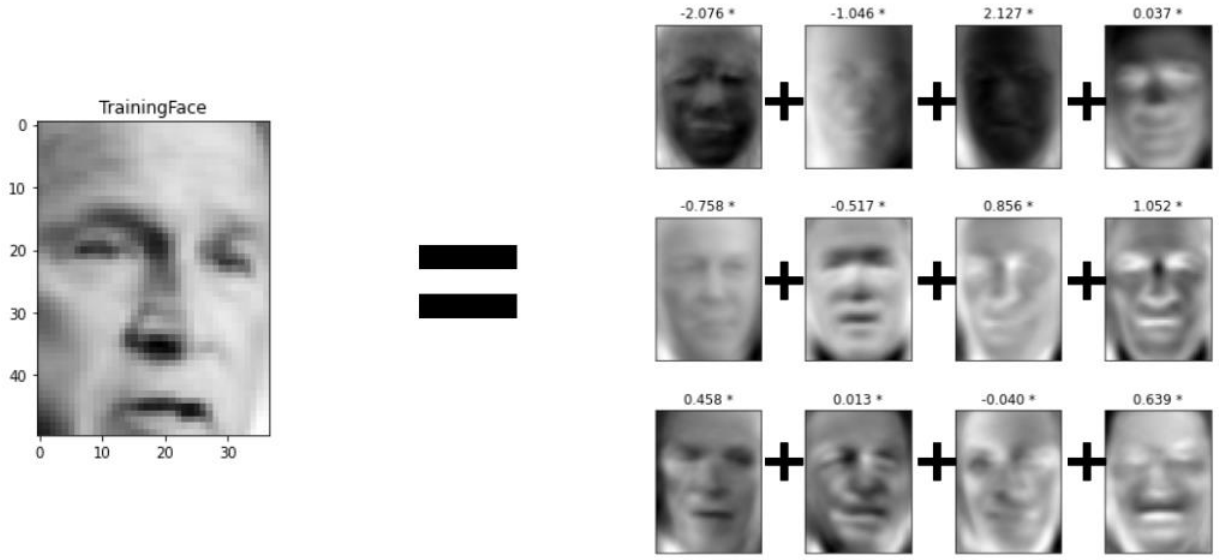

Рис. 1.1. Ілюстрація прикладу роботи методу Eigenfaces [2]

Даний метод дозволяє зменшити розмірність даних і спрощує процес розпізнавання, він вразливий до змін освітлення та виразів облич. Це може призвести до значних похибок у розпізнаванні, особливо в умовах реального часу, де умови освітлення не завжди стабільні.

Метод Fisherfaces. Базується на лінійному дискримінантному аналізі (LDA) і дозволяє краще розрізняти обличчя різних людей, враховуючи варіації освітлення та виразів облич. Fisherfaces використовує інформацію про класи для максимізації міжкласової розбіжності та мінімізації внутрішньокласової розбіжності, що робить його більш ефективним для розпізнавання облич у різних умовах освітлення та з різними виразами облич, що чудово видно на рис. 1.2 [4, 6].

Даний метод є більш стійким до варіацій освітлення та виразів облич завдяки використанню лінійної дискримінантної аналізи.

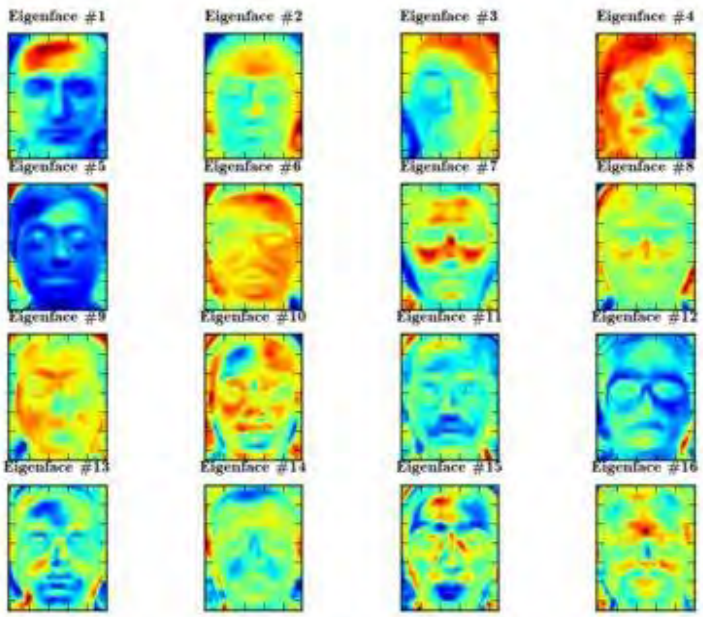

Рис. 1.2. Ілюстрація прикладу роботи методу Fisherfaces за допомогою кольорової теплової карти [8]

Однак, його ефективність значно знижується при роботі з великими наборами даних та різноманітними умовами, що обмежує його застосування в масштабних системах безпеки.

Метод локальних бінарних шаблонів (англ. – **local binary pattern (LBP)).** Використовує текстурні характеристики облич для їх розпізнавання. Цей метод є більш стійким до змін освітлення та виразів облич. LBP аналізує текстуру зображення шляхом порівняння кожного пікселя з його сусідами та кодування результатів у бінарний код. Це дозволяє створити надійні та дискримінативні ознаки для розпізнавання облич [5, 6]. На рис. 1.3 проілюстрований приклад процесу стискання за цим методом.

Метод локальних бінарних шаблонів (англ. – **local binary pattern (LBP)).** Використовує текстурні характеристики облич для їх розпізнавання. Цей метод є більш стійким до змін освітлення та виразів облич. LBP аналізує текстуру зображення шляхом порівняння кожного пікселя з його сусідами та кодування результатів у бінарний код. Це дозволяє створити надійні та дискримінативні

ознаки для розпізнавання облич [5, 6]. На рис. 1.3 проілюстрований приклад процесу стискання за цим методом.

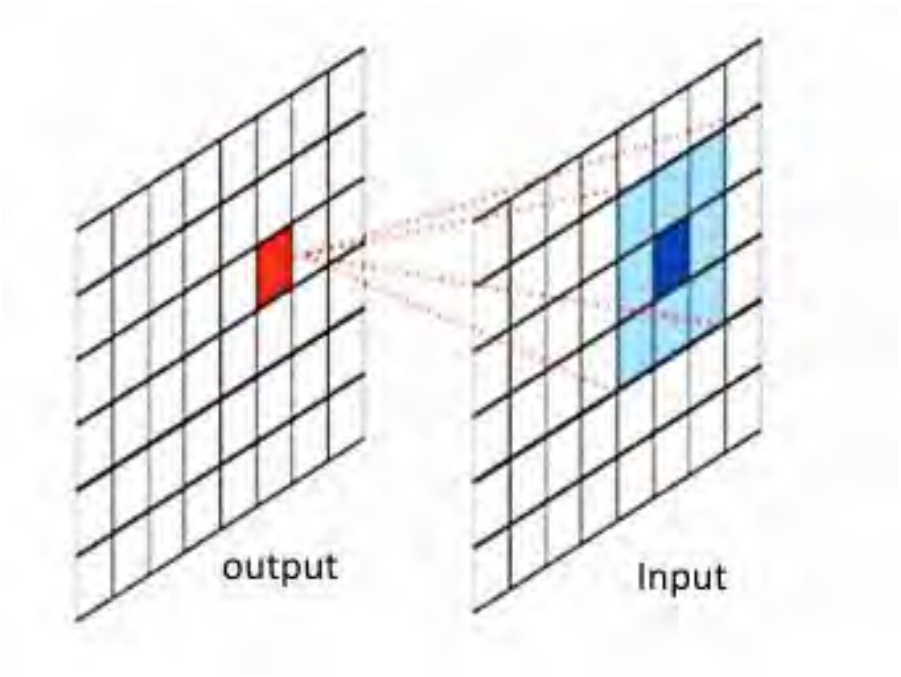

Рис. 1.3. Ілюстрація прикладу процесу стискання зображення методом LBP [11]

Метод LBP є більш стійким до змін освітлення та виразів облич завдяки аналізу текстурних характеристик. Проте, він також має свої недоліки: низька роздільна здатність зображень може призвести до втрати важливих деталей, що впливає на точність розпізнавання.

Традиційні методи розпізнавання облич, такі як Eigenfaces, Fisherfaces та локальні бінарні шаблони (LBP), мають свої переваги, але також суттєві обмеження, що відрізняє їх від сучасних підходів. Сучасні методи, засновані на машинному навчанні та глибокому навчанні, значно перевершують традиційні підходи. Вони здатні адаптуватися до різноманітних умов, забезпечуючи високу точність розпізнавання навіть у складних сценаріях. Використання нейронних мереж дозволяє враховувати більше параметрів та взаємозв'язків, що робить ці системи більш надійними та ефективними.

Таким чином, хоча традиційні методи розпізнавання облич мають свої історичні заслуги і певні переваги, їх обмеження у стійкості до змін освітлення, виразів облич та масштабованості роблять їх менш придатними для сучасних вимог систем безпеки. Це підкреслює необхідність розробки та впровадження нових, більш досконалих методів аутентифікації, що є головною метою даного проекту.

1.2.2. Сучасні засоби розпізнавання людських облич

На сьогоднішній день найбільш розповсюдженими засобами розпізнавання облич є штучні нейронні мережі. Зокрема, **згорткові нейронні мережі (англ. - Convolutional Neural Networks, (CNN))**. Це пов'язано з тим, що вони можуть ефективно аналізувати великі обсяги даних, виявляючи складні шаблони та характеристики, що робить їх ідеальними для завдань розпізнавання облич. В літературі [7] вказано, що CNN можуть значно знизити час навчання для мережі, підвищуючи її ефективність у розпізнаванні облич. CNN є основою більшості сучасних систем розпізнавання облич. Вони автоматично виділяють важливі ознаки зображень облич, такі як контури, текстури та інші деталі. CNN складаються з кількох шарів згортки, підвибірки та повнозв'язкових шарів, що дозволяє їм ефективно обробляти великі обсяги даних. Цей метод дозволяє досягати високої точності розпізнавання завдяки глибині мережі та великій кількості навчальних даних [7].

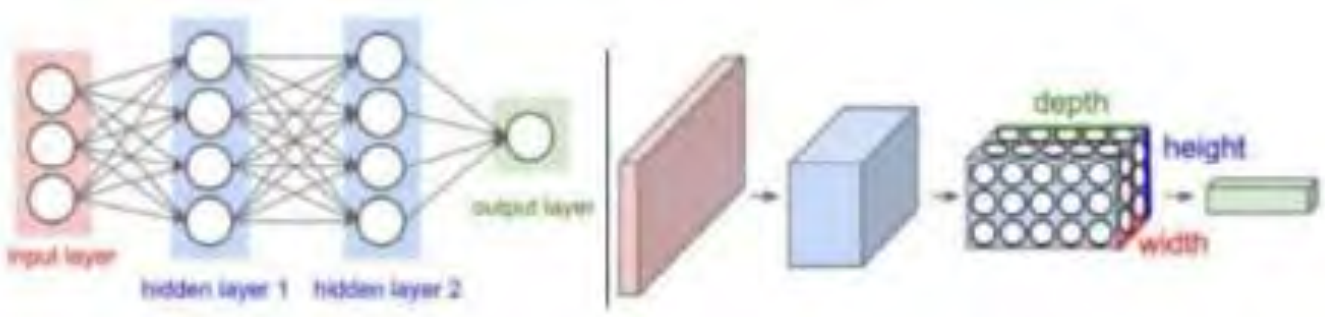

Рис. 1.4. – Схематичне зображення загальної структури CNN [8]

Основний принцип роботи CNN полягає у використанні згорткових шарів (convolutional layers) та пулінгових шарів (pooling layers), які дозволяють ефективно витягати різні ознаки з вхідних даних (рис. 1.4). CNN складаються з кількох шарів згортки, підвибірки та повнозв'язкових шарів.

Глибокі згорткові нейронні мережі (англ. - Deep Convolutional Neural Network (DCNN)) (рис. 1.5). Вони є подальшим розвитком класичних CNN, включаючи більшу кількість шарів та більш складні архітектури. DCNN дозволяють досягати ще вищої точності розпізнавання облич, особливо у великих наборах даних та складних умовах освітлення [9].

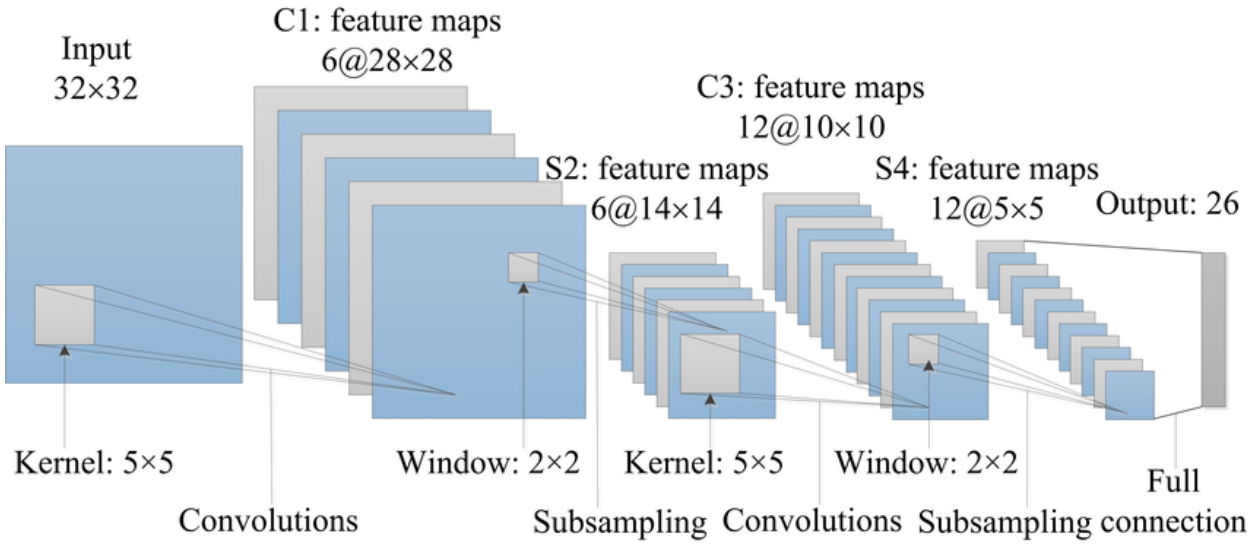

Рис. 1.5. Ілюстрація прикладу структури DCNN

Сучасні засоби, такі як згорткові нейронні мережі (CNN, DCNN та ін.), значно перевершують традиційні підходи. Вони здатні автоматично виділяти важливі ознаки зображень облич, такі як контури, текстури та інші деталі, що забезпечує високу точність розпізнавання навіть у складних умовах.

Таким чином, хоча традиційні методи розпізнавання облич мають свої історичні заслуги, їх обмеження у стійкості до змін освітлення, виразів облич та масштабованості роблять їх менш придатними для сучасних вимог систем

безпеки. У розділі 4 було проведено більш детальний аналіз архітектур нейронних мереж, що будуть використовуватись у проекті, з метою показати переваги сучасних підходів у розпізнаванні облич.

1.2.3. Сучасні методи підготовки даних для інтелектуальної аутентифікації

Підготовка даних для інтелектуальної аутентифікації є одним з найважливіших завдань в автоматизації розпізнавання облич. Очевидно, що вона є багатоетапним та складним процесом.

Перший етап - **збір даних**, полягає у накопиченні множини різних зображень облич, які створять навчальну базу даних для наступного навчання ШНМ. Навчальна база даних повинна повинна містити множину облич людей різного віку, статі, етнічних груп, з різними виразами облич, при різному освітленні та з різних ракурсів. Це дозволяє моделі навчитися розпізнавати обличчя в будь-яких умовах, наближених до реальних життєвих ситуацій.

Наприклад, зображення можуть включати людей з посмішкою, сумними, здивованими виразами, а також зображення, зроблені під різними кутами та при різному освітленні.

Підвищення точності розпізнавання облич у різних умовах, таких як неоднорідне освітлення, різні пози та вирази облич, залишається важливою задачею. Розробка алгоритмів, здатних адаптуватися до такої варіативності, є ключовим напрямком досліджень. Тому на сьогодні досі існує потреба в розробленні методів і алгоритмів, які вирішують перераховані вище проблеми [12].

Другий етап - **аугментація даних.** Наступним важливим кроком є аугментація даних. Це процес, який дозволяє штучно збільшити кількість навчальних даних за допомогою різних технік. Наприклад, обертання зображень, масштабування, зміна яскравості, контрасту, додавання шуму тощо. Це важливо тому, що моделі машинного навчання потребують великої кількості даних для

ефективного навчання. Аугментація дозволяє створити різноманітні варіанти одного і того ж зображення, що допомагає моделі стати більш стійкою до змін у зовнішніх умовах. Наприклад, якщо обернути зображення обличчя на кілька градусів або змінити його яскравість, модель навчиться розпізнавати обличчя навіть у таких умовах.

Третій етап - **розмітка даних.** Це процес визначення ключових точок облич та створення аннотацій, які будуть використані для навчання моделей. Ключові точки облич можуть включати положення очей, носа, рота та інших важливих частин обличчя. Ці аннотації допомагають моделі зрозуміти, як виглядає обличчя і які його основні характеристики. Наприклад, визначення положення очей і рота може допомогти моделі розрізняти обличчя навіть при різних виразах або нахилах голови.

На сьогоднішній день в Інтернеті накопичено великий об’єм різних баз даних або, як їх ще називають, датасетів, проте вони не можуть бути використані без додакового доопрацювання та адаптації під конкретні вирішувані задачі, а також доволі часто вони мають обмежений доступ. Тому перед розробниками постає завдання розробки оригінальної бази даних для навчання нейромереж.

1.3. Проблеми з якими стикаються розробники засобів автоматизованої аутентифікації облич

1.3.1. Підвищення точності розпізнавання облич

Нейронні мережі дозволяють використання різних методів та порівняння їх результатів для виявлення оптимального рішення, що буде використано у створенні системи. Будуть використовуватись різні методи та описано процес використання комбінаторики різних методів. Найголовніша перевага нейронних мереж - навчання і використання різних методів одночасно для досягнення оптимальних цілей.

Одним з найважливіших аспектів у розпізнаванні облич є точність ідентифікації. Сучасні дослідження показують, що застосування глибокого навчання та згорткових

нейронних мереж значно підвищує точність розпізнавання, навіть у складних умовах освітлення або при частковому закритті обличчя. Глибоке навчання дозволяє системам адаптуватися до нових умов та вдосконалювати алгоритми ідентифікації на основі накопиченого досвіду [13].

Модернізація звичайних згорткових нейронних мереж (CNN) може включати різні підходи та техніки для поліпшення їх продуктивності та ефективності. Основним методом модифікації є зміна архітектури CNN для роботи з більш специфічними даними або завданнями. Серед таких мереж можна виділити VGG, ResNet, MobileNet та багато інших [15].

1.3.2. Зміцнення захисту приватності

Проблема захисту приватності в системах розпізнавання облич набуває все більшого значення. Розробники впроваджують передові методи шифрування та анонімізації даних для забезпечення конфіденційності інформації про осіб. Крім того, використовуються технології блокчейн для створення безпечних та незмінних баз даних, що забезпечує високий рівень захисту персональних даних [14]. В подальших дослідженнях буде розглянуте додавання захист системи та питання розвитку системи для забезпечення доступу до системи віддалено.

1.4. Мета та постановка задач

Сучасні системи інтелектуального керування доступом до приміщень набувають все більшого значення для забезпечення безпеки та комфорту в житлових та офісних приміщеннях. Такі системи постійно розвиваються за рахунок нейромережевих технологій та складних електронних схем, пропонуючи нові можливості та стаючи невід'ємною частиною повсякденного життя. Аналіз сучасних підходів до розпізнавання облич, включно з використанням згорткових нейронних мереж, методів опорних векторів та інших технік глибокого навчання, підкреслив значний прогрес у точності та швидкості обробки даних.

Однак, варто зазначити, що існують певні проблеми, пов'язані з перенавчанням моделей та їх обмеженим використанням у деяких випадках, для досягнення високої точності необхідно ретельно підбирати моделі та архітектури нейронних мереж, а також проводити численні експерименти з параметрами навчання. Ще однією важливою проблемою є те, що багато існуючих систем розпізнавання облич розроблені комерційними компаніями і призначені для продажу. Це означає, що дослідники та розробники часто не мають прямого доступу до внутрішніх механізмів та даних цих систем, що значно ускладнює процес розробки нових, більш досконалих технологій. Деякі системи забезпечують аутентифікацію облич, але не інтегровані з автоматизованим керуванням вхідними дверима. Інші системи автоматизують процеси відкривання та закривання дверей, але не мають можливостей розпізнавання облич. Також існують рішення, які поєднують ці дві функції, але вони часто є дорогими, складними, або мають високий рівень фрагментарності технологій, адже вони теж створені комерційними компаніями для продажу. Таким чином, існує потреба у створенні вітчизняної системи інтелектуальної аутентифікації облич та автоматизованого керування вхідними дверима. Розроблення такої системи дозволить попередити несанкціонований доступ та підвищити рівень захисту приватних та комерційних об'єктів.

Актуальність теми дипломного проекту полягає у тому, що сучасні інтелектуальні системи інтелектуальної аутентифікації та автоматизованого керування вхідними дверима здатні підвищувати рівень безпеки без значного залучення людських ресурсів. На сучасному ринку існує обмежена кількість повністю доступних рішень у сфері інтелектуальної аутентифікації облич та автоматизації процесів керування вхідними дверима. Розробники таких систем зіштовхуються з проблемою фрагментованості даних, що стримує їх розвиток та широке застосування. Більшість наявних систем пропонують лише часткові рішення або мають обмежену функціональність.

З огляду на вказане, **метою** дипломного проекту є розробка системи інтелектуальної аутентифікації облич і автоматизації процесів керування

вхідними дверима, яка буде конкурентоспроможною зарубіжним аналогам.

Для досягнення мети необхідно вирішити наступні **задачі**:

1. Проаналізувати сучасний стан проблеми інтелектуальної аутентифікації людських облич та відомі технічні розробки щодо автоматизованого керування вхідними дверями, визначити їх переваги та недоліки.

2. Розробити структурну схему системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

3. Розробити інтелектуальні моделі (штучні нейронні мережі) системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

4. Провести навчання та експериментальні дослідження працездатності штучних нейронних мереж системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

5. Розробити алгоритмічно-програмне забезпечення системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

6. Розробити схему електричну принципову системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

1.5. Висновки аналізу сучасного стану проблеми інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

1. Проаналізовано сучасний стан проблеми інтелектуальної аутентифікації облич, зокрема з використанням згорткових нейронних мереж, та інших методів та засобів глибокого навчання, які зумовили значний прогрес у точності та швидкості обробки даних.

2. Було визначено, що існують проблеми, пов'язані з перенавчанням моделей та їх обмеженим використанням у випадках, коли модель настільки

добре адаптується до навчальних даних, що втрачає здатність ефективно працювати на нових, невідомих даних. Це може призводить до значного зниження точності розпізнавання облич у реальних умовах, де освітлення, ракурси та вирази облич можуть сильно варіюватися, що є дуже актуальним до теми проекту.

3. Аналіз показав, що сучасні системи інтелектуального керування доступом до приміщень набувають все більшого значення для забезпечення безпеки та комфорту в житлових та офісних приміщеннях. Такі системи постійно розвиваються за рахунок нейромережевих технологій та складних електронних схем, пропонуючи нові можливості та стаючи невід'ємною частиною повсякденного життя

4. Було визначено, що впровадження новітніх методів алгоритмів розпізнавання облич зустрічає низку викликів. Наприклад, для досягнення високої точності необхідно ретельно розробляти моделі та архітектури нейронних мереж, а також проводити численні експерименти з параметрами навчання. Це вимагає значних обчислювальних ресурсів та часу. Крім того, кожна конкретна задача може вимагати унікального підходу, що ускладнює універсальне застосування однієї моделі для різних сценаріїв.

5. Проаналізувавши сучасний стан проблеми інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима було виявлено, що багато з існуючих систем розпізнавання облич розроблені комерційними компаніями і призначені для продажу. Це означає, що дослідники та розробники часто не мають прямого доступу до внутрішніх механізмів та даних цих систем, а це значно обмежує можливості для проведення порівняльних досліджень та тестування нових алгоритмів.

6. Узагальнюючи, підсумком аналізу є те, що на ринку інтелектуальної аутентифікації було створено багато розробок, що забезпечують рівень безпеки шляхом попередження несанкціонованого доступу та можуть бути інтегрована з іншими системами контролю доступу для посилення їх захисних функцій, проте вони зустрічається з низкою випробувань для кожного розробника, що усладнює для дослідників та розробників розробку подібних проектів.

2. СТРУКТУРНА СХЕМА СИСТЕМИ ІНТЕЛЕКТУАЛЬНОЇ АУТЕНТИФІКАЦІЇ ОБЛИЧ І АВТОМАТИЗАЦІЇ ПРОЦЕСІВ КЕРУВАННЯ ВХІДНИМИ ДВЕРНИМА

2.1. Загальна інформація про структурну схему системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

Структурна схема системи інтелектуальної аутентифікації та автоматизованого керування вхідними дверима представлена на рис. 2.1, ілюструє управління доступом фізичних осіб через вхідні двері. Ця схема ілюструє логічну взаємодію між основними компонентами системи, показує їх функціональні зв'язки та загальну архітектуру.

Система інтелектуальної аутентифікації облич та автоматизації процесів керування вхідними дверима складається з декількох ключових компонентів, які забезпечують її ефективну роботу. Центральне місце в системі займає модуль камери, що виконує функцію первинного перетворювача зображень. Камера фіксує обличчя осіб, що наближаються до дверей, і передає зображення на подальшу обробку.

Зображення порівнюються з даними, заздалегідь збереженими у базі даних облич, що дозволяє системі верифікувати особу. Управління доступом здійснюється через мікроконтролер, який є мозковим центром системи. Він отримує дані від штучної нейронної мережі (ШНМ), що аналізує зображення. Мікроконтролер керує магнітними електронними замками, відкриваючи або закриваючи доступ до приміщення. Система містить також засоби передачі та збереження інформації, що забезпечують взаємодію між компонентами.

Модуль датчиків стану дверей використовується для визначення стану відчинення або зачинення дверей. Він забезпечує точний контроль дверей та передає інформацію до центрального контролера системи. Це дозволяє системі автоматично реагувати на зміну стану дверей, забезпечуючи безпеку та зручність користувачів.

Датчики постійно моніторять стан дверей та передають дані до мікроконтролера. Мікроконтролер аналізує дані та визначає, чи є проблема з дверима (механічне блокування або електронний збій). Якщо виявлено механічне блокування, мікроконтролер надсилає сигнал на пульт охорони або вахтера. Якщо виявлено серйозний електронний збій, мікроконтролер надсилає сигнал безпосередньо електрикам або технічній службі. Комунікаційний модуль, такий як GSM-модуль або модуль Wi-Fi, може бути доданий для надсилання сигналів на пульт охорони, вахтера або технічну службу залежно від умов та системи по місцю встановлення.

Датчик напруги. Цей датчик може вимірювати струм та напругу в електричних ланцюгах. Він дозволяє виявляти збої в електронних компонентах, таких як перевантаження або коротке замикання без фізичного контакту з провідниками. Він підвищує надійність системи, забезпечуючи своєчасне виявлення та реагування на електронні несправності, це потенційно небезпечні ситуації, що можуть призвести до пошкодження обладнання або пожежі.

У системі інтелектуальної аутентифікації облич та автоматизації процесів керування вхідними дверима використання датчика стану дверей (reed-switch) та механічного датчика (наприклад, Honeywell 914CE18-3) забезпечує підвищену надійність та безпеку. Датчик стану дверей (reed-switch) визначає стан відчинення або зачинення дверей без фізичного контакту, що зменшує знос. Датчик реагує на зміну магнітного поля, що дозволяє швидко та точно контролювати доступ. Механічний датчик, у свою чергу, визначає механічне блокування дверей та їх точне положення через фізичний контакт, що дозволяє виявляти фізичні перешкоди. Використання обох датчиків забезпечує дублювання функцій контролю, що підвищує надійність системи, а також різні типи виявлення проблем: reed-switch забезпечує швидкий контроль стану дверей, тоді як механічний датчик виявляє механічні блокування. Цей комплексний підхід до моніторингу стану дверей, який дозволяє підвищити загальну ефективність та безпеку системи.

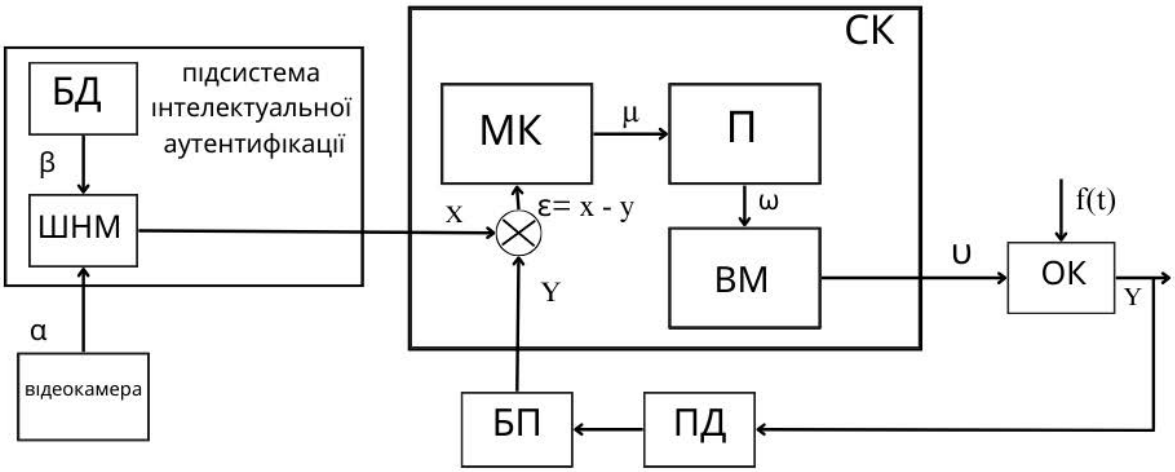

Рис. 2.1. Організаційна структурна схема функціонування системи інтелектуальної аутентифікації облич і автоматизації процесів керування

Умовні позначення до рис 2.1.

СК – система керування

ШНМ – штучна нейронна мережа

МК – мікро контролер

БД – база даних

П – перетворювач

ВМ – виконавчий механізм

ПД – підсистема датчиків (для моніторингу стану дверей)

α – вхідний сигнал камери

β – еталонні зображення користувачів

X сигнал про позитивний результат аутентифікації

величина сигналу розузгодження

сигнал, надісланний від мікроконтролера для відкриття дверей перетворений сигнал для виконавчого механізму дверей

відкривання дверей, забезпечене системою керуваввння

ОК об єкт керування, представлений дверима

f(t) влив зовнішнього середовища

сигнал від датчику про закритий стан дверей

2.2. Структурна схема підсистеми інтелектуальної аутентифікації облич

Структурна схема підсистеми інтелектуальної аутентифікації облич предтавлена на рис. 2.2.

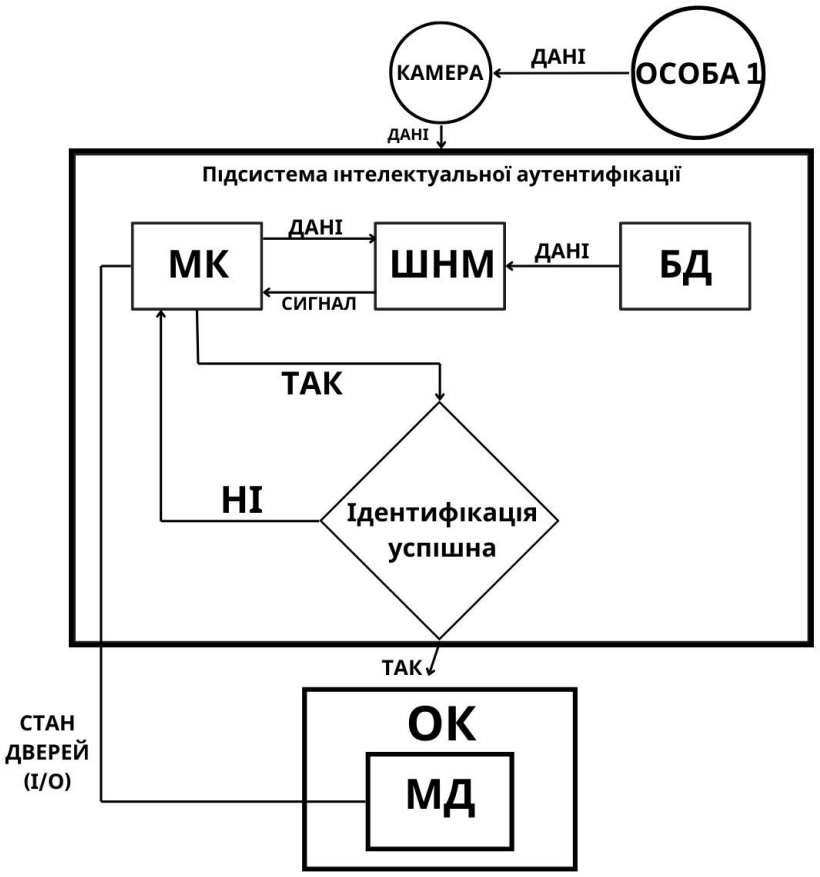

Рис. 2.2. Структурна схема підсистеми інтелектуальної аутентифікації облич

Підсистема інтелектуальної аутентифікації облич складається з декількох ключових компонентів, які забезпечують її ефективну роботу. Центральне місце в системі займає модуль камери, що виконує функцію первинного перетворювача зображень. Камера фіксує обличчя осіб, що наближаються до дверей, і передає зображення на подальшу обробку.

Обробка даних здійснюється за допомогою модуля штучного інтелекту, який аналізує зображення, отримане від камери, і порівнює його з базою даних. Штучний інтелект використовує алгоритми глибокого навчання для точної ідентифікації особи, що значно покращує точність системи.

Штучна нейронна мережа працює у постійному циклі перевірки даних,які поступають від камери і при виявленні людини, ідентифікує її особистість та робить перевірку з користувачами, зареєстрованими у системі.

Штучна нейронна мережа підключена до бази даних облич, де зберігаються еталонні зображення осіб для порівняння. Цей компонент важливий для верифікації особи, оскільки саме він дозволяє порівняння отриманого зображення з наявними у базі даних для верифікації особистості користувача.

Підсистема інтелектуальної аутентифікації облич надає на мікроконтролер логічну 1 при вдалій ідентифікації особи та 0 при не вдалій.

Засоби передачі та збереження інформації грають ключову роль у забезпеченні взаємодії між компонентами системи. Вони дозволяють ефективно обмінюватися даними між камерою, базою даних, модулем штучного інтелекту та мікроконтролером.

2.3. Опис технічної складової автоматизації процесу керування вхідними дверима та його компонентів

Автоматизація процесу керування вхідними дверима є важливою складовою частиною загальної системи інтелектуальної аутентифікації облич та автоматизації доступу. Елементи системи, відповідальні за процес керування вхідними дверима забезпечують ефективне та безпечне управління доступом до приміщень на основі даних, отриманих від підсистеми інтелектуальної аутентифікації облич. У цьому розділі детально розглянуто основні компонент, принципи їх роботи та взаємодії, а також заходи, що забезпечують її надійність та безпеку.

Мікроконтролер (МК) є центральним елементом підсистеми, який отримує та обробляє дані від інших компонентів. Він виконує команди, що стосуються відкриття та закриття дверей, а також реагує на сигнали про проблеми.

Мікроконтролер приймає сигнали від штучної нейронної мережі (ШНМ) про успішну або неуспішну аутентифікацію облич (логічна 1), а також від модуля датчиків (логічна 1) та розраховує величину сигналу розугодження ε:

$$\varepsilon = X - Y, \tag{2.1}$$

де ε - величина сигналу розузгодження, X - сигнал про позитивний результат аутентифікації, Y - сигнал від датчику про закритий стан дверей.

Якщо двері відкриті і не потребують корекції стану, сигнал $Y = 0$, тому функція $\varepsilon = 1$, у випадку, коли двері не закрились, $Y = 1 \Rightarrow \varepsilon = 0$, що означає необхідність відповідних дій. На основі цих даних він приймає рішення про відкриття або закриття дверей. Мікроконтролер також контролює стан електронних компонентів системи, забезпечуючи своєчасне виявлення та реагування на несправності.

Магнітні електронні замки забезпечують фізичне блокування або розблокування дверей, що є важливим для контролю доступу до приміщень. Магнітні замки працюють на основі електромагнітного принципу. Подача електричного струму утримує двері зачиненими, а його відключення дозволяє їх відкрити. Замки отримують команди від мікроконтролера, що забезпечує їх синхронізовану роботу з іншими компонентами системи.

Модуль датчиків стану дверей (МД) використовується для визначення стану відчинення або зачинення дверей та уникнення електронних несправностей та пожеж. Модуль датчиків складається з трьох основних типів датчиків: датчика стану дверей (reed-switch [24])), механічного датчика (наприклад, Honeywell 914CE18-3 [25]) та датчика напруги (ACS712 [26]). Датчик стану дверей (reed-switc [24]) реагує на зміну магнітного поля, що дозволяє швидко та точно визначити стан дверей без фізичного контакту.

Механічний датчик Honeywell 914CE18-3 визначає механічне блокування дверей та їх точне положення через фізичний контакт. Датчик напруги ASC712 є необхідним для моніторингу електричних параметрів системи, що дозволяє своєчасно виявляти та реагувати на електронні збої, він підвищує надійність системи, забезпечуючи своєчасне виявлення та реагування на електронні несправності, це потенційно небезпечні ситуації, що можуть призвести до пошкодження обладнання або пожежі. Використання всіх типів датчиків забезпечує надійний контроль стану дверей та виявлення можливих проблем.

Комунікаційний модуль може забезпечити передачу сигналів на пульт охорони, вахтера або технічну службу, що дозволить своєчасно інформувати відповідні служби про стан системи та можливі проблеми. Залежно від умов та системи по місцю встановлення, можуть використовуватися різні типи комунікаційних модулів, такі як GSM-модуль або модуль Wi-Fi. Комунікаційний модуль може отримувати сигнали від мікроконтролера про стан дверей та можливі проблеми і передавати їх відповідним службам. Це забезпеччить оперативне реагування на несправності та підвищить загальну надійність системи, детальніше розглянуто у розділі 2.4.

2.3.1. Опис процесу керування автоматизованим відкриттям дверей

Відкриття дверей. Після успішної аутентифікації обличчя ШНМ надсилає сигнал на мікроконтролер. Мікроконтролер обробляє сигнал і надсилає команду на магнітні електронні замки для відкриття дверей. Датчик стану дверей (reed-switch [24]) підтверджує факт відкриття дверей, що дозволяє системі відстежувати реальний стан дверей у режимі реального часу.

Закриття дверей. Після проходження особи через двері, датчики стану дверей фіксують їх закриття. Мікроконтролер отримує сигнал від датчиків і надсилає команду на магнітні електронні замки для блокування дверей. Це забезпечує автоматичне закриття дверей після проходження користувача, що підвищує безпеку та зручність використання системи.

Реагування на проблеми. Якщо датчики виявляють механічне блокування дверей, мікроконтролер надсилає сигнал на пульт охорони або вахтера. Це дозволяє оперативно реагувати на механічні проблеми, що можуть заважати нормальній роботі дверей. Якщо виявлено електронний збій, мікроконтролер надсилає сигнал безпосередньо електрикам або технічній службі через комунікаційний модуль. Це забезпечує своєчасне виявлення та усунення електронних несправностей, що можуть вплинути на роботу системи.

Забезпечення безпеки. Елементи автоматизації процесів керування вхідними дверима забезпечують безпеки завдяку постійному моніторингу стану дверей та оперативному реагуванню на більшість можливих проблем. Використання різних типів датчиків дозволяє виявляти як механічні, так і електронні збої, що підвищує загальну надійність системи. Комунікаційний модуль може забезпечувати своєчасне інформування відповідних служб про будь-які інциденти, що дозволяє швидко вжити необхідних заходів для їх усунення.

2.4. Комунікаційний модуль та його роль у системі інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверним

Комунікаційний модуль відіграє важливу роль у забезпеченні безпеки та ефективності системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима. Хоча розроблювана система може функціонувати без цього модуля, його встановлення може значно підвищити рівень контролю та оперативного реагування на різні ситуації. У цьому розділі розглянуто типи комунікаційних модулів, їхні функції та заходи для забезпечення їхньої надійності.

2.4.1. Типи можливих комунукаційних модулів у системі інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

GSM-модуль забезпечує мобільний зв'язок через мережі стільникового зв'язку, що дозволяє передавати сигнали навіть у віддалених місцях, де немає доступу до інших видів зв'язку. Це особливо корисно для об'єктів, розташованих у важкодоступних районах або будівель, де немає стабільного інтернет-з'єднання. Основним недоліком GSM-модуля є залежність від якості покриття мережі оператора мобільного зв'язку. У місцях зі слабким сигналом ефективність роботи модуля може знижуватися. Крім того, використання GSM-модуля може вимагати додаткових витрат на послуги мобільного зв'язку.

Модуль Wi-Fi забезпечує високошвидкісну передачу даних через бездротову локальну мережу. Це дозволяє швидко і надійно передавати сигнали на пульт охорони, вахтера або технічну службу. Wi-Fi модулі легко інтегруються в існуючу інфраструктуру будівлі, де вже є доступ до інтернету. Основним недоліком Wi-Fi модуля є обмежений радіус дії та залежність від стабільності бездротової мережі. У великих будівлях або місцях з багатьма перешкодами сигнал може втрачати силу, що впливає на надійність передачі даних. Також можливі проблеми з безпекою мережі, якщо вона не захищена належним чином.

2.4.2. Функції комунікаційного модуля

Комунікаційний модуль може надсилати повідомлення про стан дверей, зокрема про їх відчинення або зачинення, а також про виявлення будь-яких несправностей чи спроб несанкціонованого доступу. Це дозволяє охоронцям оперативно реагувати на будь-які інциденти та забезпечувати безпеку об'єкта. У разі виявлення проблем із дверима (наприклад, механічного блокування або електронного збою), комунікаційний модуль може надсилати

сигнали на пульт вахтера. Це дозволяє вахтеру своєчасно вжити необхідних заходів для усунення проблеми та забезпечення нормального функціонування системи. Комунікаційний модуль може надсилати сигнали про серйозні електронні несправності безпосередньо до технічної служби. Це забезпечує швидке реагування на технічні проблеми та мінімізує ризик тривалого простою системи.

2.4.3. Забезпечення стабільної та безперебійної роботи комунікаційного модуля

Для забезпечення стабільної та безперебійної роботи комунікаційного модуля необхідно врахувати кілька важливих аспектів. Комунікаційний модуль повинен бути підключений до джерела безперебійного живлення (UPS), щоб забезпечити його роботу навіть у разі відключення електроенергії. Це особливо важливо для GSM-модулів, які повинні залишатися функціональними для передачі сигналів у будь-яких умовах. Для Wi-Fi модулів важливо забезпечити мінімізацію перешкод у бездротовій мережі. Це можна досягти шляхом налаштування мережі на менш завантажені канали, встановленні його у відповідному місці та використання сучасних стандартів бездротового зв'язку, таких як Wi-Fi 6, що забезпечують кращу продуктивність і стабільність з'єднання. Комунікаційні модулі повинні регулярно перевірятися на працездатність. Це включає тестування зв'язку, оновлення програмного забезпечення та перевірку всіх з'єднань. Регулярне обслуговування допомагає виявляти та усувати потенційні проблеми до того, як вони вплинуть на роботу системи. Для захисту даних, що передаються через комунікаційні модулі, необхідно використовувати сучасні методи шифрування. Це допоможе запобігти несанкціонованому доступу до інформації та забезпечити конфіденційність переданих даних, що може зменшити відсоток можливості несанкціонованого доступу до приміщення і в цілому збільшити захист будівлі.

Таким чином, комунікаційний модуль може бути дуже важливим елементом системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима, а його встановлення залежить від конкретних умов та потреб об'єкта, де буде використовуватися система. Використання комунікаційних модулів дозволяє підвищити рівень безпеки та оперативності реагування на різні ситуації, що робить систему більш ефективною та надійною.

2.5. Висновки розділу структурна схема системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

У цьому розділі було детально розглянуто структурну схему системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима. Розробка структурної схеми дозволила визначити основні компоненти системи, їх функції та взаємодію, а також заходи для забезпечення надійності та безпеки системи.

Система інтелектуальної аутентифікації облич та автоматизації процесів керування вхідними дверима є комплексним рішенням, яке включає різні компоненти для забезпечення безпеки та зручності користувачів. Основні елементи системи, такі як модуль камери, штучна нейронна мережа, мікроконтролер, магнітні електронні замки та модуль датчиків стану дверей, працюють у тісній взаємодії для забезпечення ефективного контролю доступу. Мікроконтролер є центральним елементом системи, який отримує та обробляє дані від інших компонентів. Він виконує команди, що стосуються відкриття та закриття дверей, а також реагує на сигнали про проблеми. Завдяки мікроконтролеру система може автоматично реагувати на зміну стану дверей та виявляти можливі несправності. Використання різних типів датчиків, таких як датчик стану дверей (reed-switch [24]), механічний датчик (Honeywell 914CE18-3 [25]) та датчик напруги (ACS712), забезпечує надійний контроль стану дверей та виявлення можливих проблем.

Це дозволяє системі своєчасно реагувати на механічні та електронні збої, що підвищує загальну надійність системи. Комунікаційний модуль, такий як GSM-модуль або модуль Wi-Fi, може бути доданий до системи для підвищення рівня контролю та оперативного реагування на різні ситуації. Його встановлення залежить від конкретних умов та потреб об'єкта, де буде використовуватися система. Використання комунікаційних модулів дозволяє своєчасно інформувати відповідні служби про стан системи та можливі проблеми, що підвищує її ефективність та надійність. Для забезпечення стабільної та безперебійної роботи системи необхідно враховувати кілька важливих аспектів, таких як резервне живлення, мінімізація перешкод у мережі, регулярне тестування та обслуговування, а також використання сучасних методів шифрування для захисту даних. Це дозволить запобігти несанкціонованого доступу та забезпечити конфіденційність переданих даних.

Таким чином, структурна схема системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима є важливим етапом у розробці та впровадженні цієї системи. Вона дозволяє користувачам детально зрозуміти взаємодію між компонентами, визначити їх функції та забезпечити надійність та безпеку системи в приміщенні. Схема дозволяє забезпечити достатній рівень контролю доступу та оперативне реагування на будь-які несправності.

3. РОЗРОБКА ШТУЧНОЇ НЕЙРОННОЇ МЕРЕЖІ ДЛЯ АВТОМАТИЗАНОЇ ІНТЕЛЕКТУАЛЬНОЇ АУТЕНТИФІКАЦІЇ ОБЛИЧ

3.1. Використання TensorFlow у розробці нейронних мереж

TensorFlowє одним із провідних інструментів у галузі машинного навчання та штучного інтелекту, розробленим командою Google Brain. Як відкрита програмна платформа, вона забезпечує широкий спектр інструментів для розробки та навчання нейронних мереж, що дозволяє вирішувати складні завдання, пов'язані з обробкою даних, класифікацією, прогнозуванням та багатьма іншими аспектами штучного інтелекту, на рис. 3.1 відображено інтерфейс користувача платформи [22]

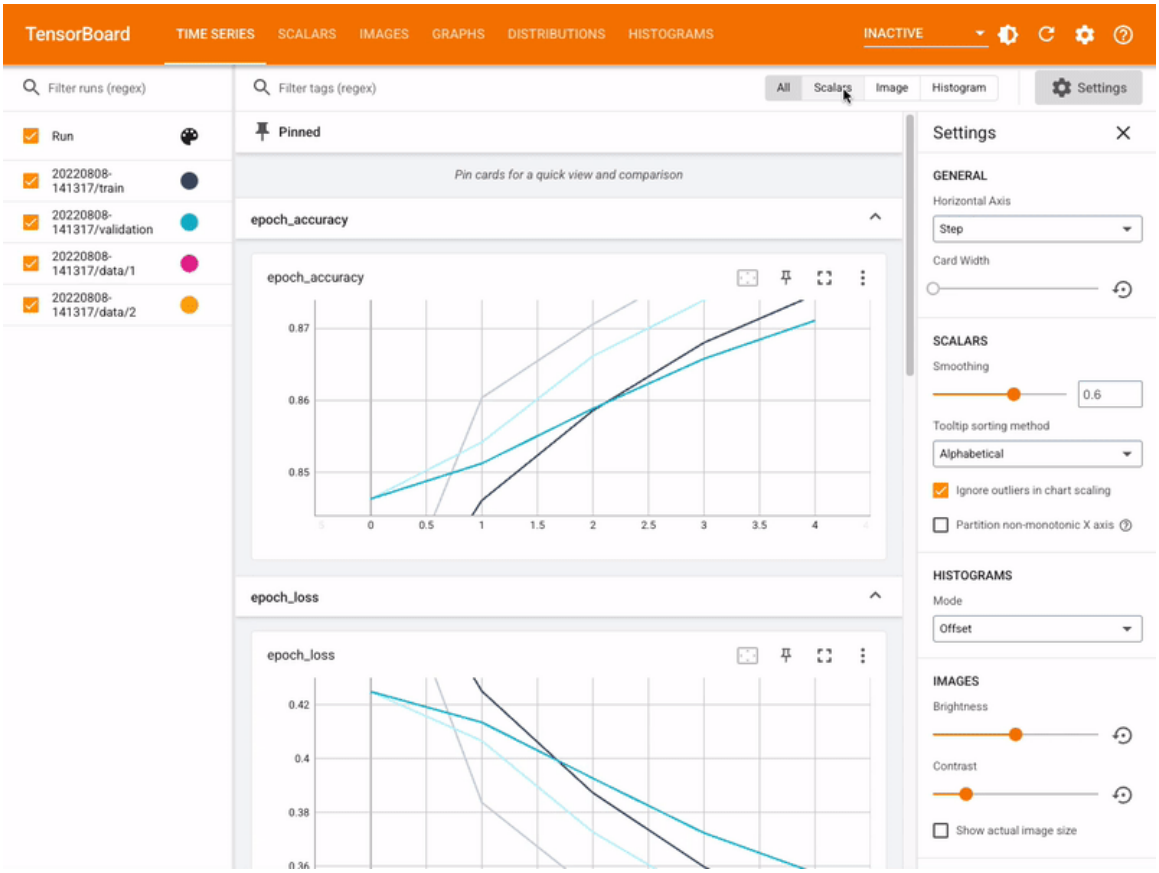

Рис. 3.1. Інтерфейс одного з інструментів середовища TensorFlow [22]

Гнучка архітектура TensorFlow дозволяє легко маніпулювати математичними операціями та шаровими абстракціями, які є основою нейронних мереж. Це дуже корисно, оскільки сприяє експериментуванню з новими моделями та швидкому впровадженню змін. Завдяки модульній структурі TensorFlow можна швидко змінювати архітектуру мережі, додавати нові шари та оптимізувати процес навчання. Це особливо важливо для нашого проекту, оскільки дозволяє швидко адаптувати моделі до специфічних вимог розпізнавання облич [22].

Масштабованість є ще однією важливою перевагою TensorFlow. Платформа підтримує розподілену обробку, що дозволяє ефективно використовувати ресурси багатьох пристроїв для навчання моделі. Це надзвичайно важливо для проекту з розпізнавання облич та керування вхідними дверима, де потрібно обробляти великі обсяги даних в реальному часі. Можливість масштабування дозволяє покращити швидкість обробки та точність розпізнавання облич. Підтримка розподіленої обробки у TensorFlow дозволяє ефективно масштабувати процеси обчислень, використовуючи як один CPU чи GPU, так і цілу мережу пристроїв у хмарних обчисленнях. Це допомагає оптимізувати обробку великих обсягів даних у реальному часі, що може стати критично важливим для точного та швидкого розпізнавання облич у проекті керування вхідними дверима, якщо його буде встановлено на великих підприємствах та великих об’єктах. В умовах великої кількості дверей та потреби у великих ресурсах для обчислення та роботи системи, TensorFlow забезпечує необхідну продуктивність та надійність [22].

Широкий спектр функціональностей TensorFlow робить його надзвичайно привабливим для розробників та дослідників. Завдяки великій спільноті користувачів та розробників, існує доступ до значного обсягу ресурсів для навчання та підтримки. Це включає в себе детальну документацію, готові до використання модулі та передовий досвід, який можна застосувати у власних проектах.

Така підтримка дозволяє зосередитися безпосередньо на процесі розробки моделей, не витрачаючи час на написання базових функцій з нуля. Крім того, можливість швидко отримувати допомогу та знаходити рішення на різних етапах розробки та вдосконалення моделей нейронних мереж є величезною перевагою [22].

Враховуючи всі ці переваги, використання TensorFlow у проекті забезпечить не лише високу точність розпізнавання облич та ефективне керування вхідними дверима, але й сприятиме швидкому розвитку та оптимізації нейронних мереж для вирішення конкретних завдань. У даному дослідженні було обрано TensorFlow через його гнучкість, масштабованість, підтримку спільноти та високу продуктивність. Ці характеристики роблять його ідеальним вибором для потреб проекту з розпізнавання облич та автоматизації процесу керування вхідними дверима [22].

Найпростіший спосіб встановити TensorFlow – це використання командного рядка (Command Prompt) з наступною командою: `pip install tensorflow`.

3.2. Вимоги до штучної нейронної мережі для автоматизаної інтелектуальної аутентифікації облич

Для ефективної роботи розроблюваної системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима, розроблювана ШНМ для автоматизаної інтелектуальної аутентифікації облич повинна відповідати наступним вимогам забезпечення:

1. високої точності ідентифікації, з урахуванням того, що похибка не повинна перевищувати 5%;
2. швидкої обробки даних в режимі реального часу;
3. економії енергоспоживання та обчислювальних ресурсів;
4. гнучкості, універсальності та легкої модернізації.

3.3. Розробка баз даних для навчання та тестування штучної нейронної мережі для автоматизаної інтелектуальної аутентифікації облич

Основою для навчання шнм велику кількість зображень облич людей. Було використано загальнодоступні датасети, LFW (Labeled Faces in the Wild) [27, 28, 29]. База даних містить понад 13 000 зображень облич, зібраних з Інтернету. Кожне обличчя підписано ім'ям людини, яка на ньому зображена. - CelebA (CelebFaces Attributes Dataset (CelebA) - це масштабний набір атрибутів облич, що містить понад 220 тисяч зображень знаменитостей. Зображення в цьому наборі даних охоплюють великі варіації поз і захаращення фону.) Набір даних WIDER FACE - це еталонний набір даних для розпізнавання облич, зображення з якого вибрано з загальнодоступного набору даних WIDER. У датасеті є 32 203 зображення і позначено 393 703 обличчя з високим ступенем варіативності масштабу, пози та оклюзії.

Для успішного навчання штучних нейронних мереж для розпізнавання облич необхідно мати анотовані зображення, де кожне обличчя на зображенні чітко позначене. Якщо використовується датасет зображень без міток, необхідно провести анотування, щоб забезпечити точність та надійність навчання.

Як було зазначено у розділі 1, технічний процес розмітки даних для навчання нейронної мережі є важливим етапом у створенні системи розпізнавання облич. Цей процес включає в себе три кроки.

1. Збір даних, при якому були збережені зображення з різних датасетів, одні з яких будуть використані для навчання нейронної мережі, що навчиться ідентифікувати образи облич, а інші, з готовим анотуванням атрибутів – для створення образів умовних персон, яким буде дозволений доступ до приміщень. Важливо, щоб було багато зображень цих персон в різних умовах (ракурс, вираз обличчя, різноматні перекриття частин облич іншими фізичними об’єктами і тп.)

2. Наступним етапом йде нормалізація зображень, такі як видалення шуму та покращення якості зображень та анотування даних. Але оскільки при навчанні використовуються оброблені зображення, то залишається лише сортування.

3. Останнім фактором залишається анотування. Вона буває ручна, напівавтоматична, або автоматизована розмітка зображень. Кожен з цих методів має свої переваги та недоліки, які впливають на точність та ефективність процесу анотування.

Ручна анотування зображень є найбільш трудомістким та часозатратним методом. Проте вона забезпечує найвищу точність, оскільки кожне зображення перевіряється та позначається вручну. Це гарантує, що всі анотування є дійсними та правильними.

Повністю автоматичні методи використовують алгоритми машинного навчання для автоматичного визначення та анотування облич на зображеннях. Цей підхід є найшвидшим і найефективнішим для великих датасетів, оскільки не потребує людського втручання. Проте точність цих методів може бути нижчою порівняно з ручною або напівавтоматичним анотуванням, особливо якщо алгоритм не був добре навчений або якщо дані містять складні випадки. Особливо цьому може сприяти проблема перенавчення глибоких моделей штучних нейронних мереж у кінцевому продукті, які описано у розділі 1.

Для прикладу, буде проілюстровано процес ручної розмітки зображень для анотування зображень, тому що для встановлення системи на місці, публічні датасети зображень не підійдуть. Обов’язково потрібно зробити власний датасет зображень для аутентифікації користувачів з активним доступом. У майбутньому я планую розглянути можливості використання напівавтоматичних та автоматичних методів анотування з комбінацією інших методів визначення облич, щоб підвищити ефективність процесу без значної втрати точності.

Додатковим кроком може бути створення навчальних наборів даних, а саме розподіл даних на навчальні, тестові та валідаційні набори, але у проекті це буде зроблено у кодовому вигляді.

Приклад ручного анотування зображень.

Процес анотування доволі часто також предбачає складнощі пов’язані з обмеженим доступом до ефективних програм та алгоритмів, які ефективно аналізують зображень на наявність на них облич. Тому для прикладу у проекті була обрана ілюстрація ручного анотування зображень, оскільки це дуже простий метод. Але треба брати до уваги, що на великих датасетах це може бути надзвичайно важким завданням і навіть абсолютно безглуздим.

Технічна складова цього процесу може виглядати так:

1. Відкривається папка зі зображеннями, які треба анотувати (рис. 3.1).
2. Використовується інтерфейс інструмента, з яким проводиться анотування для створення рамок навколо облич на кожному зображенні (рис. 3.2).
3. Збереження готового анотування й у форматі XML або TXT (рис. 3.3). Обов’язково треба переконатися, що анотування зберігаються у тій же структурі папок, що й зображення.

Рис. 3.2. Приклад облич у базі даних LFW [23].

3.4. Синтез штучної нейронної мережі

У процесі розробки інтелектуальної системи аутентифікації облич, важливим завданням є вибір оптимальної архітектури нейронної мережі, яка забезпечить високу точність та ефективність роботи системи. Враховуючи проведений аналіз розділу 1, було вирішено приділити увагу використанню моделей глибокого навчання для обробки зображення, а саме, використання алгоритмів згорткових нейронних мереж (CNN) для екстракції ознак обличчя. Було проведено огляд популярних архітектур CNN та їх придатність до проекту.

3.4.1. VGG (Visual Geometry Group)

VGG є одним з найпростіших у реалізації, пропонуючи стандартизовану архітектуру, яка демонструє високу ефективність у багатьох задачах комп'ютерного зору. Простота цих моделей може сприяти легкості розуміння та модифікації системи, що є корисним для легкого встановлення системи та покращенням безпосередньо встановленої системи.

Основний недолік VGG полягає у високому споживанні пам'яті та обчислювальних ресурсів. Це може стати проблемою для мобільних пристроїв або систем з обмеженим обладнанням.

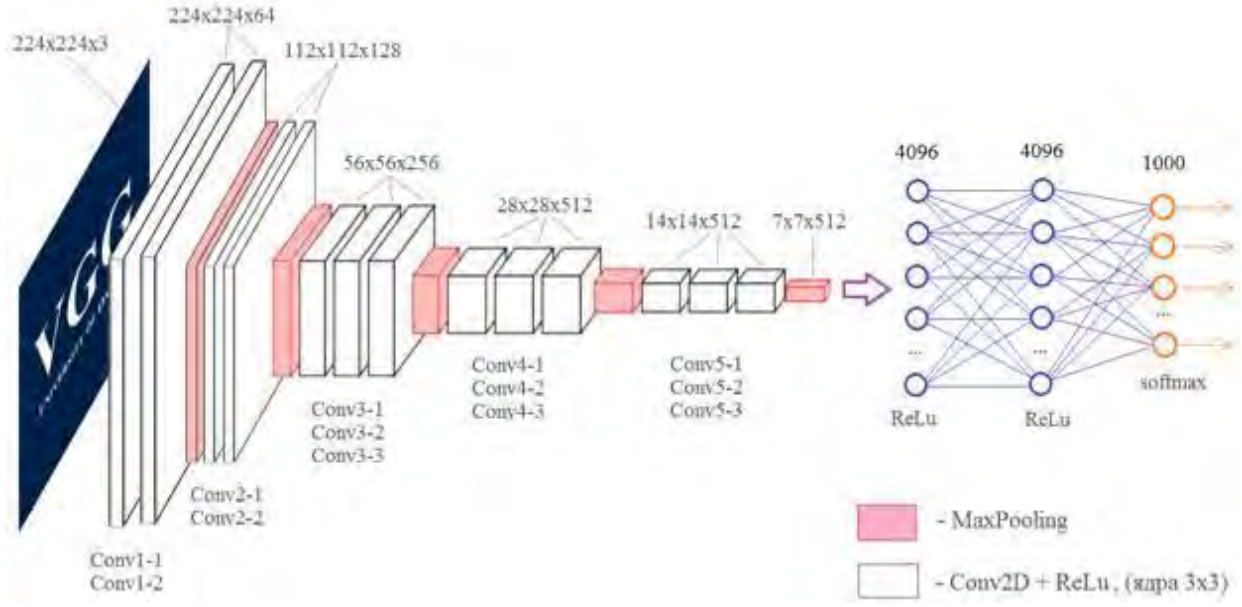

Рис. 3.1. Архітектура моделі VGG

3.4.2. ResNet (Residual Networks)

Архітектура ResNet вирішує проблему зникання градієнта, що є важливою перевагою для глибоких нейронних мереж, завдяки використанню залишкових блоків. Ця архітектура дозволяє створювати дуже глибокі моделі, що позитивно впливає на точність розпізнавання облич. Висока точність є необхідною для системи, яка використовуватиметься у важливих сферах, де помилки можуть мати серйозні наслідки, таких як система інтелектуальної аутентифікації облич.

Ідея, яка лежить у основі ResNet отримала назву глибоке залишкове навчання (deep residual learning), яке лягло в основу мережі ResNet. Суть цієї ідеї полягає в тому, що навчити «залишкову» функцію значно простіше, ніж вихідну. Це пов'язано з тим, що залишкові блоки дозволяють моделі вчитися на різниці між передбаченням і фактичними даними, що полегшує оптимізацію глибоких мереж.

У мережах VGG-16 і VGG-19 було всього 16 і 19 шарів. У мережі GoogLeNet – 22 шари, а в першому варіанті ResNet – 152 шари. Зараз це число досягає тисяч рівнів у глибину.

Існує дуже багато варіантів цієї архітектури, де додаються різні керуючи шари для регулювання передавання обхідних даних, але доволі часто звичайний «обхідний» шлях, показує хороші результати, часто навіть кращі, ніж інші модифіковані варіанти, тому у написанні проектного коду було використовувано модель ResNet 50.

Проте треба розуміти, що незважаючи на великі переваги, ResNet вимагає значних обчислювальних ресурсів для ефективної роботи. Однак, проект може дозволити собі таку складність, оскільки використовується потужна апаратна платформу з процесором Ryzen 6 5800H та графічним процесором GeForce RTX 3060 Mobile. Ця архітектура була оптимізована компанією NVIDIA, вона видає достатньо високий відсоток якості та має декілька версій.

3.4.3. MobileNet

MobileNet оптимізована для мобільних і вбудованих систем, пропонуючи ефективне споживання ресурсів без значної втрати точності. Це робить її ідеальною для застосунків, де необхідно забезпечити баланс між продуктивністю та енергоефективністю.

При всій ефективності та легкості використання, MobileNet може не досягати такої ж точності, як більш складні моделі, як наприклад, ResNet або VGG. Це може бути критичним у випадках, де безпека є найважливішою метою, оскільки точність розпізнавання облич має вирішальне значення. Однак, варто зауважити, що MobileNet може бути корисним в ситуаціях критичної необхідності використання системи з обмеженими ресурсами, де швидкість роботи є пріоритетом. Також, цю модель можна використовувати для проведення тестів під час встановлення системи або для швидкого прототипування нових ідей без значних витрат ресурсів.

3.4.4. Опис розробленої штучної нейронної мережі

Вхідний та вихідний вектори системи. Вхідний вектор системи складається з анотованих зображень облич, які завантажуються з датасетів CelebA і LFW. Кожне зображення нормалізується та перетворюється у формат, який може бути оброблений нейронною мережею. Для нейромережі ResNet. Це 224 на 224 пікселі. Тобто вхідний вектор має розмірність 224 на 224 Вихідний вектор являє собою ймовірності приналежності зображення до певної категорії (ідентичності особи), тобто від 0 до 1.

Для навчання системи використовувався метод навчання з учителем. Вхідні дані містять зображення облич, а вихідні дані – відповідні мітки (ідентичності). Модель навчається на основі цих пар (вхід-вихід), намагаючись мінімізувати помилку передбачення.

В якості алгоритму оптимізації був використаний алгоритм зворотного

поширення помилки (backpropagation) з градієнтним спуском. Реалізація алгоритму здійснюється за допомогою бібліотеки TensorFlow, яка автоматично обчислює градієнти та оновлює вагові коефіцієнти мережі.

Вагові коефіцієнти (weights) – це параметри, які визначають вплив кожного нейрону на вихідний сигнал. Ініціалізація вагових коефіцієнтів здійснюється випадковим чином з діапазону від 0 до 1. Це реалізовано за допомогою вбудованих методів TensorFlow. Далі з кожною ітерацією. або ж епохою (епоха – це один повний цикл навчання на всьому датасеті), вагові коефіцієнти змінюються і головна мета штучної нейронної мережі – після кожної епохи оновити такі коефіцієнти, щоб помилка передбачення була мінімальною. У коді цей процес реалізований через функції тренування (fit) бібліотеки TensorFlow. Умова зупинки розробленої нейронної мережі – це досягнення 3 епох без значного покращення результатів. Це реалізовано за допомогою callback-функції EarlyStopping з параметром patience, що дорівнює 3.

Функція активації визначає вихід нейрону на основі його вхідних сигналів. У даній реалізації використовуються такі функції активації, як ReLU для прихованих шарів і Softmax для вихідного шару.

3.5. Аналіз коду та пояснення використаних блоків

У коді було використано такі основні бібліотеки:

1. **TensorFlow** -для створення та тренування нейронної мережі.
2. **Scikit-learn** - для попередньої обробки даних і розділення датасету на тренувальний та тестовий.

Основні блоки коду складаються з:

1. Завантаження та підготовка даних. Зображення завантажуються з різних датасетів (CelebA, LFW, WIDER_train, WIDER_val) та підготовлюються для подальшої обробки.

2. Побудова архітектури моделі на основі ResNet50 з додаванням додаткових шарів.

3. Компіляція моделі з вибором оптимізатора (Adam) та функції втрат (binary_crossentropy).

4. Модель тренується з використанням генераторів даних та зупиняється, коли досягнута умова зупинки.

5. Оцінка моделі на тестовому датасеті для оцінки її точності.

3.6. Програмний код та висновки

Програмний код написаний на високорівневій мові програмування Python для синтезування інтелектуальної моделі (штучної нейронної мережі) системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима. Розроблений код демонструє підключення бази даних еталонних зображень облич людей для аутентифікації персон. Він забезпечує анотаування зображень, створення, компіляцію, тренування та оцінку моделі штучної нейронної мережі (рис. 3.4). Код аналізує зображення взяті з датасету зображень – CelebA (202 599 фотокарток) для навчання, проводиться попередня перевірка на датасеті WIDER_val, при не досягненні умови точності, проводиться повторне навчання, з додаванням даних з датасету WIDER_train, а потім навчена модель проводить аутентифікацію з бази даних користувачів з готовою анотування зображень LFW (11 зареєстрованих персон).

Код складається з таких блоків (додаток А):

1. Імпорт бібліотек (рис. 3.2, 3.3). В цьому блоку відбувається імпорт необхідних бібліотек та модулів для роботи з даними, моделями та метриками.

2. Callback для зупинки навчання при досягненні точності. Визначається клас StopAtAccuracy, який є callback'ом для зупинки тренування моделі при досягненні певного рівня точності на валідаційному наборі.

3. Функції для завантаження зображень. Містить функції load_images_from_dir та load_celeba_images, які завантажують зображення з вказаних директорій.

4. Функції для тренування моделі (рис. 3.4, 3..5). Включає функції train_model для тренування моделі з оптимізованими параметрами та evaluate_model для оцінки моделі на тестовому наборі.

5. Основна функція main. В цій функції відбувається завантаження даних з різних директорій, розподіл їх на навчальний та валідаційний набори, тренування моделі та оцінка її результатів на тестових наборах. Також передбачено можливість додавання додаткових даних для покращення результатів моделі.

6. Функція retrain_with_additional_data (рис. 3.8). Визначає функцію для повторного тренування моделі з додаванням нових даних для поліпшення її точності.

7. Виклик функції ain (рис. 3.7). Виклик основної функції ain для виконання всіх кроків: завантаження даних, тренування моделі та оцінки результатів. Цей код призначений для роботи з зображеннями облич для аутентифікації

доступ за домовленістю з авторами

Рис. 3.2. Імпорт всіх бібліотек

доступ за домовленістю з авторами

Рис. 3.3. Завантаження зображень та анотування

доступ за домовленістю з авторами

Рис. 3.4 Підготовка генераторів даних

доступ за домовленістю з авторами

Рис. 3.5 Частина коду для тренування моделі

доступ за домовленістю з авторами

Рис. 3.7. Основна функція ain

доступ за домовленістю з авторами

Рис. 3.8. Функція для повторного тренування з додавання нової даних

4. НАВЧАННЯ ТА ЕКСПЕРИМЕНТАЛЬНІ ДОСЛІДЖЕННЯ ПРАЦЕЗДАТНОСТІ ШТУЧНОЇ НЕЙРОННОЇ МЕРЕЖІ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОЇ АУТЕНТИФІКАЦІЇ ОБЛИЧ І АВТОМАТИЗАЦІЇ ПРОЦЕСІВ КЕРУВАННЯ ВХІДНИМИ ДВЕРИМА

4.1. Стратегія досягнення мети моделі штучної нейронної мережі системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

Стратегія досягнення мети моделі штучної нейронної мережі полягала у поступовій інтеграції додаткових даних, проведенні експериментів з різними наборами даних, і оптимізації гіперпараметрів моделі. Для досягнення мети ідентифікації осіб з точністю не менше 95% були використані наступні підходи та методики:

1. Навчання моделі відбувалось в ітеративному режимі, де після кожного циклу тренування проводилось тестування точності на валідаційних наборах даних. У разі недостатньої точності, модель донавчалась з використанням додаткових даних з набору WIDER_train. Цей підхід дозволив поступово покращувати точність моделі та уникнути перенавчання.

2. Для оцінки прогресу моделі використовувались проміжні тестування на наборах даних, відмінних від тренувальних. Це допомогло виявити потенційні проблеми з узагальненням та забезпечити стабільну продуктивність моделі на нових даних.

3. У процесі навчання проводилась оптимізація гіперпараметрів моделі, таких як кількість епох, розмір міні-батчів, швидкість навчання та інші. Це дозволило знайти оптимальні налаштування, які забезпечують найкращий баланс між точністю та часом навчання.

4. Після досягнення високої точності на тестових наборах даних, модель тестувалась на аутентифікацію на нових особах з набору LFW.

Успішне проходження цього етапу підтвердило здатність моделі досягати високої точності (не менше 95%) в реальних умовах використання системи.

4.2. Перше експериментальне дослідження працездатності штучної нейронної мережі системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

Навчання штучної нейронної мережі – це завжди дуже довгий та ресурсомісткий процес, у розділі 3 було було налоголошено, що для швидкого синтезу нейромережі краще використовувати архітектуру MobileNet, процес навчання якої може дати менш точні результати, але відбуватись набагато швидше та потребувати менших обчислювальних ресурсів. Один прогон моделі може займати різний час через різні вхідні дані. Враховуючи, що вагові коефіцієнти з самого початку визначаються випадково, цей процес може займати різний час на різному обладнанні. Для першого експеременту було використано 3 людини для тестування та лише 1 датасет для навчання, на рис. 4.1 представлена ілюстрація процесу навчання штучної нейронної мережі при першому експеременті. Навчання моделі при першому експериментальному дослідженні процесу навчання штучної нейронної мережі займало від 10 хвилин до пів години. Процес тестування штучної нейронної мережі на 3 особах, з 940 зображеннями цих осіб у різних умовах зайняв для першої особи 21 секунду, для другої особи 8 секунд та для третьої особи 5 с. Точність навченої нейронної мережі була для першої особи – 95 % (рис. 4.2), для другої особи – 100 % (рис. 4.3), для третьої – 100% (рис. 4.4).

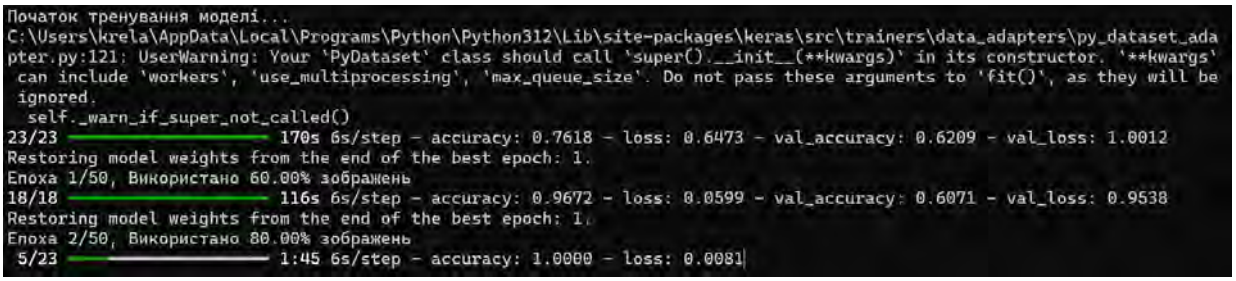

Рис. 4.1. Ілюстрація процесу навчання штучної нейронної мережі

```
'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Colin_Powell' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Colin_Powell' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Colin_Powell' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Colin_Powell' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Colin_Powell' 'Tony_Blair' 'Colin_Powel
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair'
 'Tony_Blair' 'Tony_Blair' 'Tony_Blair' 'Tony_Blair']
Точність верифікації для Tony_Blair: 0.95
```

Рис. 4.2. Ілюстрація процесу тестування натреваної моделі штучної нейронної мережі на еталонному зображенні першої особисті

```
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell'
 'Colin_Powell' 'Colin_Powell' 'Colin_Powell' 'Colin_Powell']
Точність верифікації для Colin_Powell: 1.00
```

Рис. 4.3. Ілюстрація процесу тестування натреваної моделі штучної нейронної мережі на еталонному зображенні другої особисті

```
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush' 'George_W_Bush' 'George_W_Bush'
 'George_W_Bush' 'George_W_Bush']
Точність верифікації для George_W_Bush: 1.00
```

Рис. 4.4. Ілюстрація процесу тестування натреваної моделі штучної нейронної мережі на еталонному зображенні третьої особисті

4.3. Фінальне експериментальне дослідження працездатності штучної нейронної мережі системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

Проаналізувавши вхідні, тривалість одного прогону моделі та оцінювання точності вихідних даних, стало очевидним, що створена модель має недолік у кількості осіб для аутентифікації для точного визначення, адже навіть при перевірці трьох осіб, модель видавала не гарантоване роспізнавання облич. Були проведені деякі оптимізації роботи системи, а також додано більше вхідних даних для проведення навчання штучної нейронної мережі системи інтелектуальної аутентифікації – було додано бібліотеку WIDER_train для повторного навчання моделі, на випадок, якщо оцінюванно точності не співпало з очікуваними результатами аутентифікації, проміжне тестування на датасеті WIDER_test, використано більше осіб для аутентифікації з датасету LFW. Було створено можливість обрати кількість зображень для навчання моделі, що дозволить нейромережі навчитися набагато швидше, якщо для навчання використовуються великі обчислювальні ресурси.

Тривалість навчання нової моделі сильно залежить від кількості зображень, які використовуються для першої спроби навчання. При обиранні лише 500 зображень з першого датасету, нейромережа доходить до 95 % точності при тестуванні на 11 особах за приблизно 30 хвилин хвилин, адже їй треба проводити багато тестувань та додаткових навчань, при обиранні 1500 зображень, результат у 95 % отримується за 10-20 хвилин, при обиранні 2000 зображень результат отримується за більший проміжок часу та потребує набагато більше ресурсів. Експериментальним дослідженням, було визначено, що приблизний оптимальний результат – 1500. При обиранні більшого числа зображень – швидкість збільшиться, але збільшиться кількість ресурсів необхідних для споживання ШНМ.

4.4. Дослідження впливу різних факторів на точність та швидкість роботи штучної нейронної мережі системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

У процесі навчання та тестування моделі було досліджено вплив різних факторів на її продуктивність. Основними факторами, що впливали на точність та швидкість роботи моделі, були вибір базової архітектури моделі, кількості навчальних зображень, використання різних

Вибір базової архітектури моделі, у даному випадку ResNet50, має великий вплив на результати. Моделі з більшою кількістю параметрів можуть мати кращу точність, але вимагатимуть більше часу для навчання та обчислювальних ресурсів.

Збільшення кількості навчальних зображень значно впливає на точність моделі, проте може збільшити час навчання та обчислювальні витрати. Оптимальна кількість зображень для досягнення певного рівня точності може варіюватися від задачі до задачі. В даному випадку, для досягнення 95% точності, потрібно близько 1500 зображень для базового навчання, з можливістю

подальшого донавчання на більших наборах даних. Також треба брати до уваги при навчанні моделі те, що завантаження у програму великого обсягу данних приводить до використання великої кількості оперативної пам’яті, що може сильно вплинути на працездатність системи.

4.5. Висновки навчань та експериментальних досліджень працездатності штучної нейронної мережі системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

Під час експериментальних досліджень та навчань моделі штучної нейронної мережі для системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима були отримані наступні висновки:

1. Результати експериментів підтвердили можливості розробленої штучної нейронної мережі для системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима проводити ідентифікацію людей з точністю 95 відсотків. Цей показник є достатнім для практичного використання системи у реальних умовах.

2. Для контролю швидкості навчання була розроблена можливість встановлення кількості початкових зображень. Це дозволяє оптимізувати використання обчислювальних ресурсів, що є важливою можливістю для великих обсягів даних та обмежених потужностей обробки.

3. Навчання моделі може займати від 10 до 30 хвилин залежно від кількості використовуваних даних та налаштувань гіперпараметрів. Важливим фактором, який впливає на швидкість є баланс між навантаженням на обчислювальний механізм та витратами часу на навчання.

4. Модель показала високу чутливість до якості вхідних даних. Використання чистих, добре оброблених зображень суттєво підвищувало точність і стабільність результатів. Однак, навіть з використанням змішаних та різних наборів даних розроблена модель доволі швидко доходить до необхідної точності аутентифікації особистості.

5. Експерименти проводились у контрольованих умовах з використанням стандартизованих наборів даних, таких як LFW, CelebA та WIDER. Для оцінки продуктивності використовувались окремі валідаційні та тестові набори даних, що дозволяло об'єктивно оцінити результати моделі.

6. Основна стратегія полягала у порівнянні різних варіантів системи та оптимізації цільової функції. Важливу роль відігравала поступова інтеграція додаткових даних для тренування моделі, що дозволяло покращити її продуктивність та точність.

Ці висновки свідчать про успішність досліджень та ефективність працездатності розробленої штучної нейронної мережі системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

5. РОЗРОБКА АЛГОРИТМІЧНО-ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОЇ АУТЕНТИФІКАЦІЇ ОБЛИЧ І АВТОМАТИЗАЦІЇ ПРОЦЕСУ КЕРУВАННЯ ВХІДНИМИ ДВЕРИМА

5.1. Алгоритмічне забезпечення роботи мікроконтролера системи автоматизованого керування вхідними дверима

Розроблене алгоритмічне забезпечення роботи мікроконтролера системи автоматизованого керування вхідними дверима представлено на рис. 5.1. Розроблене алгоритмічне забезпечення роботи мікроконтролера системи автоматизованого керування вхідними дверима складається з таких основних етапів:

1. Ініціалізація. На цьому етапі система виконує початкові налаштування та перевірку стану всіх необхідних датчиків.

2. Отримання сигналу. Система постійно моніторить сигнал від датчика стану дверей (ДС), який сповіщає про відкриття або закриття дверей.

3. Перевірка стану дверей. Якщо датчик ДС фіксує, що двері знаходяться у відкритому стані, система переходить до наступного етапу. Якщо двері закриті, система повертається до етапу моніторингу сигналу.

4. Очікування. Система очікує протягом 5 секунд, щоб дати можливість особі пройти через двері.

5. Закриття дверей. Після закінчення часу очікування, система подає сигнал для закриття дверей. Датчик ДС фіксує, що двері знаходяться у закритому стані.

6. Аналіз додаткових даних. Система перевіряє сигнали з додаткових датчиків Д1, Д2 та Д3, які можуть сповіщати про нештатні ситуації (датчики напруги, магнітний та механічний).

7. Реакція на нештатні ситуації. Якщо один або кілька датчиків фіксують нештатну ситуацію, система надсилає сигнал до служби обслуговування для подальшого реагування.

8. Повернення до початку. Після виконання всіх дій, система повертається до етапу моніторингу сигналу від датчика ДС.

Такий алгоритм забезпечує керування вхідними дверима, реагуючи на зміну їх стану та аналізуючи додаткові дані для виявлення можливих несправностей чи нештатних ситуацій.

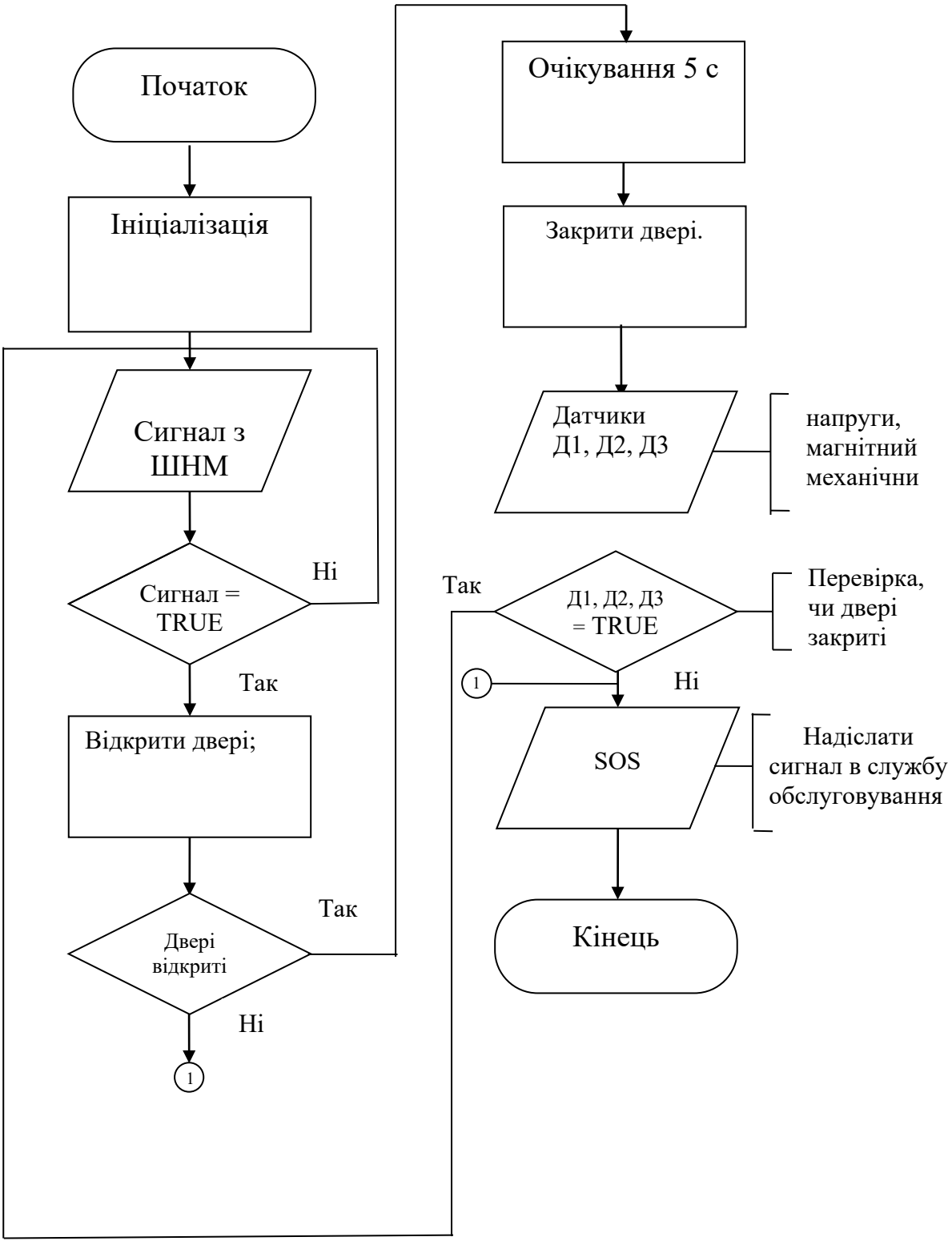

Рис. 5.1. Блок-схема алгоритмічного забезпечення роботи мікроконтролера системи автоматизованого керування вхідними дверима

5.2. Алгоритмічне забезпечення системи інтелектуальної аутентифікації облич

Алгоритмічне забезпечення системи інтелектуальної аутентифікації облич представлене блок-схемою на рис. 5.2, використовується для ідентифікації та перевірки осіб на основі їх облич. Ця система використовує штучну нейронну мережу для розпізнавання облич та автоматичної аутентифікації користувачів.

Основні етапи алгоритму складаються з:

1. **Збору даних**. Процес інтелектуальної аутентифікації обличчя починається зі збору даних. Це можуть бути зображення або відеозаписи облич користувачів.

2**. Попередньої обробки даних**. Зібрані дані піддаються попередній обробці. Зображення обличчя перетворюються у формат (224x224 пікселів), що є стандартним розміром для подальшої обробки нейронною мережею.

3. **Розподілу даних**. Дані розподіляються на навчальний та валідаційний набори. Це дозволяє моделі навчитись на одному наборі даних і перевірити свою ефективність на іншому.

4. **Тренування ШНМ**. Модель штучної нейронної мережі тренується на навчальному наборі даних. Процес тренування включає в себе багато епох, протягом яких модель намагається мінімізувати похибку і покращити точність розпізнавання.

5. **Оцінки точності моделі**. Після кожної епохи тренування модель оцінюється на валідаційному наборі даних. Якщо точність (μ) на валідаційному наборі перевищує 98%, модель допускається до наступного етапу.

6. **Аутентифікації особистості**. На цьому етапі модель перевіряється на наборі для аутентифікації, де знову оцінюється точність (μ1). Якщо точність перевищує 95%, аутентифікація вважається успішною, і система дає сигнал для відкриття дверей.

7. **Завершення**. Якщо модель досягає необхідної точності на всіх етапах, процес аутентифікації завершується успішно. У протилежному випадку, процес тренування повторюється з додаванням нових даних для покращення моделі.

Розроблений алгоритм, представлений на рис. 5.2 забезпечує ефективну роботу систему розпізнавання облич для аутентифікації користувачів системи

інтелектуальної аутентифікації облич, використовуючи сучасні технології машинного навчання та штучного інтелекту.

Рис. 5.2. ББлок-схема алгоритмічного забезпечення системи інтелектуальної аутентифікації облич

5.3. Програмне забезпечення синхронізації роботи мікроконтролера та системи автоматизованого керування вхідними дверима

Цей розділ описує приклад розробки програмного забезпечення для синхронізації роботи мікроконтролера та системи автоматизованого керування вхідними дверима, основна мета якого - забезпечити ефективне управління дверима, включаючи функції розпізнавання користувачів, контролю доступу та моніторингу стану дверей.

Приклад алгоритму роботи коду програмного забезпечення синхронізації роботи мікроконтролера та системи автоматизованого керування вхідними дверима виглядає так:

1. Ідентифікація користувача проходить таким чином - камера виявляє присутність користувача і зображення з неї передаються ШНМ для обробки.

2. Перевірка доступу також відбувається за рахунок ШНМ. Мережа звіряє дані користувача з базою даних і у разі позитивного результату - надається дозвіл на доступ.

3. Управління дверима забезпечує мікроконтролер, який керує замками для відкриття або закриття дверей.

4. Моніторинг стану дверей здійснюється за допомогою датчиків - у разі виявлення несправностей або проблем - надсилається сигнал на відповідні служби.

Нижче розроблений приклад коду для реалізації описаних функцій.

```
#include <xc.h>
#include <stdio.h>
#include <stdlib.h>
```

Рис. 5.3. Імпорт бібліотек

Імпорт білбліотек представлений на рис. 5.3, на рис.5.4 представлені налаштування пінів та ініціалізація мікроконтролера

доступ за домовленістю з авторами

Рис. 5.4. Налаштування пінів та ініціалізація мікроконтролера

На рис. 5.4 та рис. 5.5 представлені налатування ініціалізації та головна функція коду.

доступ за домовленістю з авторами

Рис. 5.5. Головна функція коду

5.4. Розробка інтерфейсу користувача системи інтелектуальної аутентифікації облич і автоматизації процесу керування вхідними дверима

Приклад коду простого інтерфейсу користувача системи інтелектуальної аутентифікації облич і автоматизації процесу керування вхідними дверима з візуальними індикаторами стану системи, було розроблено на мові Python з використанням бібліотеки Tkinter. Інтерфейс буде мати індикатор стану дверей - відкриті чи закриті, та індикатор результату аутентифікації – успішна чи невдала. На рис. 5.6 представлено для інтерфейсу користувача.

доступ за домовленістю з авторами

Рис. 5.6. Код для інтерфейсу користувача

Розроблений інтерфейс користувача системи інтелектуальної аутентифікації облич і автоматизації процесу керування вхідними дверима використовує чіткі, зрозумілі написи, виділяє важливу інформацію жирним шрифтом і кольором, щоб максимально полегшити сприйняття користувачем. З таким інтерфейсом ористувач може легко зрозуміти стан системи та побачити результат аутентифікації. Для подальшого вдосконалення, можна додати оновлення стану системи в реальному часі, можливість налаштувань, журнал подій і інші вижливі функції.

5.5. Висновки розробки алгоритмічно-програмного забезпечення системи інтелектуальної аутентифікації облич і автоматизації процесу керування вхідними дверима

У цьому розділі було представлено розробки алгоритмічно-програмного забезпечення системи інтелектуальної аутентифікації облич і автоматизації процесу керування вхідними дверима, яку можна описати так:

1. Була розроблена схема алгоритмічного забезпечення мікроконтролера, представлена на рис. 5.1, що має забезпечувати управління вхідними дверима, що, в свою чергу, дозволяє реалізувати автоматичне відкриття та закриття на основі сигналів від системи розпізнавання облич. Мікроконтролер обробляє сигнали від системи розпізнавання облич і приймає рішення про доступ, керуючи електронними замками дверей

2. Алгоритмічне забезпечення системи інтелектуальної аутентифікації облич, зображене на рис. 5.2, дозволяє розробити ШНМ з високою точність ідентифікації осіб. Використання штучної нейронної мережі дозволяє досягти точності понад 95% при тестуванні на стандартизованих наборах даних. Основні етапи алгоритму включають збір даних, попередню обробку, розподіл на навчальні та валідаційні набори, тренування моделі та перевірку точності. Успішна ідентифікація користувача призводить до відкриття дверей

3. Розроблене програмне забезпечення синхронізації роботи мікроконтролера та системи автоматизованого керування вхідними дверима забезпечує ідентифікацію користувача, перевірку доступу, управління дверима та моніторинг їх стану. Це дозволяє створити ефективну систему керування доступом.

4. Розроблений інтерфейс користувача забезпечує зручність у використанні системи. Інтерфейс дозволяє користувачам легко взаємодіяти з системою аутентифікації, отримувати доступ до вхідних дверей та відстежувати стан системи. Розроблений інтерфейс може сприяє підвищенню ефективності

використання системи в реальних умовах.

Завдяки використанню сучасних технологій машинного навчання та штучного інтелекту, система забезпечує контроль доступу та зручність використання для кінцевих користувачів. Оптимізація алгоритмів та програмного забезпечення дозволила досягти високої продуктивності і забезпечити функціонування системи в різних умовах експлуатації. У цьому розділі було охоплено весь процес алгоритмічно-програмного забезпечення системи інтелектуальної аутентифікації облич і автоматизації процесу керування вхідними дверима.

6. СХЕМА ЕЛЕКТРИЧНА ПРИНЦИПОВА СИСТЕМИ ІНТЕЛЕКТУАЛЬНОЇ АУТЕНТИФІКАЦІЇ ОБЛИЧ І АВТОМАТИЗАЦІЇ ПРОЦЕСІВ КЕРУВАННЯ ВХІДНИМИ ДВЕРИМА

6.1. Список всіх елементів електричної принципової схеми системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

У цьому розділі було розглянуто вибір електронних компонентів для створення принципової схеми системи аутентифікації облич і автоматизації процесів керування вхідними дверима, який складається представлена на рис. 6.1 та складається з таких елементів:

1. мікроконтролера PIC 16F818. Це основний контролер, який керує всією системою.

2. інтерфейсної мікросхеми CP2102. Вона забезпечує зв язок між мікроконтролером та комп ютером через SB-порт.

3. роз єму SB-типу. Вони використовуються для підключення живлення та передачі даних.

4. польових транзисторів з N-каналом IRL 44N . Вони керують струмом великої амперності, які необхідні для керування замками або іншими потужними пристроями.

5. резисторів SMD 0805. Вони використовуються для обмеження струму та налаштування робочих режимів компонентів.

6. діоди SS14. Вони захищають від зворотного струму та використовуються заради стабілізація напруги.

7. імпульсного трансформатора Pulse Electronics PH9185NL. Він забезпечує ізоляцію та перетворення напруги.

8. фотоелементу LDR (англ. Lig t Dependent Resistor) GLS5209. Цей фотоелемент використовується у PIR датчику.

10. блоку живлення 5V 2.5A Power Supply. Він забезпечує живлення компонентів системи.

11. блоку живлення LEDMO 12V 5A Power Supply Adapter. Це додаткове джерело живлення запезпечує роботу м кроконтролера та деяких елементів системи.

12. конденсатори Murata GRM155R61A106 A01 забезпечують фільтрацію та згладжування напруги.

13. проводів AWG 22. Ці проводу з діаметром 0.64 мм використовується для з'єднання компонентів, забезпечуючи необхідний рівень провідності для передачі сигналів і живлення

Ця система розпізнає обличчя та автоматично керує замками вхідних дверей, забезпечуючи високий рівень безпеки та зручності для користувачів. PIR датчик виявляє рух, LDR перевіряє рівень освітлення для цього, а мікроконтролер приймає рішення на основі вхідних даних та алгоритмів розпізнавання обличчя. Транзистори керують електричними замками, а імпульсний трансформатор та конденсатори забезпечують стабільну роботу всієї системи.

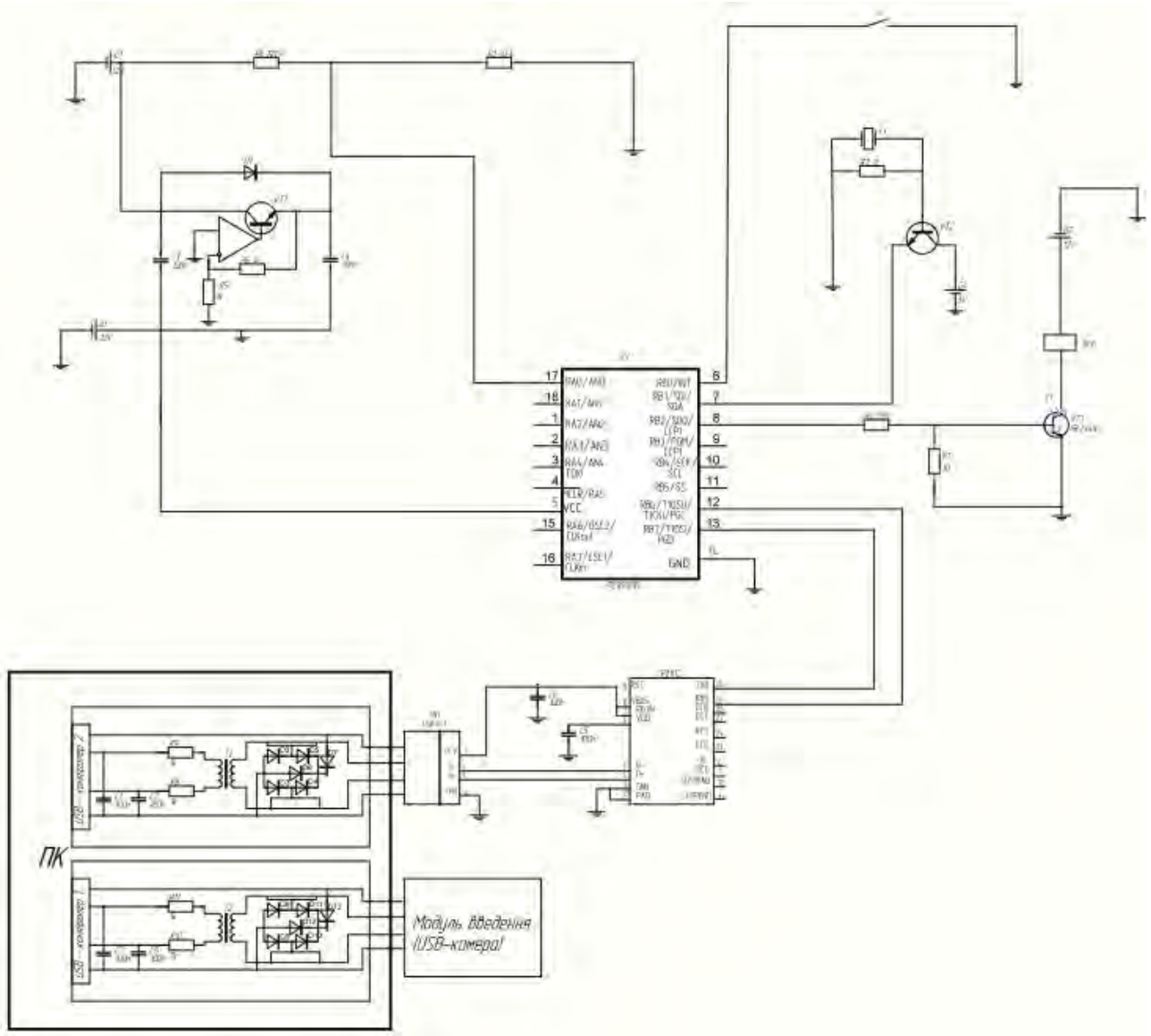

Рис. 6.1. Електрична принципова схеми системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

6.2. Функції основних компонентів схеми електричної принципової системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

Функції основних компонентів схеми електричної принципової системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима представлені таким списком:

1. за обробку сигналів від датчиків та виконання програмного забезпечення, яке керує всією системою відповідає мікроконтролер PIC16F818.

2. реагує на рух, забезпечуючи контроль над механічними перешкодами при замиканні дверей PIR датчик.

3. за забезпечення надійного обміну даними між мікроконтролером та зовнішніми пристроями через SB інтерфейсна мікросхема CP2102.

4. за забезпечення високої потужності для керування електромеханічними замками використовуються польові транзистори IRL 44N.

5. дозволяє системі адаптуватись до перебоїв напруги, покращуючи точність контролю дверей датчик напруги.

6.3. Принцип роботи системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

Принцип роботи системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима полягає у етапах обробки даних, керування пристроями та взаємодії між компонентами системи.

Система інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима складається з кількох основних компонентів, які забезпечують злагоджену роботу всіх підсистем. Мікроконтролер отримує сигнали від датчиків, обробляє їх і приймає рішення про відкриття або закриття дверей

6.3.1. Принцип роботи мікроконтролера PIC16F818

Мікроконтролер PIC16F818 є центральним елементом системи, який керує всіма процесами. Він відповідає за:

1. **ініціалізацію** системи при включенні.
2. **обробку сигналів** від PIR датчика, датчика струму та датчика reed-switc .
3. **керування** магнітним замком для відкриття закриття дверей.

Мікроконтролер отримує сигнали від датчиків через аналогові та цифрові входи, обробляє їх за допомогою вбудованого програмного забезпечення та приймає відповідні рішення.

6.3.2. Обмін даними через USB

Інтерфейсна мікросхема CP2102 забезпечує зв'язок між мікроконтролером та комп ютером через SB-порт. Це дозволяє передавати дані про стан системи, отримувати оновлення програмного забезпечення та налаштування. CP2102 перетворює сигнали ART мікроконтролера у формат, зрозумілий для SB-порту комп ютера.

6.3.3. Обробка сигналів від датчиків

Система використовує декілька датчиків для забезпечення точної роботи:

1. PIR датчик, який виявляє рух біля дверей і передає сигнал мікроконтролеру, який аналізує його для визначення наявності особи. Процес відбувається за допомогою сигналу з LDR, який допомагає визначити це.
2. Датчик стану дверей reed-switc реагує на зміну магнітного поля, що дозволяє швидко та точно визначити стан дверей без фізичного контакту.
3. Датчик напруги є необхідним для моніторингу електричних параметрів системи, що дозволяє своєчасно виявляти та реагувати на електронні збої, він підвищує надійність системи, забезпечуючи своєчасне виявлення та реагування на електронні несправності, це потенційно небезпечні ситуації, що можуть призвести до пошкодження обладнання або пожежі.

Використання всіх типів датчиків забезпечує контроль стану дверей та виявлення можливих проблем.

6.3.4. Керування електромеханічними замками

Польові транзистори IRL 44N використовуються для керування електромеханічними замками. Вони дозволяють керувати струмом, необхідним для активації замків. Мікроконтролер через цифрові виходи керує транзисторами, які вмикають або вимикають електроживлення замків залежно від результатів обробки сигналів та алгоритмів розпізнавання облич.

6.3.5. Живлення системи

Система живиться від двох блоків живлення, а саме блока жвилення на 5V 2.5A, який забезпечує живлення для мікроконтролера та інших малопотужних компонентів та блока живлення на 12V 5A, який забезпечує додаткове живлення для таких елементів як електромеханічні замки.

Конденсатори Murata GRM155R61A106 A01 забезпечують фільтрацію та згладжування напруги, що забезпечує стабільну роботу системи, захищаючи її від збоїв у живленні.

6.4. Інтеграція всіх компонентів у єдину систему інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

Усі компоненти інтегровані у єдину систему, яка працює за наступним принципом:

1. При включенні система ініціалізує всі компоненти.
2. PIR датчик, датчик напруги та датчик reed-switc постійно моніторять оточення і передають дані мікроконтролеру.
3. Мікроконтролер обробляє отримані сигнали і, за необхідності, запускає алгоритм розпізнавання облич.
4. У разі успішної аутентифікації, мікроконтролер активує транзистори, які відкривають електромеханічні замки.

5. Обмін даними через SB дозволяє моніторити стан системи та забезпечує її роботу.

Ця система забезпечує зручність для користувачів, автоматично керуючи замками вхідних дверей на основі розпізнавання облич.

6.5. Висновки розробленої схеми електричної принципової системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима

Розроблена схема електричної принципової системи інтелектуальної аутентифікації облич та автоматизації процесів керування вхідними дверима має забезпечувати високу ефективність і надійність у забезпеченні доступу до приміщень. Було проведено аналіз та написані висновки, а саме:

1. Розроблена система розпізнавання облич на базі згорткових нейронних мереж має забезпечувати високу точність ідентифікації користувачів, навіть при змінних умовах освітлення та різних виразах облич. Використання високочутливих камер і сенсорів дозволяє зменшити кількість помилкових позитивних та негативних спрацьовувань, забезпечуючи надійність системи.

2. Автоматизація процесів керування вхідними дверима з використанням мікроконтролерів та датчиків має забезпечити швидке та безперебійне відкривання та закривання дверей. Система може бути інтегрована до існуючих механізмамів блокування дверей, що дозволяє легко впроваджувати її в різні типи будівель і споруд.

3. Розроблена трьохрівнева системи безпеки, що включає розпізнавання облич та контроль доступу, перевірка за допомогою датчиків стану деверй та датчика напруги, знижує ризик несанкціонованого доступу.

4. Схема розроблена таким чином, що може бути легко масштабована для використання в різних умовах, від житлових приміщень до великих комерційних будівель. Структура з легко замінними дозволяє легко додавати нові функціональні можливості та інтегрувати додаткові системи безпеки.

5. Використання енергоефективних компонентів та оптимізація алгоритмів роботи системи дозволяє знизити енергоспоживання, що є

важливим для тривалого безперервного функціонування. Система може працювати від альтернативних джерел живлення, таких як сонячні батареї, що підвищує її автономність.

6. Інтерфейс користувача розроблений з урахуванням зручності та інтуїтивної зрозумілості, що спрощує процес реєстрації нових користувачів та налаштування системи. Система забезпечує швидку ідентифікацію та мінімальний час очікування для користувачів.

Підсумовуючи висновки, розроблена схема електричної принципової системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима має демонструвати високу ефективність, надійність і безпеку, що робить її перспективною для впровадження в різні типи об'єктів. Подальший розвиток системи може включати інтеграцію з іншими біометричними методами, що додатково підвищить рівень безпеки та зручності використання.

ЗАГАЛЬНІ ВИСНОВКИ

Проект, присвячений розробці системи інтелектуальної аутентифікації облич і автоматизованого керування вхідними дверима, включав 6 важливих етапів. Системи інтелектуальної аутентифікації та автоматизованого керування вхідними дверима здатні підвищувати рівень безпеки без значного залучення людських ресурсів.

1. На першому етапі було проведено аналіз сучасного стану проблеми інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима, на підставі якого було визначено основні проблеми. Головними проблемами є перенавчання цих моделей на навчальних даних, що може призвести до значного зниження точності розпізнавання на відмінних від навчальних даних. Також впровадження новітніх алгоритмів розпізнавання облич зустрічає низку викликів, таких як необхідність ретельної розробки моделей та архітектур нейронних мереж, проведення численних експериментів з параметрами навчання, що потребує значних обчислювальних ресурсів та часу. Проаналізувавши стан проблеми інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима, було виявлено, що багато існуючих систем розпізнавання облич розроблені комерційними компаніями і призначені для продажу, що обмежує можливості дослідників для проведення порівняльних досліджень та тестування нових алгоритмів. Незважаючи на те, що сучасні розробки забезпечують високий рівень безпеки та можуть бути інтегровані з іншими системами контролю доступу, користувачі все ж стикаються з низкою випробувань, головними з яких є ціна та фрагментарність даних.

2. На другому етапі було розробено структурну схему системи інтелектуальної аутентифікації облич і автоматизації процесів керування дверима, що дозволило визначити основні компоненти системи, їх функції та взаємодію для забезпечення стабільної роботи системи. Основні елементи системи, такі як модуль камери, штучна нейронна мережа, мікроконтролер, магнітні електронні замки та модуль датчиків стану дверей, працюють у тісній взаємодії для ефективного контролю доступу. Мікроконтролер є центральним елементом, який обробляє дані та виконує команди, забезпечуючи автоматичну реакцію на зміну стану дверей і виявлення несправностей.

Додаткові комунікаційні модулі, такі як GSM або Wi-Fi, підвищують рівень контролю та оперативного реагування. Схема дозволяє забезпечити достатній рівень контролю доступу та оперативне реагування на будь-які несправності.

3. На третьому етапі було розроблено штучну нейронну мережу для системи автоматизованої інтелектуальної аутентифікації облич на високорівневій мові програмування Python. Запропоновані методи розв'язання проблеми перенавчання моделей на навчальних даних включають поступове збільшення навчальних даних та проведення тестів на зображеннях з різних джерел, таких як Wider_train, Wider_val, lfw_deepfunneled та Celeba_dataset. ШНМ використовує датасети CelebA і LFW для навчання. Зображення нормалізуються до розміру 224 на 224 пікселів і обробляються нейронною мережею ResNet. Навчання проводиться методом з учителем з використанням алгоритму зворотного поширення помилки та градієнтного спуску, реалізованого в TensorFlow. Для підвищення ефективності навчання застосовується функція EarlyStopping. Основні компоненти системи включають завантаження і підготовку даних, побудову архітектури моделі, компіляцію, тренування та оцінку точності на тестових датасетах. Крім того, було розглянуто використання MobileNet для мобільних і вбудованих систем, яка забезпечує ефективне споживання ресурсів при прийнятній точності. MobileNet ідеально підходить для застосувань з обмеженими ресурсами та швидким прототипуванням, хоча може поступатися точністю складнішим моделям, таким як ResNet чи VGG. Це рішення дозволяє збалансувати продуктивність і енергоефективність, що важливо для впровадження в реальних умовах з обмеженими ресурсами, або тестуванню системи.

4. На четвертвому етапі у процесі експериментальних досліджень було розроблено та протестовано систему інтелектуальної аутентифікації облич з автоматизацією керування вхідними дверима. Система використовує нейронну мережу ResNet, що навчається на датасетах CelebA і LFW, досягаючи точності ідентифікації 95%. Для оптимізації використання обчислювальних ресурсів була впроваджена можливість налаштування кількості початкових зображень. Модель демонструє що навчання займає від 10 до 30 хвилин, залежно від обсягу даних і налаштувань гіперпараметрів. Експерименти проводилися з використанням стандартизованих наборів даних, а також поступового збільшення навчальних

даних, що забезпечило об'єктивну оцінку результатів моделі і дозволило уникнути значного зниження точності на нових даних.

5. На п’ятому етапі було розроблено алгоритмічно-програмне забезпечення системи інтелектуальної аутентифікації облич і автоматизації процесу керування вхідними дверима. У цьому розділі було представлено розробки алгоритмічно-програмного забезпечення системи інтелектуальної аутентифікації облич і автоматизації процесу керування вхідними дверима, що має забезпечувати управління вхідними дверима, що дозволяє реалізувати автоматичне відкриття та закриття на основі сигналів від системи розпізнавання облич. Алгоритмічне забезпечення системи інтелектуальної аутентифікації облич дозволяє розробити ШНМ з високою точність ідентифікації осіб. Використання штучної нейронної мережі дозволяє досягти точності понад 95% при тестуванні на стандартизованих наборах даних. Розроблене програмне забезпечення синхронізації роботи мікроконтролера та системи автоматизованого керування вхідними дверима забезпечує ідентифікацію користувача, перевірку доступу, управління дверима та моніторинг їх стану. Розроблений інтерфейс користувача забезпечує зручність у використанні системи. Інтерфейс дозволяє користувачам легко взаємодіяти з системою аутентифікації, отримувати доступ до вхідних дверей та відстежувати стан системи. Розроблений інтерфейс може сприяє підвищенню ефективності роботи системи.

6. На останньому, шостому, етапі була розроблена схема електрична принципова системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима. що забезпечує високу точність та швидкість розпізнавання облич, яка була досягнута завдяки розробленій та навченій штучній нейронній мережі. Інтеграція мікроконтролерів та датчиків дозволяє швидко та надійно автоматизувати процеси відкривання і закривання дверей. Трьохрівнева система безпеки значно знижує ризик несанкціонованого доступу, а зручний інтерфейс користувача спрощує налаштування та використання системи. Розроблена схема залишає можливість подальшого розвитку, яка полягає у тому, що система може бути інтегрована з іншими біометричними методами аутентифікації. Була розроблена специфікація всіх елементів схеми електричної принципової системи інтелектуальної аутентифікації облич і автоматизації процесів керування вхідними дверима.

Узагальнюючи, розроблена система забезпечує:

1. високу точність та швидкість розпізнавання облич, яка була досягнута завдяки розробленої та навченій штучній нейронній мережі.

2. бесперебійну роботи системи, яка була досягнута за рахунок ретельного проектування структурної схеми та алгоритмічно-програмного забезпечення.

3. зручність, яку для користувачів забезпечив інтерфейс системи розроблений таким чином, щоб система була максимально проста та інтуїтивно зрозуміла.

4. можливість подальшого розвитку, яка полягає у тому, що система може бути інтегрована з іншими біометричними методами, що додатково підвищить рівень безпеки та зручності використання.

На сьогоднішній день все зростає актуальність теми розробленої системи. Це пов'язано з швидким розвитком штучних нейронних мереж та потребою впровадження більшої кількості автоматичних систем аутентифікації у житлові та комерційні об'єкти. Таким чином, розроблена система має перспективи для впровадження у різні типи об'єктів, забезпечуючи високий рівень безпеки та комфорту для користувачів.

ПЕРЕЛІК ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Хорошун О.В. Особливості використання інформаційного порталу для систематизації та зберігання інформації / Хорошун О.В., Дегтярьова Л. М. // Новітні інформаційні системи та технології – 2018. – № 9. – Режим доступу до ресурсу: https://dspace.pdau.edu.ua/server/api/core/bitstreams/6fbf681a-4f9a-4691-be71-d515cc5bc82a/content

2. Turk, M. Eigenfaces for recognition / Turk, M., Pentland, A. // Journal of Cognitive Neuroscience – 1991. – № 3. pp 71–86. DOI: 10.1162/jocn.1991.3.1.7

3. Guangcheng Zhang. Boosting Local Binary Pattern (LBP) - Based Face Recognition -Advances in Biometric Person Authentication /Guangcheng Zhang, Xiangsheng Huang, Stan Z. Li // Sinobiometrics 2004, LNCS 3338, pp. 179–186, 2004 – Режим доступу до ресурсу: https://link.springer.com/chapter/10.1007/978-3-540-30548-4_21

4. Ahonen T. Face Recognition with Local Binary Patterns / Timo Ahonen, Abdenour Hadid, Matti Pietikäinen // Computer Vision - ECCV 2004, Volume 3021 (2004), pp 469–481. ISBN: 978-3-540-21984-2 – Режим доступу до ресурсу: https://link.springer.com/chapter/10.1007/978-3-540-24670-1_36

5. Rahim A. Face Recognition using Local Binary Patterns (LBP) / Rahim A., Hossain N., Wahid T., Azam S. // Global Journal of Computer Science and Technology Graphics & Vision Volume 13 Issue 4 Version 1.0 (2013) – Режим доступу: https://globaljournals.org/GJCST_Volume13/1-Face-Recognition-using-Local.pdf

6. Belhumeur P. N. Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection/ Belhumeur P. N., Hespanha J. P., Kriegman D. J. // IEEE Transactions on Pattern Analysis and Machine Intelligence Volume 19 Issue 7 July (1997) pp. 711–720; DOI: 10.1109/34.598228

7. Lawrence S. Convolutional neural networks for face recognition/ S. Lawrence, Giles C.L., Ah Chung Tsoi // Proceedings CVPR IEEE Computer Society Conference on Computer Vision and Pattern Recognition –1996. DOI: 10.1109/CVPR.1996.517077

8. Fisherface /Philipp Wagner// Bytefish.de [Електронний ресурс]. — Режим доступу: https://www.bytefish.de/blog/fisherfaces.html

9. Baliar V. Face Recognition Efficiency for Different Environmental Influence Conditions / Baliar V., Fokin R., Mazurkiewicz O. // 2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T). DOI: 10.1109/PICST54195.2021.9772120

10. Charu C. Aggarwal, Neural Networks and Deep Learning: A Textbook - 1st Edition // Springer, 2018 - 520p.

11. Mahmoud Harmouch. This post goes in-depth analysis and application of LBP (Local Binary Patterns) for image feature extraction. // Medium [Електронний ресурс]. — Режим доступу: https://medium.com/swlh/local-binary-pattern-algorithm-the-math-behind-it-%EF%B8%8F-edf7b0e1c8b3

12. О. В. Яловега, Система виявлення обличчя на зображенні з використанням глибинної згорткової нейронної мережі/ О. В. Яловега, Р. А. Мельник ///Науковий вісник НЛТУ України : збірник наукових праць. Львів, 2022, том 32, № 2. – 96 с. DOI: 10.36930/40320209

13. Mei Wang, Weihong Dengl. Deep Face Recognition/ Mei Wang, Weihong Dengl // Neurocomputing, 2021, 429, pp 215–244 – Режим доступу до ресурсу: https:// doi.org/10.1016/j.neucom.2020.10.081

14. Matri P. SLoG: Large-Scale Logging Middleware for HPC and Big Data Convergence/ Matri P., Carns P., Ross R., Costan A., Pérez M., Antoniu G., // 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS) ; DOI: 10.1109/ICDCS.2018.00156

15. Черепанська І.Ю. Автоматизація процесу керування вибором пристроїв орієнтування при проектуванні гнучких інтегрованих систем: дис. канд. техн. наук: 05.13.07 “Автоматизація процесів керування” / Ірина Юріївна Черепанська. – Житомир, ЖДТУ, 2008. – 380 с

16. Черепанська І.Ю. Прецизійна приладова система вимірювання кутів: дисертація. д-ра т. наук: 05.11.01 – «Прилади та методи вимірювання механічних величин» /Ірина Юріївна Черепанська. –Київ, 2019. – 132 с.

17. Планування, моделювання та верифікація процесів в гнучких виробничих системах: практикум. Навчально-методичний посібник до виконання практичних, лабораторних і самостійних занять студентів спеціальності 7.05020201, 8.05020201 "Автоматизоване управління технологічними процесами" всіх форм навчання / І. Ю. Черепанська, В. А. Кирилович, А. Ю. Сазонов, Б. Б. Самотокін / [під. заг. ред. В. А. Кириловича] – Житомир, ЖДТУ 2015. – 274 с.

18. A. Shashua, "Geometry and Photometry in 3D Visual Recognition," PhD thesis, Massachusetts Institute of Technology, 1992.

19. Схема електрична принципова. [Електронний ресурс]. — Режим доступу: https://wiki.tntu.edu.ua/

20. ДСТУ 2.702:2013. Єдина система конструкторської документації. Правила виконання електричних схем. [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ua/catalog/doc-page?id_doc=60892

21. Жученко А. І. Технології штучного інтелекту та основи машинного зору в автоматизації: теорія і практика / А. І. Жученко, І. Ю. Черепанська, А. Ю. Сазонов, Д. О. Ковалюк. – Київ, КПІ 2019. – 386 с.

22. Комплексная платформа для машинного обучения TensorFlow. [Електронний ресурс]. –Режим доступу: https://www.tensorflow.org/?locale=ua&hl=ru

23. Biometric update.com [Електронний ресурс]. – Режим доступу: https://www.biometricupdate.com/201912/labeled-faces-in-the-wild-creators-and-anil-jain-each-honoured-for-biometrics-contributions

24. U-PROX. [Електронний ресурс]. – Режим доступу: https://www.u-prox.systems/doc_wdcout

25. MICRO SWITCH Miniature Precision Limit Switches/ Honeywell 002381 Issue 9. [Електронний ресурс]. – Режим доступу: https://prod-edam.honeywell.com/content/dam/honeywell-edam/sps/siot/zh-cn/products/switches/limit-switches/miniature-limit-switches/914ce-series/documents/sps-siot-micro-switch-914ce-limit-product-sheet-002381-9-en-ciid-146337.pdf?download=fals

26. ACS712 Current Sensor. [Електронний ресурс]. – Режим доступу: https://components101.com/sites/default/files/component_datasheet/ACS712%2030a%20range%20current%20sensor%20datasheet.pdf

27. WIDER FACE: A Face Detection Benchmark /Multimedia Laboratory, Department of Information Engineering, The Chinese University of Hong Kong [Електронний ресурс]. – Режим доступу: http://shuoyang1213.me/WIDERFACE/

28. Ziwei Liu. Large-scale CelebFaces Attributes (CelebA) Dataset/Ziwei Liu Ping Luo Xiaogang Wang Xiaoou Tang/[Електронний ресурс]. – Режим доступу: https://mmlab.ie.cuhk.edu.hk/projects/CelebA.html

29. Labeled Faces in the Wild Home [Електронний ресурс]. – Режим доступу: https://www.u-prox.systems/doc_wdcout

ДОДАТКИ