

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра інженерії програмного забезпечення

Пояснювальна записка

до магістерської роботи
на ступінь вищої освіти магістр
на тему: «Інформаційна технологія розпізнавання військової
техніки з використанням аерофотозйомки на основі комп'ютерного зору»

Виконав: студент 6 курсу, групи ПДМ-62
спеціальності 121 Інженерія програмного забезпечення
(шифр і назва спеціальності/спеціалізації)

Гангало І.М.

(прізвище та ініціали)

Керівник Жебка В.В.

(прізвище та ініціали)

Рецензент _____

(прізвище та ініціали)

Нормоконтроль _____

(прізвище та ініціали)

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут інформаційних технологій

Кафедра Інженерії програмного забезпечення

Ступінь вищої освіти -«Магістр»

Спеціальність підготовки – 121 «Інженерія програмного забезпечення»

ЗАТВЕРДЖУЮ

Завідувач кафедри

Інженерії програмного забезпечення Негоденко О.В.

“ ____ ” _____ 2022 року

ЗАВДАННЯ НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

ГАНГАЛУ ІГОРЮ МИКОЛАЙОВИЧУ

(прізвище, ім'я, по батькові)

1. Тема роботи: Інформаційна технологія розпізнавання військової техніки з використанням аерофотозйомки на основі комп'ютерного зору _____

Керівник роботи: Жебка Вікторія Вікторівна, д.т.н., доцент, завідувач кафедри ТЦР,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом вищого навчального закладу від «12» жовтня 2022 року №122.

2. Строк подання студентом роботи 31.12.2022

3. Вхідні дані до роботи

Дані про безпілотні літальні апарати, їх класифікація та застосування.

Комп'ютерний зір як складова систем розпізнавання об'єктів

Науково-технічна література з питань, пов'язаних з розпізнаванням об'єктів, створенням наборів даних, обробкою зображень та навчанням нейронних мереж.

4. Зміст розрахунково-пояснювальної записки(перелік питань, які потрібно розробити).

4.1 Системи ідентифікації, трекінгу та моделі машинного навчання

4.2 Вимоги та оцінка якості системи.

4.3 Опис математичних моделей та проектування системи.

4.4 Опис проектування системи.

5. Перелік демонстраційного матеріалу (назва основних слайдів)

1. Актуальність проблеми
2. Алгоритм проведення розвідувальних дій
3. Порівняння продуктивності та швидкодії технологій розпізнавання
4. Створення датасету
5. Метод максимальної дисперсії (Оцу)
6. Порівняння моделей алгоритму YOLO
7. Порівняльний аналіз версій датасетів

6. Дата видачі завдання 14.10.2022

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	14.10-25.10	
2	Вимоги до системи	28.10-05.11	
3	Оцінка якості тестування до системи	06.11-09.11	
4	Побудова методу	11.11-20.11	
5	Концепція та архітектура програмного забезпечення	21.11-30.11	
6	Вступ, висновки, реферат	30.11-05.12	
7	Розробка презентації	06.11-11.12	

Студент _____
Керівник роботи _____

РЕФЕРАТ

Текстова частина магістерської роботи 88с., 24 рис., 43 джерела.

КОМП'ЮТЕРНИЙ ЗІР, РОЗПІЗНАВАННЯ ОБ'ЄКТІВ, БПЛА, YOLO, ДАТАСЕТ, МЕТОД ОСУ

Мета – покращення процесу розпізнавання військової техніки за допомогою інформаційної технології на основі комп'ютерного зору.

Об'єкт – процес розпізнавання військової техніки.

Предмет – методи та засоби комп'ютерного зору та аерофотозйомки.

Методи дослідження: оптимізаційні методи, методи математичної статистики.

Наукова новизна даної роботи полягає в наступному розроблено інформаційну технологію розпізнавання військової техніки з використанням аерофотозйомки на основі комп'ютерного зору, що дозволяє покращити процес ведення бойових дій

Упровадження розробленого застосунку допоможе користувачам швидше визначати позиції техніки противника, визначати її клас, кількість та передавати інформацію користувачу.

Під час виконання роботи було проаналізовано існуючі методи розпізнавання та відстеження об'єктів, визначено їх переваги та недоліки, завдяки чому було сформоване технічне завдання проекту.

Проаналізовано можливості алгоритму розпізнавання YOLO. Створено набір даних, який було модифіковано методом Осу, навчено нейронну мережу, за допомогою модифікованого датасету та проведено аналіз результатів.

Галузь використання – інформаційна технологія може бути імплементована в системи управління військами для розпізнавання та відстеження військової техніки, в тому числі за допомогою БПЛА.

ЗМІСТ

ВСТУП	10
1 КОМП'ЮТЕРНЕ БАЧЕННЯ, ЯК ОСНОВА АЕРОФОТОЗЙОМКИ	11
1.1 Теоретичні аспекти технології комп'ютерного бачення	11
1.2 Поняття комп'ютерного бачення.	12
1.3 Задачі комп'ютерного бачення.....	14
1.4 Комп'ютерне бачення в військовій справі	16
2 Сучасні методи отримання даних аерофотозйомки	19
2.1 Аерофотозйомка, як засіб отримання розвідданих	19
2.2 Різновиди БпЛА	22
2.2.1 Дрони та безпілотні апарати на службі ЗСУ	25
2.3 Сфери використання БпЛА	28
2.4 Методи та проблематика аерофотозйомки.....	30
2.5 Способи передачі та отримання даних з літальних апаратів	32
2.6 Дослідження проблем безпеки БпЛА	35
2.6.1 Методи виявлення БпЛА.....	37
2.6.2 Методи атаки на БпЛА	40
2.6.3 Міри протидії БпЛА	42
3. Проектування системи та опис мат моделі	49
3.1 Методи розпізнавання об'єктів	49
3.1.1 Сфери застосування методів розпізнавання об'єктів.....	50
3.1.2 Систематизація методів розпізнавання об'єктів.....	50
3.2 Визначення подібності шаблонів	52
3.3 Попередня обробка зображень	54
3.3.1 Підвищення якості зображень	55

3.3.2 Сегментація зображень.....	57
3.4 Трекінг об'єктів та його способи	60
3.4.1 Класифікація показників оцінки для трекінгу об'єктів	63
4. ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ.....	65
4.1 Загальне уявлення про систему	65
4.2 Вибір алгоритму виявлення об'єктів.....	66
4.2.1 Порівняння характеристика популярних методів розпізнавання .	67
4.2.2 Порівняння моделей алгоритму YOLO	69
4.3 Формування датасету та тренування нейронної мережі.....	71
4.3.1 Сервіси для створення датасетів	71
4.3.2 Вплив розміру датасету на якість розпізнавання	72
4.3.3 Використання методу Оцу під час створення датасету	73
4.4 Результати тренування нейронної мережі.....	75
ВИСНОВКИ.....	11
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	12
Додаток.....	17

УМОВНІ ПОЗНАЧЕННЯ

- AFIZ – аеродромна зона польотної інформації (aerodrome flight information zone)
- АТСА – район управління повітряним рухом відомчим органом УПР (air traffic control area)
- АТСЗ – зона управління повітряним рухом відомчим органом УПР (air traffic control zone)
- CNN – convolutional neural network
- CTR – диспетчерська зона (control zone)
- GPS – система глобального позиціонування (Global Positioning System)
- HOG – histogram of oriented gradients
- MOT – Multiple Object Tracking
- MOTA – Multi-Object Tracking Accuracy
- MOTP – Multi-Object Tracking Precision
- R-CNN - Region-based Convolutional Neural Networks
- SIFT – scale-invariant feature transform
- SSD – Single Shot MultiBox Detector
- SVM – support vector machines
- VLOS – пряма видимість (Visual line of sight)
- АФА – аерофотоапарат
- БПЛА – безпілотний літальний апарат
- ВПП – використання повітряного простору
- ДПЛА – дистанційно-пілотовані літальні апарати (ДПЛА)
- ЗУ – Закони України
- ПС – повітряне судно
- ССН – система супутникової навігації
- ШНМ – штучна нейронна мережа

ВСТУП

Використання інформаційних технологій (ІТ) для розпізнавання військової техніки за допомогою аерофотозйомки на основі комп'ютерного зору є відносно новою і цікавою розробкою. Ця технологія має потенціал докорінно змінити спосіб, в який військовослужбовці виявляють загрози і реагують на них. Поєднуючи можливості комп'ютерного зору і аерофотозйомки, військові можуть більш точно і швидко виявляти і реагувати на потенційні загрози.

Використання ІТ для розпізнавання військової техніки за допомогою аерофотозйомки базується на алгоритмах комп'ютерного зору. Ці алгоритми призначені для аналізу зображень, отриманих з аерофотозйомки, та ідентифікації різних об'єктів і ознак. За допомогою комп'ютерного зору військові можуть швидко і точно ідентифікувати різні типи техніки, такі як танки, вертольоти та інші транспортні засоби. Крім того, вони також можуть ідентифікувати різні типи будівель і місцевості.

Мета – покращення процесу розпізнавання військової техніки за допомогою інформаційної технології на основі комп'ютерного зору.

Об'єкт – процес розпізнавання військової техніки.

Предмет – методи та засоби комп'ютерного зору та аерофотозйомки.

Методи дослідження: оптимізаційні методи, методи математичної статистики.

Наукова новизна даної роботи полягає в наступному: розроблено інформаційну технологію розпізнавання військової техніки з використанням аерофотозйомки на основі комп'ютерного зору, що дозволяє покращити процес ведення бойових дій. Упровадження розробленого застосунку допоможе користувачам швидше визначати позиції техніки противника, визначати її клас, кількість та передавати інформацію користувачу. Під час виконання роботи було проаналізовано існуючі методи розпізнавання та відстеження об'єктів, визначено їх переваги та недоліки, завдяки чому було сформоване технічне завдання проекту.

Проаналізовано можливості алгоритму розпізнавання YOLO. Створено набір даних, який було модифіковано методом Осу.

1 КОМП'ЮТЕРНЕ БАЧЕННЯ, ЯК ОСНОВА АЕРОФОТОЗЙОМКИ

1.1 Теоретичні аспекти технології комп'ютерного бачення

Здавна людина використовує органи чуттів для розпізнавання оточуючого світу. Очі – один з таких модулів тіла людини, який відповідає за зчитування образів оточуючого середовища. Проте для того, щоб відтворити та проаналізувати існує ціла зорова система, яка складається з очного яблука, зорового нерва та додаткових структур. Вся ця складна структура слугує лише для одного – обробка та аналіз інформації, яку може зібрати людина навколо себе. Використовуючи всі органи чуттів мозок відтворює об'єкт, визначає приблизну відстань, кольори чи становить він загрозу та інші параметри. Сучасні вчені намагаються автоматизувати все, що пов'язано з людською діяльністю і зоровий апарат не виключення(рис 1.1).

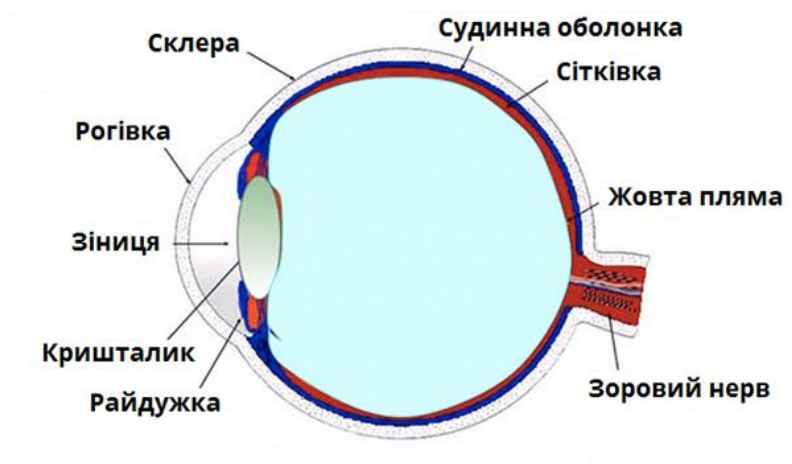


Рисунок 1.1 – Схематичне зображення будови очного яблука [33]

Використовуючи математику та інші науки науковці працюють над дослідженням та створенням методів для вирішення повсякденних та комерційних задач. Складність полягає у тому, що в залежності від завдань, які постають перед вченим чи розробником методи для тієї чи іншої галузі є вузько направлені. Наприклад: система для поливу газону суттєво відрізняється від контролю якості

товарів на виробництві. Також, враховуючи, що для аналізу зчитаних даних потрібні спеціально запрограмовані комп'ютери, то для застосування галузі комп'ютерного зору необхідно продовжувати дослідження.

Як і в людини, комп'ютерний зір застосовується у поєднанні з чимось, з конкретною метою, для вирішення певних задач. На підприємстві комп'ютерне бачення використовується лише як модуль зчитування, який передає дані до сховища чи безпосередньо устаткування, яке обробляє інформацію та проводить з нею певні дії.

Не зважаючи на небувалий розвиток інформаційних технологій та різноманіття рішень, як хмарних так і фізичних, впровадити комп'ютерний зір в повсякденне життя людей дуже ризиковано і вдається лише невеликому відсотку компаній з мільярдними бюджетами.

1.2 Поняття комп'ютерного бачення.

Комп'ютерний зір – це міждисциплінарна наукова галузь, яка займається тим, як комп'ютери можуть отримувати високорівневе розуміння з цифрових зображень або відео. З точки зору інженерії, він прагне зрозуміти і автоматизувати завдання, які може виконувати зорова система людини.[5] Дані для обробки можуть отримуватись з різних джерел, наприклад: масиву камер, відеорядом та іншими.

Використання комп'ютерного бачення можливе в різних сферах життєдіяльності. Як для заміни людини у системах комп'ютерного зору, таких як системи відеоспостереження, моделювання, індексації або як доповнення біологічному зору, як в системах автопілоту автомобіля.

В шістдесятих роках минулого століття, в університетах, які були першопрохідцями в галузі штучного інтелекту, розпочалися перші дослідження комп'ютерного зору. Вони мали на меті імітувати людський орган зору з метою наділення роботів розумною поведінкою. У 1966 році з'явилася думка, що це можна зробити за допомогою літнього експерименту, прикріпивши камеру до комп'ютера і попросивши його "описати те, що він бачив". Що відрізняло комп'ютерну уяву і

передбачення від звичайної обробки віртуальних зображень на той момент, так це перевага отримувати тривимірну структуру з фотографій з метою формування повного уявлення про місце події. Дослідження в 1970-х роках сформували ранні основи для алгоритмів машинного зору, що існують сьогодні. Вони включають виявлення граней зображень, маркування деформацій, неполієдричне та полієдричне моделювання, представлення елементів як взаємозв'язків менших систем, оптичне випромінювання та оцінку руху. Наступне десятиліття побачило дослідження, засновані на надзвичайно суворому математичному аналізі та кількісних компонентах комп'ютерної уяви та передбачення. Вони складаються з масштабно-просторової концепції, виведення форми з різноманітних сигналів, включаючи затінення, відстань фокусування і текстур, а також контурні моделі, відомі як змійки. Дослідники також з'ясували, що багато з цих математичних принципів можуть розглядатися в рамках тієї ж оптимізації, що і регуляризація та Марковські мережі. В дев'яностих роках деякі з попередніх досліджень стали розвиватися сильніше ніж інші. А саме, наукові праці в області проєкційних тривимірних реконструкцій привели до підвищення інформативності калібрування цифрових камер. З появою методів оптимізації для калібрування камер було усвідомлено, що багато ідей вже були досліджені в ідеях корекції пакетів з області фотограмметрії. Це призвело до появи методів розріджених тривимірних реконструкцій сцен з декількох знімків. В той же час, версії скорочень графів були використані, щоб очистити сегментацію фотографій. Це десятиліття також вперше ознаменувалося використанням стратегій статистичного вивчення для розпізнавання обличчя на цифрових знімках. Наприкінці дев'яностих років відбулися суттєві зміни, пов'язані з прискореною взаємодією між областями зображень та комп'ютерної уяви і передбачення. Це включало рендеринг на основі зображень, морфінг зображень, інтерполяцію вигляду, зшивання панорамних зображень та ранній рендеринг з м'яким полем. У сучасних наукових працях спостерігається відродження методів, заснованих на характеристиках, що використовуються разом з методами машинного освоєння та складними системами оптимізації. Точність алгоритмів глибокого вивчення на декількох еталонних

моделях та прогностичних статистичних наборах для завдань, починаючи з класифікації, сегментації та оптичного потоку, покращила попередні методи.

1.3 Задачі комп'ютерного бачення

Розпізнавання об'єктів в комп'ютерному зорі, обробці зображень і машинному зорі це з'ясувати чи містять вхідні дані об'єкт або явище, які підпадають під задані параметри. Проблемою є те, що випадкові явища чи предмети не можуть бути розпізнані машиною з достатньою точністю в більшості ситуацій, на відміну від людини.

Науковці освітлюють такі проблеми розпізнавання:

- ідентифікація – розпізнавання унікального екземпляра об'єкта, такого як сітківка ока, автомобільний номер, знаки розрізнення військовослужбовців;
- виявлення – відеоряд перевіряють на наявність певних умов. Деякі спортивні організатори використовують комп'ютерний зір у поєднанні з штучним інтелектом для визначення траєкторії польоту м'яча та обрахування шансу влучення в ціль;
- розпізнавання – об'єкт чи множина об'єктів можуть бути розпізнані на двовимірному чи тривимірному зображенні.

Також існують більш специфічні завдання, такі як пошук зображень за вмістом, оцінка положення, розпізнавання символів, тощо.

Проте, сучасні методи вирішення цієї задачі охоплюють лише невеликий спектр об'єктів. Деякі з них можуть бути розпізнані майже зі сто-відсотковою вірогідністю, наприклад геометричні фігури. Інші ж, лише за певних умов. Обличчя людини може бути приховане маскою, а у зв'язку з технічними обмеженнями сьогоденного обладнання не можуть бути зчитані для ідентифікації особи.

Рух об'єктів вирішує завдання, що пов'язані з оцінкою послідовності зображень для їх подальшої обробки. З таких можна виокремити три основні напрямки розпізнавання об'єктів у русі:

- одометрія – метод визначення місцезнаходження та орієнтації камери за допомогою вивчення відповідних зображень, які вона надає;
- стеження – аналіз визначених об'єктів в кадрі та їх супроводження;
- оптичний потік – закономірність видимого руху об'єктів, поверхонь і країв у візуальній сцені через відносний рух між спостерігачем і сценою, тобто є фактичним поєднанням одометрії та стеження(рис 1.2).



Рисунок 1.2 – Тривимірне подання оптичного потоку [11]

Відновлення зображень використовують для усунення цифрового шуму, який може бути викликаний дефектами обладнання. Замість фізичної боротьби з проблемою використовують комп'ютерний зір, який дає змогу мінімізувати вплив небажаних побічних продуктів захоплення зображення (рис. 1.3).

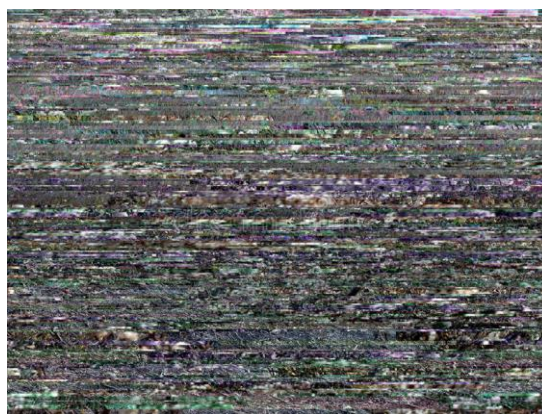


Рисунок 1.3 – Зображення цифрового шуму [8]

Розрізняють нижчий та вищий рівні видалення шумів. Нижчий рівень впливає за допомогою різного типу фільтрів. Вищий аналізує відеодані та на основі різноманітних тригерів управляє процесами фільтрації.

Відновлення зображення відрізняється від покращення зображення тим, що останнє призначене для підкреслення властивостей зображення, які роблять зображення більш привабливим для спостерігача, але вже не обов'язково для надання точних даних з наукової точки зору. Методи покращення зображення (наприклад, контрастне розтягування або розмиття за допомогою процедури найближчого сусіда), що використовуються за допомогою програм обробки зображень, не включають в себе апіорну модель процедури, яка створює фотографію.

За допомогою покращення фотографій шум можна ефективно видалити, втративши роздільну здатність, а для відновлення об'єкта слід застосовувати більш досконалі стратегії обробки фотографій.

1.4 Комп'ютерне бачення в військовій справі

Використання комп'ютерного бачення не обійшло і військову сферу. Так у багатьох процесах почали застосовувати штучні «очі», які значно прискорюють та спрощують виконання задач, які раніше потребували значних людських ресурсів.

Так, вчені з Американського університету науки і техніки в Бейруті, Ліван, опублікували документ, в якому йдеться про використання машинного бачення для виявлення мін [4]. В документі висвітлено навчання моделі, в яку було завантажено тисячі зображень мін. Різні ракурси, різні умови освітлення, фото з обмеженою видимістю об'єкта були проаналізовані та позначені, як конкретний тип боєприпасів. Це дало змогу науковцям стверджувати, що їх система розпізнає міни з вірогідністю в 99,6%(рис. 1.4). При цьому показники знижуються, якщо алгоритм зчитує об'єкт, який раніше був проаналізований. Це доводить, що технології

комп'ютерного зору недосконалі, потребують покращення або додаткового навчання, яке значно збільшує час на розробку програмного продукту.

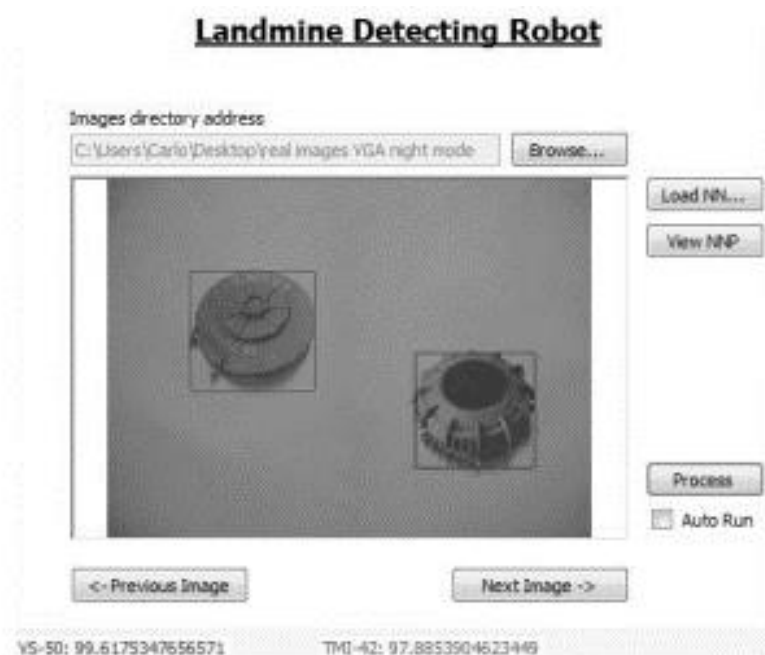


Рисунок 1.4 – Класифікація мін VS-50 та Tellermine 42 [4]

Також комп'ютерне бачення можна використовувати для контролю якості в умовах військової промисловості. Наприклад компанія Integro-tech пропонує пристрій, який за допомогою комп'ютерного зору досліджує частини зброї і за допомогою машинного зору могла виявляє перфорацію, зазубрини, вм'ятини або інші пошкодження для досягнення бездоганного результату та найвищої відмовостійкості.

Використовують комп'ютерний зір і у картографії. З самого початку цивільного використання БПЛА їх основною задачею була картографія і першими з цивільних хто використав дрони за таким призначенням були фермери. Зараз доволі розповсюджені технології для створення тривимірних карт місцевості з використанням безпілотників, зокрема і у військовій справі. Створення карт рельєфу дає змогу військам ефективно використовувати переваги техніки у поєднанні з рельєфом для нанесення максимальної шкоди ворогу та збереження особового складу. Прикладом є Розрахунково-графічний комплекс Броня,

розроблений для стрільби з гранатометів, мінометів і танків із закритих вогневих позицій. Активна співпраця з благодійними фондами та військовими дає змогу розробникам покращувати програму з часів ведення антитерористичної операції на сході і вже в повномасштабній війні. (рис. 1.5)

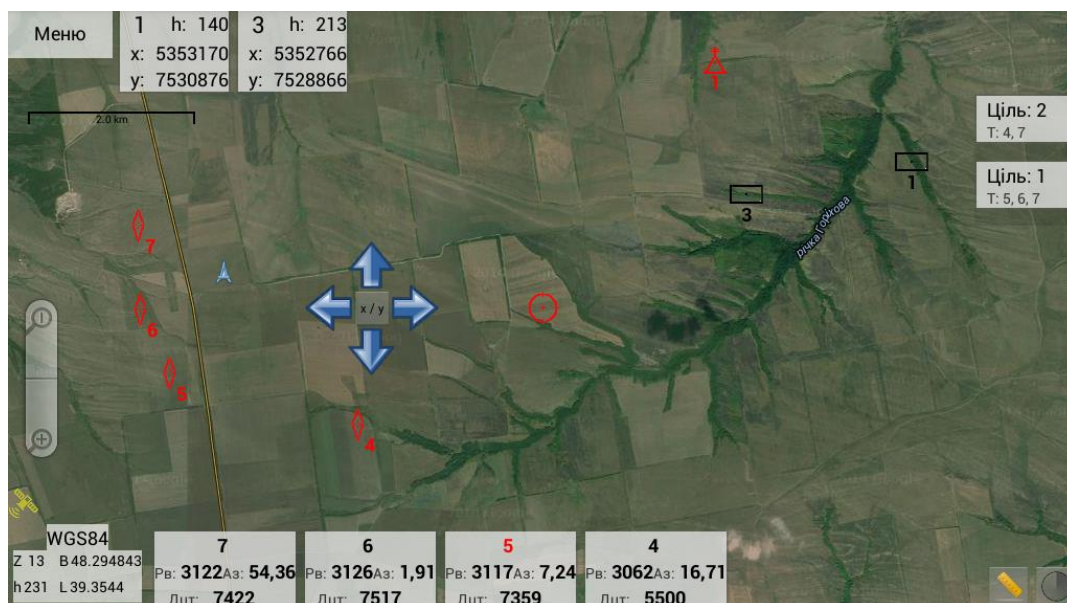


Рисунок 1.5 – Інтерфейс РГК Броня [31]

Функціонал програми дозволяє проводити розрахунки для трьох танків за 5-7 хвилин, коли без додатку на це витрачається не менше 20. Безперечно для використання програми необхідні кваліфіковані екіпажі, проте у сучасних умовах достатньо планшета для командира взводу та зв'язок для того щоб вести вогонь по противнику. Крім того, інтеграція з картами Генерального штабу дозволяє використовувати програму і для переміщення. Загалом програмне забезпечення подібного типу значно підвищує шанси на успішне ведення бою, збереження військової техніки та особового складу.

Отже, досліджувати та використовувати комп'ютерне бачення почало вже давно. З кожним роком методи та системи продовжують вдосконалюватися, проте немає однієї ідеальної системи для використання у всіх галузях та випадках, що зумовлює подальший розвиток цього напрямку і визначає його перспективність.

2 СУЧАСНІ МЕТОДИ ОТРИМАННЯ ДАНИХ АЕРОФОТОЗЙОМКИ

2.1 Аерофотозйомка, як засіб отримання розвіданих

Здавна людство мріяло побачити себе з висоти пташиного польоту. Починаючи з далекого минулого люди пройшли шлях від стрибків з веж та повітряних зміїв до реактивних та безпілотних літальних апаратів. Але крім того, щоб побувати у повітрі, людина хотіла поділитися побаченим – внаслідок цього і почала з'являтися аерофотозйомка.

Аерофотозйомка – це фотографування з літака або інших повітряних платформ.

Платформи для аерофотозйомки включають літаки, вертольоти, безпілотні літальні апарати (БПЛА або "дрони"), повітряні кулі, дирижаблі та дирижаблі, ракети, голубів, повітряних зміїв або використання камер руху навіть у вигляді стрибків з парашутом або вінгсьютів.

Аерофотозйомка зазвичай стосується саме фотографій з висоти пташиного польоту, які зосереджуються на ландшафтах та наземних об'єктах. Але суттєво відрізняється від зйомки "повітря-повітря", в яких один або декілька літаків використовуються як літаки-переслідувачі, що супроводжують та фотографують інші літаки в польоті.

Аерофотозйомка вперше була застосована французьким фотографом і повітроплавцем Гаспаром-Феліксом Турнашоном у 1858 році, однак зроблені ним зображення не збереглися до наших часів, тому найдавнішим збереженим аерофотознімком вважають зроблений Джеймсом Уоллесом Блеком та Семюелом Арчером Кінгом «Бостон, як його бачать орел і дика гуска», який датовано 1860 роком (рис. 2.1).

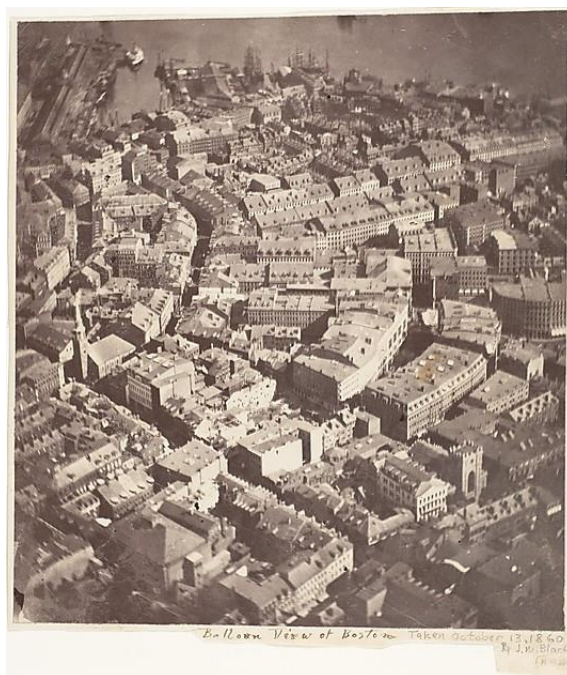


Рисунок 2.1 – Найдавніший збережений аерофотознімок [37]

Хоч на початку Першої світової війни потенціал аерофотозйомки не був оцінений сповна, вже в 1913 році в Німеччині була прийнята на озброєння перша аерофотокамера «Гьорц». Проривним в цей період став стереоскопічний метод аерофотозйомки, застосований капітаном Джоном Муром-Брабазоном у 1915 році. Це дозволило визначати висоту об'єктів шляхом порівняння фотографій, зроблених під різними кутами. Всього за Першу світову війну було зроблено понад п'ятсот тисяч фотографій місцевості, що лише підтверджує ефективність аерофотозйомки у військових цілях. Під час Другої світової війни тенденції в розвитку аерофотозйомки в розвідувальних операціях значно зросли. Наукові прориви того часу дали змогу виконувати завдання на значній висоті, високій швидкості та зі значно більшою роздільною здатністю, що значно покращувало якість розвідданих.

Саме завдяки можливості охопити значні площі та зібрати якомога більшу кількість інформації аерофотозйомку стали використовувати у військовій справі, а саме у розвідці.

Воєнна розвідка – спецслужба, що підпорядковується Міністерству оборони або Генеральному штабу (залежить від військової доктрини країни).

Завданням розвідки є добування розвідувальних даних про воєнно-політичний стан справ в окремих міжнародних районах і коаліціях держав можливого або реального противника, їх збройні сили та військово-фінансовий потенціал, чисельність особового складу, дислокацію, репутацію, характер пересувань, наміри військ (сил), сильні та слабкі сторони військ (сил), а також про театри воєнних дій. Армійська розвідка ведеться в усій смузі (оперативному районі) бойових дій військ (сил), на флангах і на всю напруженість їх бойових завдань. Розвідка планується, готується і ведеться таким чином, щоб виключити раптовість дій противника і добувати розвідувальні дані, необхідні для ефективного застосування військ (сил), способу ураження і радіоелектронного придушення.

Воєнна розвідка поділяється на:

- стратегічну – охоплює найбільшу кількість інформації та здійснюється органом воєнної розвідки держави;
- оперативну – що організовується на рівні об'єднаних штабів для підготовки та проведення операцій;
- тактичну – інформацію необхідну для ведення бою, налагоджується начальниками штабів, частин і підрозділів.

Незалежно від виду розвідки її значущість важко переоцінити. В сучасних конфліктах, починаючи з конфліктів в Іраку 1991 року безпілотні літальні апарати почали генерувати нові показники. Після аналізу та оцінки інформації перед вченими США постала проблема дальності і часу польоту. Необхідні були розвідувальні комплекси, які могли долати відстань близько 1000 кілометрів та більше, а також передавати інформацію в режимі реального часу. Проте не всім країнам необхідні були БпЛА такої дальності. Наприклад Ізраїль не мав потреби в польотах на більше ніж 400 кілометрів – тому це зумовило виникнення різноманітних комплексів з різною дальністю, призначенням та непомітністю. [34]

2.2 Різновиди БПЛА

Не існує єдиного стандарту, коли йдеться про класифікацію БПЛА. Оборонні відомства мають свій власний стандарт, а цивільні особи мають свої вільні категорії БПЛА, які постійно розвиваються. Люди класифікують їх за розміром, дальністю польоту і витривалістю, і використовують систему рівнів, яка застосовується військовими.[7]

БПЛА розрізняють за такими типами:

- безпілотні некеровані (аеростати, зонди);
- безпілотні автоматичні;
- безпілотні апарати пілотовані дистанційно(ДПЛА).

Також їх розрізняють за способом старту (за допомогою шасі, пускового пристрою чи платформи) та повернення (спуском на парашуті, падінням на вловлювач, посадкою на шасі).

Наприклад, Міністерство оборони США поділяє БПЛА на 5 комплексних категорій, зображених у таблиці 2.1.

Таблиця 2.1 – Класифікація БПЛА

№	Розмір	Навантаження (кг.)	Максимальна висота (м. над рівнем моря)	Швидкість (км/год.)
1	Малі	0 – 9	365	185
2	Середні	9 – 25	1050	Менше 460
3	Великі	Менше 600	Менше 5500	Менше 460
4	Більші	Більше 600	Менше 5500	Більше 460
5	Найбільші	Більше 600	Більше 5500	Більше 460

До дуже малих БПЛА відносяться конструкції з розмірами від масштабу великої комахи до 30-50 см завдовжки. Комахоподібні БПЛА з маховими або поворотними крилами є відомим мікродизайном. Вони надзвичайно малі за

розміром, дуже легкі і можуть використовуватися для шпигунства і біологічної боротьби. Більші БПЛА використовують звичайну конфігурацію літака. Вибір між маховими або поворотними крилами є питанням бажаної маневреності. Конструкції на основі махових крил дозволяють здійснювати посадку і приземлення на невеликих поверхнях. Прикладами таких апаратів є CyberQuad Mini, Skate від US Aurora Flight Sciences та нещодавно передані українським військовим компанією Prox Dynamics дрони Black Hornet з вагою повного набору обладнання лише 1.3 кілограми, дальністю польоту більше двох кілометрів і розмірами не більше долоні (рис. 2.2).



Рисунок 2.2 – Black Hornet в руках українського солдата[36]

Дрони такої конструкції дають змогу виконувати швидкі та непомітні спостереження при підготовці та під час бою, що значно підвищує обізнаність особового складу в обстановці та дає можливість до швидкого маневру, а низька вага повного комплексу для оператора дає змогу транспортувати його без особливих зусиль.

Клас малих БПЛА (який також іноді називають міні-БПЛА) відноситься до БПЛА, які мають хоча б один розмір більше 50 см і не більше 2 метрів. Деякі з конструкцій цієї категорії повністю базуються на моделях з фіксованим крилом, а

більшість запускаються вручну шляхом підкидання в повітря. Прикладами представників цього невеликого класу БПЛА є:

- турецький Bayraktar;
- американський військовий RQ-7 Shadow (рис 2.3);
- RQ-11 Raven, створений за допомогою компанії US Aero Vironment.



Рисунок 2.3 – БПЛА RQ-7 Shadow [3]

Середній клас БПЛА відрізнити від інших дуже просто: вони занадто важкі для перенесення однією людиною, але ще менші ніж легкий літак. Мають розмах крил від 5 до 10 метрів і можуть нести навантаження 100-200 кілограмів. Для прикладу BAE systems Skyeeye R4E, the RQ-5A Hunter або US Boeing Eagle Eye.

До великих БПЛА відносяться переважно військові зразки з бойовим навантаженням, такі як:

- US General Atomics Predator модифікацій A і B;
- US Northrop Grumman Global Hawk;
- EADS Harfang.(рис 2.4).



Рисунок 2.4 – Розміри БПЛА Harfang у порівнні з людським зростом [24]

Незалежно від розмірів, сучасні БПЛА можуть передавати зображення з камери чи будь-які інші дані в режимі реального часу, що дає змогу використовувати навіть цивільні дрони за подвійним призначенням.

2.2.1 Дрони та безпілотні апарати на службі ЗСУ

Сучасні умови ведення війни сприяють надзвичайній винахідливості українських громадян. Не обійшла ця тенденція і безпілотні літальні апарати. Документовані факти, як 15-річний хлопець з Київщини використовуючи власний цивільний дрон передавав позиції ворога українським військовим і вніс свій вклад в оборону Києва[32].

Після початку повномасштабної війни люди навчились модифікувати дрони в ударні для скидання з них вибухівки. Так українським бойовим підрозділом «Аеророзвідка» вже в квітні 2022 року було продемонстровано відео як вибухівку скидають прямо на ворожу техніку. В підрозділі зазначили, що використовували для цього октокоптери R18 (рис. 2.5), які були модифіковані для роботи відразу з декількома вибуховими пристроями. [42]

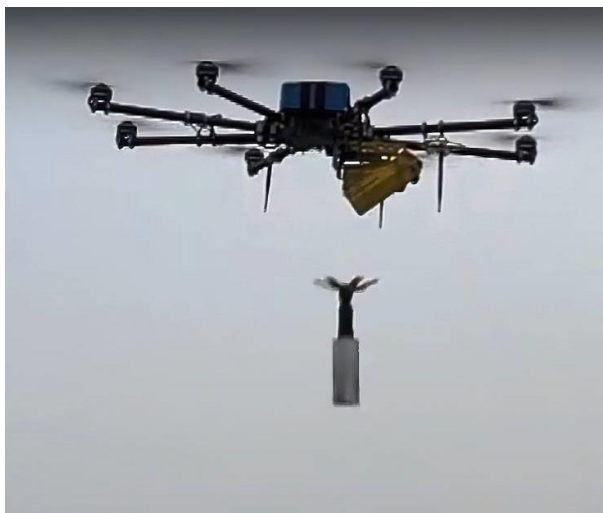


Рисунок 2.5 – Ортокоптер R18 [38]

Також існують модифікації від інженерів-аматорів для цивільних коптерів DJI Mavic 3, які друкують на 3D-принтерах модулі та продають їх оптом та вроздріб на маркетплейсах країни (рис. 2.6).

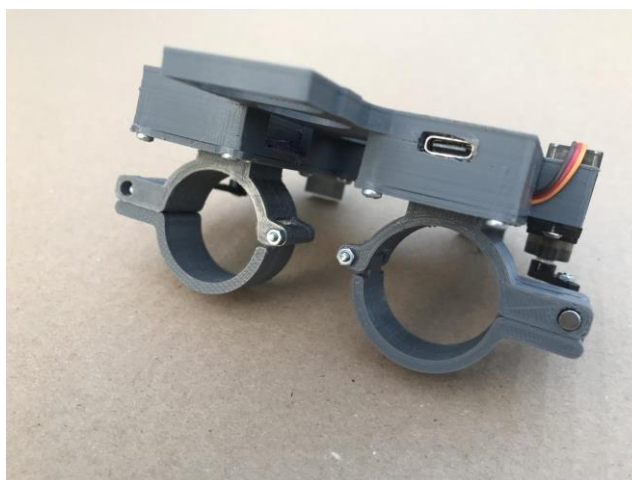


Рисунок 2.6 Саморобна система скидання для DJI Mavic 3[39]

У зв'язку з нагальними потребами армії різноманіття БПЛА в Збройних силах України досягло свого піку. Різноманітні класи та види дронів, подекуди подвійного призначення використовуються на повну. Основними БПЛА ЗСУ є:

- розвідувальні («Лелека-100», «Фурія», «Валькірія»);
- ударні (сімейство PD першого та другого покоління);

- дрони каміказде («Switchblade», «RAM II UAV»);
- саморобні ударні (Коптер «Бандерик», переобладнані великі аграрні дрони).

В цей список можна додавати нескінченну кількість продукції DJI та інших виробників цивільних дронів[30]. А також провести порівняльну характеристику професійних БПЛА, які використовуються українськими військовими у таблиці 2.2.

Таблиця 2.2 – Порівняльна характеристика професійних БПЛА в українському війську[43]

Назва	Вартість (млн. грн)	Злітна вага (кг.)	Довжина маршруту (км.)	Час у повітрі (год.)	Застосування
PD-2	30	55	1100	10	Розвідка, коригування артилерії
ACS-3М	18,6	23	2500	30	Розвідка
Фурія	4,8	5,5	200	3	Розвідка, коригування артилерії
Лелека - 100	2,7	5,5	100	2,5	Розвідка
Sparrow	3	3	70	1,25	Розвідка, коригування артилерії
Punisher	1,9	7,5	90	1,5	Ударний

2.3 Сфери використання БпЛА

В усьому світі дрони використовують в багатьох напрямках. Умовно можна поділити області використання БпЛА на дві сфери: цивільну та військову. Основними сферами цивільного використання є:

- комерційні зйомки та кіноіндустрія, а саме створення сцен, для яких раніше потрібні були значні ресурси та зусилля. Тепер для генерації якісного зображення та підвищення якості можна використовувати обладнання, яке значно дешевше та простіше для освоєння;
- використання БпЛА в якості транспортного засобу для людей. Так, у Китаї компанія EHang виконала вже більше 5 польотів з 2018 року, у тому числі в несприятливих погодних умовах (рис 2.7). В майбутньому, коли штучний інтелект зможе відстежувати та контролювати повітряний простір, безпілотні таксі заповнять небо над великими містами. Проте зараз повітряні таксі мають більше недоліків, ніж переваг і потребують значних допрацювань перед введенням в комерційну експлуатацію[9].



Рисунок 2.7 – Випробування безпілотного таксі над озером Яньци[29]

- виконувати роль точки доступу. За допомогою спеціально обладнаних БпЛА можна розгортати тимчасові станції зв'язку і на основі цього виявляти осіб, які знаходяться у розшуку;

- в медичних цілях. Під час швидкого поширення вірусу COVID-19 влада таких країн, як Іспанія, Японія та Китай використовували безпілотники для доставки ліків, обробки місцевості від вірусу та транспортування хворих[14];
- в аграрній сфері. Існує безліч варіацій комерційних дронів для використання в сільськогосподарській ніші. Від спостереження та маніпуляцій з худобою до аналізу ґрунту, оцінки якості повітря, оброки посівів від шкідників, тощо (рис. 2.8);



Рисунок 2.8 – Обробка поля з дрону [40]

- транспортування вантажів. Послуга також набула широкого поширення під час крайньої епідемії. Найбільш широкого розповсюдження набула в США. Таку доставку можна замовити на рівні зі звичайною кур'єрською доставкою, яку виконує людина. Але суттєва проблема постає у тому, що вулиці міст майже неможливо використовувати для руху безпілотних транспортних засобів, а використання дронів обмежено на рівні законодавства в деяких штатах;
- підводні роботи. За останні роки суттєво збільшилась кількість випадків використання підводних дронів з метою дослідження флори та фауни, доступу до глибин світового океану, а також огляду та маніпуляцій над підводними магістралями.

Натомість використання в правоохоронній сфері безпілотних літальних апаратів лише почало набувати популярності. Як заміна гелікоптерам спеціальні дрони виконують ті ж самі функції, маючи лише певні обмеження в дальності

польоту вони здатні автоматично супроводжувати ціль за допомогою методів трекінгу об'єктів та передавати інформацію в реальному часі, але при цьому використовуючи значно менше ресурсів. Для поліцейського гелікоптера необхідний екіпаж як мінімум з двох осіб, а також обслуга, в той час, коли оператор може керувати декількома дронами, а обслуговування таких апаратів значно дешевше та швидше в міру розповсюдженості деталей та необхідності нижчої кваліфікації працівників для маніпуляцій з ними. Також місце його перебування зазвичай віддалене від центрів великих міст, а тому від моменту команди до безпосередньої роботи проходить значно більше часу, ніж розгортання дрону на деякій відкритій місцевості, площі або даху будинку. Також відносна непомітність БПЛА дає змогу непомітно слідувати за ціллю, не викликаючи підозри.

З точки зору неpubлічного використання дрони мають такі варіації застосування:

- розгін несанкціонованих мітингів та протестів, допомога в уникненні масових заворушень;
- моніторинг дорожнього руху та дорожньо-транспортних пригод;
- спостереження та розвідка;
- перехоплення кадрів з інших безпілотників;
- боротьба з дронами;
- ведення вогню.

Враховуючи сучасні реалії з катаклізмами, епідеміями та іншими надзвичайними ситуаціями, людство намагається впровадити автоматизацію процесів та використовує всі можливі технології.

2.4 Методи та проблематика аерофотозйомки

Аерофотозйомка підсумовує в собі декілька видів знімків:

- плановий – відбувається при відхиленні аерофотоапарату(АФА) не більше ніж на 3 градуси від вертикальної осі;

- горизонтальний – знімок, що отримано при прямовисному положенні АФА, без будь-яких відхилень;
- кольоровий – передає поверхню в кольорах, наближених до натуральних;
- перспективний – зображення, що має різний масштаб в різних його частинах, що не сприяє використанню такого знімку у вимірювальних цілях без застосування спеціальних приладів;
- топографічний – отриманий за допомогою топографічних АФА;
- комбінований – такі зображення можуть бути отримані різними шляхами. Наприклад поєднанням декількох фото, зроблених з однієї точки під різними кутами або з різних точок, під одним і тим самими кутом, тощо.

Оскільки аерофотозйомка – це і є фотографія, то їй властиві і всі недоліки роботи зі знімками. Так помилки можна класифікувати як за походженням, так і за формою[20].

Таблиця 2.3 – Класифікація помилок аерофотозйомки

№	Тип помилки	Систематична	Випадкова
1	Геометричне спотворення	<ul style="list-style-type: none"> • відхилення об'єктива; • компенсація руху об'єктива. 	<ul style="list-style-type: none"> • усадка плівки (відбувається на старих зразках); • атмосферне заломлення світла.
2	Геометричне зміщення	Викривлення земної поверхні	<ul style="list-style-type: none"> • рельєфне зміщення (властиве для гірських районів); • помилка детектора.
3	Пов'язане радіометричним датчиком	з <ul style="list-style-type: none"> • відхилення експозиції; • геометрія сенсору. 	Двонаправлене відбиття (наприклад, ефекти "гарячих точок та взаємне затінення)

Продовження таблиці 2.3. – Класифікація помилок аерофотозйомки

№	Тип помилки	Систематична	Випадкова
4	Радіометричні умови	Погодні умови	<ul style="list-style-type: none"> • хмари; • кут нахилу сонця.

Геометричні помилки здебільшого впливають на розмір та розташування об'єктів на зображенні. Вони можуть виникати у зв'язку з проблемами обладнання, яке використовують для фотографування, швидкості польоту та повітряного засобу, а також місцевості. Зміщення рельєфу призводить до похибки в визначенні розмірів об'єктів, а також значно ускладнює цифровий аналіз фотографії та її обробку в цілому.

Радіометричні помилки зазвичай спричинені калібруванням камери, точкою спостереження, а також типами фільтрів. Це призводить до вимушених маніпуляцій з гистограмою зображення, що збільшує час обробки та призводить до підвищення кількості похибок.

2.5 Способи передачі та отримання даних з літальних апаратів

З початку використання безпілотних апаратів постала проблема зв'язку з оператором. Проблема стосувалася в основному повітряних апаратів, оскільки наземні можна було поєднати навіть дротом, що дозволяло оперувати дронами на незначних відстанях.

Безпілотні повітряні апарати також можуть бути незалежні від методів зв'язку. Наприклад Ту-141 «Стриж», багаторазовий оперативно-тактичний БпЛА. В основу принципу його роботи в закладені заздалегідь параметри, такі як маршрут, висоти та швидкість та інші (рис. 2.9).



Рисунок 2.9 – Ту-141 в музеї ВПС ВС України [16]

Під час польоту апарат здійснює фотофіксацію в інфрачервоному діапазоні, записує на внутрішній накопичувач, згодом, після посадки інформація потрапляє в центр обробки. Саме через це досягається показник високої непомітності, але швидкість реакції на отримані дані недостатня. За подібним принципом працює іранський дрон-камікадзе Shahed 136 (або його російська версія Герань-2). Використовуючи інерціальну систему навігації, яка ґрунтується на властивостях інерції тіл, не передає зображення і радіосигналів, що дещо унеможливує знаходження його точного місцеположення, але двигуни, які використовуються в його конструкції занадто шумні, що дає можливість локалізувати їх з точністю до декількох кілометрів.

Проте сучасні розвідувальні БпЛА повинні передавати дані в режимі реального часу, саме тому їх зв'язок має бути безперервним і якісним. Канали комунікації можна поділити на чотири типи:

- безпілотник до безпілотника(D2D). Не стандартизований варіант комунікації, зазвичай використовує протокол підключення Peer-to-Peer(P2P), який є ненадійним. Однорангова мережа P2P має дуже низький рівень захищеності, якщо зловмисник отримає доступ до одного вузла, то отримає і до всіх інших, що поставить під загрозу всю мережу і може викрити місцеположення оператора. Також такий тип мережі вразливий до атак на відмову в обслуговуванні (DoS та DDoS);

- безпілотник-наземна станція(D2GS). Такий тип зв'язку базується на використанні стандартизованих протоколів, таких як Wi-Fi 802.11 (2,4 ГГц та 5ГГц), а також Bluetooth. Це наражає на небезпеку пасивних та активних атак;
- безпілотник-супутник(D2S). Використовуючи системи навігації безпілотник може надсилати координати в реальному часі, що дозволяє при втраті сигналу повернутися до точки вильоту. Такий тип зв'язку досить високовартісний, але вважається найбезпечнішим, тому широко використовується військовими. Розвинені країни змогли створити свої системи навігації, схожі за будовою, але незалежні одна від одної, що показано в таблиці 2.4.

Таблиця 2.4 – Існуючі варіанти супутникового зв'язку різних країн.

	GPS	GLONASS	Galileo	Beidou
Власник	США	Росія	ЄС	Китай
Висота	20,180 км	19,130 км	23,222 км	21,150 км
Кількість діючих супутників	24	24	24 + 6 резервних копій	28
Частота передачі сигналу (ГГц)	1.563-1.587 1.215-1.239 11.164-1.189	1.593-1.610 1.237-1.254 1.189-1.214	1.559-1.592 1.164-1.215 1.260-1.300	1.561098 1.589742 1.20714 1.26852
Точність локалізації (в метрах)	0.3 -5	2-4	0.01 - 1.0	0.1 - 3.6

- безпілотник-мережа(D2N). Використовує мережу з частотами 3 ГГц, 4 ГГц, 4G + (LTE) та 5 ГГц – стільниковий зв'язок. Під час використання такого типу мереж необхідно забезпечувати спеціальний захист для уникнення витоку даних.

2.6 Дослідження проблем безпеки БпЛА

Використання дронів суттєво полегшує життя людей та приносить користь на всіх рівнях суспільства. Але порушується питання безпеки та конфіденційності, які не регулюються в нашій країні. Що призводить до використання дронів, в тому числі, зловмисниками. Багато країн світу піднімали питання щодо ліцензування пілотів та реєстрації дронів, зокрема США, держави-члени ЄС, Китай та інші визначили певні правила реєстрації та використання БпЛА вагою менше 25 кілограмів. Наприклад, законодавство Німеччини вимагає лише дозвіл на політ і обмежує фіксацію громадян, а також визначає дальність польоту в 1 кілометр. Уряд США вимагає ліцензування пілота, дозвіл на вильоти і сертифікати на літальний апарат. Відповідно до Закону України Про затвердження Авіаційних правил України «Правила використання повітряного простору України», а саме другого розділу: «польоти безпілотних ПС масою до 20 кг включно виконуються без подання заявок на ВПП, без отримання дозволів на ВПП, без інформування органів управління Повітряних Сил ЗС України та органів ОЦВС, органів Державної прикордонної служби України, органів ОПР та відомчих органів УПР, за умови дотримання таких вимог:

- польоти виконуються без перетинання державного кордону України;
- польоти виконуються поза межами встановлених заборон та обмежень ВПП, крім випадків, установлених Положенням про ВПП;
- польоти виконуються не ближче 5 км від зовнішніх меж злітно-посадкових смуг аеродромів або не ближче 3 км від зовнішніх меж злітно-посадкової

смуги ЗПМ/вертодромів, крім випадків узгодження з експлуатантом аеродрому/ЗПМ/вертодрому;

- польоти виконуються не ближче 500 м від пілотованих ПС;
- польоти не виконуються над:
 - скупченням людей на відкритому просторі та над місцями щільної забудови;
 - об'єктами (зонами), які визначені Міністерством оборони України, Міністерством інфраструктури України, Міністерством внутрішніх справ України, Державною прикордонною службою України, Службою безпеки України, Національною поліцією України, Національною гвардією України, Державною фіскальною службою України, Службою зовнішньої розвідки України, Управлінням державної охорони України, іншими військовими формуваннями та правоохоронними структурами, утвореними відповідно до законів України, та відносно яких здійснюється охорона / державна охорона (за умови позначення території навколо цих об'єктів інформаційними знаками про заборону польотів безпілотних ПС та/або шляхом оприлюднення меж такої заборони), крім випадків виконання польотів за дозволом зазначених вище повноважних органів;
- польоти виконуються в межах прямої видимості (VLOS);
- максимальна висота польоту не вище:
 - 120 м над рівнем земної (водної) поверхні поза межами CTR, AFIZ, ATCA, ATCZ, спеціально встановлених зон, зарезервованого повітряного простору для забезпечення польотів за спеціально встановленими маршрутами польотів державної авіації;
 - 50 м над рівнем земної (водної) поверхні в межах CTR, AFIZ, ATCA, ATCZ, спеціально встановлених зон, зарезервованого повітряного простору для забезпечення польотів за спеціально встановленими маршрутами польотів державної авіації або якщо інформація про

фактичний статус елементів структури повітряного простору на час виконання польоту відсутня;

- 50 м над статичними перешкодами на горизонтальній відстані не більше 100 м від таких перешкод, як відхилення від зазначених вище обмежень по висоті, на запит власника такого об'єкту;
- швидкість польоту безпілотної ПС складає не більше 160 км/год;» [35]

Зараз за дотриманням ЗУ слідкувати важко, але повітряний простір над критичними об'єктами постійно знаходиться під охороною. Багато хто вважає, що описаних в Законі положень недостатньо і потрібно ліцензувати пілотів, БпЛА та видавати дозволи, але в умовах повномасштабної війни пріоритет для реалізації подібного проекту низький, а тому може бути реалізований після перемоги України.

Оскільки безпілотники мають невеликі розміри і доступні широкому загалу, вони можуть використовуватися для скоєння терактів та інших порушень правопорядку. Після війни, коли кустарна модифікація дронів досягне свого піку, буде існувати високий ризик використання БпЛА у злочинних цілях, тому проблема реєстрації дронів та ліцензування пілотів стає критичною.

2.6.1 Методи виявлення БпЛА

Оскільки розповсюдження безпілотників, у тому числі з приладами дистанційного скидання вантажу, тепловізорами, іншими спеціальними засобами стало майже неконтрольованим і їх реєстрація, ніяк не контролюється державою – це може призвести до виникнення правопорушень пов'язаних з конфіденційністю. Крім того БпЛА всіх видів використовує і ворог. Саме тому постає проблема їх виявлення та протидії.

Існує декілька способів для виявлення безпілотників:

- радіолокаційний. Такі системи часто застосовуються як в цивільному, так і у військовому сегментах. Такі системи можуть виявляти здебільшого великі повітряні об'єкти. Мінусом таких систем є те, що вони не ефективні проти

цілей, що летять на низькій висоті або цілей, які зависають у повітрі. На радарі такі цілі часто відображаються як птахи. Також варто зазначити, що використання потужних радіолокаційних станцій генерує випромінювання, яке є шкідливим для людей, до того ж такий спосіб не може виявляти цілі за перешкодами, що в сумі унеможлиблює використання подібних установок поруч з населеними пунктами. Перевагами такого методу виявлення є: можливість роботи на великих дистанціях, за умови відсутності перешкод, виявлення автономних безпілотників (таких, що рухаються без зв'язку з оператором за заданим заздалегідь маршрутом), достатній шанс виявлення повітряних цілей в несприятливих погодних умовах та в умовах недостатньої оглядовості;

- радіочастотний. Під час використання дронів, які передають інформацію в реальному часі, існує постійний радіозв'язок між БпЛА та оператором. Такі дані групуються спеціальним чином та відправляються в частотних діапазонах, які створені для організації безпроводного доступу. Тож і виявити їх значно складніше, оскільки вони схожі на звичайні пакети, що передаються в мережі інтернет – це суттєво ускладнює виявлення дронів.[17] Особливостями використання радіочастотної системи виявлення є відсутність необхідності відправки радіосигналу (потрібен лише пасивний радіочастотний датчик), в загальному простіша конструкція дозволяє знизити рівень кваліфікації персоналу, а також пришвидшити її розгортання, можливість визначення місцеположення оператора БпЛА, відсутність випромінювання дозволяє встановити детектор в межах населеного пункту. Використання пасивних датчиків зумовлює неможливість ідентифікації дронів, що не мають зв'язку з оператором, сильне навантаження частот, на яких працюють БпЛА ускладнює виявлення саме даних, які надсилаються між оператором та дроном, використання безпілотниками направлених антен потребує знаходження станції розпізнавання безпосередньо на шляху між оператором та ПС, також застосування подібних датчиків в міських умовах

знижує їх ефективність у зв'язку за затуханням сигналу, який проходить через велику кількість об'єктів;

- акустичне розпізнавання. Кожен безпілотник має свій акустичний відбиток, який генерується двигуном та пропелерами, який можна відрізнити використовуючи спеціальні мікрофони. Зазвичай системи такого типу використовують декілька віддалених звукових датчиків для розрахунку приблизного місцеположення БпЛА. Недоліками такого методу є обмежена зона виявлення, швидкість звуку доволі низька, тому отримана інформація про місцезнаходження дрону може бути спотворена, в умовах військового часу використання звукових датчиків майже неможливе, звукові сенсори вразливі до несприятливих погодних умов, дедалі більша кількість беззвучних моделей БпЛА Перевагами такого методу є визначення дронів без зв'язку з оператором[17];
- оптичне розпізнавання. Базується на технологіях комп'ютерного зору та штучного інтелекту, потребує постійного вдосконалення. Перевагами такого методу є: можливість використання будь-яких камер, виявлення та ідентифікація об'єктів здійснюється за допомогою штучного інтелекту, що за умови достатньої навченості безвідмовно розпізнає БпЛА, застосування камер інфрачервоного спектру дозволяє застосовувати технологію вночі. Недоліками такої технології є: низька ефективність в умовах обмеженої оглядовості та залежність від погодних явищ, оптичним пристроям потрібне регулярне обслуговування, що потребує постійної наявності обслуговуючого персоналу безпосередньо поруч з датчиками та ускладнює розгортання великої мережі камер;
- інфрачервоне виявлення. Основна особливість інфрачервоних камер – робота вночі. Крім цього, перевагами такого методу є: їх дешевизна та низькі вимоги до обслуговування дозволяють розгорнути велику мережу, а також такі камери стійкі до погодних умов.[1] Мінусами такої технології є низька

роздільна здатність камер, ускладнене виявлення деяких дронів, які мають невеликий тепловий слід або електродвигуни.

Оскільки кожен з методів має свої плюси та мінуси, то їх ефективність поодиноці не є високою. Тому часто використовують комбінацію з декількох технологій. Найчастіше використовують радіолокаційні та радіочастотні методи, теплове, акустичне та оптичне виявлення. Досить ефективними є такі комбінації:

- аудіолокаційне, відеолокаційне та радіолокаційне виявлення;
- використання радіочастотних, радіолокаційних, оптичних та теплових датчиків. [22]

2.6.2 Методи атаки на БпЛА

Кібератака – спрямований акт агресії, що впливає на певні функції пристрою або системи. Кінцеві цілі атак можуть бути набагато глибші, ніж до певних збоїв в системі. Зазвичай кібератака є комплексом дій, що складаються з декількох дій (рис 2.10).



Рисунок 2.10 – Схематичне зображення етапів кібератаки на БпЛА

Для скоєння кібератаки можна використати три категорії точок входу в систему БпЛА (рис. 2.11):

- радіоканал;
- повідомлення;
- бортові система.

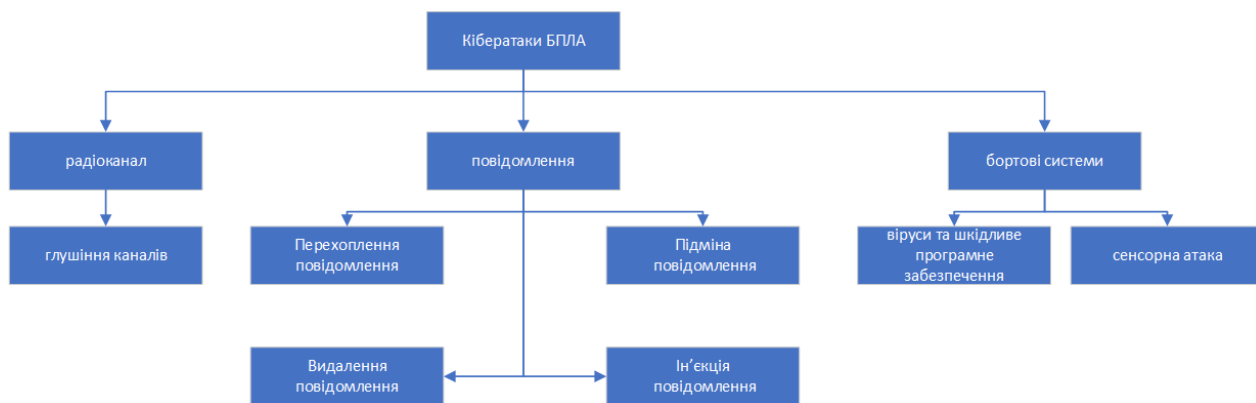


Рисунок 2.11 – Класифікація кібератак на БПЛА

Також всі кібератаки можна поділити на 6 класів:

- перехоплення повідомлень – пасивна атака, яка має на меті перехопити інформацію, тобто побачити те, що бачить БПЛА. Також ціллю хакерів може стати вторинна інформація, наприклад, місцезнаходження оператора БПЛА, або мету його вильоту;
- радіоперешкоди – найпростіша з атак, атака на відмову в обслуговуванні. Здійснюється шляхом створення сигналів більшої потужності, ніж є в каналі зв'язку, що в результаті призводить до отримання приймачами лише шумів. Під час такої атаки втрачається зв'язок зі супутниковою навігацією, яка в свою чергу не дозволяє повернутися БПЛА на точку старту автоматично;
- видалення повідомлень – працює за схожим принципом, що і перехоплення повідомлень, але вимагає менше зусиль для виконання. Атака в основному перешкоджає отриманню БПЛА команд від оператора, що призводить до повернення на точку зльоту або захоплення дрону ;
- ін'єкція повідомлень – клас кібератаки, під час якої створюються несанкціоновані повідомлення і передаються в канал управління. Така атака може бути поділена на «сліпу» ін'єкцію (створюється хакером самостійно, без урахування характеристик БПЛА) та ін'єкцію повторення (повідомлення, які вже були відправлені в канал зв'язку спотворюються та надсилаються повторно). Такі атаки проводяться з метою перевантаження каналу і

заміщення оригінальних повідомлень спотвореними, що призводить до відмови обладнання [10];

- атака бортової системи – такий стиль атак спрямований на апаратно-програмне забезпечення, таке як сенсорні модулі, контролери, система та інші. Такі атаки можуть застосовуватись в різноманітних цілях. Наприклад довготривалий вплив вірусів на БПЛА може призвести до його втрати;
- підміна повідомлень – клас кібератак, який передбачає створення повідомлень, які виглядають як істинні повідомлення від відправника. Такі атаки, спрямовані на канал навігації для того, щоб підмінити місцезнаходження БПЛА.

2.6.3 Міри протидії БПЛА

Існує певний перелік заходів протидії проти різних кібератак на БПЛА. Для виявлення БПЛА, деякі типи контрзаходів потребують механічних систем, що розгортають відповідну фізичну мережу. Але механічні системи не є досить зручними, тому слід приділити увагу контрзаходам, що не потребують вищевказаних систем.

Деякі заходи протидії можуть бути незадовільними для конкретної кібератаки в тому сенсі, адже кожен контрзахід може бути застосований до більш ніж одного типу атак. Різні атаки мають власні критерії розбіжності, наприклад, вектори та об'єкти атаки, але наслідки використання у них можуть бути спільними. Прикладом таких критеріїв розбіжностей може бути вірусна атака та атака з підробкою керуючих повідомлень, що мають різні типи нападу, але результат по завершенню у них може бути спільним – неправильної поведінки БПЛА.

Контрзаходи можна поділити на основі їх функціональних сфер застосування на три категорії:

- попередження;
- запобігання;
- виявлення і пом'якшення наслідків (рис. 2.12).

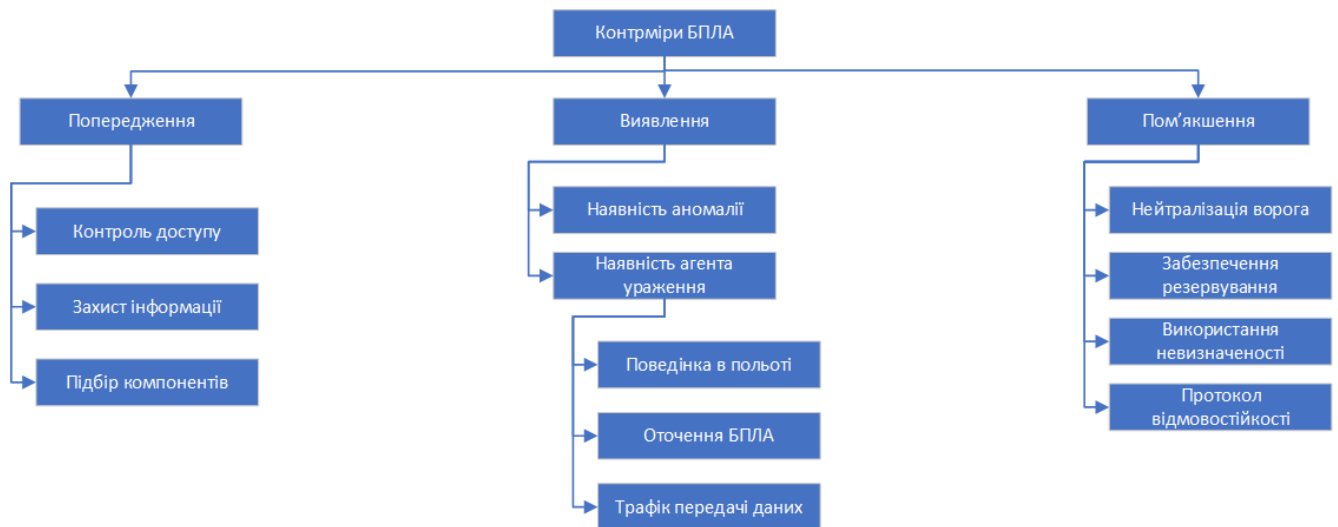


Рисунок 2.12 – Основні методи протидії БпЛА

Попередження. Такі контрзаходи працюють за трьома методами:

- запровадження контролю доступу до системи так, щоб тільки персонал, що має відповідні права і програмний агент могли встановлювати контакт з БПЛА;
- захист автентичності, цілісності та конфіденційності даних таким чином, щоб не допустити прийняття помилкових або фальшивих команд і відомостей;
- використання лише програмних компонентів та системних прошивок без вразливостей, що можуть з'явитися.

Але, не всі вищевказані методи можна застосовувати до кожної кібератаки. Наприклад, для того щоб протидіяти сенсорній атаці, необхідно впроваджувати та проектувати БПЛА, застосовуючи лише сенсори, що мають характеристики в межах очікуваного робочого діапазону. Також необхідно вибрати відповідний гіроскоп, на який, у його робочому типовому діапазоні, не впливає навколишній акустичний шум. Але, такі контрзаходи не завжди є потрібними для інших атак. Окрім вибору гіроскопу, компоненти бортової системи, для убезпечення себе від відкриття більшої кількості точок входу для атаки, мають бути оснащені функціями захисту від несанкціонованого втручання.

Не дивлячись на групування контрзаходів в одному класі, профілактичні контрзаходи можуть мати зовсім різну реалізацію. Для запобігання видаленню вірусних атак і повідомлень застосовують контроль доступу, що може являти собою деякі вузли (базуються на паролях схеми аутентифікації через загальні бездротові канали). Якщо бездротовим зв'язком є Wi-Fi, контроль доступу може здійснюватися як дозвіл на встановлення з'єднання з БПЛА, але з пристроями у яких попередньо зареєстровані MAC-адреси.

Через фільтр MAC-адрес, окрім контролю доступу, можна відтворювати запобігання атаки на деаутентифікацію шляхом приховування ідентифікатора точки доступу БПЛА, а не трансляції. Повідомлення про асоціацію та аутентифікацію, що за замовчуванням передаються відкритим текстом, мають бути зашифровані, для запобігання бездротового прослуховування. Тому необхідне шифрування відповідних даних. Одним з таких видів шифрування є симетричне шифрування з таємним розподілом ключів.

Схема шифрування є унікальною в тому сенсі, адже вона може бути реалізована на загальнодоступних радіомодулях і не потребує будь-якої апаратної модифікації.

Конфіденційність даних може бути досягнута за допомогою методів захисту на фізичному рівні. Система зв'язку з використанням БПЛА є як захист від прослуховування шляхом передачі на фізичному рівні штучних шумових сигналів разом з інформаційними сигналами. Створена схема для визначення оптимального розподілу потужності між інформаційними та штучними шумовими сигналами, завдяки якому мінімізується комбінація ймовірності втрати передачі та втрати секретності. Ще одним не менш важливим компонентом є керування висотою польоту БПЛА для досягнення бажаного показника інформаційного рівня секретності. Використання мобільності БПЛА дає змогу максимізувати ступінь секретності інформації від прослуховування на землі, шляхом спільної оптимізації траєкторії польоту БПЛА та потужності передачі над обмеженим горизонтом.

Виявлення. Виявити кібератаки можна такими двома способами:

- виявити наявність агента, що проявляє атаку. Атакуючий агент – це елемент, який створює вплив від імені зловмисника або фактично виконує атаку. Проявлятися він може, у різних формах в залежності від виду атаки. Наприклад, потужний радіосигнал може бути агентом атаки для глушіння каналу зв'язку, що створює перешкоди, по типу вірусної атаки;
- наявність аномалій, та їх виявлення. Такі аномалії можуть існувати в структурі використання, радіосигналу, бортових ресурсів, руху літака, трафіку зв'язку тощо.

Через пасивну природу пристрою для прослуховування, при атаці агентом перехоплення повідомлень є сам зловмисник. Такі пасивні пристрої для прослуховування, виявити нелегко. Але існують опосередковані методи виявлення, що використовують вторинну інформацію, наприклад, тепло, що генерується електронними схемами пристрою. Використовуючи інфрачервону камеру з тепловим пошуком, БПЛА має можливість сканувати свою наземну зону покриття на наявність будь-якого прихованого перехоплювача даних.

Дуже важливо, щоб БПЛА мала найновішу база даних вірусних сигнатур до початку польоту. Атаку повторної підміни та повторення повідомлень можна виявити за допомогою спостереження за наявністю підроблених та відтворених повідомлень. Зробити це можна за допомогою криптографічних алгоритмів.

Здійснення нападу на канал може бути виявлено шляхом спостереження за самим агентом атаки, тобто завадових сигналів в одному і тому ж радіоканалі. Моніторинг сумарної прийнятої потужності в частотному каналі є простим методом виявлення присутності завадового сигналу.

Статус присутності сигналу можна призначити, якщо відношення потужності завади до відношення потужності прийнятого сигналу вище порогового значення. Необхідно дуже точно вибрати поріг виявлення, адже це може вплинути на точність виявлення. Для проведення порівняння можна проаналізувати використання суми квадратів відношення потужностей в якості статистики

рішення. Адже у порівнянні з сигналами без завад, протилежні сигнали можуть викликати корельовані зміни у всіх вимірних значеннях відношення.

На додаток до вищевказаних методів виявлення кібератаки, існують методи з підборкою GPS-сигналів шляхом перевірки аномалій в характеристиках радіосигналів GPS. Проявлення таких аномалій відбувається у вигляді надмірно низького рівня шуму та сильного рівня прийнятого сигналу. Вищевказані значення також можна спостерігати у значеннях автоматичного регулювання підсилення GPS-приймачів, фазової затримки сигналу, кута приходу GPS-сигналів тощо. Замість зосередження уваги на одній фізичній характеристиці, можна розглядати декілька, у сукупності з використанням штучної нейронної мережі (ШНМ) зі зворотним зв'язком.

Окрім отримання радіосигналу, підробку GPS можна виявити шляхом знаходження аномалій у розрахованих координатах місцеположення. Такі методи дають змогу обчислювати координати БПЛА з отриманих навігаційних повідомлень і порівнювати їх з координатами, оціненими за допомогою еталонної моделі. Застосування такого методу дає змогу виявити GPS підміну, якщо похибка між двома координатами більша за поріг.

Запобігання. У результаті кібератаки можуть бути відповідні збитки та негативні наслідки, але їх можна зменшити за допомогою наступних методів:

- забезпечення резервування;
- уникнення агента атаки;
- відмовостійкий протокол;
- використання невизначеності;
- нейтралізація зловмисника.

Нейтралізація зловмисника – є засобом протидії, що виводить з ладу пасивний підслуховуючий пристрій шляхом глушіння його приймача. Таке глушіння каналу запускається об'єктом атаки на зловмисника. Він перешкоджає роботі радіоприймача того хто прослуховує, через що, він не зможе виявити канал зв'язку для передачі повідомлення.

Атакуючи і записуючи атаки, можна проаналізувати методи роботи супротивника, що може бути ефективним контрзаходом для зменшення впливу агента атаки шляхом його уникнення. Прикладом цього може бути атака глушіння каналів зв'язку з БПЛА, що дає змогу уникнути сильних сигналів, що утворюють перепони, шляхом динамічного перемикання на інший радіоканал.

Завдяки здійсненню спектрального зондування, система виявляє сигнали перешкод. Якщо результат виявлення позитивний, система переключає всі БПЛА, з каналу, що атакується, на інший вільний канал.

Ще одним таким контрзаходом проти глушіння навігаційних каналів є забезпечення резервування шляхом встановлення декількох приймачів, які є різними для ССН. Якщо ж навігаційні повідомлення від однієї ССН глушаться, отримати навігаційні повідомлення від іншої ССН все ще можливо. Такий контрзахід є економічно вигідним та ефективним, оскільки існують готові комерційні приймачі системи, що приймають декілька типів сигналів ССН. Також ще одним позитивним фактором, є висока вартість для супротивника.

Ще одним аспектом використання такого методу є пом'якшення наслідків сенсорної атаки, особливо коли її запобігання протидії зазнало невдачі.

Для отримання повноцінного удару для БПЛА, потрібно щоб зловмисник повністю передбачив поведінку атаки. Таким чином, потрібно зменшити вплив атаки, додавши невизначеності в поведінку БПЛА, зробивши її менш передбачуваною. Яскравим прикладом для опису цього методу є теорія ігор, що забезпечує основу для моделювання впливу невизначеності в поведінці декількох акторів один на одного. Для цього можна поєднати кооперативну локалізацію та теорії ігор, щоб пом'якшити вплив атаки підміни навігаційних повідомлень. Окрім вищевказаних аспектів, кооперативна локалізація дає змогу визначити місцезнаходження, використовуючи лише відомості про три інші БПЛА, що знаходяться поблизу нього. Для функціональності такої кооперативної локалізації, БПЛА повинен знати свої відносні відстані до всіх БПЛА, що співпрацюють, а ці БПЛА, що співпрацюють, повинні бути ознайомлені з координатами власного

місцезнаходження. Таким чином, кооперативна локалізація не спрацює, якщо один із сусідів зазнає поразки від підробки навігаційних повідомлень.

Глушіння каналів управління дає змогу БПЛА-мішеням отримати заборону передачі команд від наземного пункту управління. Через відсутність команд управління БПЛА може літати безцільно або впасти на землю. Щоб пом'якшити наслідки після втрати сигналів управління на певний період часу БПЛА повинно перейти у стан втраченого зв'язку та виконати відмовостійкий протокол. Цей протокол є заздалегідь визначеною процедурою, що може керувати БПЛА для автономного виконання набору інструкцій для досягнення бажаного стану. Вищевказана процедура спрямовує БПЛА на повернення до бази, польоту до заздалегідь визначеного місця, після чого він самознищиться з уникненням захоплення. Безвідмовний протокол, зазвичай, використовують коли всі інші контрзаходи з пом'якшення наслідків не дали результату. Такий метод називають відкатом назад або перекиданням вперед, який повертає або перенаправляє БПЛА в безпечний стан.

Отже, людство все частіше використовує БПЛА в різних сферах свого життя, полегшуючи його. Але не варто забувати про безпеку, власну та оточення. Можливо слід переглянути Законодавство і додати в нього персональну реєстрацію дронів, оскільки пілотування завжди пов'язане з ризиком і необхідні критерії для регулювання кваліфікації оператора. І незважаючи на всі недоліки, БПЛА з професійної техніки поступово переходять у власне користування, тому можна припустити, що у майбутньому більшість українців будуть мати власні дрони для використання їх у різних сферах життя.

3. ПРОЕКТУВАННЯ СИСТЕМИ ТА ОПИС МАТ МОДЕЛІ

3.1 Методи розпізнавання об'єктів

Розпізнавання об'єктів протягом десятиліть є областю інтенсивних досліджень. Воно є однією з областей комп'ютерного зору та обробки зображень. Розпізнавання зображень – технологія, яка виявляє схожі екземпляри на фото та відео. Алгоритм цієї технології, в загальному, базується на знаннях, про певні об'єкти, які порівнюються з даними на зображенні для визначення ідентичних предметів. Проте кожна сфера застосування вимагає індивідуалізації алгоритму відповідно до своїх потреб. В загальному підходи до проблеми розпізнавання об'єктів можна поділити на дві групи: нейронні та безнейронні.

Нейронні методи, в свою чергу можна поділити на:

- регіональні згорткові нейронні мережі (R-CNN), які включають в себе Fast R-CNN, Faster R-CNN, Mask R-CNN, Mesh R-CNN [12];
- однозарядний мультибоксовий сповіщувач(SSD). Такий підхід дискретизує вихідний простір обмежувальних рамок на набір рамок за замовчуванням з різними співвідношеннями сторін і масштабами відповідно до розташування об'єкта на карті [15];
- You Only Look Once (YOLO) – ймовірності класів та обмежувальні рамки, які відокремлені у просторі становлять регресійну задачу виявлення об'єктів цим методом, що значно прискорює роботу системи, навіть за високої роздільної здатності зображень [21];
- деформовані згорткові мережі – ключовою перевагою такої мережі є адаптивність до змін геометричних властивостей об'єктів та підвищене фокусування на окремих регіонах зображення;

Безнейронні мережі в свою чергу можна поділити на:

- гістограму орієнтованих градієнтів (HOG), що визначається описувачем ознак. Такий метод рахує появу орієнтації градієнта в певних частинах зображення;
- метод Віоли-Джонса – бібліотека для розпізнавання об'єктів шляхом машинного навчання, спочатку використовувався для вирішення проблеми розпізнавання обличь;
- Масштабно-інваріантне перетворення ознак (SIFT) – алгоритм в сфері комп'ютерного бачення для ідентифікації, визначення та пошуку відповідності локальних ознак.

3.1.1 Сфери застосування методів розпізнавання об'єктів

Серед безлічі варіантів застосування алгоритмів розпізнавання можна виділити наступні групи:

- сортування – включає в себе ідентифікацію та визначення місцезнаходження. Може використовуватися на складах з метою сортування нових товарів;
- перелік – визначає об'єкти потрібного класу та рахує їх кількість, зазвичай застосовується в фармацевтичній сфері;
- контроль якості – використовується на підприємствах для огляду готової продукції;
- пошук за зображенням – визначає всі об'єкти на фото та порівнює з об'єктами у мережі інтернет або у визначеній базі даних;
- розпізнавання місцевості – на відміну від пошуку за зображенням результатом цього алгоритму є загальне уявлення про зображення та визначення узагальнених класів об'єктів, які на ній знаходяться;
- позиціонування – визначення розташування певного об'єкта.

3.1.2 Систематизація методів розпізнавання об'єктів

Нажаль не існує єдиного алгоритму, який можна застосувати до всіх потреб, які може вирішити технологія розпізнавання об'єктів, у зв'язку зі специфічністю

вимог кожної галузі. Не зважаючи на це, можна класифікувати методи та їх способи застосування використавши певні критерії:

- відображення об'єкта. Виділяють такі основні способи базування інформації про об'єкт, як зовнішній вигляд або його геометричні властивості. Моделі зовнішності створюються на основі інформації про похідні від ознак частин фото, які займає об'єкт. Така модель створюється на етапі формування, за допомогою кількох навчальних фото. Геометрична модель використовує форми об'єкта, які в подальшому пов'язуються з системою координат. Такі моделі зазвичай генеруються людиною;
- підвищення якості знімків – задача методів цього класу забезпечити якість зображення, максимально можливу для даних умов, а саме: зниження рівню цифрового шуму, нівелювання впливу погодних умов, відмовстійкість до перевантаження даними, тощо;
- зіставлення та загальна кількість елементів даних, що використовуються – такі дані можна поділити на три умовні групи: необроблені інтенсивні значення пікселів, граничні дані та низькорівневі ознаки.
- стратегія співставлення – розпізнавання об'єкта на фото відбувається співставлення в певній точці алгоритму. Частина алгоритмів мають на меті оптимізацію властивостей перетворення, які відображають співвідношення між моделлю та її проекцією;
- набір даних про об'єкт вміщає в себе дані моделі про локальні чи глобальні властивості об'єкта, який підлягає розпізнаванню. Використовуючи локальні дані модель поділяється на сектори, що в свою чергу отримуються з певних ділянок зображення, які ідентифікують об'єкт. Такий підхід зазвичай використовують для виявлення складних і структурованих об'єктів. Глобальні дані, в свою чергу, представлені набором векторів глобальних функцій, які використовуються для розпізнавання простих геометричних об'єктів в 2D і 3D;

- очікувана дисперсія об'єкта – використовується для відображення різних представників одного і того ж класу. Такий метод може бути вразливим до погодних умов, освітлення, зміни положення камери.

3.2 Визначення подібності шаблонів

Проблеми розпізнавання шаблонів (патернів) є надважливими для покращення вимірювання подібності і дистанції. Подібність вимірює наскільки схожими є об'єкти в порівнянні з заданою множиною моделей. Поділення таких множин на певні категорії дозволяє встановити показники схожості між подібними предметами та різницю між предметами, що відрізняються. Це потрібно для використання їх в певних ситуаціях для збільшення ефективності класифікації. Всього є декілька категорій:

- Евклідова метрика. Спочатку необхідно визначити координати точок (3.1, 3.2)

$$a = \{a_1, a_2, \dots, a_n\}^T \quad (3.1)$$

$$c = \{c_1, c_2, \dots, c_n\}^T \quad (3.2)$$

де a, c – точки з координатами

Після цього визначається дистанція між точками a та c :

$$\begin{aligned} P(a, c) &= \sqrt{(a_1 - c_1)^2 + (a_2 - c_2)^2 + (a_n - c_n)^2 + L} \\ &= \sqrt{\sum_{i=1}^n (a_i - c_i)^2 + L} \end{aligned} \quad (3.3)$$

Оскільки отриману інформацію необхідно нормалізувати, потрібно нівелювати вплив виміру шаблону P .

- відстань Махаланобіса. Складність застосування дистанції Махаланобіса виникає у зв'язку з тим, що сума матриці коваріацій обчислюється лише у випадку, коли дано відомий набір шаблонів.

$$p^2 = (a - M)^T \sum^{-1} (a - M) \quad (3.4)$$

де a – вектор характеристики;

M – середнє значення.

- форма Мінга. Відстань між векторами a та c визначається у формулі:

$$P_m(a, c) = \left[\sum_n |a_n - c_n|^m \right]^{1/m} \quad (3.5)$$

де m – натуральне число;

$a_n c_n$ – значення n порядку для коефіцієнтів a, c .

З цього слідує, що при $m=1$,

$$P_1(a, c) = \sum_n |a_n - c_n| \quad (3.6)$$

- функція кутової подібності є косинусом кута між модулями векторів a, c . Перевагою цієї функції є незалежність від масштабування і повороту координат.(3.7)

$$S(a, c) = \frac{a^T c}{|a||c|} \quad (3.7)$$

3.3 Попередня обробка зображень

Попередня обробка зображень – процес, який включає в себе дії, які мають відбутися для форматування зображення перед його використанням для прогнозування та навчання моделей. Може включати в себе такі кроки, як зміна орієнтації, розміру та кольору. Попередня обробка зображень може пришвидшити час навчання моделі, зменшити розміри великих вхідних зображень без зниження ефективності моделі. [26] На якість вхідних даних також впливають фактори оточуючого середовища. Наприклад положення об'єкта в процесі зйомки та його освітленість можуть вплинути на однорідність якості даних, що в подальшому негативно впливає на обробку та розпізнавання образів. Саме необхідно проводити попередню обробку зображень перед їх використанням. Це дозволить розділити по сегментам цільову область зображення та передати її в функцію розпізнавання. Попередня обробка зазвичай включає в себе покращення, сегментацію, усунення непотрібних ділянок зображення(рис. 3.1).



Рисунок 3.1 – Блок-схема алгоритму попередньої обробки зображення

3.3.1 Підвищення якості зображень

Підвищення якості зображення – один з методів обробки зображень. Він призначений для підвищення візуальної якості та ефектів, після яких зображення стає зручнішим для подальших дій з зображенням. Оброблене зображення після використання методу має стати більш придатним для сегментації, але не обов'язково має бути схожим на оригінальний знімок.[18] Підвищення якості зображень можна умовно поділити на гистограми вирівнювання та гамма-корекцію.

Вирівнювання гистограм опираючись на теорію імовірностей виділяє зображення, що виражається зазвичай в регулюванні градацій зображення, їх збільшення з великою кількістю пікселів. Для виділення зображення необхідно перетворювати гистограми сірих кольорів для отримання сірих значень пікселів. Вирівнювання гистограм відбувається за допомогою формули 3.3. Припускаючи, що метод вирівнювання гистограм обробляє рівень сірого зображення, то потрібно порахувати рівень сірого зображення, отримавши одновимірну гистограму, яку можна записати формулою (3.8):

$$h(n) = k_n \quad k = 0, 1, \dots, L - 1 \quad (3.8)$$

де $h(n)$ – кількість пікселів, які мають значення n для відтінків сірого на зображенні.

Після цього необхідно нормалізувати гистограму до імовірнісної, тоді отримуємо (3.9)

$$P_s(s_n) = \frac{k_n}{K} \quad (3.9)$$

де $k = 0, 1, \dots, L - 1$;

K – загальна кількість пікселів у фото;

$0 \leq s_n \leq 1$.

Це рівняння представляє нормалізоване значення градації n сірого кольору. Якщо припустити, що t означає покращене значення сірого кольору і представляє метод перетворення, можна зробити висновок:

$$t = Q_G(s) \quad (3.10)$$

де $Q_G(s) \in [0,1]$ -постійно зростаюча функція;

при $s \in [0,1]$ маємо $Q_G(s) \in [0,1]$.

З цього слідує:

$$t = Q_G(s_n) = \sum_{i=0}^n \frac{k_i}{K} = \sum_{i=0}^n P_s(s_i) \quad (3.11)$$

де $k = 0,1, \dots, L - 1$;

$$0 \leq s_n \leq 1.$$

Можна зробити висновок, що при підрахуванні сукупної імовірності розподілу всіх значень сірого кольору, можна одержати результати вирівнювання гістограми, а також відобразити значення сірого в рамках $[0,255]$ або інших інтервалів за потреби.

Гамма-корекція – метод зміни експоненціалів. Мета цього алгоритму полягає в тому, щоб подолати експоненціальний закон зміни вихідного сигналу і вхідного збудження, під час отримання зображення або його виводу на екран, щоб перетворити його в лінійну форму(3.11)

$$t = C_s^\gamma \quad (3.12)$$

де C – константа;

γ – дійсне число, яке контролює перетворення;

s – конкретне значення пікселя після коригування.

3.3.2 Сегментація зображень

Являючи собою основу аналізу зображення, основною метою сегментації є поділ зображення на певні області, які стануть передумовами для виділення потрібних областей. Якщо представити зображення поняттям множини, то задачею сегментації буде поділення цієї множини на підмножини відповідно до заданих умов. Пікселі, розташовані на зображенні поруч зазвичай мають спільні властивості, наприклад відтінки кольорів. Та все ж пікселі відрізняються, на зображенні проводяться певні лінії, які і розділяють його на зони – сегменти. Існує таке поняття, як порогова сегментація, вона обробляє і ділить зображення на області, згідно з пороговими значеннями. Такий метод зазвичай має специфічні припущення, які залежать від даного зображення. Методи порогового значення можна умовно поділити на дві категорії:

- метод фіксованого порогу;
- метод динамічного порогу.

Метод фіксованого порогу сегментує зображення шляхом встановлення спеціального обмеження. Такий метод зазвичай застосовується в бінарних зображеннях. Після закінчення процесу порогової сегментації зображення можна визначити у вигляді формули (3.13)

$$h(a, b) = \begin{cases} 1 & f(a, b) > T \\ 0 & f(a, b) \leq T \end{cases} \quad (3.13)$$

де $h(a, b)$ – мітка області після граничного перетворення;

$f(a, b)$ – значення сірого на зображенні;

T – поріг сегментації.

Роблячи висновок, ймовірність щільності розподілу кожного рівню сірого на зображенні обчислюється за формулою (3.14)

$$P_i = \frac{k_i}{K}, \sum_{i=0}^{255} P_i, i \in [0,255] \quad (3.14)$$

де K - загальна кількість пікселів на зображенні.

Задавши початковий рівень сегментації T , пікселі на зображенні поділяться на дві категорії: C_1 та C_2 , де: C_1 містить сірі пікселі в інтервалі $[0, \dots, T]$, а C_2 містить пікселі з рівнями сірого в інтервалі $[T + 1, \dots, 255]$.

Обчислюємо імовірність розподілу сірого(3.15):

$$e_1 = \sum_{i=0}^{T_0} P_i, \quad (3.15)$$

$$e_2 = \sum_{i=T_0+1}^{255} P_i = 1 - e_1$$

Після цього розраховуємо середні значення сірого рівня r_1 та r_2 для категорій C_1 та C_2 , а також повне значення сірого r (3.16):

$$r_1 = \sum_{i=0}^{T_0} i \cdot \frac{P_i}{e_1},$$

$$r_2 = \sum_{i=T_0+1}^{255} i \cdot \frac{P_i}{e_2} \quad (3.16)$$

$$r_2 = \sum_{i=T_0+1}^{255} i \cdot P_i$$

Розраховуємо дисперсії θ_1 та θ_2 для категорій C_1 та C_2 (3.17):

$$\begin{aligned}\theta_1^2 &= \sum_{i=0}^{T_0} (i - r_1) \frac{P_i}{e_1}, \\ \theta_2^2 &= \sum_{i=T_0+1}^{255} (i - r_2) \frac{P_i}{e_2}\end{aligned}\quad (3.17)$$

Розраховуємо міжкласову дисперсію θ_y^2 зображення і внутрішньокласову дисперсію θ_E^2 (3.18):

$$\begin{aligned}\theta_E^2 &= e_1 \theta_1^2 + e_2 \theta_2^2 \\ \theta_y^2 &= e_1 (r_1 - r)^2 + e_2 (r_2 - r)^2\end{aligned}\quad (3.18)$$

де дисперсія θ^2 для всього сірого відтінку на зображенні (3.19):

$$\theta^2 = \theta_E^2 + \theta_y^2 = \sum_{i=0}^{255} (i - r) \cdot P_i \quad (3.19)$$

Оскільки дисперсія градацій сірого зображення є константою, то поріг T буде дорівнювати (3.20):

$$T = \max \left\{ \frac{\theta_y^2(T)}{\theta_E^2(T)} \right\}, T \in [0, 255] \quad (3.19)$$

В цьому і полягає основна ідея Оцу. Вибір оптимального порогу T , щоб після поділу зображення на категорії C_1 та C_2 , відповідно до граничних значень, воно могло відповідати максимальній дисперсії між C_1 та C_2 і мінімальній дисперсії в межах категорії.

3.4 Трекінг об'єктів та його способи

Проблема відстеження об'єктів з'явилася тоді ж, коли з'явилися перші методи комп'ютерного бачення. Трекінг об'єктів має на меті ідентифікувати об'єкт, надати йому певні графічні рамки та продовжувати оновлювати їх, по мірі переміщення об'єкта у кадрі. Відстеження об'єктів також має певний функціонал, який може видати номер ідентифікованому об'єкту для підрахунку схожих за характеристиками. В сучасному світі трекінг об'єктів за допомогою технологій комп'ютерного зору став дуже поширеним у багатьох сферах життєдіяльності, наприклад: відслідковування обстановки на дорогах, розпізнавання маршрутів руху підозрілих осіб у натовпі, тощо.

Є декілька найпопулярніших методів відстеження об'єктів на відеоряді:

- Simple Online And Realtime Tracking (SORT) – просте відстеження в реальному часі та онлайн. Такий метод ігнорує певні об'єкти поза визначеною ціллю. Також він використовує розташування та величину рамок обмеження. В цьому алгоритмі використовуються регіональні згорткові нейронні мережі. Незалежність від руху камери та відокремлених об'єктів дозволяє за допомогою лінійної моделі постійної швидкості визначити рух цілей у потоці кадрів. Такий метод має оцінки MOTA 74.6, IDF1 76.9, 30 FPS[6];
- DeepSORT – оскільки звичайний SORT не може обробити складні сценарії, велике навантаження об'єктами, різні перспективи камери, в DeepSORT було замінено показники подібності на методику, яка об'єднує дані про переміщення та об'єкт. Використовуючи класифікатори і алгоритм видалення шарів класифікації метод генерує вектор, який використовується для відображення результату. Також DeepSORT використовує восьмивимірну систему координат, яка, крім звичайних тривимірних, включає в себе рамку обмеження, співвідношення сторін, висоту та швидкості в координатах знімку. Такі покращення відрізняють в кращу

сторону цей метод від звичайного SORT, зменшуючи зміну ідентифікації на 45% та підвищуючи ефективність обробки складних сценаріїв. Завдяки цьому метод отримав такі показники трекінгу об'єктів: MOTA 75,4, IDF1 77,2, але нижчий показник кадрів на секунду, всього 13;

- FairMOT – створений на основі CenterNet метод відстеження, що не потребує прив'язки до якорів. Вирішення проблеми відстеження об'єктів з позиції мультизадачного навчання та повторного розпізнавання даних в одній системі є надвичайно вигідним рішенням, але майже завжди такі методи конфліктують між собою, що призводить до нерівномірного розподілення ресурсів, що в результаті призводить до того, що система схильна використовувати лише один з методів. Саме тому було винайдено FairMOT. Завдяки однаковому розподіленню навантаження на процеси пошуку та повторної ідентифікації така система має баланс між точністю та швидкістю (рис 3.2). Результати роботи методу відображені у наступних оцінках: MOTA 77.2, IDF 79.8, 25.9 кадрів на секунду;

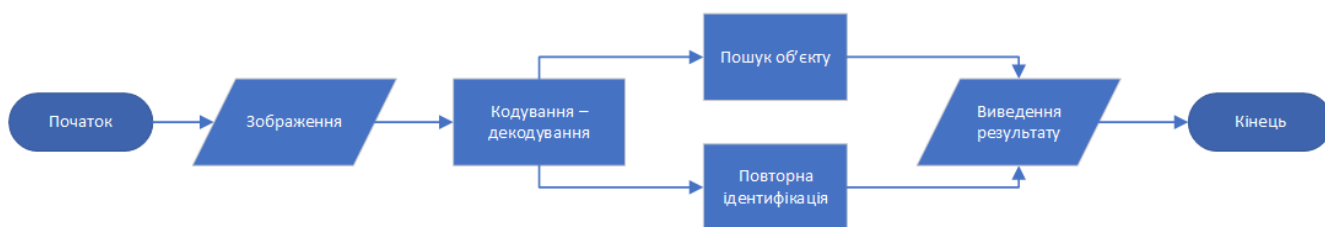


Рисунок 3.2 – Алгоритм роботи модуля FairMOT

- ByteTrack – принципом роботи цього модуля є припущення, що подібність з трекарами забезпечує досить достовірну інформацію для розпізнавання об'єктів та сцени в зонах виявлення з низькою вірогідністю. Для досягнення найкращих характеристик метод BYTE був оснащений детектором YOLOX, який дав можливість створити такий потужний модуль, який отримав наступні оцінки: MOTA 80,3, IDF1 77,3 30 FPS. На рисунку 3.3 зображено алгоритм роботи модуля.

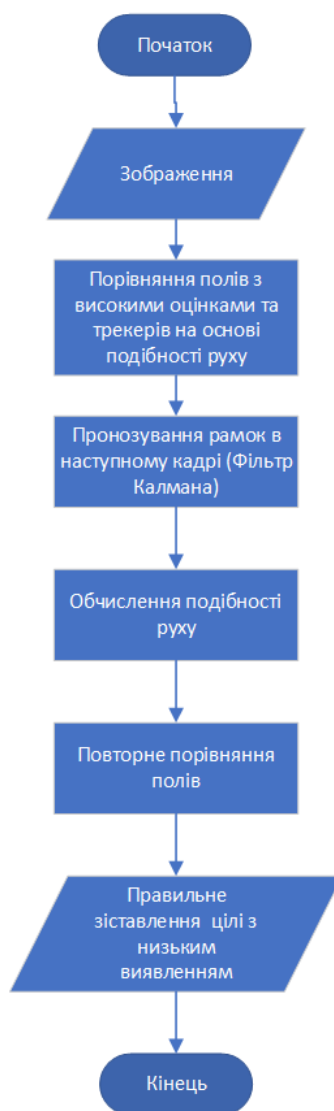


Рисунок 3.3 – Алгоритм роботи модуля ByteTrack

- TransMOT – часово-просторовий граф-перетворювач, котрий впорядковує траєкторії цілей за допомогою зважених графів, які були створені за допомогою просторових співвідношень об’єктів, що відстежуються. Після створення графів система використовує їх для генерації різних перетворювачів. Це відрізняє модель від звичайного перетворювача завдяки структурі об’єктів, що підвищує її ефективність. Подальше представлення каскадної структури аналогій для підвищення швидкості і точності трекінгу дозволяє обробляти випадки з помилковими результатами і довготривалі замикання системи. Це дозволяє досягати розробникам оцінок MOTA 76,7 та IDF1 75,1 на частоті 9,6 кадрів в секунду;

Проаналізувавши методи, можна зробити висновок, що використання модуля ByteTrack є найбільш ефективним, у порівнянні з іншими та дозволить обробляти швидше та якісніше, ніж більшість існуючих рішень для трекінгу об'єктів, що і зображено у таблиці 3.1 [23].

Таблиця 3.1 – Класифікація помилок аерофотозйомки

Спосіб трекінгу	MOTA	IDF1	FPS
SORT	74.6	76.9	30
deepSORT	75.4	77.2	13
FairMOT	77.2	79.8	25.9
ByteTrack	80.3	77.3	30
TransMOT	76.7	75.1	9.6

3.4.1 Класифікація показників оцінки для трекінгу об'єктів

Multiple Object Tracking (MOT) – сукупність оцінок виявлення різноманітних об'єктів визначених класів у відеопотоці, відстеження цих об'єктів у наступних кадрах за допомогою унікальних ідентифікаторів, а також використання цих ідентифікаторів в послідовних кадрах.

Ключовими кроками в роботі алгоритму MOT є:

- отримання безперервного відеопотоку;
- ділення відеопотоку на окремі кадри із визначеною частотою;
- виявлення об'єктів, присутніх у кадрах;
- визначення місцеположення об'єктів у кадрах;
- ідентифікація та аналіз подібних об'єктів у кадрі.

Використовують MOT в таких сферах, як відеоспостереження, БпЛА та робототехніка.

Оцінювати ефективність методів трекінгу можна за такими параметрами:

- MOTA(Multi-Object Tracking Accuracy) – точність відстеження багатьох об'єктів. Найбільш близька міра відображення у порівнянні з розпізнаванням

людиною. Мінусом такого методу оцінки є не врахована міра помилки локалізації та нерівномірні коефіцієнти виявлення і асоціації[25];

- MOTP(Multi-Object Tracking Precision) – точність стеження за багатьма об'єктами. Вимірюється локалізаційна точність, нормалізується відношення між прогнозами та їх істиною. Недоліком є неостатня оцінка реальної ефективності відстеження у зв'язку зі збільшеною точністю оцінки трекара[28];
- IDF1(The Identification Metrics) – методи ідентифікації. Вони визначають точність асоціації, а не коефіцієнт виявлення;
- FPS(Frames Per Second) – частота запису або відображення послідовних кадрів.

Так метрики, як MOTA і MOTP в своїй роботі використовують такі параметри:

- точність ідентифікації та локалізації об'єктів;
- відстеження об'єктів у кадрі;
- налаштування граничних значень.

Підсумовуючи вищесказане, можна зробити висновок, що існує безліч методів розпізнавання об'єктів, які були створенні для використання у спеціальних умовах і можуть бути не ефективні під час використання в інших випадках. Для підвищення ефективності розпізнавання було створено спеціальні методики, застосувавши які, окремо чи в комплексі, можна збільшити кількість зображень для тренування моделі. Використання методів відстеження об'єктів на відеоряді також вимагає значного обсягу тренувальних зображень. Використавши певні оцінки, можна обрати той чи інший метод, в залежності від складності задачі розпізнавання та супроводження цілей на вхідному потоці даних.

4. ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ

4.1 Загальне уявлення про систему

Інформаційна технологія розпізнавання військової техніки з використанням комп'ютерного зору та аерофотозйомки – це програмний модуль, який використовує комп'ютерний зір та аерофотозйомку для виявлення та ідентифікації військової техніки. Система може застосовуватися для надання розвідувальної та спостережної інформації військовослужбовцям, щоб допомогти їм приймати рішення на будь-якому рівні командування. Складається з декількох компонентів, які працюють разом, щоб забезпечити бажані результати. Першим компонентом є система комп'ютерного зору, яка відповідає за аналіз та інтерпретацію аерофотознімків, зроблених БпЛА. Ця система здатна виявляти різні об'єкти, такі як легку колісну та гусеничну техніку, а також вантажівки, з певною ймовірністю. Другим компонентом системи є система аерофотозйомки. Елемент відповідає за аерофотозйомку місцевості і передачу її до системи комп'ютерного зору. В цій ролі виступають БпЛА різного класу. Фотографії використовуються для забезпечення детального огляду місцевості, що дозволяє системі більш точно ідентифікувати особливості, які їй необхідно проаналізувати. Алгоритм роботи системи представлено на рисунку 4.1.



Рисунок 4.1 – Логіка роботи інформаційної технології

4.2 Вибір алгоритму виявлення об'єктів

Алгоритми виявлення об'єктів використовуються для ідентифікації об'єктів на зображенні або відео. Вони застосовуються в різних додатках, включаючи автомобілі з автопілотом, розпізнавання облич, різні системи безпеки. Найбільш поширеним типом алгоритму виявлення об'єктів є згорткова нейронна мережа (CNN). CNN – тип алгоритму глибокого навчання, який використовує шари нейронів для обробки даних. ШНМ здатні ідентифікувати об'єкти на зображенні, розпізнаючи закономірності в даних. Вони використовуються для різноманітних завдань, включаючи виявлення об'єктів, розпізнавання зображень і сегментацію.

Іншим типом алгоритму виявлення об'єктів є машина опорних векторів (SVM). SVM – тип керованого алгоритму машинного навчання, який використовується для класифікації даних (рис. 4.2).

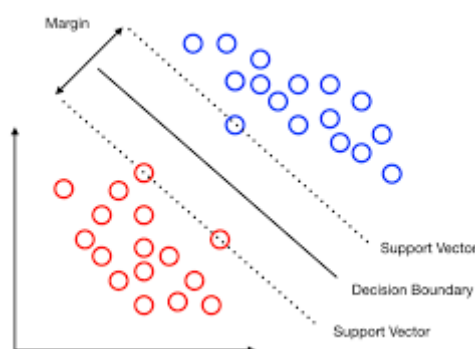


Рисунок 4.2 – Опорний вектор та відступ між 2 класами [2]

SVM здатні ідентифікувати об'єкти на зображенні шляхом розпізнавання шаблонів у даних. Ці алгоритми можуть бути використані для виконання різноманітних задач, включаючи виявлення об'єктів, розпізнавання зображень і сегментацію. Третій тип алгоритму виявлення об'єктів – згорткові нейронні мережі на основі регіону (R-CNN). R-CNN – це тип алгоритму глибокого навчання, який використовує комбінацію згорткових шарів і шарів на основі регіонів для обробки даних. ШНМ здатні ідентифікувати об'єкти на зображенні, розпізнаючи

закономірності в даних. При виборі алгоритму виявлення об'єктів важливо враховувати тип даних і додаток, який створюється. ШНМ найкраще підходять для задач розпізнавання зображень, в той час як SVM – для задач класифікації. R-CNN найкраще підходять для задач виявлення об'єктів. Також важливо враховувати швидкість і точність алгоритму. Різні алгоритми будуть мати різні рівні точності і швидкості, тому важливо обрати алгоритм, який найкраще підходить для відповідних задач.

4.2.1 Порівняння характеристика популярних методів розпізнавання

OpenCV - це бібліотека комп'ютерного зору з відкритим вихідним кодом, яка надає широкий спектр можливостей для обробки зображень. Вона використовується в різних додатках, включаючи розпізнавання обличчя, виявлення об'єктів і відстеження руху.[19] OpenCV написана на мові C++ і доступна для платформ Windows, Mac OS X та Linux. Перевагами OpenCV є:

- відкритий код;
- кросплатформеність;
- ефективність в сфері обробки зображень та відео завдяки широкому спектру алгоритмів;

Такі особливості бібліотеки забезпечують її швидкий розвиток та підтримку іншими користувачами у разі виникнення складнощів. Натомість негативними аспектами фреймворку є:

- низька ефективність при роботі з програмним забезпеченням, яке використовує глибоке навчання;
- складна в розгортванні та налаштуванні.

TensorFlow - бібліотека з відкритим вихідним кодом для машинного навчання. Використовується для додатків глибокого навчання, таких як обробка природної мови, розпізнавання зображень і розпізнавання мови. TensorFlow написана на мові Python і доступна для платформ Windows, Mac OS X та Linux. На відміну від OpenCV, TensorFlow ефективно обробляє завдяки спрямованості на

глибоке навчання. База документації достатньо докладна для швидкого розгортання, що дає змогу розгорнути її без ускладнень. Відкритий код сприяє тривалій підтримці та модифікації бібліотеки. Оскільки фреймворк використовує технології глибокого навчання, то це ускладнює точне налаштування та знижує швидкість роботи, що негативно впливає на ефективність її використання в обробці поточкових даних.

YOLO (You Only Look Once) - алгоритм глибокого навчання, який використовується для виявлення об'єктів. Це одноступенева система виявлення об'єктів, яка є швидкою і точною. YOLO написаний на мові C і доступний для платформ Windows, Mac OS X та Linux. Можна виділити такі переваги цієї технології:

- проста у використанні;
- у порівнянні з іншими має високу швидкість розгортання та роботи, а також широкий спектр алгоритмів для обробки даних, в тому числі і поточкових;

Натомість потужність у цієї бібліотеки відносно невисока, як і кількість документації. Проте це сприяє використанню її у проектах, які потребують швидкого розгортання, можливо, навіть на деяких персональних комп'ютерах в польових умовах.

Підводячи підсумки, то кожен з цих методів має свої переваги та недоліки. OpenCV - це бібліотека для обробки зображень та комп'ютерного зору, але вона не надає можливостей глибокого навчання. TensorFlow - бібліотека для машинного навчання, але вона не така швидка і точна, як YOLO. YOLO – система виявлення об'єктів, яка є швидкою і точною, але вона не забезпечує такого рівня гнучкості, як OpenCV або TensorFlow.

Виходячи з наведеного вище, можна зробити висновок, що YOLO є найкращим вибором для додатків глибокого навчання. Він швидкий, ефективний, зручний і має відкритий вихідний код, що робить його ідеальним для широкого спектру застосувань. Крім того, модуль має велику спільноту учасників, що

постійно його вдосконалюють. З цих причин YOLO є найкращим вибором для додатків глибокого навчання.

4.2.2 Порівняння моделей алгоритму YOLO

YOLOv5 – це модель виявлення об'єктів, розроблена командою YOLO. Вона базується на низці алгоритмів глибокого навчання і покликана бути більш ефективною і точною, ніж її попередники. YOLOv5 пропонує покращену точність і швидкість у порівнянні з YOLOv3, з вищою середньостатистичною точністю (mAP) до 50% і швидшим часом висновку до 2 разів. YOLOv5 також пропонує покращену підтримку користувацьких наборів даних, що дозволяє краще узагальнювати і покращувати продуктивність на невидимих даних. Крім того, YOLOv5 має низку нових функцій, таких як покращена архітектура моделі, багатомасштабне навчання і покращене доповнення даних.

Також в середині алгоритму YOLOv5 можна виділити декілька навчених заздалегідь моделей, порівняних у таблиці 4.1.

Таблиця 4.1 – Порівняння моделей алгоритму YOLO

Model	Size	mAP (50-95)	Speed cpu b1	Speed V100 b1	Speed V100 b32	params	FLOPs
YOLOv5n	640	28.0	45	6.3	0.6	1.9	4.5
YOLOv5s	640	37.4	98	6.4	0.9	7.2	16.5
YOLOv5m	640	45.4	224	8.2	1.7	21.2	49.0
YOLOv5l	640	49.0	430	10.1	2.7	46.5	109.1
YOLOv5x	640	50.7	766	12.1	4.8	86.7	205.7
YOLOv5n6	1280	36.0	153	8.1	2.1	3.2	4.6
YOLOv5s6	1280	44.8	385	8.2	3.6	12.6	16.8
YOLOv5m6	1280	51.3	887	11.1	6.8	35.7	50.0

Продовження таблиці 4.1 – Порівняння моделей алгоритму YOLO

Model	Size	mAP (50-95)	Speed cpu b1	Speed V100 b1	Speed V100 b32	params	FLOPs
YOLOv5l6	1280	53.7	1784	15.8	10.5	76.8	111.4

У таблиці згадуються такі величини:

- size – розмір вхідного зображення;
- mAP – метрика, яка використовується для вимірювання точності моделей виявлення об'єктів. Вона обчислюється як середнє значення середньої точності (mAP) прогнозів моделі на наборі тестових зображень при різних порогах перетину з об'єктом (IoU) в діапазоні 50-95%;
- Speed CPU b1 – процесор, розроблений компанією SpeedCPU Technologies, який оптимізований для додатків YOLO;
- SpeedV100 b1 і SpeedV100 b32 - це два різних варіанти графічного процесора NVIDIA Volta V100, які застосовуються для виявлення та класифікації об'єктів на зображеннях та відео;
- FLOPs – це міра кількості обчислень, які комп'ютер може виконати за секунду.

Проаналізувавши дані таблиці можемо дійти до висновку, чим складніше модель – тим більше часу на її обробку потрібно. Проте це забезпечує вищу якість розпізнавання у порівнянні з простішими моделями цього ж алгоритму. (рис. 4.3)

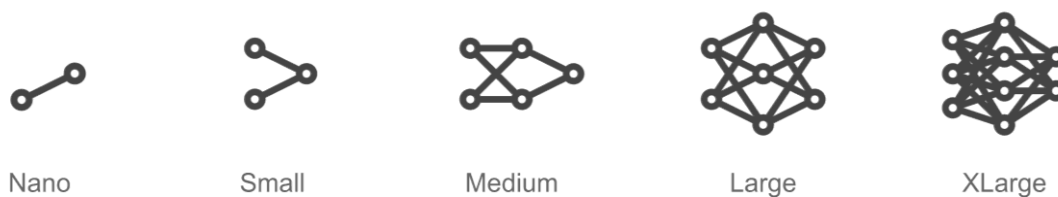


Рисунок 4.3 – Схематичне зображення попередньо навчених моделей [27]

4.3 Формування датасету та тренування нейронної мережі

Для створення набору даних для навчання нейронної мережі потрібна велика кількість зображень. Має бути не менше 5000 фотографій одного і того самого об'єкту, але чим більше даних, тим краще. Дані повинні бути організовані в структурованому вигляді, щоб нейронна мережа могла легко отримати до них доступ і обробити. Наприклад, якщо задача нейронної мережі розпізнавати зображення, то повинен бути набір даних зображень з мітками, що відповідають об'єкту, який мережа має знайти. Після збору даних, можна попередньо обробити їх, щоб полегшити роботу нейронної мережі. Це може включати в себе нормалізацію даних, видалення будь-яких викидів і перетворення їх в числовий формат.

4.3.1 Сервіси для створення датасетів

Під час формування набору даних для навчання нейронної мережі необхідно використовувати спеціалізоване програмне забезпечення, яке може відмітити на зображенні шуканий об'єкт. Загалом можна поділити таке ПЗ на дві категорії, а саме веб-сервіси та десктопні додатки.

Roboflow – це сервіс для створення наборів даних для додатків машинного навчання. Він пропонує широкий спектр функцій, таких як автоматичне маркування, доповнення даних та перевірка даних. Roboflow також надає веб-інтерфейс для легкого доступу до наборів даних та інструменти для створення та управління наборами даних (рис. 4.4).

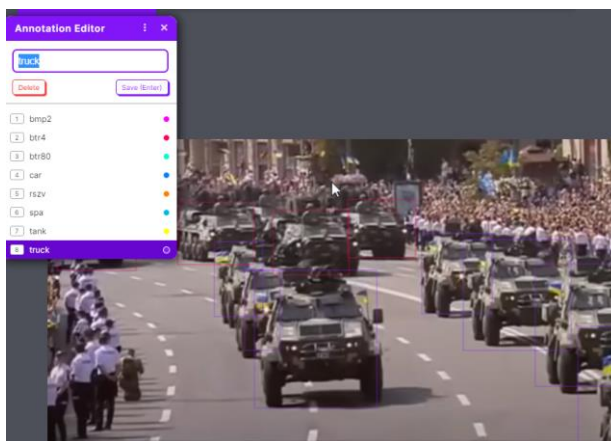


Рисунок 4.4 – Використання сервісу Roboflow

LabelImg – ще один сервіс для створення наборів даних для додатків машинного навчання. Це інструмент з відкритим вихідним кодом для маркування зображень і пропонує графічний інтерфейс користувача (GUI) для легкої анотації. Він також забезпечує підтримку автоматичної анотації та доповнення даних[13].

Як Roboflow, так і LabelImg пропонують послуги зі створення наборів даних для додатків машинного навчання. Roboflow має ширший набір функцій, включаючи автоматичне маркування, доповнення та перевірку даних, а також веб-інтерфейс. LabelImg – це десктопний додаток, який може працювати без доступу в інтернет, що виключає можливість витоку даних під час роботи з ним. Таким чином, як Roboflow, так і LabelImg є чудовими сервісами для створення наборів даних для додатків машинного навчання.

4.3.2 Вплив розміру датасету на якість розпізнавання

Більший набір даних дозволяє отримати більш точні та надійні результати розпізнавання зображень. З таким набором даних алгоритм машинного навчання має більше точок даних для використання для навчання, що підвищує ймовірність ідентифікації правильного об'єкта на зображенні. Це пов'язано з тим, що алгоритм може використовувати точки даних для вивчення більш складних шаблонів і краще розпізнавати відмінності між об'єктами. Однак, більший набір даних може також призвести до надмірного пристосування, коли алгоритм є занадто специфічним і

добре працює тільки на тому наборі даних, на якому він був навчений. Це означає, що коли алгоритм тестується на новому наборі даних, він може працювати не так добре, як на початковому наборі даних. Щоб запобігти цьому, важливо використовувати методи регуляризації, такі як перехресна перевірка та рання зупинка, щоб гарантувати, що алгоритм не підлаштовується під дані.

Крім того, більший набір даних може також призвести до більш дорогих в обчислювальному плані операцій. Зі збільшенням розміру набору даних для навчання алгоритму машинного навчання потрібно більше обчислень, що може призвести до збільшення часу навчання та збільшення ресурсів, необхідних для процесу навчання. Якість набору даних також важлива. Набір даних з більшою кількістю шуму та нерелевантних точок даних може призвести до низької продуктивності, навіть зважаючи на значну кількість даних. Важливо мати високоякісний набір даних з релевантними точками даних і невеликою кількістю шумових точок.

Отже, розмір набору даних є важливим фактором, коли мова йде про якість розпізнавання зображень. Більший набір даних може призвести до більш точних результатів, але він також може призвести до надмірної підгонки, більш тривалого часу навчання і гіршої продуктивності, якщо набір даних поганої якості. Важливо використовувати методи регуляризації, щоб запобігти надмірному пристосуванню і забезпечити високу якість набору даних.

4.3.3 Використання методу Оцу під час створення датасету

Метод Оцу – це популярний метод сегментації зображень, який використовується для автоматичної класифікації зображення на два або більше класів. Вперше він був запропонований Нобуюкі Оцу в 1979 році і з тих пір став одним з найбільш широко використовуваних методів сегментації зображень. В основі методу Оцу лежить ідея максимізації дисперсії між двома класами пікселів на зображенні. Метод працює шляхом знаходження оптимального порогового значення для поділу пікселів на два класи, з метою максимізації дисперсії між

двома класами. Метод Оцу мав великий вплив на розробку наборів даних для машинного навчання і додатків штучного інтелекту. Метод часто використовується як етап попередньої обробки при створенні наборів даних, оскільки він може допомогти зменшити шум і поліпшити якість даних. Це може бути особливо корисно для наборів даних зображень, де метою є точна класифікація зображень на різні класи. Використовуючи метод Оцу, набір даних можна розділити на два класи, які легше розрізнити, тим самим підвищуючи точність алгоритмів машинного навчання. Метод Оцу також корисний для створення наборів даних для завдань керованого навчання. Використовуючи метод для створення двійкового розбиття даних, алгоритми машинного навчання можуть більш ефективно навчатися на основі даних. Метод також може бути використаний для створення наборів даних для задач неконтрольованого навчання, оскільки він може допомогти виявити кластери точок даних, які можуть бути використані для навчання алгоритмів. В цілому, метод Оцу мав великий вплив на розвиток наборів даних для машинного навчання та додатків штучного інтелекту. Метод може бути використаний для створення наборів даних з кращою точністю, зменшення шуму та виявлення кластерів точок даних. Використовуючи метод Оцу для попередньої обробки, можна створювати набори даних, які більше підходять для алгоритмів машинного навчання, тим самим підвищуючи їх точність і продуктивність.

Використавши великий набір даних було натреновано дві моделі. Модель, результати якої знаходяться зліва, була натренована без використання методу максимальної дисперсії (Отсу). Графіки справа відображають натренований датасет з використанням цього методу. Отже, покращення при використанні методу становить 4% (рис 4.5). Це можна пояснити здатністю методу визначати оптимальний поріг для кожного пікселя зображення, що дозволяє краще сегментувати зображення та більш точно класифікувати дані.

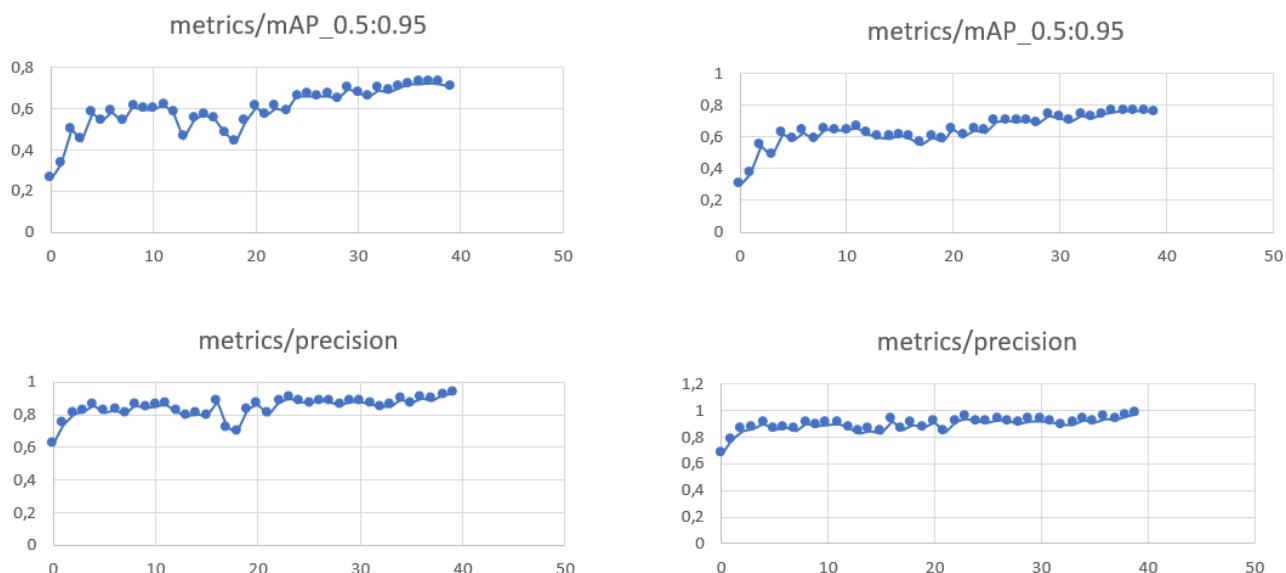


Рисунок 4.5 – Порівняльний аналіз версій датасетів

4.4 Результати тренування нейронної мережі

Після того, як набір даних підготовлений, модель може бути навчена на ньому. Процес навчання передбачає оптимізацію параметрів моделі з метою зменшення похибки моделі. Модель повинна бути протестована на тестовому наборі даних для вимірювання точності моделі. Після того, як модель навчена та пройшла валідацію, вона може бути використана для виявлення військової техніки в режимі реального часу.

У зв'язку з військовим станом у країні провести справжнє тестування на реальній військовій техніці у музеї не можливо, були використані зображення з останнього параду військової техніки на День Незалежності України[41]. На відеоряді можна було побачити різноманітні варіації військової техніки з ракурсу, віддалено наближеного до зйомки з дрону. Після аналізу зображень нейронною мережею було помічено військову техніку з певною ймовірністю (рис 4.6).

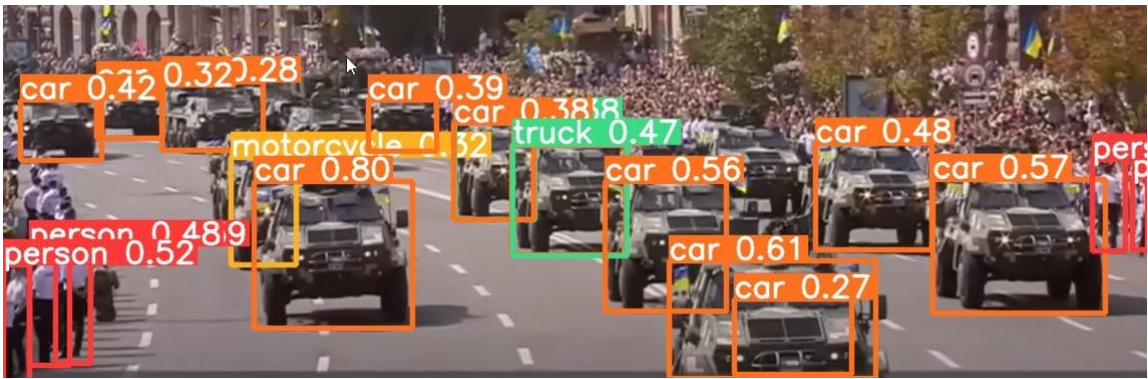


Рисунок 4.6 – Результат роботи модуля розпізнавання об'єктів

На фото зображено безліч об'єктів, що значно ускладнює обробку. Також така кількість цілей для алгоритмів розпізнавання погіршує читабельність результатів для особи, яка буде проводити аналіз вихідних даних. Точність розпізнавання можна покращувати завдяки розширенню датасету.

Отже, можна зробити висновки, що YOLO є ефективним алгоритмом виявлення об'єктів, який здатен виявляти військову техніку з високою точністю. Алгоритм базується на згорткових нейронних мережах (CNN) і здатний ідентифікувати об'єкти на зображеннях та відео з високою точністю. Навчання YOLO на спеціальному наборі даних з військовою технікою вимагає більшої кількості даних, які можуть бути зібрані з різних джерел, таких як військові бази даних, публічні зображення та відео. Дані повинні бути анотовані, щоб забезпечити мітки для об'єктів на зображеннях і відеозаписах. А процес навчання потребує великої кількості даних і вимагає ретельної оптимізації параметрів моделі для досягнення найкращих результатів.

ВИСНОВКИ

Мета роботи покращення процесу розпізнавання військової техніки за допомогою інформаційної технології на основі комп'ютерного зору досягнута. В роботі:

1. Проаналізовано предметну область комп'ютерного зору, її задачі та застосування у військовій справі.
2. Досліджено методи отримання даних, а саме аерофотозйомку, її види, методи та проблеми, а також спосіб отримання даних. До того ж було класифіковано характеристики безпілотних літальних апаратів та сфери їх використання (в тому числі і у військовому напрямку). Досліджено проблеми безпеки БПЛА
3. Проаналізовано алгоритми розпізнавання об'єктів та їх трекінгу.
4. Удосконалено методику розпізнавання зображення на рахунок покращеного датасету з використанням сервісу Roboflow та використання методу Оцу, на основі.
5. Досліджено доступні фреймворки для розпізнавання об'єктів, їх порівняння. Варіанти створення датасету, аналіз отриманих даних.
6. Перспективними напрямками подальших досліджень є створення такого комплексу інформаційних технологій, що буде вирішувати проблеми розпізнавання військових об'єктів, слідів присутності, тощо. Такі модулі матимуть змогу зчитувати та передавати координати об'єктів в єдину систему управління військами, відслідковувати їх зміни. Це дасть змогу автоматизувати збір певних категорій розвідданих і їх передачу до командирів різних рівнів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. «Main Benefits Of The SPYNEL Infrared Sensors», <https://www.hghinfrared.com/Applications/Security/Main-Benefits-Of-The-SPYNELInfrared-Sensors>. (Дата звернення: 30.09.2022).
2. A Brief Overview of Support Vector Machines (SVM). URL: <https://www.iunera.com/kraken/fabric/support-vector-machines-svm>. (Дата звернення: 30.10.2022).
3. AAI RQ 7 Shadow - Alchetron, The Free Social Encyclopedia. URL: <https://alchetron.com/AAI-RQ-7-Shadow>. (Дата звернення: 26.09.2022).
4. Achkar, Roger, and Michel Owayjan. «Implementation of a vision system for a landmine detecting robot using artificial neural network.» arXiv preprint arXiv:1210.7956. 2012р.
5. Aggarwal, Geetika, Neil Mansfield, and Frederique Vanheusden. «An insight on Computer Vision Deploying Image Processing and Object Detection: Applications and Future Research Opportunities.» Organized by Department of Information Technology. 2021р.
6. Bewley, Alex, et al. «Simple online and realtime tracking.» 2016 IEEE international conference on image processing (ICIP). IEEE, 2016р.
7. Classification of the Unmanned Aerial Systems | GEOG 892: Unmanned Aerial Systems. URL: <https://www.e-education.psu.edu/geog892/node/5>. (Дата звернення: 23.09.2022).
8. Digital Noise stock image. Image of grey, abstract, green. URL: <https://www.dreamstime.com/stock-photo-digital-noise-abstract-pattern-display-screen-image74735251>. (Дата звернення: 18.09.2022).
9. ЕНанг - у Китаї випробували аеротаксі польотами в морозну погоду — УНІАН. URL: <https://www.unian.ua/economics/transport/ehang-u-kitaji-viprobuvali-aerotaksi-pilotami-v-moroznu-pogodu-novini-ukrajina-11332568.html>. (Дата звернення: 21.09.2022).

10. Fernando Augusto Garcia Muzzi, Paulo Rogerio de Mello Cardoso, Daniel Fernando Pigatto, and Kalinka Regina Lucas Jaquie Castelo Branco, «Using botnets to provide security for safety critical embedded systems- A case study focused on UAVs» Journal of Physics Conference Series, vol. 633, no. 1, no. 012053, September 2015.
11. Franck Ruffier. PILOTE AUTOMATIQUE BIOMIMETIQUE Syst'eme generique inspire du controle visuomoteur des insectes pour : le decollage, le suivi de terrain, la reaction au vent et l'atterrissage automatiques d'un micro-aeronef. Automatic. Institut National Polytechnique de Grenoble - INPG, 2004. French.
12. Gandhi, Rohith (July 9, 2018). «R-CNN, Fast R-CNN, Faster R-CNN, YOLO — Object Detection Algorithms». Towards Data Science. Retrieved March 12, 2020.
13. LabelImg. URL: <https://github.com/heartexlabs/labelImg> (Дата звернення: 02.11.2022).
14. Lipsitch, Marc, David L. Swerdlow, and Lyn Finelli. "Defining the epidemiology of Covid-19—studies needed." New England journal of medicine 382.13 (2020): 1194-1196.
15. Liu, Wei (October 2016). «SSD: Single shot multibox detector». Computer Vision – ECCV 2016. European Conference on Computer Vision. Lecture Notes in Computer Science. Vol. 9905.
16. merignacpiste 23 - 2016 UKRAINE, STATE AVIATION MUSEUM, KIEV. URL: <https://www.merignacpiste23.fr/reportages-divers-et-musees/2016-ukraine-state-aviation-museum-kiev/>. (Дата звернення: 23.09.2022).
17. N. Eriksson: «Conceptual study of a future drone detection system Countering a threat posed by a disruptive technology», Master thesis in Product Development, Chalmers University of Technology, Gothenburg, Sweden, 2018
18. O. Costilla-Reyes, P. Scully, and K. B. Ozanyan, «Temporal pattern recognition in gait activities recorded with a footprint imaging sensor system,» IEEE Sensors Journal, vol. 16, no. 24, pp. 8815–8822, 2016.
19. OpenCV docs. URL: <https://docs.opencv.org/>. (Дата звернення: 02.11.2022).

20. Paine, David P., and James D. Kiser. Aerial photography and image interpretation. John Wiley & Sons, 2012.
21. Redmon, Joseph (2016). «You only look once: Unified, real-time object detection». Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition.
22. Slocombe, Geoff. «Drones: Anti-drone technologies.» Asia-Pacific Defence Reporter (2002) 48.2 (2022): 27-29.
23. Top 5 Object Tracking Methods. Object tracking aims at estimating. URL: <https://medium.com/augmented-startups/top-5-object-tracking-methods-92f1643f8435>. (Дата звернення: 12.10.2022).
24. Trois drones Harfang de conception israélienne livrés au Maroc - Le Desk. URL: <https://mobile.ledesk.ma/enoff/trois-drones-harfang-de-conception-israelienne-livres-au-maroc/> (Дата звернення: 26.09.2022).
25. Wang, Zhongdao, et al. «Towards 25.» European Conference on Computer Vision. Springer, Cham, 2020.
26. Why pre-processing and augmentation matters for computer vision. URL: <https://blog.roboflow.com/why-preprocess-augment/>. (Дата звернення: 30.09.2022).
27. yolov5/README.md at master · ultralytics/yolov5. URL: <https://github.com/ultralytics/yolov5/blob/master/README.md>. (Дата звернення: 30.10.2022).
28. Yoon, Kwangjin, et al. «Data association for multi-object tracking via deep neural networks.» Sensors 19.3 (2019): 559.
29. Аеротаксі випробували в морозну погоду - Автосвіт - Курс України. URL: <https://kurs.com.ua/amp/novost/297874-aerotaksi-ispitali-v-moroznuju-pogodu>. (Дата звернення: 21.09.2022).
30. Гангало І.М. Особливості використання аерофотозйомки для виявлення та розпізнавання військової техніки// II Міжнародна науково-технічна конференція «Системи І технології зв'язку, інформатизації та

кібербезпеки: актуальні питання і тенденції розвитку». – Київ: ВІТІ, 2022. С. 53-55.

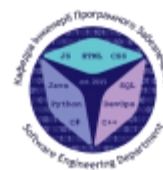
31. ГРК Броня - Armor | Facebook. URL: <https://www.facebook.com/armor.tbs/photos> (Дата звернення: 18.09.2022).
32. Дев'ятикласник із дроном допомагав військовим нищити окупанта цілими колонами і зупиняти наступ на Київ. URL: <https://tsn.ua/ato/dev-yatiklasnik-iz-dronom-dopomagav-viyskovim-nischiti-okupanta-cilimi-kolonami-i-zupinyati-nastup-na-kiyiv-2085715.html>. (Дата звернення: 25.09.2022).
33. Зоровий аналізатор. Будова ока — урок. URL: <https://miyklas.com.ua/p/biologiya/8-klas/organi-chuttia-i-sensorni-sistemi-368750/budova-i-robota-organu-zoru-368701/re-452c1db6-6e4a-4d87-b05c-6e289e39e63e>. (Дата звернення: 18.09.2022).
34. Мосов, С. П., і С. Й. Хорошилова. «Особливості застосування стратегічної безпілотної розвідувальної авіації у воєнних конфліктах ХХІ століття.» Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняхівського (2018р): 97-102.
35. НАКАЗ від 11.05.2018 № 430/210 Про затвердження Авіаційних правил України «Правила використання повітряного простору України» URL: <https://zakon.rada.gov.ua/laws/show/z1056-18?find=1&text=%D0%B1%D0%B5%D0%B7%D0%BF%D1%96%D0%BB#w11> (Дата звернення: 23.09.2022).
36. Оператор оцінив мікродрони Black Hornet, які використовують ЗСУ – Мілітарний. URL: <https://mil.in.ua/uk/news/operator-otsinyv-mikrodrony-black-hornet-yaki-vykorystovuyut-zsu/>. (Дата звернення: 26.09.2022).
37. Перші фото та селфі, зроблені людьми у різних ситуаціях (11 ФОТО) — Радіо ТРЕК. URL: https://radiotrek.rv.ua/articles/istoriya_fotografii_podorozh_u_chasi_245788.html (Дата звернення: 26.09.2022).
38. Росіян вночі лякають зграї Байрактарів. <http://nova.net.ua/rosiian-vnochi-liakaiut-zhrai-bairaktariv/>. (Дата звернення: 25.09.2022).

39. Система скидання Подвійна 2D30 для коптера DJI MAVIC 3. URL: https://prom.ua/ua/p1685847588-sistema-skidannya-podvijna.html?utm_source=google_pmax&utm_medium=cpc&utm_content=pmax&utm_campaign=Pmax_cpa_war_voentorg
40. Там, де трактор не проїде і літак не пролетить. Що роблять аграрні дрони - BBC News Україна. URL: <https://www.bbc.com/ukrainian/features-45055373>. (Дата звернення: 23.09.2022).
41. У центрі Києва до Дня Незалежності відбувся військовий парад – YouTube. URL: <https://www.youtube.com/watch?v=3i1gcNeH2AA&vl=uk>. (Дата звернення: 01.11.2022).
42. Українські сили з дронів скинули вибухівку на техніку росіян – Мілітарний. URL: <https://mil.in.ua/uk/news/ukrayinski-sily-z-droniv-skynuly-vybuhivku-na-tehniku-rosiyan/>. (Дата звернення: 25.09.2022).
43. Які дрони використовує українська армія — Forbes.ua. URL: <https://forbes.ua/war-in-ukraine/armii-droniv-yak-u-viyni-v-ukraini-bpla-zaminyuyut-artileriyu-aviatsiyu-i-kateri-06122022-10273>. (Дата звернення: 24.09.2022).

ДОДАТОК



ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ
ТЕХНОЛОГІЙ



Кафедра інженерії програмного забезпечення

МАГІСТЕРСЬКА РОБОТА

«ІНФОРМАЦІЙНА ТЕХНОЛОГІЯ РОЗПІЗНАВАННЯ ВІЙСЬКОВОЇ ТЕХНІКИ З ВИКОРИСТАННЯМ АЕРОФОТОЗЙОМКИ НА ОСНОВІ КОМП'ЮТЕРНОГО ЗОРУ»

Виконав: студент групи ПДМ-62 Гангало Ігор Миколайович

Керівник: д.т.н., доцент, завідувач кафедри Технологій цифрового
розвитку Жебка В.В.

Київ - 2022

МЕТА, ОБ'ЄКТ, ПРЕДМЕТ ДОСЛІДЖЕННЯ

Мета дослідження: покращення процесу розпізнавання військової техніки за допомогою інформаційної технології на основі комп'ютерного зору

Об'єкт дослідження: процес розпізнавання військової техніки

Предмет дослідження: методи та засоби комп'ютерного зору та аерофотозйомки

АЛГОРИТМ ПРОВЕДЕННЯ РОЗВІДУВАЛЬНИХ ДІЙ



Таблиця 1 - Класифікація розвідувальних БПЛА

№	Розмір	Навантаження (кг.)	Максимальна висота (м. над рівнем моря)	Швидкість (км/год.)
1	Малі	0 – 9	365	185
2	Середні	9 – 25	1050	Менше 460
3	Великі	Менше 600	Менше 5500	Менше 460
4	Більші	Більше 600	Менше 5500	Більше 460
5	Найбільші	Більше 600	Більше 5500	Більше 460

3

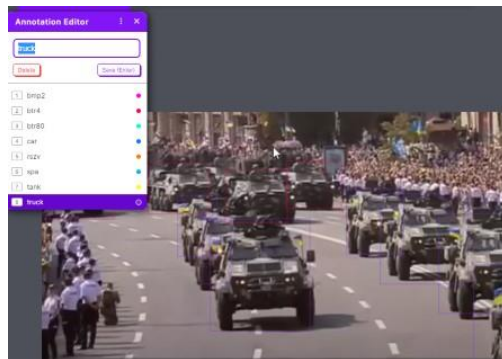
ПОРІВНЯННЯ ПРОДУКТИВНОСТІ ТА ШВИДКОДІЇ ТЕХНОЛОГІЙ РОЗПІЗНАВАННЯ

Досліджуючи методи розпізнавання об'єктів було використано датасет PASCAL VOC. Для використання в технології розпізнавання військових об'єктів важлива точність (mAP) та оброблені кадри в секунду (FPS).

Технології розпізнавання	Набір даних	mAP	FPS
Fast YOLO	2007+2012	52.7	155
YOLO	2007+2012	63.4	45
Fastest DPM	2007	30.4	15
Fast RCNN	2007+2012	70	0.5

4

СТВОРЕННЯ ДАТАСЕТУ



Використання сервісу Roboflow

5

МЕТОД МАКСИМАЛЬНОЇ ДИСПЕРСІЇ (ОТСУ)

Алгоритм розділяє пікселі двох класів ("корисні" і "фонів"), розраховуючи такий поріг, щоб внутрішньокласова дисперсія була мінімальною

$$T = \max \left\{ \frac{\theta_y^2(T)}{\theta_E^2(T)} \right\}, T \in [0, 255]$$



Застосування на одному з зображень датасету

6

ПОРІВНЯННЯ МОДЕЛЕЙ АЛГОРИТМУ YOLO

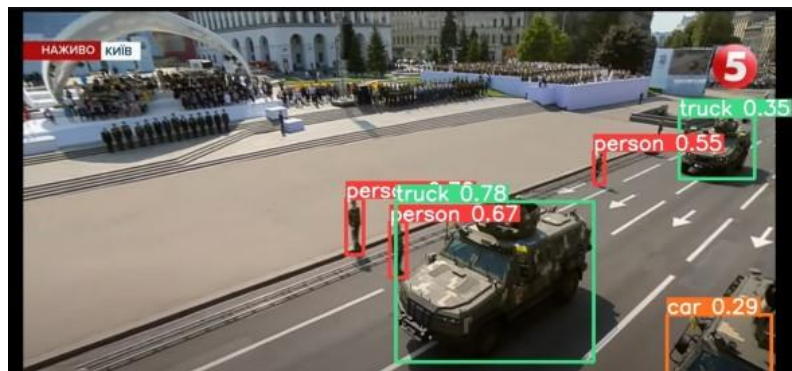
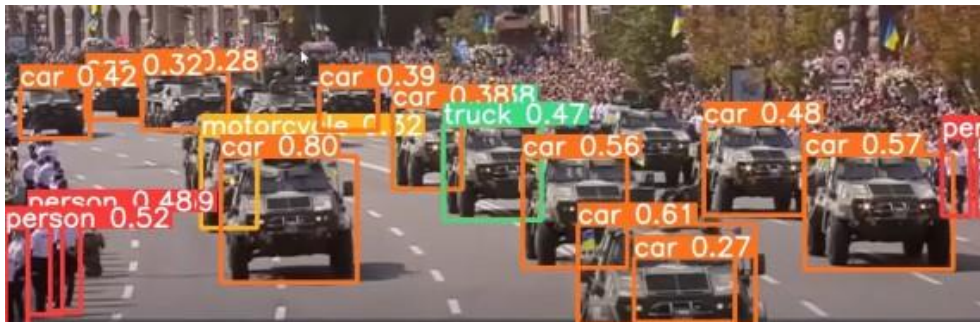
Model	size (pixels)	mAP ^{val} 5095	Speed CPU b1 (ms)	Speed V100 b1 (ms)	Speed V100 b32 (ms)	params (M)	FLOPs @640 (B)
YOLOv5n	640	28.0	45	6.3	0.6	1.9	4.5
YOLOv5s	640	37.4	98	6.4	0.9	7.2	16.5
YOLOv5m	640	45.4	224	8.2	1.7	21.2	49.0
YOLOv5l	640	49.0	430	10.1	2.7	46.5	109.1
YOLOv5x	640	50.7	766	12.1	4.8	86.7	205.7
YOLOv5n6	1280	36.0	153	8.1	2.1	3.2	4.6
YOLOv5s6	1280	44.8	385	8.2	3.6	12.6	16.8
YOLOv5m6	1280	51.3	887	11.1	6.8	35.7	50.0
YOLOv5l6	1280	53.7	1784	15.8	10.5	76.8	111.4



Схематичне зображення попередньо навчених моделей для тренування

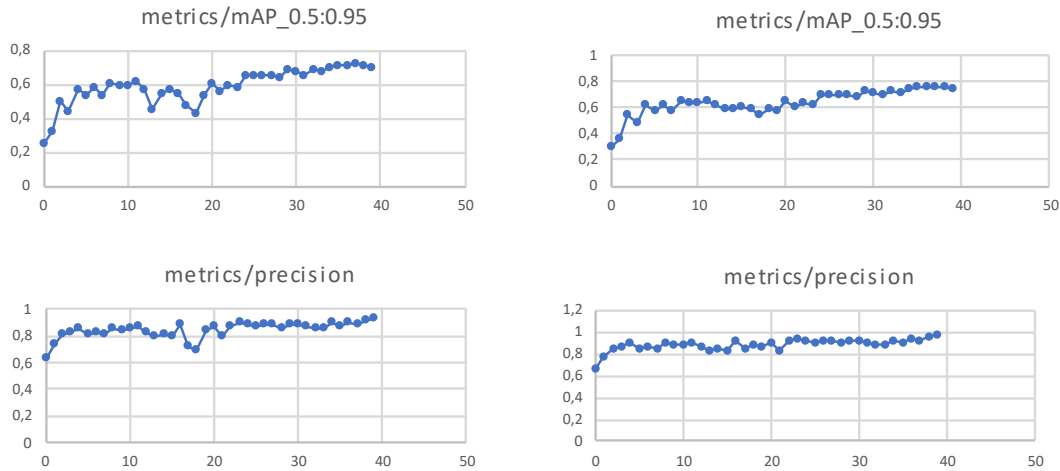
7

РЕЗУЛЬТАТ РОБОТИ ЗАПРОПОНОВАНОГО В РОБОТІ МЕТОДУ РОЗПІЗНАВАННЯ НА ОСНОВІ НАВЧЕНОЇ МОДЕЛІ



8

ПОРІВНЯЛЬНИЙ АНАЛІЗ ВЕРСІЙ ДАТАСЕТІВ



Покращення при використанні методу становить 4%.

9

ВИСНОВКИ

Мета роботи покращення процесу розпізнавання військової техніки за допомогою інформаційної технології на основі комп'ютерного зору досягнута. В роботі:

1. Проаналізовано предметну область комп'ютерного зору, її задачі та застосування у військовій справі.
2. Досліджено методи отримання даних, а саме аерофотозйомку її види, методи та проблеми, а також спосіб отримання даних. До того ж було класифіковано характеристики безпілотних літальних апаратів та сфери їх використання (в тому числі і у військовому напрямку). Досліджено проблеми безпеки БПЛА
3. Проаналізовано алгоритми розпізнавання об'єктів та їх трекінгу.
4. Удосконалено методіку розпізнавання зображення на рахунок покращеного датасету з використанням сервісу Roboflow та використання методу Отсу, на основі.
5. Досліджено доступні фреймворки для розпізнавання об'єктів, їх порівняння. Варіанти створення датасету, аналіз отриманих даних.

10

АПРОБАЦІЯ

Статті:

1. Гангало І.М. Розпізнавання об'єктів за допомогою технологій комп'ютерного зору// Телекомунікаційні та інформаційні технології. №2, 2022. Прийнята до друку.

Тези доповідей

1. Гангало І.М. Особливості використання аерофотозйомки для виявлення та розпізнавання військової техніки// II Міжнародна науково-технічна конференція «Системи І технології зв'язку, інформатизації та кібербезпеки: актуальні питання і тенденції розвитку». – Київ: ВІПІ, 2022. С. 53-55