**МIНIСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**Західноукраїнський національний університет**

**Факультет комп’ютерних інформаційних технологій**

Кафедра комп’ютерної інженерії

**Смагула Тетяна Ігорівна**

**«Алгоритм підрахунку кількості людей в відеопотоці на основі виділення облич/Algorithm for people counting in the video stream based on face detection»**

спеціальність: 123 - Комп’ютерна інженерія

освітньо-професійна програма - Комп’ютерна інженерія

Кваліфікаційна робота

Виконав студент групи КІм-21

Т.І. Смагула

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Науковий керівник:

к.т.н., доц. Ю.М. Батько

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Кваліфікаційну роботу допущено

до захисту:

"\_\_\_" \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ р.

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_Л. О. Дубчак

**Тернопіль – 2022**

РЕЗЮМЕ

Кваліфікаційна робота на тему “Алгоритм підрахунку кількості людей в відеопотоці на основі виділення облич” зі спеціальності 123 «Комп’ютерна інженерія» освітнього ступеня «магістр» написана обсягом 85 сторіноки і містить 21 ілюстрацію, 2 таблиці, 2 додатків та 52 джерел за переліком посилань.

Метою роботи є розробка алгоритму підрахунку кількості людей у відеопотоці на основі детекції їх облич для систем моніторингу.

Методи досліджень. Для розв’язання поставлених задач у кваліфікаційній роботі використано методи та алгоритми: обробки цифрових зображень (для провдення попреденьої обробки зображень); детекції об’єктів (для виділення людських облич у відеопотоці); об’єктно-орієнтованого програмування (для проектування та програмної реалізації програмного додатку).

Результати дослідження: алгоритм предекативного підрахунку кількості людей в відеопотоці на основі виділення облич, програмний додаток моніторингу та аналізу областей спостереження.

Результати роботи можуть бути використані в створенні нових систем охоронних систем з елементами автоматизованого підрахунку людей, для наукових досліджень та в навчальному процесі.

Орієнтовні напрямки розвитку досліджень: розроблення інтелектуалізованих алгоритмів виділення людських облич які приховані зе елементами одягу, створення нових програмних засобів та шаблонів для навчання програмних систем даного типу.

КЛЮЧОВІ СЛОВА: СТАТИСТИЧНІ ФІЛЬТРИ, ДЕТЕКЦІЯ ОБ’ЄКТІВ, ОХОРОННІ СИСТЕМИ, СИСТЕМИ МОНІТОРИНГУ.

RESUME

Graduate qualification work on “Algorithm for automatic completion of program code for integrated development environments ” specialty 123 – Computer Engineering is 86 pages long and contains 33 illustrations, 2 tables, 2 appendices and 52 references.

The aim of the of the work is to develop algorithm for counting number of people in a videostream based on the detection of their faces for monitoring systems.

Research methods. To solve the problems in the qualification work, methods and algorithms were used: digital image processing (for pre-processing of images); object detection (for highlighting human faces in a video stream); object-oriented programming (for the design and software implementation of a software application).

Research results: an algorithm for predicative counting of the number of people in a video stream based on the selection of faces, a software application for monitoring and analyzing surveillance areas.

The results of the work can be used in the creation of new systems of security systems with elements of automated counting of people, for scientific research and in the educational process.

Indicative directions of research development: development of intellectualized algorithms for the selection of human faces hidden by elements of clothing, creation of new software tools and templates for training software systems of this type.

KEYWORDS: STATISTICAL FILTERS, DETECTION OF OBJECTS, SECURITY SYSTEMS, MONITORING SYSTEMS.

ЗМІСТ

[Вступ 7](#_Toc119809555)

[1 Програмно-апаратні охоронні системи відеоспостереження 10](#_Toc119809556)

[1.1 Системи відеоспостереження їх особливості та сфери застосування 10](#_Toc119809557)

[1.2 Передача інформації на основі відеопотоку 22](#_Toc119809558)

[1.3 Програмні додатки систем моніторингу 27](#_Toc119809559)

[1.4 Постановка задач дослідження 29](#_Toc119809560)

[1.5 Висновки до розділу 30](#_Toc119809561)

[2 Методи та алгоритми обробки цифрових зображень у відеопотоці 31](#_Toc119809562)

[2.1 Методи та алгоритми обробки цифрових зображень 31](#_Toc119809563)

[2.2 Алгоритми детекції об’єктів на цифрових зображеннях 38](#_Toc119809564)

[2.3 Алгоритм підрахунку кількості людей у відеопотоці 45](#_Toc119809565)

[2.4 Висновки до розділу 50](#_Toc119809566)

[3 Програмний додаток детекції та підрахунку кількості людей у відеопотоці 51](#_Toc119809567)

[3.1 Структура програмного додатку моніторингу охоронної області 51](#_Toc119809568)

[3.2 Програмні модулі системи підрахунку людей у відеопотоці 64](#_Toc119809569)

[3.3 Тестування та аналіз реалізованого програмного додатку 67](#_Toc119809570)

[3.4 Висновки до розділу 71](#_Toc119809571)

[Висновки 73](#_Toc119809572)

[Список використаної літератури 74](#_Toc119809573)

[Додаток А Лістинг програмного модуля аналізу текстів 77](#_Toc119809574)

[Додаток Б Світлокопії виданих публікацій 80](#_Toc119809575)

# Вступ

Актуальність роботи. Для ведення сучасного бізнесу одоним з факторів є забезпечення безпеки виробицьва та захист внутрішньоої технічної та персональної документації. Тому завдання покращення виявлення загроз і досягнення оптимального захисту за допомогою системи моніторингу відеоспостереження, що активується датчиками є типовими та широко впроваджуваними технологіями. Якщо необхідно підвищити ефективність безпеки бізнесу та зменшити витрати на фізичну охорону, відеоспостереження з моніторингом стане ідеальним рішенням.

Це передове рішення безпеки тепер відкриває двері для дистанційного моніторингу камер спостереження командою віддажених охоронців в режимі 24/7. У багатьох випадках підприємства можуть заощадити до 80% на вартості найму фізичної охорони завдяки інвестиціям у системи відеоспостереження.

Як правило, підприємства, які керують об’єктами з великими периметрами та значними активами для захисту, інвестують у системи відеоспостереження з цілодобовим моніторингом, щоб виявляти та справлятися з загрозами безпеці, такими як організовані крадіжки та проникнення. Віддалений моніторинг є ідеальним рішенням для підприємств і організацій, які потребують захисту значних активів.

Масові зібрання натовпу, такі як спортивні ігри чи концерти, можуть бути джерелом різноманітних ризиків для окремих осіб, особливо викликаних надмірною кількістю людей у певному місці. Перевищення значення, яке вважається безпечним, може призвести до того, що в деяких надзвичайних ситуаціях люди отримають травми або загинуть. Організатори повинні знати кількість людей, які зібралися в будівлі або на закритому відкритому просторі. Крім того, люди часто відчувають занепокоєння, перетинаючи додаткові установки для підрахунку. Окрім того можут виникнути проблеми у випадку необхідності швидкого виходу з будівлі. Крім того, поведінка натовпу під час входу в об'єкт через широкі двері унеможливлює використання інших оптичних або механічних засобів, таких як системи променів випромінювання. Інфрачервоні бар'єри неефективні, тому що вони часто вважають групу людей, що знаходяться близько один від одного, як одну людину. Проблема також полягає в тому, що такі рішення зазвичай не здатні розпізнавати напрямок руху пішоходів. Тому задача створення алгоритму підрахунку кількості людей у відеопотоці є актуальною.

Метою роботи є розробка алгоритму підрахунку кількості людей у відеопотоці на основі детекції їх облич для систем моніторингу.

Для досягнення даної мети ставились наступні завдання:

* провести класифікацію охоронних систем з елементами відеоспостереження;
* проаналізувати архітектурні особливості протоколів потокової передачі інформації;
* провести аналітичний огляд програмних модулів систем моніторингу об’єктів охорони;
* проаналізувати існуючі методи детекції обєктів на цифрових зображеннях в відеопотоках;
* розробити алгоритм автоматичного підрахунку людей в відеопотоці на основі детекції облич;
* реалізувати програмну систему моніторингу та підрахунку кількості людей у відеопотоці на основі детекції людських облич.

Об’єкт дослідження – процес обробки відеопотоків.

Предмет дослідження – методи та алгоритми детекції рухомих об’єктів.

Наукова новизна одержаних результатів визначається наступним чином:

проведено комплексний аналіз та класифікацію алгоритмів попередньої обробки цифрових зображень за допомогою фільтрації, що надало можливість підкреслити їх переваги та недоліки, а також розробити власний алгоритм детекції людських облич на основі ковзного вікна;

розроблено алгоритм детекції людських облич на основі ковзного вікна, що дозволило зменшити обчислювальну складність процесу та підвищити точність виявлення людей на кадрах відеопотоку.

Практична цінність одержаних результатів полягає в тому, що:

розроблено та проведено теоретичне дослідження програмного додатку підрахунку кількості людей у відеопотоці на основі детекції їх облич, що дозволило в подальшому програмно реалізувати та провести дослідження розроблених алгоритмів;

реалізовано програмне забезпечення для підрахунку кількості людей у відеопотоці на основі детекції їх облич та з використанням алгоритмів попередньої обробки цифрових зображень.

Публікації та апробація до випускної кваліфікаційної роботи. За результатами наукових досліджень, проведених у випускній кваліфікаційні роботі, підготовлено тези доповіді «Аналіз алгоритмів попередньої обробки зображень систем автоматизованого моніторингу» обсягом 1 сторінка на VІ Науково-практичній конференції молодих вчених і студентів «Інтелектуальні комп’ютерні системи та мережі», а також «Аналіз алгоритмів сегментації для систем автоматизованого аналізу зображень» обсягом 1 сторінка на VІ Науково-практичній конференції молодих вчених і студентів «Інтелектуальні комп’ютерні системи та мережі».

1 Програмно-апаратні охоронні системи відеоспостереження

## Системи відеоспостереження їх особливості та сфери застосування

Електронна система безпеки відноситься до будь-якого електронного обладнання, яке може виконувати операції безпеки, такі як спостереження, контроль доступу, тривога або контроль вторгнення на об'єкт або територію, що використовує живлення від мережі, а також резервне живлення, як батарея тощо. Це також включає деякі таких операцій, як електричні, механічні механізми. Визначення типу системи безпеки базується виключно на зоні, що підлягає захисту, та її загрозах.

Електронна безпека пов’язана з використанням інновацій у оборонному напрямку шляхом передбачення несанкціонованого доступу до осіб і власності. Уряди країн та фізнесові структури є універсальними та основними замовниками таких адміністрацій безпеки та бізнес-секції також використовують системи безпеки для своїх працівників для забезпечення безпеки. У ці дні можна спостерігати їх використання в діапазоні від побутових програми та невеликих магазинів до трансконтинентальних корпорацій.

Електронні системи безпеки значною мірою включають сигналізацію, засоби контролю доступу та відеоспостереження (телевізори закритого типу), які широко використовуються. Завдяки всім цим продуктам відеоспостереження набули додаткового значення.

Електронні системи безпеки широко використовуються на корпоративних робочих місцях, комерційних місцях, торгових центрах тощо. Ці системи також використовуються на залізничних станціях, у громадських місцях тощо. Системи дуже вітаються, оскільки вони можуть працювати з віддаленої зони. І ці системи також використовуються як системи контролю доступу, системи розпізнавання та запобігання пожежі та системи обліку відвідуваності. Оскільки загальновідомо, що рівень злочинності зростає з кожним днем, тому більшість людей зазвичай не почувають себе комфортно, доки не забезпечать впевненість у своїй безпеці, чи то в офісі, чи вдома. Тому користувачі постійно перебувають у пошуку кращих електронних та технічних систем для забезпечення безпеки.

Класифікація системи безпеки може бути здійснена різними способами, виходячи з функціонування та використання технології, умов необхідності відповідно. Виходячи з функціонування системи електронної безпеки поділяють на чотири основіні групи (рисунок 1.1).

Системи електронної безпеки

Система безпеки відеоспостереження

Система виявлення/пожежної сигналізації

Система контролю доступу/відвідуваності

Система пошуку та виявлення осіб

Рисунок 1.1 – Класифікація систем електронної безпеки

Системи відеоспостереження. Це процес спостереження за підозрілим об’єктом або територією, що підлягає охороні. Основна частина електронної системи безпеки спостереження складається з камер або камер відеоспостереження, які є очима системи спостереження. Система складається з різних видів обладнання, яке допомагає візуалізувати та зберігати записані дані спостереження. IP-камери замкнутого зв'язку та системи відеоспостереження передають інформацію про зображення до місця віддаленого доступу. Головною особливістю цієї системи є те, що вона може використовувати будь-яке місце, де можна спостерігати за діями людей. Деякі з систем відеоспостереження включають камери, мережеве обладнання, IP-камери та монітори. У цій системі можна виявити злочин через камеру, активувати сигналізацію після отримання сигналу від камер, які підключені до системи відеоспостереження. Для занепокоєння щодо виявлення переривання або виникнення підозри на території, що охороняється, чи можливостях, повна операція базується на системі відеоспостереження через Інтернет. На рисунку 2.1 наведена схема побудови системи спостереження.



Рисунок 1.2 – Система відеоспостереження

Система IP відеоспостереження. Система IP-відеоспостереження розроблена з метою безпеки, що дає клієнтам можливість контролювати та записувати відео/аудіо за допомогою системи/мережі IP-ПК, наприклад, локальної мережі або Інтернету. Простіше кажучи, система IP-спостереження включає в себе використання системного комутатора Polaroid, комп’ютера для перегляду, спостереження та збереження відео/аудіо, як показано на малюнку нижче.

У системі IP-відеоспостереження оцифровані відео/аудіопотоки можуть надсилатися в будь-яку область, навіть якомога далі і ширше, якщо потрібно, за допомогою дротової або віддаленої IP-системи, що забезпечує контроль відео та запис з будь-якого місця з доступом до системи/мережі. Приклад структури системи ІР відеоспостереження наведено на рисуноку 1.3.



Рисунок 1.3 – Мережа IP-спостереження

Системи пожежної сигналізації та оповіщення. Її також можна назвати системою виявлення та тривоги, оскільки вона подає тривожне сповіщення про занепокоєння при виявленні переривання чи підозри, що відбувається на охоронюваній території чи об’єкті. Система, як правило, складається з детектора, який використовує датчик, за яким слідує сигналізація або схема сповіщення. Основною функцією цієї системи є швидке гасіння пожежі, що розвивається, і тривога мешканців перед тим, як станеться вражаюча шкода, шляхом заповнення охоронюваної зони газом або сумішшю для гасіння. Для виявлення доступні різні типи датчиків, але використання датчиків суто залежить від вимог програми, як-от домашня автоматизація, виявлення пожежі на складі, попередження про вторгнення тощо.

Системи контролю відвідуваності та доступу. Систему, яка забезпечує захищений доступ до об’єкта або іншої системи для входу чи контролю, можна назвати системою контролю доступу. Вона також може діяти як система забезпечення відвідуваності, яка може відігравати подвійну роль. Відповідно до облікових даних користувача та володіння система контролю доступу класифікується, що користувач використовує для доступу, робить систему іншою, користувач може надати різні типи облікових даних, як-от PIN-код, біометричні дані або смарт-картку. Система може навіть використовувати всю власність користувача для кількох задіяних засобів контролю доступу.

Застосування електронної системи безпеки. Електронна система безпеки розширює своє застосування в різних сферах, таких як домашня автоматизація, житлові (будинки та квартири), комерційні (офіси, банківські шафи), промисловість, медицина та транспорт. Деякі з додатків, що використовують електронні системи безпеки, це електронні системи безпеки для залізничних купе, електронне око з охороною, електронні системи голосування є найбільш часто використовуваними електронними системами безпеки.

Існує багато різних способів забезпечити безпеку будинку чи підприємства, і вирішити, який тип системи безпеки потрібен, може бути важко. Хитрість полягає в тому, щоб з’ясувати, що кожна система здатна забезпечити. Однією з ключових відмінностей є те, що камери спостереження спостерігають, а охоронна сигналізація охороняє. У той час як камери спостереження призначені для спостереження за всім, що знаходиться в їхньому полі зору, і дозволяють переглядати раніше записаний матеріал, сигналізація чекає, доки не спрацює їхня спеціалізована зона, і надсилає сповіщення, чи то місцева сирена, чи професійна служба моніторингу.

У наш час існує багато типів камер спостереження, але їх спільна очевидна особливість: усі вони дозволяють спостерігати та записувати те, що відбувається навколо об’єкту охорони. На сьогодоні існують камери для будь-якої ситуації від тонкої, невеличкої кульової камери до витонченої маленької вежі. Найефективніші камери – це дротові постійні світильники, які охоплюють критичні зони.

Бездротові камери спостереження. Хоча бездротові камери легше переміщувати, ніж дротові камери відеоспостереження, вони не є ідеальними як постійні системи. Вони часто залежать від акумуляторів і локального Wi-Fi, що обмежує кількість камер, які можна використовувати – навіть потужні мережі часто можуть транслювати лише два-три канали. Крім того, бездротові камери обмежують якість відео до 1,3 Мп, що не дозволяє вам ідентифікувати деталі для подальшого використання як докази.

Провідна мережа відеоспостереження. З іншого боку, провідна система може обслуговувати стільки камер, скільки вам потрібно. Система відеоспостереження ідеально підходить для моніторингу майже в реальному часі, тим більше, що якість зображення може досягати 8 Мп. Самі фізичні камери, особливо кульові моделі, також є чудовим засобом стримування. З іншого боку, вони більш сприйнятливі до пошкоджень, але вони, як правило, міцніші, ніж бездротові камери.

На відміну від систем відеоспостереження, системи охоронної сигналізації є повністю автономними. Як і камери, кожен датчик охоплює певну зону, але призначений для виявлення небажаного вторгнення та попередження про небезпеку. Датчики дверей і вікон є поширеними, а також датчики розбиття скла та руху.

Усі вони мають здатність діяти негайно після спрацьовування. Службу моніторингу або поліцію можна попередити, і місцева сирена може зазвучати, щоб запобігти подальшому пошкодженню вашого майна. Також можна контролювати, коли сигналізацію ввімкнути чи зняти з охорони, а сучасні охоронні сигналізації мають інтуїтивно зрозумілі сенсорні екрани, сумісні зі смартфоном, доступ до яких можна отримати без проводів.

Однак ці системи сигналізації не є корисними для відстеження того, що відбувається після їх спрацьовування. Вони можуть лише реєструвати, яка зона периметра була порушена, коли; датчики не в змозі надати деталі, які пропонує хороша система відеоспостереження.

Найкращим налаштуванням часто є поєднання різних типів систем безпеки, встановлених спеціально для вашого місця розташування та потреб професійними установниками систем безпеки.

Проаналізуємо переваги та недоліки кожного з тежнічних рішень при побудові систем безпеки.

1. Контрольовані системи безпеки. Контрольована система сигналізації є однією з найпопулярніших систем безпеки для будинку, доступних на ринку. Зазвичай ця система працює, сповіщаючи кол-центр, групу безпеки або екстрених служб щоразу, коли система виявляє пограбування, пожежу чи інші надзвичайні ситуації. Ця система буває двох типів: система безпеки, що контролюється компанією, і системи безпеки з самоконтролем.

a. Системи безпеки з самоконтролем. Як випливає з назви, системи безпеки з самоконтролем – це ті, які користувач може контролювати самостійно. Ці системи включають датчики руху, датчики дверей, камери безпеки, а також сирени, які викликають або надсилають текстові повідомлення на мобільний телефон, коли спрацьовують.

Більшість систем самоконтролю тепер постачаються з мобільними програмами, які дозволять вам дистанційно контролювати свій дім за допомогою телефону та інших мобільних пристроїв. Крім того, ця система також надає вам можливість зателефонувати в поліцію або попросити охорону перевірити наявність ознак злому щоразу, коли отримуєте сповіщення, а на об’єкті охорони нікого немає.

Незважаючи на те, що системи безпеки з самоконтролем вважаються сучасними та ефективними, вони все ж мають достатню частку плюсів і мінусів.

Переваги систем з самоконтролем:

Користувач отримує сповіщення в режимі реального часу щоразу, коли система активується, що дозволяє швидко реагувати, наприклад викликати поліцію або відправляти людей для перевірки майна.

Вони зручні і можуть бути легко перенесені в інший район або новий будинок, оскільки можна встановлювати та деінсталювати системи самостійно.

Їхні системи камер можуть відстежувати та записувати відео порушників.

Системи безпеки з самоконтролем доступні.

Недоліки систем з самоконтролем:

Для роботи систем безпеки з самоконтролем потрібне з’єднання Wi‑Fi. Він не працюватиме у разі відключення електроенергії.

Користувач може пропустити сповіщення про порушника, якщо перебуватиме в зоні, де немає мобільного зв’язку.

Більшість систем самоконтролю не мають систем сигналізації для відлякування зловмисників.

Покриття їхніх систем камер обмежено лише територією, де вони встановлені.

Необхідно встановлювати кілька камер безпеки, якщо необхідно охопити більше зон об’єкту охорони, що збільшує фінансові затрити на систему охорони.

b. Контрольовані системи безпеки з використанням охоронних компаній. Системи безпеки, що контролюються компанією, контролюються та експлуатуються професійними організаціями та персоналом. Ці системи включають дверні датчики, детектори руху, камери, датчики розбиття скла, гучні сирени, щоб налякати зловмисників, і тиху сигналізацію.

Незважаючи на те, що кожна система має різні функції, більшість систем безпеки, що контролюються компаніями, створені для попередження відповідних контакт-центрів щоразу, коли зловмисник проникає у ваш дім, коли система знаходиться під охороною.

Крім того, користувач також отримаєте телефонний дзвінок для підтвердження, щоб перевірити, чи система сигналізації не спрацювала помилково. Організація безпеки надішле охоронну компанію або поліцію для розслідування, якщо ви не відповідаєте або не відповідаєте на дзвінок.

Подібно до систем безпеки з самоконтролем, ці системи також мають значні крадіжки та перешкоди.

Переваги:

Більшість систем безпеки, що контролюються компаніями, працюють на стільниковому радіо або традиційних телефонних лініях і постачаються з резервним акумулятором. Це допоможе їм продовжувати роботу, коли буде відключення електроенергії.

Користувачам не потрібно самостійно зв’язуватися з органами влади або телефонувати їм, якщо їх телефон недоступний або коли користувач перебуває поза межами охоронної зони.

Сигналізації та сирени більш ніж достатньо, щоб відлякати зловмисників, щойно вони проникнуть у вашу власність, запобігаючи пошкодженню та крадіжці.

Якщо системи безпеки, що контролюються компанією, встановлено належним чином, вони можуть усунути будь-які сліпі зони та охопити весь ваш будинок.

Недоліки:

Якщо система випадково спрацює, вам потрібно буде відповісти на дзвінок, щоб вимкнути її. В іншому випадку негайно зв’яжуться з владою.

Якщо охоронна компанія або поліція буде направлена та не виявить ознак насильницького проникнення чи злому, з вас можуть стягнути плату за помилкову тривогу.

Потрібно завжди вмикати сигналізацію перед виходом з охоронної зони, щоб вона була активною.

Ця система безпеки зазвичай вимагає щомісячної плати та контракту.

2. Неконтрольовані системи безпеки. Неконтрольована система безпеки – це ще один тип системи безпеки, який підходить для захисту вашого майна. Ця система працює, вмикаючи оглушливу сирену всередині та з вашої території, коли спрацьовує сигналізація.

Неконтрольовані системи безпеки складаються з таких елементів безпеки, як датчики руху, контрольна панель, датчики розбиття скла, сирени, датчики дверей і вікон, а також датчики диму. Все це можна встановити самостійно або за допомогою професіонала.

Деякі системи навіть сумісні зі смартфонами, що дозволяє віддалено перевіряти монітор.

До переваг даного типу систем слід віднести:

Хороший рівень безпеки, навіть незважаючи на те, що вони не такі складні та комплексні, як контрольовані системи.

Ці системи часто забезпечують самозапуск або більш статичні системи безпеки, що полегшує їх використання та роботу.

Системи безпеки без моніторингу є економічно ефективнішими та дешевшими порівняно з системами безпеки з моніторингом, оскільки вони не мають підписки чи постійної плати.

Серед недоліків:

Більшість неконтрольованих систем безпеки сильно залежать від власника. Тим не менш, вони неефективні без користувача або коли домовласника немає.

Спілкуватися з правоохоронними органами може бути важко під час лиха чи надзвичайної ситуації, оскільки ці системи не автоматизовані.

Неконтрольовані системи безпеки є менш безпечними та надійними, ніж контрольовані системи безпеки.

3. Бездротові системи охоронної сигналізації. Компоненти бездротової охоронної сигналізації чимось схожі на дротову систему. Але, як випливає з назви, він не передбачає проводки. Компоненти бездротових систем безпеки зазвичай включають детектори, датчики, камери, сигналізацію та головну панель керування.

Такі системи також мають так званий потрійний процес, а саме:

Виявлення. Це початковий крок процесу, який передбачає виявлення будь-яких змін у стані безпеки об’єкту охорони, наприклад, коли хтось розбив вікно, ненадійна сторона відчинила двері, хтось намагався відкрити сейф, система пожежної сигналізації виявила сигнали вогню тощо.

Сповіщення. Це етап, який попереджає власників будинків про можливе проникнення або небезпеку всередину та вихід із власності за допомогою сирен, систем сигналізації, проблискових вогнів тощо.

Моніторинг. Найважливіший етап процесу, який вимагає підключення сигналізації до служби моніторингу. Коли виникає надзвичайна ситуація або виникає загроза, система запускає тривогу та сповіщає моніторингову компанію. Потім компанія надсилає допомогу, наприклад пожежних рятувальників, бригаду медиків або місцеву поліцію.

Як і будь-яка інша система, бездротова охоронна сигналізація має свої переваги та недоліки.

Переваги:

Легко встановити та видалити. Домашню сигналізацію легко буде взяти з собою, якщо ви захочете змінити її розташування або переїдете в інше житло.

Ці системи доступні в комплектах DIY. Ви можете швидко встановити та налаштувати їх, оскільки не потрібно свердлити отвори та налаштовувати складну проводку.

Бездротові системи безпеки легко модернізувати. Оскільки системи не підключені, їх легко оновити та змінити. Легко переміщати пристрої та додавати нові пристрої в систему.

Немає дротів, які потрібно перерізати для грабіжників. Зломщику складно вимкнути бездротову систему безпеки будинку, оскільки між панеллю керування та пристроєм виявлення немає проводів.

Користувачі можуть легко керувати ними за допомогою дистанційного керування. Це можна зробити за допомогою пультів дистанційного керування, бездротових брелоків і мобільних додатків. Користувачі можуть легко перевірити свою систему безпеки без необхідності використання панелей керування.

Недоліки:

Вона вразливий до перешкод. Це може бути не поширеним явищем, але на бездротові системи безпеки можуть впливати перешкоди. Наприклад, великі предмети можуть блокувати їхній сигнал. Певне електричне обладнання також може створювати проблеми, через що грабіжник може заглушити бездротову систему безпеки, якщо він або вона має потрібні інструменти.

Для роботи пристроїв бездротового виявлення зазвичай потрібні батареї. Таким чином, батареї необхідно замінити за потреби, а датчики потрібно періодично перевіряти.

Схильний до злому. Грабіжник зможе заблокувати сигнали та зламати бездротову систему. Існують дешеві бездротові системи сигналізації, які не шифрують сигнали між контрольною панеллю та датчиками.

Деякі бездротові системи безпеки живлять контрольну панель від основного джерело живлення. Деяким навіть потрібні стаціонарні телефонні лінії для підключення служби моніторингу.

4. Дротові системи безпеки. Компоненти дротових систем безпеки підключаються до панелі сигналізації, яка має низьковольтну проводку. Усі точки входу будуть підключені до головної панелі керування разом із детекторами руху, клавіатурами та іншими пристроями безпеки.

Ці дротові системи сигналізації забезпечують більш надійне з’єднання, ніж бездротові системи, оскільки головна панель знає в реальному часі статус кожного пристрою в системі. Те ж саме з вищезгаданими системами, дротова охоронна сигналізація також має позитивні та негативні пакети.

Серед переваг слід відмітити:

Дротові системи надзвичайно надійні, оскільки вони не залежать від датчиків, які використовують для зв’язку радіочастоти. До тих пір, поки телефонна лінія не перерізана або проводка не пошкоджена, ці системи забезпечать максимальну безпеку.

Ці системи прості в обслуговуванні, оскільки власникам потрібно лише замінити батареї, щоб вони працювали.

Провідні системи безпеки ідеально підходять для великих площ, оскільки вони можуть мати більше датчиків порівняно з бездротовими системами.

Такі системи менш схильні до злому, ніж бездротові системи. Буде важко зламати жорсткі системи, тому що вони вимагають ручного підключення проводів для доступу до них.

Професіонали віддають перевагу дротовим системам безпеки через їх безпеку, послідовність і надійність.

Дротові системи мають багато функцій і забезпечують першокласні пристрої з відеоспостереженням високої чіткості та панелями керування в кількох областях.

Мінуси:

Провідні системи обходяться дорожче в установці. Це дороге встановлення, оскільки професіонали встановлюють обладнання безпеки.

Ці системи більш вразливі для грабіжників. Порушники можуть просто перерізати електропроводку та телефонні лінії за межами об’єкту охорони, якщо вони бажають вимкнути систему безпеки.

Обладнання дротової системи безпеки важко демонтувати. Деякі охоронні компанії відмовляються встановлювати старе обладнання на новому місці і можуть навіть не рекомендувати переносити дротові системи.

Вони мають лише одне місце керування, що означає, що поставити та зняти їх з охорони лише з головної панелі керування.

## Передача інформації на основі відеопотоку

Протокол потокової передачі – це спеціальний метод, який використовується для доставки мультимедіа через Інтернет. Іншими словами, це набір правил, які регулюють спосіб передачі даних, а також способи обробки будь-яких помилок, які можуть виникнути під час цього процесу.

По-перше, потоковий протокол – це не те саме, що кодек. Остання є спеціальною технологією для зменшення розміру ваших даних (наприклад, відеофайлу). Простіше кажучи, кодек видаляє неважливу інформацію у відео, щоб стиснути розмір файлу.

По-друге, деякі люди плутають протокол потокової передачі з форматом контейнера, що в основному означає, як зберігаються дані. Наприклад, три найпоширеніші формати пакетів для потокових відеофайлів: FLV, MP4 і MPEG‑TS.

Існує сім логічних рівнів, кожен з яких виконує певні комунікаційні функції. Щоб спростити речі, потокові протоколи працюють у межах цих рівнів, зосереджуючись лише на своїх функціях. Гаразд, це не стає складнішим, тож терпіть нас.

Один шар, який особливо заслуговує вашої уваги, це транспортний рівень. Він відповідає за передачу вашого вмісту на кінцеву платформу. Його можна передати двома способами – чере протокол керування передачею (TCP) або протокол дейтаграм користувача (UDP). Основна відмінність між цими двома протоколами полягає в тому, що TCP змушує пристрої, що спілкуються, встановлювати з’єднання для передачі даних. UDP, з іншого боку, ігнорує цей крок.

На більш практичному рівні UDP передає невеликі фрагменти інформації відносно швидше, ніж TCP. Однак це має свою ціну. Через відсутність кількох рукостискань і кроків підтвердження між пристроями дані не можуть передаватися в строгому порядку. Крім того, приймаюча сторона може взагалі не отримати деякі частини. Іноді це може призвести до незначних проблем із якістю.

Зрозуміло, що існують десятки протоколів прямої трансляції, кожен з яких виконує свою функцію. Однак можна з упевненістю виділити кілька найпопулярніших.

Протокол RTMP, який використовує протокол ТСР. Протокол RTMP, розроблений компанією Macromedia та придбаний компанією Adobe у 2005 році, досі залишається найбільш використовуваним протоколом. Він підтримує постійне, стабільне з’єднання та забезпечує зв’язок із малою затримкою. RTMP передає дані потоку, які розділені на невеликі пакети між Flash Player і сервером, щоб забезпечити мінімальні переривання та артефакти. Крім того, через фактор успадкованості RTMP підтримується більшістю потокових платформ і програмного забезпечення.

Специфікації цього протоколу були офіційно опубліковані Adobe для загального використання. За іронією долі, компанія оголосила про припинення підтримки Flash Player. Іншим недоліком протоколу RTMP є можливість перерв через низьку пропускну здатність, аж до того, що ваш потік може взагалі не початися. До списку недоліків додається те, що деякі жорсткі брандмауери можуть не дозволяти підключення RTMP через низький рівень безпеки доставки відео. Хоча, треба сказати, таке трапляється досить рідко.

До списку мінусів можна віднести стандартну затримку потоку від п’яти до 30 секунд, але її можна зменшити до двох-трьох секунд. Крім того, протокол наразі використовує відеокодек H.264 і аудіокодек AAC, які досить застарілі та не забезпечують найкращої якості. Відеокодеки: H.264. Аудіокодеки: AAC. Затримка: 3 - 30 секунд.

Переваги даного методу: підтримка багатоадресної передачі, низька буферизація, підтримка широкої платформи.

Недоліки даного протоколу: старі кодеки, дещо низька безпека, відносно висока затримка.

WebRTC (Web Real-Time Communication protocol): як UDP, так і TCP. WebRTC – це стандарт з відкритим вихідним кодом для спілкування в реальному часі, який підтримується майже всіма сучасними браузерами, включаючи Safari, Google Chrome, Firefox, Opera та інші. WebRTC підтримує високоякісні VP8 і VP9 (крім старого H.264), а також аудіокодек Opus. Найближчим часом протокол отримає підтримку абсолютно нового відеокодека AV1. Передбачається, що протокол замінить телефонію і стане основою комунікаційних послуг.

Однією з найбільших переваг WebRTC є те, що він перетворює мільйони браузерів на потокові термінали без необхідності встановлення додаткових плагінів. Крім того, WebRTC підтримує затримку менше секунди, що означає фактично режим реального часу. Також, протокол використовує адаптовану технологію бітрейту, яка дозволяє йому автоматично регулювати якість відео та запобігати будь-яким падінням і перервам.

Що стосується недоліків, то у WebRTC небагато. Деякі вважають мінусом той факт, що протокол все ще знаходиться в стадії розробки. Простіше кажучи, кодек VP8 є безоплатним, а H.264 – ні. Хоча більшість компаній підтримують VP8, деякі інші категорично проти цього рішення, яке може призвести до конфлікту. Однак варто зазначити, що всі погоджуються, що за AV1 майбутнє. Відеокодеки: VP8, VP9, H.264 (H.625 + AV1 у процесі). Аудіокодеки: Opus. Затримка: менше однієї секунди.

Переваги: не потрібні плагіни, затримка менше секунди, підтримувані кодеки.

Недоліки: нестабільність через субсекундну затримку.

FTL (протокол Faster Than Light): UDP. FTL був розроблений потоковою платформою Mixer, що належить Microsoft . На жаль, Mixer було закрито через неможливість масштабування в порівнянні з конкурентами. Однак, використання цього протоколу може бути корисним. Назва FTL говорить сама за себе. FTL – це протокол потокової передачі в реальному часі, що означає, що він підтримує затримку менше секунди. Це дозволяє залучати глядачів і спілкуватися з ними в режимі реального часу практично без затримок. FTL підтримується найпопулярнішими потоковими програмами, включаючи XSplit і OBS Studio. Він також попередньо інтегрований в ОС Windows 10 і Xbox One. Він використовує аудіокодек Opus і відеокодек H.264, щоб забезпечити гарне поєднання якості, плавного відтворення та низької затримки.

Недоліком використання FTL є те, що ваш потік трохи втратить якість. Mixer рекомендує знизити бітрейт до 7 Мбіт/с порівняно з 10 Мбіт/с у RTMP. Іншим недоліком FTL є відсутність стабільності. На відміну від своїх предків, у протоколі FTL ще не було виправлено багато помилок, що означає, що він може бути трохи непередбачуваним. Незважаючи на те, що FTL є абсолютно новим, він уже повністю інтегрований в екосистему Restream. Поки лише Mixer і Restream підтримують протокол FTL. Відеокодеки: H.264. Аудіокодеки: Opus. Затримка: менше однієї секунди.

Перевагами даного методу: наднизька затримка та спілкування в реальному часі.

Серед недоліків слід зазначити: нижча якість відео, нестабільність через затримку менше секунди, слабка підтримка.

SRT (Безпечний надійний транспорт): UDP. SRT – це протокол потокового відео з відкритим кодом, розроблений Haivision і Wowza. Вважається, що в найближчому майбутньому він замінить RTMP. Маючи ті ж переваги, SRT робить наступний крок і втілює мрію про стабільні прямі трансляції із затримкою менше секунди. Це дозволяє вам транслювати свій вміст у неоптимальних мережах. Однак одним великим недоліком є те, що опція відтворення недоступна.

Розробники стверджують, що SRT захищає ваші живі відео від тремтіння, коливань пропускної здатності та втрати пакетів. Крім того, SRT подібний до FTL і WebRTC з точки зору затримки в секунду, що дозволяє спілкуватися майже в реальному часі. Крім того, також зазначено, що протокол не залежить від кодеків, тобто він підтримує будь-який сучасний відео та аудіокодек. На жаль, враховуючи, що це все ще нова технологія, SRT не підтримується широко. Відеокодеки: кодек-агностик. Аудіокодеки: кодек-агностик. Затримка: менше однієї секунди.

Плюси даного протоклу: висока якість, стабільність, затримка до секунди, потужна підтримка кодеків.

Мінуси: слабка підтримка платформи, відсутність відтворення.

При розгляді різних протоколів було зроблено висновок, що використання сучасних механік передачі інформації через глобальну мережу інтерне дозволяє проводити обмін інформацією в режимі реального часу, тобто затримки не мають вирішального впливу на сприйняття інформації між сторонами обміну.

Класифікація потокових протоколів передачі інформації

RTMP

WebRTC

FTL

SRT

Рисунок 1.4 – Класифікація протоколі передачі інформції за допомогою відеопотоків

По суті, потоковий протокол – це набір правил, які визначають, як дані передаються через Інтернет. Проаналізовано чотири найпопулярніші протоколи прямої трансляції: RTMP, WebRTC, FTL і SRT. Кожен має свої плюси та мінуси, тобто ви можете використовувати будь-який залежно від ваших потреб.

## Програмні додатки систем моніторингу

Сучасні системи безпеки бізнесу включають все: від замків до детекторів руху та моніторів повеней. Деякі пропонують спеціальні інструменти, такі як бирки, щоб запобігти крадіжкам у магазині. Більшість систем включають інтелектуальний додаток для моніторингу та керування системою, тоді як деякі інтегруються з Alexa або Google Home для встановлення температури, увімкнення світла чи активації будильника.

SimpliSafe – це популярне рішення безпеки з недорогою ціною та простим у використанні обладнанням, яке можна встановити самостійно. Це найкращий вибір для бюджетних компаній, які потребують базової безпеки у вигляді замків, камер і моніторингу навколишнього середовища, як-от повені та пожежі.

Відсутність моніторингу для конкретного обладнання, справді бездротові камери (хоча деякі з них підтримують Wi-Fi, їх все одно потрібно підключити до джерела живлення) і обмежені можливості запису відео – ось те, де SimpliSafe втратив бали. Vivint, з іншого боку, має всі ці функції (тільки за вищу ціну). SimpliSafe також не пропонує чіткої політики щодо відшкодування, якщо його система виходить з ладу, а у вас є крадіжка або пошкодження.

Vivint має плани як для дому, так і для бізнесу, забезпечує інсталяцію на замовлення, яка може включити будь-яке наявне у вас обладнання, і має цілодобовий професійний моніторинг. Vivint пропонує розумні замки, датчики навколишнього середовища для температури або затоплення, розумні термостати та розумну панель керування для роботи з усім цим. Крім того, його камери бездротові.

Він отримав високі бали за все, крім ціни та загальних характеристик. Контракти Vivint розраховані на 42-60 місяців, що значно знизило його рейтинг. Його комплектація стандартна, але постраждала через відсутність біометричних замків. Vivint має чудовий рівень задоволеності користувачів у нашому списку, поступаючись Frontpoint і Cove.

Tattletale спеціально розроблений для потреб великих відкритих територій, таких як будівельні майданчики, комунальні послуги, місця відпочинку, підприємства садів або озеленення, школи та церкви. Особливості включають невидимі огорожі та надміцну портативну систему безпеки, яка може відстежувати близько 500 датчиків. Домашня система Tattletale також підходить для малого бізнесу, але вам потрібно придбати власні замки або обладнання доступу.

Система дуже доступна, має чудову підтримку встановлення та отримала високі відгуки користувачів. Однак він має найнижчий бал за загальні та апаратні характеристики серед систем у цьому списку. Обмежена сумісність пристроїв, гарантії на обладнання та пошкодження, відсутність інтеграції інтелектуальної платформи та неможливість використовувати систему для перевірки замків вартують очок.

## 1.4 Постановка задач дослідження

Під час проведених досліджень в даному розділі було наведено результати аналізу особливостей побудови та використання охоронних систем з елементом відеоспостереження. Проаналізовано протоколи потокової передачі інформації, їхні переваги та недоліки, а також особливості їх використання. Досліджено програмні додатки програмно-апаратних комплексів моніторингу об’єктів охорони, виділено їх основні функції.

Для досягнення поставленої мети необхідно розв’язати наступні задачі.

провести класифікацію охоронних систем з елементами відеоспостереження;

проаналізувати архітектурні особливості протоколів потокової передачі інформації;

провести аналітичний огляд програмних модулів систем моніторингу об’єктів охорони;

проаналізувати існуючі методи детекції обєктів на цифрових зображеннях в відеопотоках;

розробити алгоритм автоматичного підрахунку людей в відеопотоці на основі детекції облич;

реалізувати програмну систему моніторингу та підрахунку кількості людей у відеопотоці на основі детекції людських облич.

## 1.5 Висновки до розділу

Проведено аналіз та класифікацію охоронних систем на основі виконуваних завдань та сфер використання, що дозволило виділити основні програмні модулі та функціональні особливості систем даного типу.

Проаналізовано та проведено дослідження основних протоколів потокової передачі інформації через глобальну мережу інтернет, що дозволило виділити протокол передачі даних для системи моніторингу та підрахунку людей в відеопотоці.

Проведено аналіз програмних охоронних систем з елементами моніторингу, що дозволило виділити основні програмні функції та структури, а також архітектурні рішення, що дозволило в подальшому спроектувати архітектуру програнмого додатку підрахунку кількості людей у відеопотоці.

# 2 Методи та алгоритми обробки цифрових зображень у відеопотоці

## 2.1 Методи та алгоритми обробки цифрових зображень

Люди все ще отримують переважну більшість своїх сенсорних даних через свою зорову систему, і було докладено величезних зусиль, щоб штучно посилити цей варіант сприйняття світу. Окуляри, біноклі, телескопи, радари, інфрачервоні датчики та фотопомножувачі – усе це дає змогу покращити наше бачення світу та Всесвіту. На сьогодні навіть є телескопи на орбіті (очі за межами атмосфери) і багато з них «бачать» в інших спектрах: інфрачервоному, ультрафіолетовому, рентгенівському. Вони надають можливості які колись не могли собі уявити, при цьому цим технологіям лише кілька років і вони уже позволяють бачити в кольорах, які людина ніколи раніше не бачила неозброєним оком. Комп’ютер був необхідним для створення неймовірних зображень, які всі бачили за допомогою цих пристроїв.

На відміну від інших видів програмного забезпечення, системи зору не є повсюдними функціями повсякденне життя. Це можна пояснити тому, що проблема із зором дійсно важка як алгоритмічно так і в технічному виконанні.

Під час експериментів із системами аналізу зору та зображень або впровадження їх для практичних цілей базова інфраструктура програмного забезпечення є важливою.

Зображення складаються з пікселів, і в типовому зображенні з цифрової камери їх кількість становитиме 4–6 мільйонів пікселів, кожен з яких представлятиме колір у певній точці зображення. Цей великий обсяг даних зберігається у вигляді файлу у форматі (наприклад, GIF або JPEG), придатний для обробки комерційними програмними пакетами, наприклад як Photoshop і Paint. При розробці нових програмних засобів аналізу зображень спочатку необхідно прочитати ці файли у внутрішню форму, з якої можна отримати доступ значення пікселів. Немає нічого складного в коді, який робить це, і це не передбачає жодної фактичної обробки зображень, але це важливий перший крок.

Подібним чином програмне забезпечення для аналізу зображень має відображати зображення на екрані і зберегти їх у стандартних форматах. Напевно, корисно мати сховище для зберігання разультатів зйомки зображень. Жодна з цих операцій не змінює зображення, але просто перемістіть його в формат зручний для подальшої обробки.

Ці практичні завдання можуть вимагати більшої частини коду, задіяної в програмі для створення зображень. Процедура зміни всіх червоних пікселів на жовті, наприклад, може містити лише 10 рядків коду; але програмі потрібно прочитати зображення, вивести його на екран, і виведення результату може вимагати допдаткових 2000 рядків коду або навіть більше.

Звичайно, цей код інфраструктури (який можна розглядати як додатоковий інтерфейс програмування, або API) можна використовувати для всіх програм; так само як API можна використовувати без змін, доки не знадобляться оновлення.

Зміни в операційній системі, базових бібліотеках або додаткових функціональних можливостях можуть потребувати нових версій API. Якщо все зроблено належним чином, ці практичні аспекти системи зору для нових версій вимагатимуть незначних змін або не потребуватимуть жодних змін у програмах, які залежить від цього.

Фільтри попередньої обробки. Алгоритми попередньої обробки важливі в виявлення малих цілей. Корисність різних просторових, а також часових фільтрів не викликає сумнівів оскільки вони дозволяють виявити дрібні деталі на цифрових зображеннях. Незалежно від вибраного методу, фільтр попередньої обробки повинен виконувати завдання посилення ізольованих точок (малі цілі займають один ізольований піксель у площині зображення), збереження периферійної інформації та надання слабкої відповіді в однорідній області. Деякі з фільтрів не мають прямого застосування при аналізі малих цілей виявлення, але вони можуть мати важливе значення на етапі попередньої одробки. Для прикладу просторові фільтри це є поширений метод виявлення цілей на основі малого розміру аналізованих об’єктів при прогнозуванні фону під час використання методів обробки зображення та віднімання його з оригінального зображення. Гаусівський, статистичний і морфологічний фільтри були досліджені для невеликих програм виявлення цілей.

Фільтр Гауса. Оператор Гаусового згладжування є двовимірною згорткою оператора, який використовується для розмивання зображень і видалення деталей і шумів. Він використовує ядро, яке представляє форму та має дзвоноподібний вигляд так званий Гаусів горб.

.

Гаусове згладжування використовує цей 2-D розподіл як функцію поширення точки. Це досягається за допомогою згортки. Оскільки зображення зберігається як сукупність окремих пікселів, необхідна дискретна апроксимація функції Гауса для виконання згортки. Ядро можна скоротити на 3*s* (*s*: стандартне відхилення) межі від середнього.

Статистичні фільтри. Статистичні фільтри, описані в літературі для згладжування зображення, а ъх перелык наведено на рисунку 2.1.

Статистичні фільтри

Серединний

Вибіркова медіана

Максимальний медіанний

Максимальний серединний

Медіанний

Рисунок 2.1 – Класифікація статистичних фільтрів

Середній фільтр: він простий, інтуїтивно зрозумілий і легкий у застосуванні. Це зменшує кількість коливань інтенсивності між одним піксель і наступний. Кожне значення пікселя в зображенні замінюється серед своїх сусідів, включаючи себе. Це усуває пікселів, які не є репрезентативними для свого оточення. Середнє фільтрування базується на ядрі, яке представляє форму та розмір мікрорайону, який буде відібрано при обчисленні середнього. Часто це використовується квадратне ядро 3×3, хоча більші розміри ядра або повторне використання маленького ядра можуть бути використані для кращого (але не ідентичного) результату.

Медіанний фільтр: використовується для зменшення шуму, як і середній фільтр на зображенні. Однак краще в збереженні корисного деталі на зображенні, ніж середній фільтр. Як середній фільтр, медіанний фільтр розглядає кожен піксель на зображенні та замінює його медіаною сусіднього пікселя значення. Медіанний фільтр має дві основні переваги перед серединним фільтром:

Це більш надійна оцінка, ніж середнє. Одинокий нерепрезентативний піксель у сусідстві не вплине на медіану значно.

Це не створює нових нереалістичних значень пікселів, оскільки медіана насправді має бути значенням одного з пікселів у сусідстві.

Фільтри максимального медіани/максимального середнього: вони видаляють недоліки медіанних/середніх фільтрів (втрата важливого цікавої особливості). Ці фільтри ефективно усувають шум і зберігають геометричні особливості сигналів і є називаються фільтрами максимальної медіани. Максимальна медіана/середнє значення пікселя в його околиці обчислюється як:

,

де *y*(*m*,*n*) – результатом фільтра максимального медіани/середнього значення (2*N*+1)-го порядку;

z1, z2, z3, z4 – медіанним/середнім середнього рядка, середнього стовпця та двох діагоналей ядра згортки з центром навколо аналізованого пікселя, відповідно.

Чим більше значення *N*, тим більше придушення спайків. Ця властивість використовується для виявлення дрібних цілі.

Вибірковий медіанний фільтр: це особлива форма медіанного фільтру. Він замінює центральний піксель локальною медіаною вибраної інтенсивності пікселів у вікні.

Реконструкція фону виконується за допомогою медіанний фільтр розміру вікна *n*х*n*, за заданим рівнянням:

.

Розглядаючи альтернативне положення пікселя для медіани фільтр здатний захоплювати навіть тьмяні цілі з поступовим зменшення інтенсивності.

Морфологічні фільтри. Математична морфологія, яка базується на формі та передбачає підхід до обробки зображень. Mорфологічні операції, як правило, спрощують дані зображення, збереження їх основних характеристик форми та усунення невідповідності. Основні математичні операції морфологією є розширення та ерозія. Їх визначення і правила такі:

Позначено розширення *f* структурним елементом *g* і визначається за формулою:



Позначено ерозію *f* структурним елементом *g* і визначається за формулою:



Операція відкриття *f* у градаціях сірого з структуруючим елементом *g* визначають за наступною формулою:



Операція закриття *f* у градаціях сірого з структуруючим елементом *g* визначають за наступною формулою:



Процес відкриття (розмивання зображення шляхом структурування елемента з подальшим розширенням результату тим самим структурний елемент) усуває перемички (вузький край як набір пікселів), що з’єднує дві області зображення. Це закруглює назовні кути зображення під час виходу кути, спрямовані всередину, не змінені.

Процес закриття (розширення зображення шляхом структурування елемента з подальшим розмиванням результату ж структурний елемент) округлює спрямовані всередину кути на зображенні, не змінюючи зовнішні кути.

Ці властивості використовуються для згладжування зображення. Проблема з морфологічними фільтрами полягає в тому, що результат сильно залежить від розміру та форми конструкції елемент Адаптивний вибір розміру і форми структурування елемент є складним завданням.

Вибірковий морфологічний фільтр: дещо схожий на вибірковий медіанний фільтр. Ядро фільтра матиме нульові значення для альтернативних пікселів у вікні в рядку або стовпці або обидва, з посиланням на цікавий піксель.

На відміну від ранніх алгоритмів просторової попередньої обробки які передбачають просторовий безлад на кожному зображенні, а потім застосувати алгоритм виявлення, використані останні підходи кілька кадрів, щоб включити як часові, так і просторові інформації. Ці алгоритми часто є частиною алгоритмів Track-beforedetect (TbD). Придушення просторових перешкод алгоритми використовували лише просторову кореляцію. Додатковий підвищення продуктивності можна досягти шляхом уточнення їх до адаптуватися локально до мінливого безладу. Просторова попередня обробка алгоритми є простішими для розробки та обчислень менш дорогі, ніж алгоритми, які використовують temporal кореляція. Проте просторове співвідношення фону безлад, як правило, не такий сильний, як часова кореляція.

Адаптивний фільтр середнього та дисперсії. Вони представили модифіковану темпорал модель для переміщення безладу. Характеристика сцени є комбінацією статичного об’єкта, цілі та хмари краю. Для них були створені моделі. Пікселі уявляються як статичні або повільно рухомі об’єкти, наприклад внутрішню частину хмар і ясного неба мають приблизно постійну інтенсивність.

Моделюється часовий профіль пікселів, які бачать статичні об’єкти як постійний плюс деякий випадковий шум. Загалом ціль можна змоделювати часовий профіль пікселя, який бачить ціль як сигнал збурення, що генерується, коли ціль переміщується початковий піксель плюс дисперсія, пов’язана з випадковим шум процесу. Модель Маркова першого порядку було прийнята для моделювання тимчасового профілю пікселів, для видимих країв хмари.

Адаптивний фільтр середнього та дисперсії працює швидко ефективний, оскільки всі обчислення можна виконувати рекурсивно. Крім того, параметри, які використовуються в алгоритмах, можуть налаштовуватися автоматично. Алгоритм працює в двох етапи. Перший етап фільтра використовує відмінності часові варіації інтенсивності. Сигнали занепокоєння викликані цілями відхиляються набагато більше відносно фоновий шум. Однак, оскільки пікселі краю хмари можуть також отримати сигнали високого відхилення, отже, другий каскад фільтр додається для диференціації сигналів, викликаних цілями і пікселі краю хмари.

Сполучна лінія застою на основі точки. Проведений аналіз статистичних характеристик, особливо коваріація трьох класів часового профілю, а саме, статичний фон, ціль і межі хмари. Коваріація дозволяє відрізнити цілі від статичний фон і тимчасовий профіль хмарного безладу. Адаптивний коваріаційний фільтр підходить для статичного фону. Однак, якщо відхилення пікселів видно хмарні краї більше, ніж у статичного фону, деградація ефективності виявлення відбудеться, якщо коваріація краю хмари та цілі еквівалентні. Залишкова скронева профіль отримується шляхом віднімання базової лінії від скроневий профіль. Розподіл залишкової скроневої профіль може бути змодельований за допомогою розподілу Гауса випадки появи цілей мають значення інтенсивності, які значно відхиляються від розподілу залишку скроневий профіль.

## 2.2 Алгоритми детекції об’єктів на цифрових зображеннях

Однією з основних задач визначення появи шуканого об’єкту на зображенні є задача коректного виділення області яка пореційно може відповідати об’єкту інтересу. На сьогоднішній день існують декілька алгоритмів які вирішують дану задачу. Кожні з цих алгоритмів мають свої преваги та недоліки, проте враховуючи задані критерії проведення опрацювання зображення можна підібрати оптимальний варіант. Найкращі варіанти можна отримати в результаті поєднання різних типів фільтрів, при цьому використавши сильні сторони кожного з них. Проте такий варіант додатково ускладнює процес опрацювання зображення та вимагає додаткових часових затрат та апаратних ресурсів. Алгоритми які на сьогоднішній день показують найкращі результати та найчастіше використовують при розробках програмних комплексі наведені на рисуноку 2.2.

Алгоритми детекції об’єктів на цифрових зображеннях

Fast R-CNN

Region-based Convolutional Neural Networks (R-CNN)

Region-based Fully Convolutional Network (R-FCN)

Single Shot Detector (SSD)

Faster R-CNN

Histogram of Oriented Gradients (HOG)

Spatial Pyramid Pooling (SPP-net)

YOLO (You Only Look Once)

Рисунок 2.2 – Алгоритми детекції об’єктів на цифрових зображеннях

Fast R-CNN. Написаний на Python і C++ (Caffe) метод Fast Region-Based Convolutional Network або Fast R-CNN є навчальним алгоритмом для виявлення об’єктів. Цей алгоритм в основному усуває недоліки R-CNN і SPPnet, одночасно покращуючи їх швидкість і точність.

Переваги Fast R-CNN:

Вища якість виявлення (mAP), ніж R-CNN, SPPnet.

Навчання одноетапне, з використанням багатозадачної втрати.

Навчання може оновити всі рівні мережі.

Для кешування функцій дискове сховище не потрібне.

Метод згорткової мережі на основі регіону (RCNN) забезпечує чудову точність виявлення об’єктів за допомогою використання глибокої мережі ConvNet для класифікації пропозицій об’єктів. R-CNN, однак має помітні недоліки:

1. Навчання є багатоетапним конвеєром. R-CNN спочатку точно налаштовує ConvNet на пропозиції об’єктів, використовуючи втрату журналу. Потім він адаптує SVM до функцій ConvNet. Ці SVM діють як детектори об'єктів, замінюючи класифікатор softmax, отриманий за допомогою тонкого налаштування. На третьому етапі навчання, вивчаються регресори обмежувальної рамки.

2. Навчання дороге в просторі та часі. Для SVM і навчання регресора обмежувальної рамки, характеристики витягуються з кожного об’єкта, запропонованого на кожному зображенні записано на диск. З дуже глибокими мережами, такими як VGG16, цей процес займає 2,5 GPU-дня для 5k зображення набору VOC07 trainval. Для цих функцій потрібні сотні гігабайт пам’яті.

3. Виявлення об'єктів відбувається повільно. Під час тестування функції є витягнуті з кожної пропозиції об’єкта на кожному тестовому зображенні. Виявлення за допомогою VGG16 займає 47 с/зображення (на GPU). R-CNN працює повільно, оскільки виконує переадресацію ConvNet передавати для кожної пропозиції об’єкта без спільного використання обчислень.

Для прискорення R-CNN шляхом спільного використання обчислень було запропоновано мережі просторового пірамідального об’єднання (SPPnets). The Метод SPPnet обчислює карту згорткових функцій для все вхідне зображення, а потім класифікує кожну пропозицію об’єкта, використовуючи вектор ознак, витягнутий із спільної карти функцій. Функції витягуються для пропозиції шляхом максимального об’єднання частини карти функцій у пропозиції у вихідний файл фіксованого розміру (наприклад, 6 × 6). Кілька вихідних розмірів об’єднуються, а потім об’єднуються, як у просторовій піраміді. SPPnet прискорює R-CNN від 10 до 100 разів під час тестування час. Час навчання також скорочується втричі завдяки швидшому виділенню функцій пропозиції.

SPPnet також має помітні недоліки. Подібно до R-CNN, навчання є багатоетапним конвеєром, який включає вилучення функцій, тонке налаштування мережі з втратою журналів, навчання SVM, і, нарешті, підгонка регресорів обмежувальної рамки. Особливості є також записано на диск. Але на відміну від R-CNN, алгоритм тонкого налаштування не може оновити згорткові шари, які передують об’єднанню просторової піраміди. Не дивно, що це обмеження (фіксовані згорточні шари) обмежує точність дуже глибоких мереж.

Прискорений R-CNN – це алгоритм виявлення об’єктів, схожий на R-CNN. Цей алгоритм використовує мережу регіональних пропозицій (RPN), яка ділиться згортковими функціями повного зображення з мережею виявлення економічно ефективним способом, ніж R-CNN і Fast R-CNN. Мережа регіональних пропозицій це, по суті, повністю згорточна мережа, яка одночасно прогнозує межі об’єкта, а також оцінки об’єктності в кожній позиції об’єкта та проходить наскрізне навчання для створення високоякісних пропозицій регіону, які потім використовуються Fast R -CNN для виявлення об'єктів.

Гістограма орієнтованих градієнтів (HOG) – це в основному дескриптор ознак, який використовується для виявлення об’єктів під час обробки зображень та інших методів комп’ютерного зору. Техніка дескриптора гістограми орієнтованих градієнтів включає випадки орієнтації градієнта в локалізованих частинах зображення, таких як вікно виявлення, область інтересу (ROI) тощо. Однією з переваг HOG-подібних функцій є їхня простота та легше зрозуміти інформацію, яку вони несуть.

Реалізація алгоритму дескриптора HOG виглядає наступним чином:

Розділіть зображення на невеликі з’єднані області, які називаються комірками, і для кожної комірки обчисліть гістограму напрямків градієнта або орієнтації країв для пікселів у комірці.

Розділіть кожну клітинку на кутові контейнери відповідно до орієнтації градієнта.

Кожен піксель комірки вносить зважений градієнт у відповідний кутовий діапазон.

Групи суміжних комірок розглядаються як просторові області, які називаються блоками. Групування комірок у блок є основою групування та нормалізації гістограм.

Нормована група гістограм являє собою блокову гістограму. Набір цих блокових гістограм представляє дескриптор.

Метод згорткової мережі на основі регіону (RCNN) – це комбінація пропозицій щодо регіону та згорткових нейронних мереж (CNN). R-CNN допомагає локалізувати об’єкти за допомогою глибокої мережі та навчити модель високої ємності лише з невеликою кількістю анотованих даних виявлення. Він забезпечує чудову точність виявлення об’єктів завдяки використанню глибокої мережі ConvNet для класифікації пропозицій об’єктів. R-CNN має можливість масштабувати до тисяч класів об’єктів, не вдаючись до наближених методів, включаючи хешування.

Region-based Fully Convolutional Networks або R-FCN – це регіональний детектор для виявлення об’єктів. На відміну від інших регіональних детекторів, які використовують дорогу регіональну підмережу, наприклад Fast R-CNN або Faster R-CNN, цей регіональний детектор є повністю згортковим, майже всі обчислення розподіляються на все зображення.

R-FCN складається зі спільних, повністю згорткових архітектур, як у випадку FCN, яка, як відомо, дає кращі результати, ніж Faster R-CNN. У цьому алгоритмі всі вагові шари, які можна вивчати, є згортковими та призначені для класифікації ROI за категоріями об’єктів і фонами.

Поширене сімейство глибоких мереж для виявлення об’єктів можна розділити на дві підмережі: за допомогою рівня об’єднання інтересів (RoI): спільна, «повністю згорточна» підмережа незалежно від RoI, і підмережа RoI, яка не використовує спільні обчислення.

Ця декомпозиція історично була результатом новаторських класифікаційних архітектур, таких як AlexNet і VGG Nets, які за дизайном складаються з двох підмереж – згорткової підмережі, що закінчується рівнем просторового об’єднання, за яким слідують кілька повністю підключених (fc) рівнів. Таким чином (останній) рівень просторового об’єднання в мережах класифікації зображень природним чином перетворюється на об’єднання ROI рівня в мережах виявлення об’єктів.

Але останні сучасні мережі класифікації зображень, такі як Residual Nets (ResNets) і GoogLeNets за своєю конструкцією є повністю згортковими. За аналогією це здається природним для використання усіх згорткові рівні для побудови спільної згорткової підмережі в виявленні об’єктів архітектури, не залишаючи підмережі RoI без прихованого рівня. Однак, як емпірично досліджено це наївне рішення має значно нижчу точність виявлення. Щоб вирішити цю проблему, у алгоритмі ResNet шар об’єднання ROI детектора Faster R-CNN неприродним чином вставляється між двома наборами згорткових шарів, що створює більш глибоку підмережу RoI, яка покращує точність, за рахунок нижчої швидкості через неспільне обчислення RoI.

Single Shot Detector (SSD) – це метод виявлення об’єктів на зображеннях за допомогою однієї глибокої нейронної мережі. Підхід SSD дискретизує вихідний простір обмежувальних рамок у набір стандартних рамок із різними співвідношеннями сторін. Після дискретизації метод масштабується за розташуванням на карті об’єктів. Мережа Single Shot Detector об’єднує прогнози з кількох карт об’єктів з різною роздільною здатністю, щоб природно обробляти об’єкти різних розмірів.

Переваги SSD:

SSD повністю усуває генерацію пропозицій і подальші етапи перевибірки пікселів або функцій і інкапсулює всі обчислення в одній мережі.

Легко навчати та легко інтегрувати в системи, яким потрібен компонент виявлення.

SSD має конкурентну точність для методів, які використовують додатковий крок пропозиції об’єкта, і він набагато швидший, забезпечуючи уніфіковану структуру як для навчання, так і для висновків.

Підхід SSD базується на згортковій мережі прямого зв’язку, яка створює колекцію обмежувальних рамок і балів фіксованого розміру для наявності класу об’єктів екземплярів у цих вікнах, після чого виконується немаксимальний крок придушення для створення остаточного виявлення. Ранні рівні мережі базуються на стандартній архітектурі, яка використовується для високоякісної класифікації зображень (урізана перед будь-якими шарами класифікації), яку викличе базова мережу. Потім необхідно додати до мережі допоміжну структуру для виявлення з такими ключовими функціями:

Багатомасштабні карти функцій для виявлення. Додаються згорточні шари функцій наприкінці усіченої базової мережі. Ці шари поступово зменшуються в розмірах і дозволяють прогнозування виявлень у кількох масштабах. Згорткова модель для прогнозування виявлення відрізняється для кожного шару функцій.

Згорткові предиктори для виявлення. Кожен доданий функціональний рівень (або, за бажанням, існуючий функціональний рівень з базової мережі) може створити фіксований набір передбачень виявлення за допомогою набору згорткових фільтрів. Вони вказуються поверх мережі SSD. Для шару ознак розміром *m*×*n* з *p* каналами основним елементом для прогнозування параметрів потенційного виявлення є маленьке ядро 3×3×*p* яке створює або оцінку для категорії, або зсув форми відносно вікна з відповідними координатами. У кожному з *m*×*n* місць, де застосовано ядро, воно створює вихідне значення. Вихідні значення зсуву обмежувальної рамки вимірюються відносно позиції рамки за замовчуванням відносно кожного розташування карти функцій, яка використовує для цього кроку проміжний повністю зв’язаний рівень замість згорткового фільтра).

Поля за замовчуванням і співвідношення сторін пов’язують набір рамок за замовчуванням із кожна комірка карти функцій для кількох карт функцій у верхній частині мережі. За замовчуванням комірки розміщують карту функцій у згортковий спосіб, щоб положення кожної комірки по відношенню до відповідної комірки фіксується. У кожній клітинці карти функцій прогнозується зміщення відносно форм поля за замовчуванням у клітинці, а також балів для кожного класу, які вказують наявність екземпляра класу в кожному з цих вікон. Зокрема, для кожного вікна з *k* у заданому місці, обчислюється оцінки класу *c* і 4 зміщення відносно оригіналу форми вікна за замовчуванням. Це призводить до (*c*+4)*k* фільтрів, які застосовуються навколо кожного розташування на карті об’єктів, що дає (*c*+4)*kmn* вихідних даних для карти об’єктів *m*×*n*. При аналізі поля за замовчуванням схожі на блоки прив’язки, які використовуються у Faster R-CNN, однак тут застосовуються їх до кількох функцій карти різної роздільої здільної здатності. Даний лагоритм дозволяє різні форми поля за замовчуванням у кількох функціях карти, що забезпечує ефективне дискретизування простору можливих форм вікна виведення.

Об’єднання просторових пірамід (SPP-net) – це мережева структура, яка може генерувати представлення фіксованої довжини незалежно від розміру/масштабу зображення. Вважається, що об’єднання пірамід стійке до деформацій об’єктів, а SPP-net покращує всі методи класифікації зображень на основі CNN. Використовуючи SPP-net, дослідники можуть обчислювати карти функцій із усього зображення лише один раз, а потім об’єднувати функції в довільні області (підзображення) для створення представлень фіксованої довжини для навчання детекторів. Цей метод дозволяє уникнути повторного обчислення згорткових функцій.

You Only Look Once або YOLO – один із популярних алгоритмів виявлення об’єктів, який використовують дослідники по всьому світу. За словами дослідників Facebook AI Research, уніфікована архітектура YOLO є надзвичайно швидкою. Базова модель YOLO обробляє зображення в режимі реального часу зі швидкістю 45 кадрів на секунду, тоді як менша версія мережі, Fast YOLO, обробляє вражаючі 155 кадрів на секунду, при цьому досягаючи вдвічі більшого mAP, ніж інші детектори реального часу. Цей алгоритм перевершує інші методи виявлення, включно з DPM і R-CNN, під час узагальнення з природних зображень на інші області, як-от твори мистецтва.

## 2.3 Алгоритм підрахунку кількості людей у відеопотоці

Підрахунок людей, які проходять через певні зони громадської інфраструктури, наприклад, пішохідних переходів, тротуарів, площ тощо, є практично важливим завданням. Оскільки рішення цього проблема має справу з обробкою великих потоків даних, необхідно автоматизувати процес підрахунку людей. Є багато рішень цієї проблеми, одне з них - об'єкт відстеження. Завдання об'єктного стеження - створити сліди для кожної людини. Трек унікальний вказано з особою та містить його місцезнаходження на кожному кадрі, де його видно.

На етапі аналізу програмних систем моніторингу об’єктів охорони було визначено основні етапи обробки та аналізу відеопотоків. Серед основних етапів було виділено попередню обробку, підкреслення характерних ознак та ключових точок, а також формування ковзного вікна для проходження цифровим кадром з відеопотоку. Серед основних параметрів які необхідно враховувати елемент рівня освітлення, роздільна здатність камери, а також розмір ковзного вікна. Дані параметри впливають на кінцевий результат роботи системи підрахунків людей у відеопотоці. Оскільки програмний додаток аналізу відеопотоку повинен працювати в режимі реального часу, а також проводити обробку великої кількості даних то для розробленого алгоритму детекції запропоновано ряд удовконалень. Серед яких, пропонується проводити аналізу не всіх кадрів відеопотоку, а з періодичністю 1 кадр з секунди відеопотоку. Дана періодичність була обрана базуючись на тому припущенні, що швидкість пересування дорослої середньостатистичної людини не може перевищувати 10км/год, навіть з урахуванням того що людина може бігти. Тому немає необхідності аналізувати кожний кадр відеопослідовності. Проте і зменшувати кількість кадрів які переіряються теж недоцільно, оскільки аналіз послідовних кадрів дозволяє підвищити точність детекції обличь. Це пояснюється тим, що під час руху людина може випадково приховати своє обличчя: повернути або опустити голову, стати за спину, або закрити обличчя сторонні придеметом тощо. Запропонований алгоритм використовує інформацію про шаблонні значення попредньої обробки, а також враховує розміри ковзного вікна отримані експерементальним шлюхом. Блок-схема алгоритму наведена на рисунку 2.3.



Рисунок 2.3 – Блок-схема алгоритму підрахунку кількості людей у відеопотоці на основі детекції облич

Основна ідея даного алгоритму полягає в тому, що на першому етапі відбувається пошук областей які теоретично можуть відповідати людському обличчю. Даний відбір відувається шляхому пошуку овальних областей однорідного кольору в межах ковзного вікна. Розміри ковзного вікна встановлюється шляхом попереднього налаштування системи моніторингу. На наступному етапі відбувається виділення характерних ознак та порівняння з масивом еталонів. У випадку співпадіння проводиться додаткова перевірка чи дана область з деяким зміщенням не було виділена на попередньо аналізованому кадрі відеопотоку. Якщо виділена область має відповідність з деяким зміщенням або взагалі відсутня, то вважається, що це людина. Якщо область залишається нерухомою, то вона переноситься в масив спостереження, оскільки було зроблене припущення, що людина за звичайних обставин не може протягом довгого терміну зберігати статичне положення.

Розроблений алгоритм підрахунку кількості людей у відеопотоці на основі детекції облич враховує особливості параметрів зони моніторингу а також дозволяє користувачеві вносити зміни в параметри роботи алгоритму містить наступні кроки:

1. Активація програмного забезпечення та встановлення початкових параметрів роботи.
2. Отримання отримання кадру з відеопотоку.
3. Запуск процесу сканування кадру за допомогою ковзного вікна.
4. Якщо сканування завершилось, то переходимо на крок 11, інакше вибираємо наступні координати для ковзного вікна.
5. Якщо при скануванні було виділено овальну область однорідного кольору, то обчислюємо характерні ознаки даної області.
6. Перевірка отриманих характеристик з шаблонними значеннями які відповідають людському обличчу.
7. Якщо характеристики співпадають то проводиться перевірка чи на попередніх кадрах в даному місці не було виявлено область з подібними характеристиками.
8. Якщо було знайдене співпадіння то збільшуємо лічильник кількості людей на 1 та переходимо на крок 3.
9. Якщо співпадіння не знайдено, то додавляємо дану область в масив з виділеними на попередньому кроці людьми та збільшуємо лічильник кількості людей на 1. Перехід на крок 3.
10. Проводимо перевірку масиву областей з виділеними людьми та звіряємо їх координати з активним кадром відеопотоку. Якщо на області не виявлено людину, то дана область видаляється з подальшого аналізу, вважаємо, людина залишила область моніторингу.
11. Вивід результатів підрахунку людей та завершення процесу аналізу кадру відеопотоку.

Процес моніторингу на основі покадрового аналізу відеопотоку має ряд переваг на відміну від аналізу окремо взятого зображення. Під час роботи з відеопотоком можна зменшити кількість хибно виявлених людей або взагалі не детектованих. Це стає можливо за рахунок того, що проводиться додатковий аналіз отриманих даних, що з однієї сторони збільшує час на опрацювання зображення, проте підвищеє точність отриманих результатів моніторингую

До основних переваг розробленого алгоритму відносяться:

висока швидкодія за рахунок вибіркового аналізу кадрів відеопотоку;

можливість роботи на комп’ютерах з низькими апаратними характеристиками;

проста програмна реалізація реалізації;

підвищена точність за рахунок подвійної перевірки отриманих даних;

можливість додаткового налаштування параметрів ковзного вікна в залежності від поставлених задач;

можливість налаштування роботи з будь яким апаратним забезпеченням.

Недоліки:

додаткові часові затрати через проведення повторної превірки;

залежність від якості отриманої картинки;

необхідність отримання шаблону з описом людського обличчя для процесу ідентифікації відповідних областей;

можливі похибки при умові, що людина в області моніторингу приховала своє обличчя (використала додатковий одяг, маску, великі окуляри тощо) або відвернула свою голову від обєктиву камери.

В результаті моделювання роботи запропонованого алгоритму він показав хороші результати по швидкості роботи та точності при аналізі відеопотоків. Молелювання проводилось для різних розмірів ковзного вікна, при цьому було визначено, що великі розміри негативно впливають на кінцевий результат, оскільки в область ковзного вікна може потрапити більше ніж одна людина. В тай самий час, якщо розмір ковзного вікна буде занадто маленьки, то область потенційного обличчя людини може в неї не потрапляти, що вносить похибку в отриманий результат. Оптимально встановити розмір ковзного вікна на етапі встановлення та монтужу програмно-апаратного комплексу моніторингу охоронноої зони.

## 2.4 Висновки до розділу

Проведно аналітичний огляд алгоритмів аналізу та обробки цифрових зображень на основі використання фільтрів, що дозволило обрати групу алгоритмів для проведення попередньої обробки кадру відеопотоку для проектування алгоритму підрахунку кількості людей у відеопотоці на основі детекції облич.

Розроблено алгоритм підрахунку кількості людей у відеопотоці на основі детекції облич, що дозволило реалізувати програмний додаток для системи моніторингу та підрахунку кількості людей в реальному часі.

# 3 Програмний додаток детекції та підрахунку кількості людей у відеопотоці

## 3.1 Структура програмного додатку моніторингу охоронної області

Окрім алгоритмів обробки відео, які зазвичай використовуються для спостереження за громадськими місцями, важливим доповненням є аудіоаналіз. Тим не менш, коли з'являється велика група людей, визначити їх кількість за допомогою більшості методів обробки зображень, які зазвичай використовують виявлення та відстеження об'єктів, стає дуже важко. Підходи на основі виділення фону, не можуть належним чином розділити об’єкти, коли люди ходять на дуже малій відстані або коли їхні руки з’єднані. Інші методи використовують кілька камер для вирішення проблеми сегментації або застосовують моделі людських фігур, отримані під час спостереження за переднім планом зображення. Крім того, встановлювати численні камери в розглянутій будівлі було б недоцільно.

Інші рішення, які використовують зображення камери разом із лазерними променями для відстеження ніг, вимагають розміщення датчиків на землі.

Існує фундаментальна різниця між виявленням об’єктів і відстеженням об’єктів. Коли застосовуємо виявлення об’єктів, то це означає що визначиться, де на зображенні/кадрі знаходиться об’єкт. Детектор об’єктів також зазвичай є дорожчим з точки зору обчислень і, отже, повільнішим, ніж алгоритм відстеження об’єктів. З іншого боку, засіб відстеження об’єктів прийматиме вхідні (*x*, *y*) координати розташування об’єкта на зображенні та:

Призначатиме унікальний ідентифікатор цьому конкретному об’єкту;

Відстежуватиме об’єкт під час його руху навколо відеопотоку, прогнозуючи нове розташування об’єкта в наступному кадрі на основі різних атрибутів кадру (градієнт, оптичний потік тощо).

Високоточні засоби відстеження об’єктів об’єднають концепцію виявлення об’єктів і відстеження об’єктів в єдиний алгоритм, який зазвичай розділений на два етапи:

Фаза 1 – виявлення: під час фази виявлення активується обчислювально‑дорожчий трекер об’єктів, щоб виявити, чи не потрапили нові об’єкти в поле зору, і перевірити, чи зможемо знайти об’єкти, які були «втрачені» під час фази відстеження. Для кожного виявленого об’єкта створюється або оновлюємо трекер об’єктів із новими координатами обмежувальної рамки. Оскільки наш детектор об’єктів є складним для обчислення алгоритмом то він запускається лише раз на кожні *N* кадрів (1 кадр за секунду).

Фаза 2 – відстеження: для кожного з виявлених об’єктів створюється трекер об’єктів, щоб відстежувати рух об’єкта в кадрі. Tрекер об’єктів має бути швидшим і ефективнішим, ніж детектор об’єктів.

Перевага цього гібридного підходу полягає в тому, що можна застосовувати високоточні методи виявлення об’єктів без великого обчислювального навантаження. Таке архітектурне рішення буде покладено в основу програмного додатку моніторингу. На основі виділених етапів роботи алгоритму підрахунку кількості людей на основі детекції облич бул о спроектовано архітектурну структуру програмного додатку. Найпопулярніша та поширена 3-рівнева архітектура програмного забезпечення була створена з потреби стиснути та прояснити графіки залежностей між класами та компонентами. Якби залишили лише один шар для всієї програми, ці графіки були б некерованими та заплутаними. Було б неможливо визначити якісь правила щодо важливості одного компонента над іншими. Також було б неможливо визначити 3 різні класифікатори відповідальності, які явно виражені 3 рівнями. Коли пов’язуємо клас із рівнем, то явно вказуємо на його роль у виконанні однієї з конкретних обов’язків.

Подібно до ситуації з попереднім рівнем, у багатьох сучасних проектах програмного забезпечення рівні самі стали дуже великими, оскільки містять багато класів, які залежать один від одного. Іноді цей графік залежностей настільки складний, що природним чином вимагає розбиття шарів на більш детальні підрівні. Багато відважних розробників пішли далеко, творчо підійшовши до цього питання, і представили багато нових рівнів у своїх програмах. Спрощену структуру програмного додатку наведено на рисунку 3.1.

Керуючий модуль програмного додатку

Модуль завантаження стартових параметрів

Модуль корекції параметрів роботи програми

Модуль попередньої обробки кадра

Модуль аналізу кадра

Модуль роботи з масивом міток

Модуль завантаження відеопотоку

Модуль візуалізації результатів даних

Рисунок 3.1 – Узагальнена структура програмного додатку для підрахунку кількості людей на кадрі відеопотоку

Використання модульної архітектури значно спрощує процес програмної реалізації спроектованого програмного рішення. Реалізація та відлагодження окремого модуля займає менше часу та може бути розділена в часі. В той самий час інші модулі будуть отримувати деякий тестовий набір даних, у форматі який буде повертати розроблювальний модуль. Таким чином низька швидкодія або не проведена оптимізація програмного коду не буде впливати на роботу цілого проекту. Це в свою чергу дозволить сконцентрувати увагу не на проблемах окремо взятого модуля, а розглядати проект як єдине ціле. Серед головних структурних частин слід відмітити такі:

Керуючий модуль програмного додатку призначений для організації процесу обміну інформацією між різними програмними структурами додатку. Даний модуль містить класи та методи для проведення перетворення інформації у формат який передбачений для роботи програмного модуля. Окрім того даний модуль містить технічні засоби для відєднання окремих модулів від роботи програми та підміни результатів їхньої роботи тестовими вибірками. Даний механізм було використано не етапі проектування та реалізації програмного додатку з метою проведення тестування окремо взятих модулів та перевірки якості їх роботи. Окрім того в даний модуль внесені функції перевірки наявності та справності окремих програмних модулів з метою попередження користувача про моливі помилки під час роботи програмного додатку. Вхідними даними даного модуля є вектор параметрів роботи програми. Вихідними – активні параметри роботи активного модуля, а також запити до користувача у випадку винекнення помилкової ситуації або відсутності/ не справності окремо взятого модуля або зовнішнього анаратного засобу.

Модуль завантаження стартових параметрів в якому реалізовані механізми завантаження стартових параметрів роботи програмного додатку з файлу. Окрім того у випадку відсутності або пошкодження файлу з параметрами роботи програмного додатку про це буде виведене повідомлення та запропоновано користувачеві задати їх по новій. Якщо користувач має невеликий досвід роботи з даним модулем передбачено можливість встановлення параметрів по замовчуванню. Параметри по замовчуванню не є оптимальним для вирішення окремо взятої задачі, а для отримання більш точних результатів доцільно провести їх корегування. Параметри роботи програмного додатку можна розділити на дві окремих групи:

парметри інтерфейсу;

параметри обробки цифрового зображення.

До групи параметрів інтерфейсу можна віднести:

розмір, тип шрифтів програмного додатку;

кольорова палітра графічного інтрефейсу;

формат та пункти звіту про проведену роботу;

формат та пункти текстового лог-файлу про стан роботи програми;

включення/виключення режиму тестування.

До групи параметрів обробки цифрового зображення:

розмір ковзного вікна;

шлях до файду з шаблонами облич;

параметри ядер фільтрації;

частота отримання кадрів з відеопотоку.

Вхідними даними даного модуля є вектор параметрів роботи програми. Вихідними – актуальні параметри роботи програмного додатку.

Модуль корекції параметрів роботи програми. Даний модуль є одним з додаткових та не обовязковим при роботі з програмним додатком. Проте результат його роботи може напряму вплинути на отримувані результати як позитивно підвищуючи точність отриманих результатів так і негативно вносячи в роботу програми додаткові похибки. Тому для роботи з даним модулем необхідно мати досвід роботи з програмами даного типу або вносити тільки перевірені значення.

Модуль корекції параметрів роботи програми

Функції встановлення розмірів ковзного вікна в ручному режимі

Функції встановлення розмірів ковзного вікна в автоматизованому режимі

Функції встановлення частоти отримання зображень

Функції користувацького інтерфейсу

Функції контролю отриманих даних

Корекція параметрів фільтрів

Корекція параметрів шаблонів

Рисунок 3.2 – Узагальнена структура модуля корекції параметрів роботи програми

Модуль дозволяє користувачеві безпосередньо змінювати налаштування роботи програмного додатку. Вхідними даним є набір параметрів заданих користувачем відповідно до підказок системи. Вихідними – відкореговані параметри роботи програмного додатку в залежності від особливостей області моніторингу, інтенсивності людського потоку та апаратних засобів на яких було активовано програмний додаток.

Модуль попередьої обробки кадра. В даному модулі згруповані функції обробки відеопотоку з метою отримання окремого кадра у форматі незакодованого цифрового зображення. Для цього на основі значення парметра частоти отримання кодрів з відеопотоку вирізаєтсья необхідний кадр. Після чого отримане зображення передається на вхід функцій попередньої обробки. Дані функції за допомогою статистичних фільтрів проводять процедуру видалення шумів та малоінформативних елементів зображення. Це дозволяє підвищити швидкодію програмного додатку та зменшити кіількість хибно виділених областей з потенційними людьми. Незважаючи що даний модуль збільшує час обробки зображення в цілому, проте за рахунок швидкості опрацювання зображення за допомогою фільтрів, ці часові затрати в значній мірі компенсуються за рахунок зменшеня часу роботи модуля детекції людей. На вхід даного модуля передається відеопотік або відеофайл з записом процесу моніторингу досліджувальної області. Вихідна інформація – кадр з відеопотоку з виконаною попередньою обробкою на основі фільтрації.

Модуль аналізу кадра – один з основних модулів програмної розробки. В даному моділі згруповані функції для обробки та детекції областей які потенційно містять обличчя людей. Проводячи пошук однорідних областей функції даного модуля послідовно перевіряють усі прямокутні області на наявність в них однорідних овальних плям. Після чого проводиться визначення їх зарактеристичних ознак, а саме визначення параметру колоподібності. Якщо даний параметр буде вищий за заданий поріг *T*, то така область стає претендентом на присутність в ній людини. Результати роботи даного модуля є масив можливих однорідних областей на яких було виділено/детектовано людей.

Модуль роботи з масивом міток – в даному модулі проводиться додаткова обробка отриманої після аналізу зображення інформації. А саме виходячи з того, що люди перебувають в постійному русі і малоймовірно зберігають статичне положення протягом тривалого періоду часу, тому можна зробити припущення, що на двох послідовних кадрах області на яких детектуються люди повинні відрізнятись на деяке зміщення. Якщо протягом трьох і більше секунд область перебуває в тих самих координатах, то можна зробити наступні висновки: відбулась хибна детекція людини або людина зупинилась і стоїть нерухомо. В першому випадку дана область видаляється з подальшого аналізу. В другому теж відбувається видалення детектованої області, при цьому дана процедура відувається на основі припущення, що якщо людина продовжить рух, то детектор знову її зафіксує і кількість людей на сцені буде коректно підраховано. Проте ймовірність другого варіанту є невеликою, оскільки людям не властиво при нормальних умовах пребувати нерухомо протягом довгого періоду часу.

Модуль візуалізації результатів – додатковий модуль програмної системи. Призначений для створення та відображення результатів роботи програмного додатку. Даний модуль може виводити інформацію про кількість людей на сцені, або створювати повноцінні звіти про динаміку зміни кількості людей протягом часу моніторингу. Налаштування типу звіту та його формат відбувається завдяки зручному меню.

Розроблена та спроектована структура на основі ієрархічного підходу з використанням окремих модулів на кожному рівні обраний підхід є гнучким та універсальним та дозволяє зберегти можливість коректної роботи навіть при внесених некоректних даних або помилки при роботі обного з модулів. В такому випадку користувачеві виводиться про це інформація у вигляді текстового повідомлення. Окрім того використаний модульний підхід дозволяє вносити корективи в роботу програмного додатку додаючи різні нові модулі чи модіфікуючи вже присутні, при цьому робота системи та цілісність не порушується.

Наступним етапом створення програмного додатку є процес реалізації запропонованих алгоритмів,проте перед цим доцільно провести процес моделювання можливості коректної взаємодії між різними модулями програмного додатку та функціональними модивостями запропонованих алгоритмів виконувати поставлені перед системою завдання. Моделюваня проводилось за допомогою механізмів універсальної мови моделювання (UML), а семе ввикористовувалисьь діаграми прециденів та діаграма послідовності Серед недоліків застосування універсальної мови моделювання слід відмітити:

часові затрати. Для проведення грунтовного моделювання необхідно затратити час для того, щоб діаграма була синхронізована з фактичним кодом та розумною. Діаграми UML не запускаються, але вимагають багато часу. Тому вони корисні тільки в тому випадку, якщо розробник може ними керувати.

можливі втрати інформації. Моделювання достатньо складний процес який дозволяє врахувати основні концептуальні особливості майбутнього програмного продукту. Тому ряд маловагомих деталей ігноруються. Це з однієї сторони може мати незначний вплив на кінцевий результат, проте з іншої дозволить повністю оцінити майбутню розробку.

затрати фінансових ресурсів системи. Для проведення якісного модулювання необхідне відповідне програмне забезпечення, а отже потрібні кошти на його закупівлю та підтримку у робочому стані.

Для оцінки степеня взаємодії між окремими програмними модулями використано моделювання на основі діаграми предецентів. Це важливий етап моделювання, оскільки тут проводиться дослідження не стільки окремих модулів скільки цілісність усього проекту, перевірка рівня організації предачі інформації між окремими модулями та гнучкість спроектованих структур длязберіганя, передачі та обробки інформації. Додатково розглядається функціональні можливості які отримає користувач при роботі з системою. Приклад діаграми прецеденів наведено на рисунку 3.3.



Рисунок 3.3 – Діаграма прецедентів програмної системи

Під час аналізув результатів моделювання були зроблені ряд висновків по запропонованій архітектурі та внесенні деякі правки в саму структуру програмного додатку. Аналіз діаграми прецедентів показав, що користувачі матимуть повний доступ до функціоналу запропонованого програмного додатку. За допомогою наданих програмних засобів користувачі, навіть з незначним досвідом роботи з програмними комплексами даного типу, зможуть виконати усі поставлені завдання. Програмні функції згруповані відносно завдань які вони повинні вирішувати і користувач має до них доступ через систему меню. Дане моделювання показало правильність обраної структури та набору реалізованих функцій. Крім того слід зазначити, що закладені механізми автоматизованої роботи програмних додатків дозволяють використовувати дане програмне забезпечення і користувачам з мінімальним досвідом роботи, оскільки в процесі свого функціонування усю необхідну інформацію програма буде отримувати автоматично. Процес опанування програмою є достатньо короткий та не ввимагає від нових кристувачів грибоких попередніх знань комп’ютерної техніки.

Наступний крок моделювання – це перевірка взаємодії окремих моділів між собою та перевірка на уникнення можливих конфліктів при передаванні інформації з одного модуля до іншого. Для данго дослідження було використано діаграму прецедентів на якій відображається взаємодія процесів та об’єктів яка відбувається під час роботи програми. Результат моделювання наведено на рисуноку 3.4.



Рисунок 3.4 – Діаграма послідовності програмної системи

Навдена діаграма у повній мірі дозволяє проілюстурвати можливості запропонованої архітектури програмного додатку. Діаграма візуально демонструє послідовність запуку програмних процесів в середині програмного додатку та доводить, що під час роботи програмні модулі не будуть між собою конфліктувати за право використання ресуртів чи за доступ до аналізованої інформації. Лінійна послідовність активації відповідних функцій у деякій мірі сповільнює роботу програмного додатку, проте за рахуок того, що будуть аналізуватись не всі кадри відеопотоку, а тільки 1 кадр за секунду дана ситуація не є критичною. А враховуючи, що програмний додаток повністю виконує поставлені задачі за відведені часові межі, то даний фактор можна вважати не суттєвим.

Окрім того було розглянуто набір класів які пропонується реалізувати в розробленому програмному додатку. Запропонована ієрархія класів в повній мірі описує всі ті основні об’єкти які будуть задіяні в процесі робти програми. Діаграма класів наведена на рисунку 3.5.



Рисунок 3.5 – Діаграма класів програмної системи

Запропонована ієрархія доволяє оцінити повноту охоплюваної інформації та показати, що виділені об’єкти мають мінімально потрібну кількість параметрів для їх досконалого опису та набір методів які дозволяють створити потрібний інтерфейс між окремими модулями та виконати усі поставлені завдання. Система модифікаторів доступу до окремих атрибутів та методів створює додатковий бар’єр для коректного функціонування програмного засобу. Це досягається через те, що в класах закладдено систему сеттерів яка містить в собі додаткову перевірку на правильність введеної інформації.

Етап модулювання дозволив оцінити основні елементи функціонування майбутнього програмного забезпечення, а також внести корективи в місця де могли виникати потенційні помилкові ситуації. Успішне завершення цієї ступені розробки програмного забезпеченя дозволило розпочати виконання наступної, а саме проектування графічного інтерфейсу користувача для програмної розробки.

При проектуванні графічного інтерфейсу користувача (GUI) було прийнято до уваги те що даний програмний додаток моніторингу зони спостереження буде виконувати невеликий обсяг завдань, а людський вплив в його роботу повинен бути мінімальним. Тому при дизайні інтерфейсу було обрано мінімалістичний стиль, який декларує мінімальну кількість активних елементів на головному вікні програмної розробки. Запропонований дизай графічного вікна програми моніторингу наведено на рисунку 3.6.



Рисунок 3.6 – Графічний інтерфейс користувача

Графічний інтерфейс користувач було реалізовано з врахуванням сучасних тенденцій створення програмних додатків, а саме німінальна кількість активних керуючих елементів на головному вікні програми. Більшість управлінського функціоналу та додаткових налаштувань було пренесено в головне меню програми для того що максимально звільнити візуальний простір головного вікна. Це дозволило значно спростити етап навчання роботи з програмним додатком людей з невеликим досвідом роботи з системами даного типу або з мінімальними навиками роботи з комп’ютерною технікою. Окрім того приховування від користувачів прямого доступу до напармерів налаштування роботи програми дозволяє зменшити кількість помилок в результаті некоректно введеної інформації.

Для роботи з програмою користувачеві необхідно виконати просту послідовність кроків. Даний набір чітко ілюструється підказками під час запуску програмного додатку, а також може бути проілюстрований в процесі роботи програми у вигляді підказок які з’являються. Послідовність необхідних дій відображено на рисунку 3.7:

Активація системи

Встановлення параметрів роботи

Отримання кадру з відеопослідовності

Попередня обробка

Аналіз отриманого кадру

Оцінка отриманого резульату

Рисунок 3.7 – Послідовність дій користувача при роботі з системою моніторингу зони спостереження

Як показано зі схеми дій користувача, при роботі користувач повинен виконати три основі дії з програмною системою:

активація та корекція парамемтрів роботи;

запит на отримання послідовості кадрів з відеопотоку;

моніторинг процесу обробки цифрового зображення;

оцінка запропонованого варіанту автозаповнення.

Окрім того користувач може виконати ще дві додаткові дії, які необхідні у більшій мірі для підвищення рівня коректності роботи програми. Як видно з переліку завдань які повинен здійснювати користувач можна зробити висновок, що в основному програма моніторингу буде прауювати в автономному режимі з мінімальним впливом оператора. Це дозволить використовувати програмну систему протягом тривалого періоду часу та отримувати розгорнуту статистичну інформацію у зручний для користувача час та формі.

## 3.2 Програмні модулі системи підрахунку людей у відеопотоці

Щоб програмно реалізувати лічильник людей, будемо використовувати як OpenCV, так і dlib. Було використано OpenCV для стандартних функцій комп’ютерного зору/обробки зображень разом із детектором об’єктів глибокого навчання для підрахунку людей.

Потім використано dlib для реалізації кореляційних фільтрів. Тут також можна використовувати OpenCV, однак реалізацію відстеження об’єктів dlib є більш адаптивною та має більше параметрів налаштування, тому вибір було зроблено саме на користь цієї бібліотеки для цього проекту.

Щоб досягти всіх цих цілей, необхідно визначити примірник класу TrackableObject:

клас TrackableObject:

def \_\_init\_\_(self, objectID, centrroid):

self.objectID = objectID

self.centroids = [centroid]

self.counted = False

Для використання максимально можливих функцій, що пропонуються в пакеті OpenCV та мовою python підключимо бібліотеки та створимо усі необхідні структури для зберігання та подільшої обробки отриманої інформації.

from pyimagesearch.centroidtracker import CentroidTracker

from pyimagesearch.trackableobject import TrackableObject

from imutils.video import VideoStream

from imutils.video import FPS

import numpy as np

import argparse

import imutils

import time

import dlib

import cv2

Для більшого розумінні проаналізуємо які саме функціональні можливості буде використовувати розроблюваний програмний засіб. З модуля pyimagesearch, імпортуємо на класи CentroidTracker і TrackableObject. Також запозичимо класи VideoStream і FPS модуля imutils.video, що дозволить в подальшому взаємодіяти з веб-камерою для отримання відеопотоку та розрахувати приблизну пропускну здатність кадрів в секунду (FPS). Даний набір є скоріш кориснішим на етапі тестування , проте при відсутності професійної камери в програмній системі можна використовувати і звичайні веб-камери. Також потрібно підключити imutils для виокристання зручних функцій OpenCV. Можливості бібліотеки dlib будуть використані при реалізації кореляційного трекера. OpenCV буде використовуватися для відкриття відеофайлів, запису відеофайлів і відображення вихідних кадрів на нашому екрані.

Для старту роботи програмної системи необзідно встановити початкові значення для її роботи, це родиться за допомогою наступного програмного коду:

writer = None

W = None

H = None

trackableObjects = {}

totalFrames = 0

totalDown = 0

totalUp = 0

fps = FPS().start()

Інші ініціалізації включають:

Writer - автор відео, створимо екземпляр цього об’єкта пізніше, якщо будемо писати у відео;

W і H – розміри ковзного вікна;

trackableObjects – словник, який відображає стан objectID до TrackableObject;

totalFrames – загальна кількість оброблених кадрів;

totalDown і totalUp – загальна кількість об’єктів/людей, які перемістилися вниз або вгору. Ці змінні вимірюють фактичні результати «підрахунку людей» сценарію.

Fps – інструмент оцінки кадрів за секунду для порівняльного аналізу.

Процес детекції та підрахунку займає декілька етапів.

status = "Waiting"

rects = []

if totalFrames % args["skip\_frames"] == 0:

status = "Detecting"

trackers = []

blob = cv2.dnn.blobFromImage(frame, 0.007843, (W, H), 127.5)

net.setInput(blob)

detections = net.forward()

Ініціалізуємо статус як «Waiting». Серед можливих варіанті значення статуту є наступні:

Очікування: у цьому стані оператор очікує, що люди будуть виявлені та відстежені.

Виявлення: програма в активному режимі проводить пошук людей.

Відстеження: люди відстежуються в кадрі та проводиться їх підрахунок та заноситься у список виявлених осіб.

Щоб уникнути запуску нашого детектора об’єктів у кожному кадрі та пришвидшити конвеєр відстеження, будемо пропускати кожні *N* кадрів (встановлюється аргументом командного рядка, по замовчуванні 1 кадр за секунду). Лише кожні N кадрів програма буде отримувати один кадр для проведення аналізу. Інакше можливе візуальне спостереженням за зоною інтересу.

До переваг використання бібліотеки OpenCV слід віднести велику кількість реалізованих програмних функцій, що значно спрощують процес написання програмного коду, оскільки їх можна виокристати для вирішеня простих повторюваних завдань які носять допоміжний характер. При цьому не втрачаєтсья цілісність програми та значно економиться час.

## 3.3 Тестування та аналіз реалізованого програмного додатку

Для проведеня тестових випробувань запропонованого програмного додатку було обрано апаратне забезпечення виходячи з наступних особливостей проведення тестування:

програмний додаток повинен працювати на апаратному забезпеченні середнього і вище цінового сектору;

програма не повинна використовувати додаткові зовнішні модулі або апаратні засоби, окрім тих які враховувались під час проектування програмного додатку;

Пробота програми повинна проходити в режимі реального часу, допускаються мінімальні затримки під час аналізу відеопотоку;

програма повинна працювати як з веб-камерами так і з відеофайлами, при цьому якість отриманих результатів не повинен залежать від рівня освітлення зони моніторингу.

В результаті для проведення тестування було підібрано апаратний комплекс для проведення тестування розробленої програмної системи. Технічні характеристики відповідають рівню «офісного» комп'ютера. Тобто середній ціновий діапазон, завдання які можуть бути вирішені підпадають під категорію середньої сткланості та не вимагають великих ресурсних затрат. Може використовуватися як робоче місце програміста, тестера, менеджера проекту тощо. Вимоги дощо технічних параметрів джерела отримання інформації не враховувались оскільки програма повинна працювати як з відеопотоками так і з наперез збереженими відеофайлами. Для отримання відеопотоку в режимі реального часу використовувалась звичайна веб-камера. Робоча станція має наступні технічні характеристики які представлені на рисуноку 3.8.



Рисунок 3.8 – Технічні характеристики робочої станції для тестування програмного додатку моніторингу людинопотоку

Технічні характеристики пристрою відображення зображень (DELL P2018H 19.45″ ):

матриця: TN;

роздільна здатність: 1600×900 (16:9);

частота поновлення кадрів: 75 Гц;

яскравість: 250 кд/м²;

підсвічування: WLED;

входи: HDMI 1.4, DisplayPort 1.2, VGA (D-Sub);

розміри: 570 \* 446 \* 226 мм.

Технічні параметри обраної робочої станції є достатніми для проведення запланованих тестових випробувань та для отримання достовірної інформації про функціональні моливості розробленого програмного забезпечення.

Для проведення тестування необхідно сформувати тестові групи файлів, що повинні відрізнятись один від одного та дозволити провести оцінку розробленого програмного додатку на різних рівня складності опрацювання. Для цього було виділено три групи файлів які мають різні характеристики, серед яких наявність/відсутність шумів, високий/низький рівень освітлення, кількість людей та рівень відкритості їх облич тощо. Терелік груп та параметри наведені нижче:

прості відео – в дану групу тестових відеофайлів було віднесено фали які були зроблені при хорошому освітленні, камера заходилась на рівні висоти людини, лиця приховані у мінімальної кількості людей, кількість людей на оному кадрі невелика, усі рухаються приблизно в одоному рівномірному темпі.;

відео середньої групи –на відео людські обличчя можуть відображатись не зовсім чітко, освітлення не яскраве, люди можуть як йти так і бігти, присутні елементи одягу які закривають обличчя;

складні для аналізу зображення – відео були зроблені при недостатньому або неправильно налаштованому освітлені, люди можуть рухатись в довільному темпі, групами, лицем або спиною до камери, прсутні елементи одягу, що закривають обличчя та інші фактори що ускладнюють роботу програми моніторингу.

Після проведених тестових запусків програми було додатково проведено аналіз відних відеофайлів в ручному режимі з метою перевірки точності отриманих результатів, зокрема перевікри відмотку правильно підразоваих людей з експертним підрахунком.

При моніторингу відеофайлів першої групи програмна система швидко та з мінімальними похибками знаходила на зибраженнях обличчя людей та проводила коректний підрахунок людей у потоці. Невеликі похибки були викликані поворотам голови, що спотворювало форму обличчя або воно взвгві пропадало з поля зору камери, проте коли людина знову повертала голову в правильне полодження система коректно опрацьовувала дани сутуацію та викравляла загальну кількість виділиних людей. Точність підрахунку в порівнянні з експертною оцінкою знаходилаьсна рівні 98%.

При поведенні тестування файлів другої групи результати моніторингу були гірші ніж в порівнянні з першою групою файлів. Це легко можна пояснити тим, що на зображеннях зявлялось більше стороніх шумів, а люди не завжди були повернуті обличчям до камери. Окремо слід зазначити, що наявність елементів одягу, таких як сонцезахисні окуляри, шарф ,піднятий комір, капішон або медична маска значно впливає на точність отриманих результатів. Проте за рахунок кворівневої перевірки розроблений програмний додаток у частині випадків коректно детектував люличчя та рахував людей. Точність підрахунків в даній групі файлів була на рівні 91-94%

Остання група файлів в яку були додані усі відеофайли якість картинки на яких відрізнялась великою кількістю шумових спотворень, поганою якістю освітлення неконтрольованим напрямком руху людей та іншими факторами що значно ускладнюють процес підрахунку людей. Аналіз дани файлів показав, що розроблена програмна система здійснює значну кількість пропусків людей. В більшості випадків такі люди йшли спитою до камери і відповідно система не можга їх корекно детектувати, що в подальшому призводило до похибок під час порівняння отриманого результату, та даних отриманих під час ручного підрахунку кількості пішоходів. Даний результат був очікуваний та для піднесення рівня точної детекції пропонується встановлювати декілька камер спостереження з подальшим усередненням отриманих результатів роботи.

Отримані результати підтвердили припущення, які були зроблені на етапі моделювання, що розроблений програмний код підрахунку кількості людей у відеопотоці має високу швидкодію, та проводить аналіз введеного кадру з відеопотоку або відеофайлу, при цьому частково залежний від якості вхідного відеопотоку. Зовнішні природні чинники також мають вплив на отримані підсумкові результати. Проте у випадку «ідеальних» умов, або зменшення кількості шумів за рахунок правильного підбору апаратних засобів програмний додаток показує відмінні результати.

В результаті проведених експерементів та на основі аналізу отриманих даних була сформована підсумкова таблиця де відображаються отримані результати у згрупованому вигляді. Результати оцінювались якісно та носять невеликий субєктивний характер, проте в загальному можна вважали їх достатньо достовірними. Результати наведено в таблиці 3.1

Таблиця 3.1 – Узагальнена таблиця результатів тестування

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Групи відеофайлів/зовнішній фактор | Освітлення | Наявність одягу на обличчі | Рівень розташування камери | Напрям руху | Швидкість руху |
| Прості відео | Невеликий вплив | Невеликий вплив | Вплив відчутний | Великий вплив | Вплив відсутній |
| Відео середньої групи | Невеликий вплив | Вплив відчутний | Вплив відчутний | Великий вплив | Вплив відсутній |
| Складні для аналізу зображення | Великий вплив | Великий вплив | Великий вплив | Великий вплив | Вплив відсутній |

Як видно з наведеної таблиці основні фактори які впливають на результати роботи програмного додатку це напрям руху (обличчям до камери/ від камери) та наявність одягу який приховує частину обличчя. Інші фактори мають частковий вплив та можуть нівілювати свій впли за рахунок попередньої обробки зображення.

## 3.4 Висновки до розділу

Розроблено та проведено теоретичне моделювання програмного додатку підрахунку кількості людей у відеопотоці, що надало можливість програмно реалізувати програмних додаток моніторингу та аналізу зони спостереження.

Здійснено тестування розробленого додатоку написання підрахунку кількості людей у відеопотоці на основі детекції облич людей, що підтвердило правильність у виборі механізму реалізації програми та розробленого алгоритму.

# Висновки

На основі аналізу сучасних програмних охоронних систем з елементами підрахунку людей та алгоритмів детекції людських облич у відеопотоках можна зробити такі висновки:

1. Проведено аналіз та класифікацію охоронних систем на основі виконуваних завдань та сфер використання, що дозволило виділити основні програмні модулі та функціональні особливості систем даного типу.
2. Проаналізовано та проведено дослідження основних протоколів потокової передачі інформації через глобальну мережу інтернет, що дозволило виділити протокол передачі даних для системи моніторингу та підрахунку людей в відеопотоці.
3. Проведено аналіз програмних охоронних систем з елементами моніторингу, що дозволило виділити основні програмні функції та структури, а також архітектурні рішення, що дозволило в подальшому спроектувати архітектуру програнмого додатку підрахунку кількості людей у відеопотоці.
4. Проведно аналітичний огляд алгоритмів аналізу та обробки цифрових зображень на основі використання фільтрів, що дозволило обрати групу алгоритмів для проведення попередньої обробки кадру відеопотоку для проектування алгоритму підрахунку кількості людей у відеопотоці на основі детекції облич.
5. Розроблено алгоритм підрахунку кількості людей у відеопотоці на основі детекції облич, що дозволило реалізувати програмний додаток для системи моніторингу та підрахунку кількості людей в реальному часі.
6. Здійснено тестування розробленого додатоку написання підрахунку кількості людей у відеопотоці на основі детекції облич людей, що підтвердило правильність у виборі механізму реалізації програми та розробленого алгоритму.

# Список використаної літератури

1. Смагула Т.І., Жаборинська І.В. Аналіз алгоритмів попередньої обробки зображень систем автоматизованого моніторингу. Збірник тез VІ Науково-практична конференція молодих вчених і студентів «Інтелектуальні комп’ютерні системи та мережі»., Тернопіль, 10 люстопада 2022 р. с. 28.
2. Смагула Т.І., Жаборинська І.В. Алгоритм детекції людських облич в системі відеоспостереження. Збірник тез VІ Науково-практична конференція молодих вчених і студентів «Інтелектуальні комп’ютерні системи та мережі»., Тернопіль, 10 люстопада 2022 р. с. 28.
3. Bradski G. Learning OpenCV - Computer Vision with the OpenCV Library, 2018. 580 с.
4. Гонсалес Р., Вудс Р., Эддинс С. Цифровая обработка изображений в среде MATLAB, М.: Техносфера, 2016. 616 с.
5. Сафонов В. О. Параметризованные типы данных. История, теория, реализация и применение. М.: Издательство Санкт-Петербургского университета, 2019. 116 c.
6. Секунов Н.Ю. Самоучитель Visual C++ 6.0. М.: СПб: BHV, 2018. 960 c.
7. Страуструп Б. Язык программирования C++. М.: Радио и связь,2019. 350 c.
8. Страуструп Бьерн Дизайн и эволюция С++ М.: ДМК Пресс, 2016. 446c.
9. Сойфер В.А. Методы компьютерной обработки програмних кодов М.: Физматлит, 2020. 784 с.
10. Оппенгейм А. Цифровая обработка сигналов. М.: Техносфера,2016. 856с.
11. Прэтт У. Цифровая обработка изображений. В 2-х книгах: пер. с англ. М.: Мир,2019. 792 с.
12. Грузман И.С. Цифровая обработка изображений в информационных системах: учеб, пособие. 2002. 352 с.
13. Яне Б. Цифровая обработка сигналов. М.: Техносфера, 2017. 584 с.
14. Селянкин В.В. Компьютерное зрение. Анализ и обработка сигналов: учебное пособие. 2019. 152с.
15. Форсайт Д. Компьютерное зрение. Современный подход. 2014. 928 с.
16. Поляков А. Методы и алгоритмы компьютерного анализа. 2019. 545 с.
17. Безрядин С. Н. Преобразование яркости в программном обеспечении. 2016. 211с.
18. Баженова И. Ю. Язык программирования С++ . 2017. 366 с.
19. Бартлетт Н. Программирование на Delphi Путеводитель. 2016. 116с.
20. Вебер Дж. Технология программирования в подлиннике. 2017. 256с.
21. Волш А. И. Основы программирования на С++для World Wide Web. 2016. 458с.
22. Абрамов С. А. Задачи по программированию. 2018. 256 с.
23. Березин Б.И. Начальній курс программирования на языках высокого уровня. 2016. 331с.
24. Бондарев В.М. Основы программирования. 2017. 446с.
25. Вирт Н. Алгоритмы и структуры данных. 2019. 345с.
26. Гладков В. П. Задачи по информатике на вступительном экзамене в вуз и их решения: Учебное пособие. 2021. 516с.
27. Грогоно П. Программирование на языке Java. 2022. 216с.
28. Дагене В.А. 100 задач по программированию. 2019. 106с.
29. Джамса К. Библиотека программиста Java. 2019. 656с.
30. I.Merino, J. Azpiazu 2D Features Detector And Descriptor Selection Expert System. 2019. – С. 51–61.
31. Заварикин В.М. Основі информатики и вычислительной техники. 2019. 556с.
32. Кен А. Язык программирования С++. 2017. 378с.
33. Керниган Б. Язык программирования Java. 2022. 391с.
34. Ляхович В.Ф. Руководство к решению задач по основам информатики и вычислительной техники. 2014. 127с.
35. Мейнджер Дж. С++ Осноы программирования. 2017. 346с.
36. Миков А. И. Информатика. Введение в компьютерные науки. 2018. 442с.
37. Могилев А. В. Информатика: Учеб. пособие для студ. 2019. 629с.
38. Нотон П. JAVA:Справ.руководство. 2016. 447с.
39. Нотон П. Полный справочник по Java. 2017. 556с.
40. Ренеган Э.Дж. 1001 адрес WEB для программистов:Новейший путеводитель программиста по ресурсам World Wide Web. 2021. 512с.
41. Томас М. Секреты программирования для Internet на Java. 2017. 396с.
42. Семакина И. Г. Информатика. Задачник-практикум. 2019. 476с.
43. Сокольский М.В. Все об Intranet и Internet. 2018. 254с.
44. Тассел Д. Стиль, разработка, эффективность, отладка и испытание программ. 2021. 56с.
45. Тюрин Ю.Н. Анализ данных на компьютере. 2019. 384с.
46. Флэнэген Д. Java in a Nutshell. 2018. 473с.
47. Чен М.С. Программирование на С++:1001 совет:Наиболее полное руководство по С++ и Visual С++. 2017. 640с.
48. Эферган М. С++: справочник. QUE Corporation.2018. 256с.
49. Sinha P. Perceiving and Recognizing threedimensional forms. 2016. 278р.
50. Pablo F. Fast Explicit Diffusion for Accelerated Features in Nonlinear Scale Spaces. 2013. 187с.
51. Березький О.М., Дубчак Л.О., Мельник Г.М. Методичні рекомендації до виконання кваліфікаційної роботи з освітнього ступеня “Магістр”. Спеціальність: 123 - Комп’ютерна інженерія. Магістерська програма - Комп’ютерна інженерія". Тернопіль: ЗУНУ, 2022. 32 с.
52. Гураль І.В., Дубчак Л.О. Методичні вказівки до оформлення курсових проектів, звітів про проходження практики, випускних кваліфікаційних робіт для студентів спеціальності «Комп’ютерна інженерія» Тернопіль: ТНЕУ, 2019. 33 с.