

3.5 Застосування інформаційної технології детектування аномалій у відеоряді для підвищення безпеки транспортних засобів

Відеоспостереження (англ. Video surveillance) – це процес спостереження за різноманітними об'єктами, що реалізується із застосуванням відеокамер – оптико-електронних та мікропроцесорних пристроїв, призначених для візуального контролю навколишнього середовища, з метою безпеки життя, діяльності та майна сучасної людини.

Такими процесами та об'єктами можуть бути, наприклад, автомобілі, що рухаються по перехрестю, по вулиці або по замиській трасі, дорожнє покриття під час контролю його стану та якості, безпека будь-якого інфраструктурного об'єкту чи транспортного засобу.

Аномалія відеоряду камер спостереження за перебігом транспортних процесів – це будь-яке відхилення від звичайного стану, наприклад, проїжджої частини вулиць, перехресть, замиських магістралей. Наприклад, це поява нерухомого транспортного засобу там, де зазвичай рухаються автомобілі чи поява людини на проїжджій частині вулиці поза зони пішохідного переходу.

Пошук аномалій у відеорядах – це надсучасний науковий напрям, що стосується багатьох галузей науки та техніки. Він потребує використання надсучасних обчислювальних технологій, у тому числі нейронних мереж. Власне, завдяки цим технологіям та розвитку обчислювальної техніки пошук аномалій у відеорядах взагалі став можливий.

Щодо аномалій відеоряду камер спостереження у автотransпортних системах, то вони належать до корисної інформації, тобто стають свідченням якихось порушень у нормальному перебігу спостережуваних процесів. Наприклад, зіткнення автомобілів на перехресті чи попадання людини на проїжджу частину вулиці це аномалія з точки зору організації та безпеки руху транспортних засобів. В цьому випадку реєстрація та детектування аномалій є основним завданням системи відеоспостереження з метою безпеки дорожнього

руху. Використання для обробки таких відеоданих сучасних обчислювальних методів робить можливим створення інтелектуальних систем для прийняття відповідних безпекових рішень в транспортних системах.

Крім того, системи відеоспостереження зараз дуже активно використовуються при створенні так названих безпілотних чи роботизованих транспортних засобів. Без таких систем створення та експлуатація останніх практично неможлива.

Аномалії у відеоряді камер відеоспостереження можуть бути також обумовлені, наприклад, несправностями апаратури або перешкодами в тракті передавання сигналу від відеокамер до реєструючої та аналітичної апаратури. Звісно, що такі аномалії не є корисними та інформативними. Їх треба виявляти, а причини їх появи потрібно усувати.

Таке використання систем відеоспостереження в автотransпортних системах обумовлює актуальність даного дослідження.

Останнім часом у світовому інформаційному просторі з'явилося багато різноманітних методів детектування аномалій в часових рядах взагалі, та у відеорядах камер відеоспостереження зокрема. З'явилося багато статей, присвячених дослідженням у цьому напрямі. Ці статті в більшості дуже неконкретні, багато оглядових. Отримати з них дійсно корисну практичну інформацію дуже важко, тому що розробники програмного забезпечення до інтелектуальних IP відеокамер ретельно охороняють свої розробки.

З іншого боку, деякі фірми, що розробляють програмне забезпечення універсального характеру, наприклад Microsoft, оприлюднюють обчислювальні схеми для обробки відеоданих, набори тестових програм, програми для машинного навчання та інше. Загалом, це величезні обсяги обчислювальної та відео інформації. Дослідникам і розробникам сучасних систем відеоспостереження важко орієнтуватися в цьому різноманітті методів для виявлення аномалій.

Нами була переглянута велика кількість статей, досліджень, монографій та публікацій в Інтернеті, що в кілька разів перевищує список літератури до даної

роботи. Ті роботи, в яких ми не зустріли, на наш погляд, раціональних, корисних теоретичних та практичних розробок чи там були повтори деяких відомостей, не увійшли до списку використаних джерел. Допомогла в проведенні нашого дослідження стаття [281] українських дослідників методів пошуку аномалій у відеорядах, в якій зроблена спроба зробити аналіз таких методів.

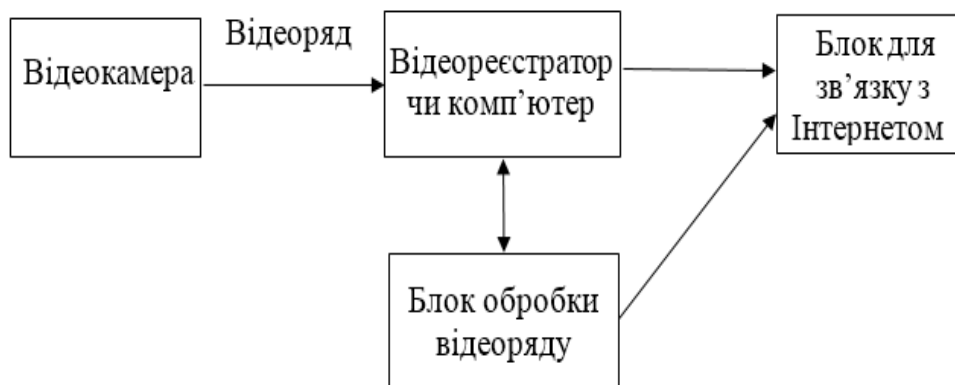
В свою чергу, ми теж намагалися [282] розкрити сутність наведених методів пошуку аномалій, провести їх класифікацію та оглянути технічні рішення для реалізації відеоспостереження з подальшим автоматичним інтелектуальним аналізом для пошуку аномалій в транспортних системах з метою підвищення безпеки транспортних засобів, пішоходів, водіїв та пасажирів.

Великий обсяг відеоданих, які продукуються останнім часом, потребує автоматизованої обробки із залученням потужних комп'ютерів, спеціалізованого програмного забезпечення та новітніх інтелектуальних інформаційних технологій. Зараз роль людини в аналізі відеоряду, з точки зору пошуку аномалій, практично зведена до мінімуму. Це пояснюється і великим обсягом відеоданих, що потребують аналізу, і низькими можливостями людини порівняно з обчислювальною технікою (швидкість роботи, особливості зору та інше).

В рамках поставленої задачі дослідження нас цікавили технології, системи і методи, що були запропоновані та розроблені в світі для отримання, обробки та аналізу відеорядів та зображень, включаючи задачі машинного зору, класифікація зображень, детектування об'єктів та аномалій, тощо.

В [281] вказано, що всі системи відеоспостереження, незалежно від виду, включають такі технічні компоненти: блок живлення, кабель, жорсткий диск для запису і зберігання відеосигналу з камер, монітор, відеореєстратор або комп'ютер для локального перегляду та зберігання відеозапису, Інтернет для використання відеореєстратора з хмарним сервісом при перегляді відеозапису в онлайн режимі.

Вважаємо, що систему відеоспостереження та систему детектування аномалій в відеоряді на її основі можна представити у вигляді наступної функціональної блок-схеми (мал. 1).



Малюнок 1. Функціональна блок-схема системи
детектування аномалій у відеоряді

Система детектування аномалій в відеоряді чи система відеоспостереження функціонує наступним чином. Відеоряд, тобто корисний сигнал від відеокамери, який є результатом відеоспостереження, потрапляє до віореєстратора чи комп'ютера для реєстрації, подальшої обробки та зберігання.

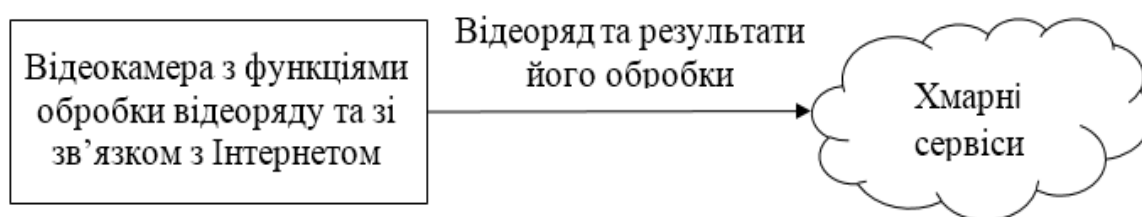
У випадку використання віореєстратора обробка відеоряду здійснюється у блоці обробки відеоряду. Цей процес обробки відеоряду з метою виявлення загроз чи аномалій у сукупності з відповідним програмним забезпеченням називається відеоаналітикою і може реалізовуватися як окремими пристроями, так і програмним забезпеченням комп'ютера чи віореєстратора. Результати роботи відеоаналітики чи сам відеоряд можуть бути передані до мережі Інтернет за допомогою блоку для зв'язку з Інтернетом.

Треба відмітити, що важко відокремити системи детектування аномалій в відеоряді від самої системи відеоспостереження, тому далі будемо вести мову про системи відеоспостереження в цілому. Тим більше, що технічний рівень

людства в цілому і, зокрема, радіоелектроніки та обчислювальної техніки дозволяє об'єднати різні функціональні блоки системи, що зображена на рис.1, без істотного збільшення габаритів.

Зараз на ринку пристроїв для відеоспостереження з'явилися автономні керовані роботизовані поворотні Internet Protocol (IP) камери відеоспостереження, які мають можливість дистанційно чи автоматично повертати об'єктиви по горизонталі і вертикалі для збільшення обсягу контрольованого простору [283]. Такі камери мають функцією відеоаналітики для первинної обробки відеоряду та зв'язок з Інтернетом для подальшого його аналізу у разі потреби.

Для роботизованої IP відеокамери з відеоаналітикою функціональна блок-схема системи детектування аномалій у відеоряді має наступний вигляд (мал. 2):



Малюнок 2. Схема системи з об'єднаними блоками для виявлення аномалій в відеоряді

Бачимо, що така відеокамера об'єднує функції декількох блоків системи, яка зображена на мал. 1. Такий пристрій для відеоспостереження самостійно може зберігати певний обсяг відеоінформації, може передавати її для зберігання по хмарним технологіям. Ця відеокамера також може обробляти отриману відеоінформацію по певним алгоритмам самостійно (в рамках своїх можливостей), а може передавати її для хмарних обчислень, якщо потрібні більш потужні обчислювальні ресурси.

Вищезазначені найсучасніші системи детектування аномалій в відеоряді – це все ж таки справа майбутнього. Тому задача класифікації дещо простішої

традиційної техніки, яка зараз переважним чином використовується у системах детектування аномалій в відеоряді у нинішній час, продовжує бути актуальною.

Прийнято виділяти кілька типів класичних систем відеоспостереження [281] в залежності від використовуваного технічного оснащення [284, 285].

1) Аналогові системи. Склад комплектуючих: AHD/HD-CVI/HD-TVI камера відеоспостереження, цифровий відеореєстратор (Digital Video Recorder (DVR)).

2) Цифрові системи. В їх основу покладено IP-технології. Аббревіатура IP зазначає збірку правил, за якими потрібно використовувати технологію Internet для обміну інформацією між комп'ютерними мережами. Мається на увазі використання IP відеокамер спільно з мережевими комутаторами. Склад комплектуючих наступний: IP камера відеоспостереження, мережевий відеореєстратор (Network Video Recorder (NVR)) та мережевий комутатор для підключення відеокамер і відеореєстраторів до мережі Інтернет.

3) Змішані (гібридні) системи. Принцип їх роботи засновано на прийомі відеозображення з аналогових камер та на оцифруванні зображення для подальшого використання.

Цифрові системи сьогодні є більш перспективними в порівнянні з аналоговими системами: покращена якість відеозображення, гнучкість і легка масштабованість, можливість глибокого аналізу і віддаленого налаштування, простота інтеграцій в існуючу комп'ютерну мережу.

Гібридні системи є поки що найбільш поширеними. В них якість одержуваного зображення поступається системам з цифровим форматом, але інші параметри роботи систем цього типу нічим не відрізняються від аналогічних характеристик цифрових систем, а це дає можливість створювати надійні і багатофункціональні системи змішаного типу.

Відмітимо, що сучасні системи відеоспостереження обов'язково використовують Інтернет і для цього мають в своєму складі або відеокамери та відеореєстратори для отримання, запису і збереження відеозображення, а також маршрутизатор та блок управління всіма відеокамерами, або одну мережеву IP-

відеокамеру для невеликих територій чи локальних завдань. Для передачі відеоінформації одночасно з декількох пунктів система відеоспостереження може складатися з декількох мережевих відеокамер.

Спробуємо наочно представити класифікацію систем детектування аномалій у відеоряді, базуючись на зазначених вище класах цих систем (мал. 3).



Малюнок 3. Класифікація систем виявлення аномалій
у відеоряді камер спостереження

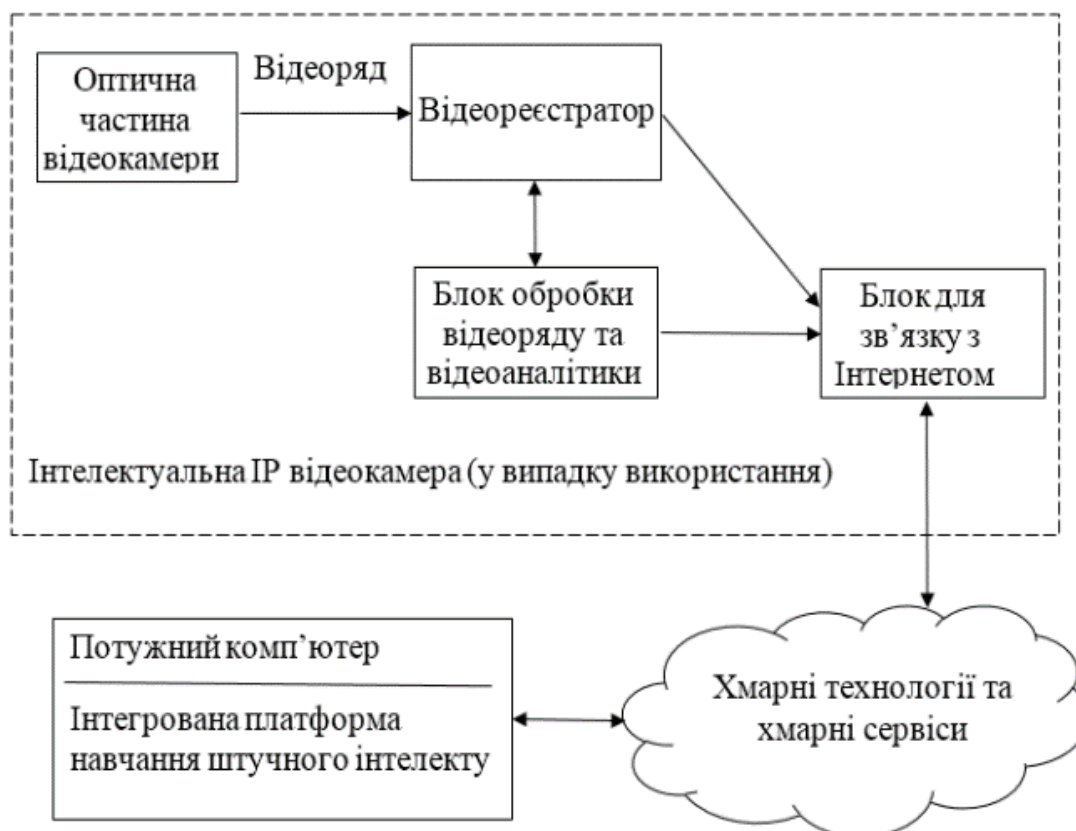
Проведений вище аналіз показує, що для сучасних відеокамер огляд систем детектування аномалій в відеоряді тотожний огляду методів виявлення аномалій в відеоряді камер спостереження. Наведені вище схеми функціонально не відрізняються, але з невинним розвитком оптики, електроніки та

обчислювальної техніки дещо змінюється апаратний склад систем детектування аномалій у відеоряді камер відеоспостереження.

Обчислювальні та комунікативні (мережеві) можливості IP відеокамер кращі, ніж у потужних комп'ютерів 2000-х років. Але ж і нові методи обробки результатів відеофіксації (а це здебільшого методи, що пов'язані з використанням нейронних мереж) потребують значно більших обчислювальних потужностей. Тут у нагоді стають мережеві можливості IP-відеокамер та хмарні сервіси, за допомогою яких за новітніми мережевими технологіями зберігаються і обробляються величезні обсяги фіксованих даних.

Тепер, маючи відомості про використання програмних чи апаратних блоків відеоаналітики в системах детектування аномалій у відеоряді камер відеоспостереження можна переробити функціональну схему такої системи (мал. 1), зробивши її більш сучасною та універсальною. Отримаємо функціональну блок-схему інтелектуальної системи детектування аномалій в відеоряді (мал. 4).

Функціональна блок-схема інтелектуальної системи детектування аномалій в відеоряді камер відеоспостереження, що зображена на мал. 4, має універсальний характер. Вона показує склад системи детектування аномалій, яка базується на звичайній відеокамері. Після відеореєстрації сигнал з відеокамери передається до блоку обробки чи до Інтернету для більш глибокої обробки за допомогою найсучасніших технологій (нейронні обчислювальні мережі та інші), для подальшого аналізу чи зберігання. Інтелектуальність в такому варіанті забезпечується сучасними алгоритмами та могутніми ресурсами хмарного середовища. У випадку використання більш кошторисної IP відеокамери, виділені штрих-пунктиром блоки наявні у складі самої камери. В залежності від задач системи та наявності певної апаратури в кожному конкретному випадку може бути свій склад системи детектування аномалій.



Малюнок 4. Схема інтелектуальної системи
детектування аномалій у відеоряді

Сучасні інтелектуальні камери відеоспостереження можуть також мати вбудовані функції відеоаналітики. Перевага тут полягає в тому, що такі можливості аналітики у відеокамерах не залежать від смуги пропускання мережі та часу відгуку сервера. Таке рішення вигідне там, де потрібна висока оперативність та негайний відгук. Відеодані в цьому випадку зберігаються на самих відеокамерах і можуть бути вилучені для аналізу будь-коли через віддалену програму-клієнт. В тому випадку, якщо для спостереження використовується інтелектуальна ІР відеокамера, вона об'єднує в собі декілька блоків зі схеми на мал. 4 (пунктирна лінія). Первинна обробка може бути виконана самою камерою (блок обробки відеоряду та відеоаналітики). Якщо потрібні більш потужні обчислювальні ресурси, наприклад, у випадку використання нейронних технологій, то використовуються хмарні ресурси.

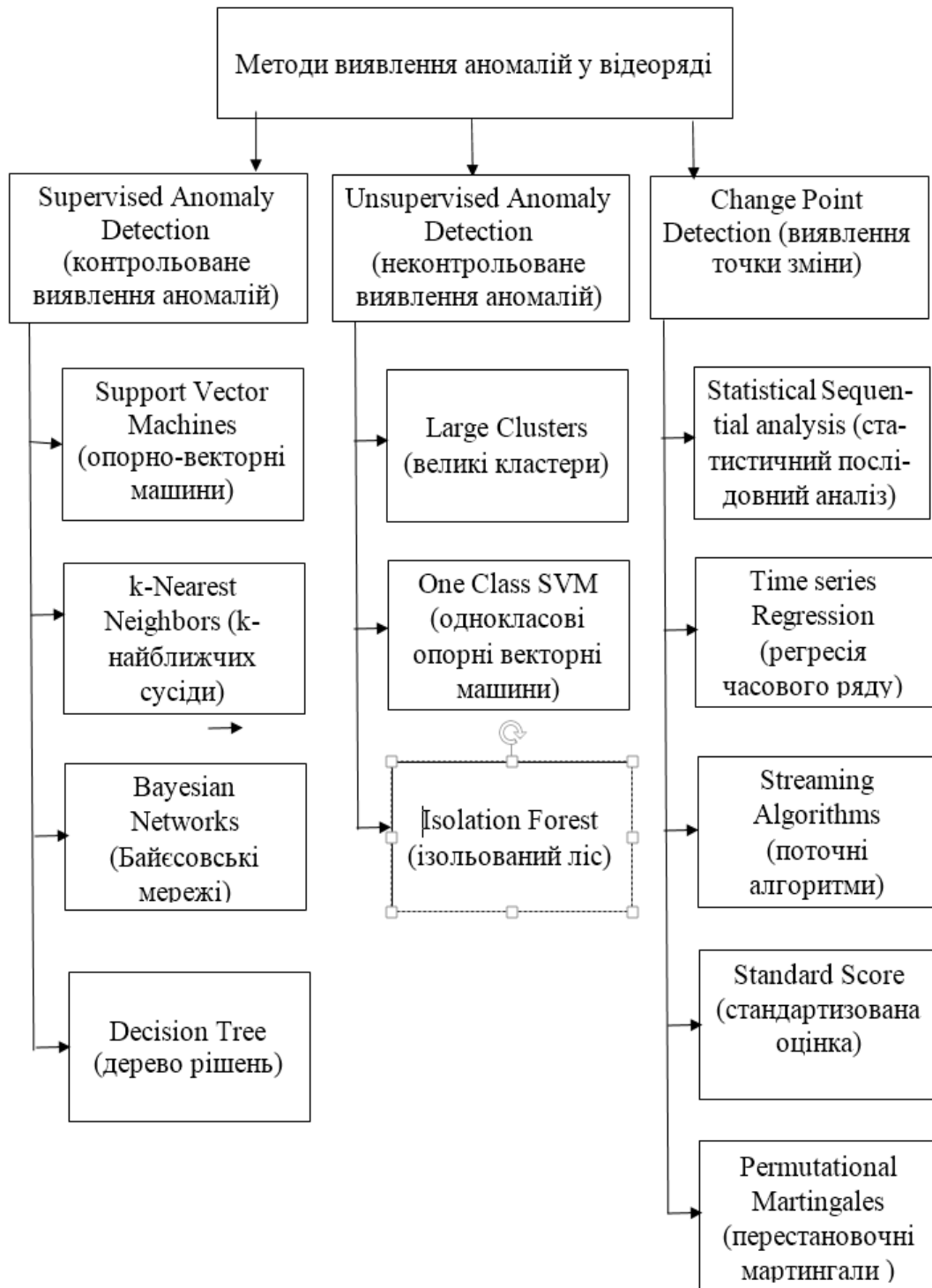
Вище нами був зроблений висновок, що відмінності між собою систем пошуку аномалій у відеоряді камер відеоспостереження обумовлені не тільки (і не стільки) технічним складом таких систем. Здебільшого це вплив тих методів, які обирають замовники і конструктори, математики, програмісти та інші спеціалісти для обробки відео інформації.

Під час пошуків джерел інформації щодо використання тих чи інших методів обробки відеорядів камер відеоспостереження для детектування аномалій нами було знайдено лише одну роботу в інформаційному просторі України, де було зроблено спробу хоча би перерахувати такі методи та дати посилання на відповідні джерела [281]. Це дуже допомогло в нашому дослідженні, в якому одним з завдань є аналіз властивостей та особливостей методів обробки відеорядів.

На даний час відомі різноманітні методи детектування аномалій у відеоряді камер відеоспостереження. Для більшої наочності представимо у графічному вигляді класифікацію таких методів (мал. 5). Їх прийнято поділяти на два класи: Supervised Anomaly Detection (контрольоване виявлення аномалій) і Unsupervised Anomaly Detection (неконтрольоване виявлення аномалій) [286].

Судячи з численних публікацій, переважно англомовних, методи детектування аномалій нерозривно пов'язані з машинним навчанням. Причому методи класу Supervised Anomaly Detection відносяться до задач навчання зі вчителем, а методи класу Unsupervised Anomaly Detection – до навчання без вчителя.

В методах, що використовують контрольоване виявлення аномалій, до машинного навчання надходять дані з мітками, які встановлюють, чи є аномалії, чи ні. Це такі методи, як опорно-векторні машини (Support Vector Machines) [281, 287], k-Nearest Neighbors (k-найближчих сусідів), Bayesian Networks (Байєсовські мережі), Decision Tree (дерево рішень) та інші [288]. Однак для них трудомісткою і проблемною задачею є правильна установка міток. Крім того, відеодані містять шум, що призводить до частих хибних спрацьовувань системи.



Малюнок 5. Класифікація методів пошуку аномалій
у відеоряді камер відеоспостереження

Розглянемо далі методи з неконтрольованим виявленням аномалій. Для цього класу методів використовують дані, для яких невідомо, які з них

нормальні, а які аномальні. При аналізі відеоспостережень ця ситуація більш притаманна, і в такому випадку використовуються, в свою чергу, різноманітні підходи.

Найпростішим рішенням є кластеризація. Дослідники виходять з припущення, що більшість даних (великі кластери) є нормою для багатьох задач, і тільки незначний процент даних є аномальними. Тобто дані, що належать до невеликих кластерів, і є шуканими аномаліями.

Інші автори використовують метод One Class Support Vector Machines (однокласові опорні векторні машини) чи One Class SVM. Вони моделюють тільки нормальні дані (на їх думку). Цей алгоритм – одна із форм класичного алгоритму SVM [285, 288]. Як впливає із назви, для його навчання достатньо мати всього один клас – "чисті" спостереження без аномалій.

Ще один, третій клас методів, базується на припущенні [281], що аномалії не тільки нечисленні, але й в них є значення атрибутів, що значно відрізняються від значень численних звичайних екземплярів. Один із прикладів цього типу - це метод Isolation Forest (ізолюваний ліс) [289], який ґрунтується на “розбитті простору ознак детектованого відеоряду у вигляді так званих ізолюючих дерев, і аномаліями виявляються точки, що значно віддаленні від інших” [281].

Ціле сімейство перспективних і поширених [281] методів вирішують задачу пошуку аномалій, як пошук точок зміни певних властивостей чи характеристик відеоряду як часового у зв’язку з тим, що кадри відео змінюються за часом. Назва методу відповідна - Change Point Detection (виявлення точки зміни) або CPD. На цій ідеї базується декілька, як вважають спеціалісти [281], ефективних методів, що дозволяють визначати моменти часу, коли відбуваються суттєві зміни в часовому ряді [290].

На жаль, обсяг статті не дає змоги більш докладно представити результати проведеного порівняльного аналізу методів пошуку аномалій у відеоряді камер спостереження.

Подальші дослідження у цьому напрямі (пошук аномалій у відеоряді) можуть відбуватися наступним чином. Навряд чи можливо одному чи декільком

дослідникам оволодіти всіма існуючими методами пошуку аномалій та перевірити їх хоча би на тестових відеоданих. Тим більше, що треба опанувати теорію та практику нейронних обчислювальних мереж. Необхідно зосередитись на двох чи трьох методах, інформація про використання яких буде здаватися найбільш достовірною. Потім провести порівняльні тестові випробування, що в умовах закритої інформації є доволі складним завданням.

Наприклад, в роботі [281] автори пропонують та самі зосередилися на використанні згорткової глибинної нейронної мережі, (CNN) [291]. Глибинні нейронні мережі набули широкого розвитку та поширення в різноманітних областях завдяки їх високій ефективності при рішенні багатьох задач при роботі з зображеннями і відео [281]. Ми теж вважаємо, що доцільно почати з цього методу.

В результаті проведення даного дослідження було виконано наступне:

1) Проведено огляд основних сучасних систем детектування аномалій в відеоряді камер відеоспостереження. Зроблений висновок, що відмінності між собою систем пошуку аномалій у відеоряді камер відеоспостереження обумовлені вибором методів для обробки відео інформації.

2) Проведено аналіз методів виявлення аномалій у відеоряді камер відеоспостереження. Для цього розроблена класифікація сучасних методів виявлення аномалій в відеоряді та розглянуто основи теорії глибинних нейронних мереж з точки зору можливості їх застосування для класифікації, локалізації, сегментації, виявлення, ідентифікації та моніторингу об'єктів (транспортних засобів чи людей на проїжджій частині) у відеоряді камер спостереження.

3) Запропонований подальший напрямок досліджень: для початку зосередитись на двох чи трьох методах пошуку аномалій у відеоряді, інформація про використання яких буде здаватися найбільше достовірною, та провести порівняльні тестові випробування обраних методів.