УДК 629.341 DOI: 10.30977/BUL.2219-5548.2022.98.0.26

АНАЛІЗ МЕТОДІВ ВИЯВЛЕННЯ АНОМАЛІЙ У ВІДЕОРЯДІ КАМЕР ВІДЕОСПОСТЕРЕЖЕННЯ НА ТРАНСПОРТІ

Симбірський Г. Д.
Харківський національний автомобільно-дорожній університет

Анотація. *Проведено огляд систем детектування аномалій у відеоряді камер відеоспостереження автотранспортного комплексу. Розроблено функціональну схему такої системи на базі інтелектуальної IP відеокамери. Проаналізовано відомі на цей час методи пошуку аномалій у відеоряді камер відеоспостереження. Проведено порівняльну класифікацію сучасних методів детектування аномалій у відеоряді. Розроблено рекомендації щодо використання таких методів у системах відеоспостереження на автотранспорті.*
Ключові слова: *аномалії відеоряду, системи детектування аномалій, класифікація методів пошуку аномалій, інтелектуальні камери відеоспостереження, відеоаналітика*.

Вступ

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 заміській трасі, дорожнє покриття під час контролю його стану та якості, система охорони, в тому числі кібербезпека, будь-якого інфраструктурного об'єкта чи транспортного засобу.

Аномалія часового ряду взагалі, а відеоряд належить якраз до таких рядів, це, як вказує саме написання цього слова, щось відмінне від норми, тобто викид чи відхилення. Пошук аномалій у часових рядах – це надсучасний науковий напрям величезного обсягу, який стосується багатьох галузей науки і техніки. Він потребує теж надсучасних обчислювальних технологій, у тому числі нейронних мереж. Власне, завдяки цим технологіям та розвитку обчислювальної техніки пошук аномалій став можливим.

Щодо аномалій відеоряду камер спостереження у автотранспортних 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. У 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 прийняття рішень у транспортних системах.

Крім того, системи відеоспостереження зараз дуже активно використовуються при створенні так званих 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 реєструвальної 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 автотранспортних системах є дуже актуальним, але воно можливе тільки завдяки застосуванню методів детектування аномалій у відеоряді, що обумовлює актуальність даного дослідження.

Аналіз публікацій

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. Отримувати з них дійсно корисну практичну інформацію дуже важко. Вочевидь фірми-розробники програмного забезпечення

до інтелектуальних IP відеокамер ретельно охороняють свої розробки.

З іншого боку, деякі фірми-розробники програмного забезпечення універсального характеру, наприклад Microsoft, оприлюднюють обчислювальні схеми для обробки відеоданих, набори тестових програм, програми для машинного навчання та ін. 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 не зустріли якихось, на наш погляд, раціональних, корисних теоретичних та практичних розробок чи там були повтори деяких відомостей, ми не включили до списку використаних джерел. Звертатися до цього списку будемо по ходу даного дослідження.

Допомогла в проведенні нашого дослідження стаття [1] вітчизняних дослідників методів пошуку аномалій у відеорядах, де була зроблена спроба зробити аналіз таких методів. Але невеликий обсяг цієї статті не дозволив розкрити сутність наведених методів пошуку аномалій, провести їх кваліфікацію, оглянути технічні рішення для реалізації відеоспостереження.

Тому аналіз технічного складу систем для виявлення аномалій у відеоряді камер відеоспостереження та огляд обчислювальних методів для цього, що є завданням пропонованої кваліфікаційної роботи, є актуальною науковою і практичною задачею.

Дане дослідження виконується у рамках кваліфікаційної магістерської роботи у Харківському національному університеті радіоелектроніки.

Мета та постановка задачі

Метою дослідження є аналіз технічного складу систем для виявлення аномалій у відеоряді камер відеоспостереження та порівняльний огляд обчислювальних методів для обробки результатів цього спостереження.

Для досягнення поставленої мети необхідно дослідити літературні джерела, тобто статті у наукових журналах, доповіді на конференціях, статті на тематичних веб-порталах, монографії та підручники, назви яких вказують на можливість находження в них корисних для даного дослідження відомостей.

Складові частини та класифікація систем детектування аномалій у відеоряді

Під час відеоспостереження інформація передається з відеокамер та телевізійних камер на певну кількість моніторів або реєструвальних пристроїв [2].

Системи відеоспостереження можуть знімати безперервно або вмикатись лише за заданою подією. Досконаліші системи стеження з використанням відеореєстраторів дозволяють створювати записи, які зберігатимуться роками, з різною якістю та з додатковими можливостями (такими як виявлення рухів та оповіщення через електронну пошту) [2].

Зазвичай відеоряд розглядається як послідовність кадрів, і суттєві зміни від одного кадру до іншого можуть вказувати на виникнення нових ситуацій, і це розглядається як вихід із стану стабільності, тобто як аномалія [1]. Тобто зрозуміло, що аномалія у відеоряді це щось відмінне від його загального характеру.

Нами був проведений аналіз чималої кількості наукових робіт, в яких розглядаються проблеми, пов'язані з дослідженням відеорядів. Це не тільки відеокамери, що використовуються для відеоспостереження у системах безпеки, але й ті відеокамери, що використовуються у багатьох інших сферах людської діяльності. Це оборона, промисловість, медичні дослідження, сільське господарство, різноманітні наукові дослідження, у тому числі космічні, та багато інших.

Великий обсяг відеоданих, які продукуються останнім часом та невпинно продовжують продукуватися, потребують 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 ін.).

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

У [1] 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 у відеоряді на її основі можна подати у вигляді такої функціональної блок-схеми (рис. 1).

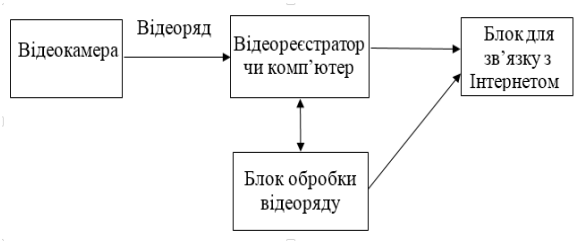

Рис. 1. Функціональна блок-схема системи детектування аномалій у відеоряді

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

Відеореєстратор – це електронний пристрій, призначений для запису, зберігання та відтворення відеоінформації [3]. Він схожий за будовою з комп'ютером або відеосервером і містить у своєму складі аналого-цифровий перетворювач (АЦП), процесор, жорсткий диск та інші компоненти. Для управління відеореєстратором на ньому встановлена спеціалізована операційна система. Перед записом оцифровані відеозображення, як правило, піддаються компресії для зменшення займаного місця на жорсткому диску. Практично всі відеореєстратори можуть працювати як з монохромними, так і з кольоровими відеозображеннями. Багато відеореєстраторів мають можливість підключення до комп'ютерної мережі для передачі відеозображень на комп'ютери віддалених користувачів.

У випадку використання відеореєстратора 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 відеореєстратора. Результати роботи відеоаналітики чи сам відеоряд можуть бути передані до мережі інтернет за допомогою блоку для зв'язку з інтернетом.

Треба відзначити, що важко відокремити системи детектування аномалій у відеоряді від самої системи відеоспостереження, тому далі в цьому розділі будемо вести мову про системи відеоспостереження в цілому. Тим більше, що технічний рівень людства в цілому і, зокрема радіоелектроніки та обчислювальної техніки, дозволяє чи дозволить в близькому майбутньому об'єднати різні функціональні блоки системи, що зображена на рис. 1, без істотного збільшення габаритів. Це буде показано далі.

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 [4]. Такі камери мають функцією відеоаналітики для первинної обробки відеоряду та зв'язок з інтернетом для подальшого його аналізу.

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

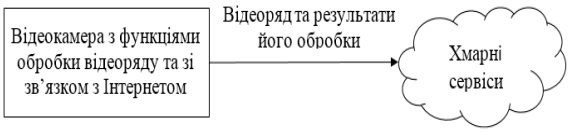

Рис. 2. Схема системи з об'єднаними блоками для виявлення аномалій у відеоряді

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

Вищезазначені найсучасніші системи детектування аномалій у 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 [1] залежно від використовуваного технічного оснащення [5, 6].

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. Абревіатура IP означає 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 такий: 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 основано на прийомі відеозображення з аналогових камер та на оцифруванні зображення для подальшого використання.

Аналогові системи не дуже сучасні, проте іноді використання цього типу систем є обґрунтованим [5].

Цифрові системи сьогодні є більш перспективними порівняно 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.

Відзначимо, що сучасні системи відеоспостереження обов'язково використовують інтернет і для цього мають у 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 подати класифікацію систем детектування аномалій у відеоряді, базуючись на зазначених вище класах цих систем (рис. 3).

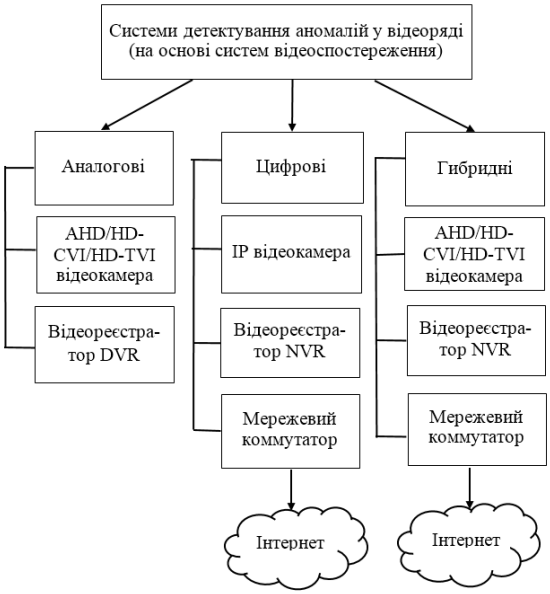

Рис. 3. Класифікація систем виявлення аномалій у відеоряді камер спостереження

Проведений вище аналіз показує, що для сучасних відеокамер огляд систем детектування аномалій у відеоряді тотожній огляду методів виявлення аномалій у відеоряді камер спостереження. Наведені вище схеми функціонально не відрізняються, але з невпинним розвитком оптики, електроніки та обчислювальної техніки дещо змінюється апаратний склад систем детектування аномалій у відеоряді камер відеоспостереження.

Для кращого розуміння можна сказати, що зараз обчислювальні та комунікативні (мережеві) можливості IP відеокамер кращі, ніж у потужних комп'ютерах 2000-х років. Ті блоки у складі таких систем, що потребували для експлуатації систем відеоспостереження окремих корпусів та багатьох кабелів, перетворилися на невеликі мікропроцесорні плати, що легко вмонтовуються до корпусів IP відеокамер. Але ж і нові методи обробки результатів відеофіксації (а це здебільшого методи, 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 новими мережевими технологіями зберігаються і обробляються величезні обсяги зафіксованих даних.

Відеоаналітика у системах детектування аномалій

Вище було зазначено, що з розвитком мікропроцесорної техніки та хмарних технологій зберігання і обробки інформації важко відокремити системи детектування аномалій у відеоряді від систем відеоспостереження. Вважаємо, що з подальшим розвитком радіоелектроніки, інформаційних технологій, обчислювальних потужностей сучасних мікропроцесорів, математичного моделювання, нейронних мереж та штучного інтелекту кожна система відеоспостереження одночасно буде і системою детектування аномалій у відеоряді.

Як можна бачити з рис. 2, сучасні інтелектуальні відеокамери являють собою систему детектування аномалій у відеоряді, а відмінності однієї системи детектування аномалій від іншої це відмінності між собою методів виявлення таких аномалій.

Можна підсумувати, що інтелектуальні відеокамери самі стають системами детектування аномалій у відеоряді за рахунок таких чинників:

- наявність у відеокамері модуля для первинної обробки результатів відеоспостереження;
- наявність у відеокамері модуля для зв'язку з інтернетом, тобто можливості користування хмарними технологіями і сервісами для зберігання та обробки інформації.

Відомі два типи задач, що пов'язані з пошуком аномалій [6] у відеорядах.

1) Виявлення викидів, що визначаються як спостереження, що значно відрізняються від інших. Алгоритми для визначення таких викидів намагаються знайти, на якій ділянці відеоряду знаходиться основна маса даних. Аномальні спостереження заважають використанню цих даних і перед машинним навчанням їх прибирають. Процедуру виявлення таких аномалій називають Outlier detection (виявлення викидів).

2) Виявлення аномальної поведінки в ситуації, коли є спостереження, що описують звичайні стани системи, а при появі нових даних потрібно визначити, чи є вони аномальними. Такий підхід називають Novelty detection (виявлення новизни). Він найбільше підходить для аналізу відеоряду і встановлення, чи є аномалії в новому кадрі порівняно з попередніми.

Одним із самих простих підходів, що використовуються при відеоспостереженні, є відеодетекція [1]. Відеодетектор попіксельно порівнює наступний кадр з попереднім або з групою кадрів і сигналізує про змінення статичних картинок. При цьому визначають заздалегідь, чи враховувати більше або менше змін у глибині кольору, чи виключати реакції на певні зони в кадрі, визначають площу змін. Самим суттєвим недоліком відеодетекції є низька перешкодостійкість. Якщо у зоні відеодетекції, для прикладу, знаходяться гілки, що гойдаються від вітру, то точність значно знижується. І це потребує безвідривного ручного контролю у реальному часі або тривалого перегляду відеоархівів, щоб відстежити важливі події. Такі перешкоди у фіксованому відеоряді є великою проблемою у процесі відеоспостереження.

Тобто до проблеми величезного обсягу відеоінформації, що невпинно накопичується у процесі відеоспостереження, додається проблема аналізу цієї відеоінформації. До того ж цей аналіз потрібно проведити здебільшого в реальному часі, тобто під час спостережень.

Ми підійшли до моменту, коли потрібно ввести нове для цього дослідження поняття. Це відеоаналітика або аналіз відеоконтенту (Video content analysis або video content analytics (VCA)) — можливість автоматичного аналізу відеоряду для виявлення та визначення часових і просторових подій [7].

Відеоаналітика порівнює не статичні картинки і не пікселі як такі, а зміни характеру активності [1]. Вона працює з динамікою, знаходить новий рух на фоні інших рухів. Коли об'єкт потрапляє в кадр або починає рухатися, аналізується і запам'ятовується його характер активності, що стає ознакою ідентичності даного об'єкта. Реакція настає при зміні цієї закономірності руху чи на появу іншого характеру руху на кадрі, і навіть їх комбінацій при накладенні. Одне з найактуальніших завдань у системах відеоспостереження – скорочення обсягу марної інформації, видалення непотрібних даних, на відміну від інших підходів відеоаналітики, коли розпізнається потрібна для людини інформація.

Цій меті служить так звана відеосемантика [1] – «короткий логічний виклад відеоінформації шляхом розкладання її на семантичні одиниці (відеосюжети), кожен з яких має свій закінчений зміст, що відрізняється і від попереднього, і від наступного відеосегмента» [8].

Одна з перших систем відеоспостереження, що працювала за технологією «коротких даних», була технологія автоматизованого спостереження під назвою Annotation of Critical Evidence (ACE) Surveillance (спостереження як анотація критичних доказів) [8]. Вона працює таким чином: відеосигнал з камери постійно обробляється на комп'ютері. При виявленні нового об'єкта або активності програмне забезпечення запускає сигнал тривоги. Критичні моментальні знімки даних автоматично фіксуються та зберігаються. Кожний такий знімок забезпечений текстовими анотаціями (пояснювальними підписами), що допомагають зрозуміти дані та підвищують керованість архівними даними.

Інший автор [9] дає таке визначення цьому новому науково-технічному напрямку. Відеоаналітика – це апаратно-програмне забезпечення або технологія, що використовує методи комп'ютерного зору для автоматизованого збору даних на підставі аналізу потокового відео (відеоаналізу), яка спирається на алгоритми обробки зображення і розпізнавання образів, що дозволяють аналізувати відео без прямої участі людини.

У принципі ці два визначення не протирічать одне одному. Обоє констатують автоматичний характер обробки та аналізу відеоінформації з використанням обчислювальної техніки. Останнім часом використанню відеоаналітики в системах відеоспостереження приділяється дуже велика увага.

Зробимо спробу розібратися в тому, як відеоаналітика співвідноситься з пошуком аномалій у відеоряді камер спостереження. В [9] наведені базові функції відеоаналітики, на яких побудовані всі інші функції її роботи.

1) Виявлення об'єктів (object detection). Виявлення об'єктів у полі зору відеокамери проводиться за допомогою відеодетекторів руху.

2) Стеження за об'єктами (object tracking). Алгоритми стеження дозволяють отримати траєкторію руху об'єкта як у полі зору однієї камери, так і за результатами стеження декількома камерами. Наприклад, так визначаються автомобілі, що рухаються з підвищеною швидкістю.

3) Класифікація об'єктів (object classification). Системи відеоаналітики класифікують об'єкти. Наприклад, типовий класифікатор об'єктів, використовуючи ознаки форми й абсолютні розміри, розподіляє об'єкти на групи: людина, групи людей, транспортний засіб тощо.

4) Ідентифікація об'єктів (object identification). Ідентифікація об'єктів є найбільш складним компонентом систем відеоаналітики. Сучасні системи відеоспостереження, обладнані блоком відеоаналітики, дозволяють ідентифікувати людей за біометричними ознаками особи або транспортні засоби за номерними знаками.

5) Виявлення (розпізнавання ситуацій). Діючи за певними алгоритмами та використовуючи ті ж операції, що в пунктах 1-4, відеоаналітичне програмне забезпечення дозволяє не лише виділяти об'єкти з потокового відео, але і розпізнавати тривожні ситуації на основі аналізу поведінки цих об'єктів. Така ситуаційна відеоаналітика може автоматично детектувати, наприклад, перетин сигнальної лінії, падіння людей, заборонену парковку, пожежі тощо.

Наведені вище базові функції відеоаналітики для систем відеоспостереження потребують для своєї реалізації різноманітних методів. Останніми роками з'явилося доволі багато таких методів. В наступному розділі зробимо спробу їх класифікувати та проаналізувати особливості застосування.

Останній пункт вищенаведених базових функцій відеоаналітики майже повністю відповідає тим задачам, які стоять перед системами детектування аномалій у відеоряді камер спостереження. Хоча все залежить від мети створення чи придбання кожної конкретної системи відеоспостереження. З клієнтом чи з замовником такої системи обговорюються її задачі. Треба підібрати такий метод виявлення аномалій у відеоряді камер відеоспостереження чи сукупність методів, щоб він чи вони були здатні вирішувати поставлені безпекові задачі. У подальших дослідженнях ми побачили, що вибір методу виявлення аномалій у відеоряді камер відеоспостереження, по-перше, дуже залежить від конкретної задачі, а по-друге – помилковий вибір методу може призвести до негативних результатів, тобто не виявляти аномалії чи порушення, навіть коли вони реально існують.

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

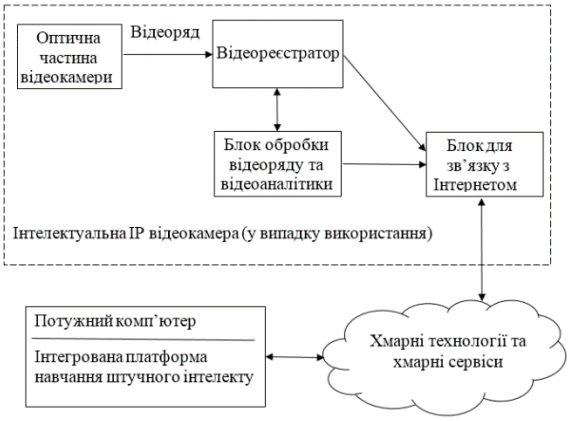

Рис. 4. Схема інтелектуальної системи детектування аномалій у відеоряді

Функціональна блок-схема інтелектуальної системи детектування аномалій в відеоряді камер відеоспостереження, що зображена на рис. 4, має універсальний характер. Вона показує склад системи детектування аномалій, яка базується на звичайній відеокамері. У цьому випадку сигнал з відеокамери, тобто відеоряд, передається на відеореєстратор для зберігання та подальших операцій. Після відеореєстрації сигнал з відеокамери передається до блоку обробки чи, якщо потрібно, 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. Залежно від задач системи та наявності певної апаратури в кожному конкретному випадку може бути свій склад системи детектування аномалій.

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 IP відеокамера, вона об'єднує в собі декілька блоків зі схеми на рис. 4 (пунктирна лінія). Первинна обробка може бути виконана самою камерою (блок обробки відеоряду та відеоаналітики). Якщо потрібні потужні обчислювальні ресурси, наприклад, у випадку використання нейронних технологій, то використовуються хмарні ресурси.

Класифікація методів виявлення аномалій у відеоряді

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 відеоінформації.

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 [1]. Це дуже допомогло у нашому дослідженні, в якому одним із завдань є аналіз властивостей та особливостей методів обробки відеорядів.

До речі, у великому списку джерел дослідження [1] немає жодної української роботи. Законодавцями у цій галузі інформаційних технологій є англомовні вчені. Тому прийнято в дослідженнях щодо пошуків аномалій у часових рядах використовувати англійські терміни та назви. Будемо теж так робити, але вважаємо за потрібне давати переклад всіх термінів та назв на державну мову, тому що це буде сприяти кращому розумінню матеріалу.

На даний час відомі різноманітні методи детектування аномалій у відеоряді камер відеоспостереження. Для більшої наочності представимо у графічному вигляді класифікацію таких методів (рис. 5). Їх прийнято поділяти на два класи: Supervised Anomaly Detection (контрольоване виявлення аномалій) і Unsupervised Anomaly Detection (неконтрольоване виявлення аномалій) [10].

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

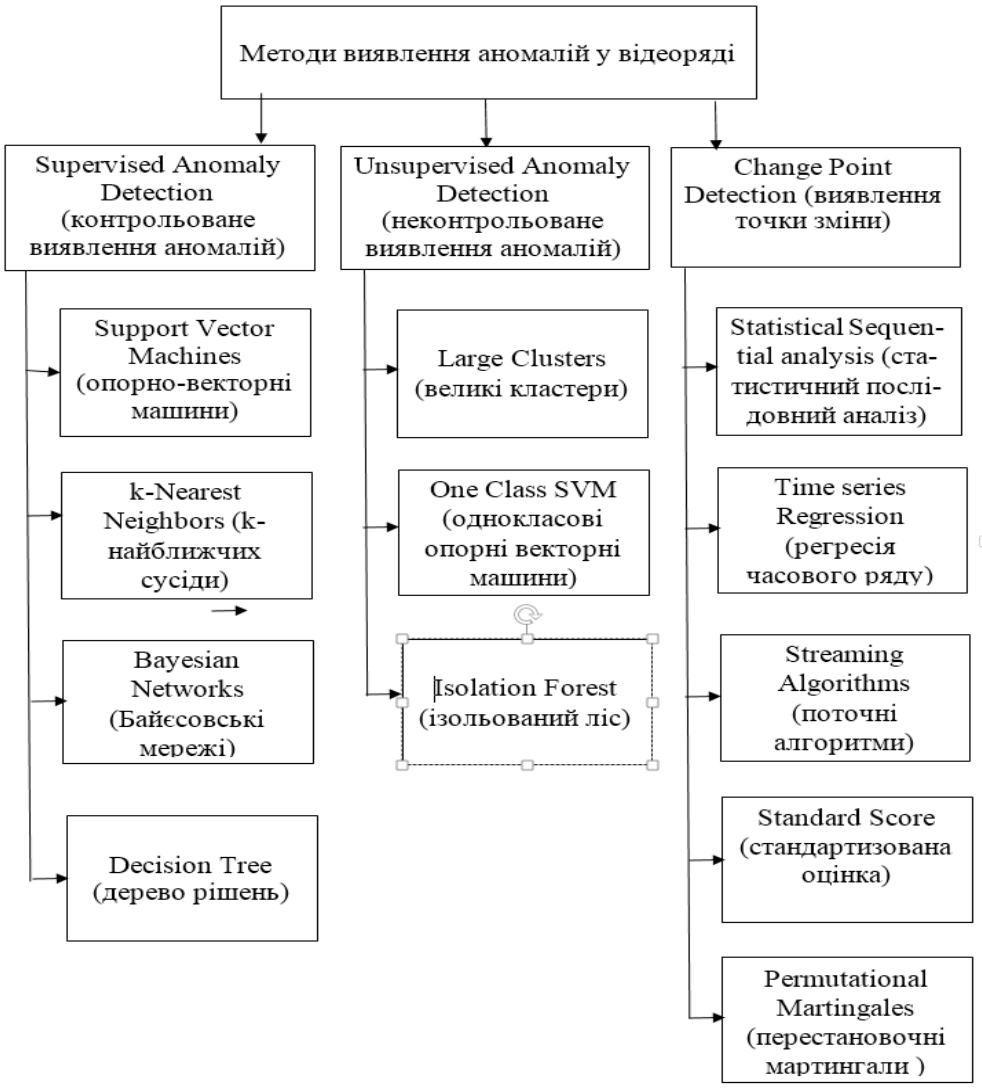

Рис. 5. Класифікація методів пошуку аномалій у відеоряді камер відеоспостереження

У 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) [1, 10], k-Nearest Neighbors (k-найближчих сусідів), Bayesian Networks (Байєсовські мережі), Decision Tree (дерево рішень) та інші [11]. Однак для них трудомісткою і проблемною задачею є правильна установка міток. Крім того, відеодані містять шум, що призводить до частих хибних спрацьовувань системи.

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 аномальним. 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 [6, 12]. Як випливає із назви, для його навчання достатньо мати всього один клас – "чисті" спостереження без аномалій.

Ще один, третій, клас методів базується на припущенні [1], 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 - метод Isolation Forest (ізольований ліс) [13], який ґрунтується на "розбитті простору ознак детектованого відеоряду у вигляді так званих ізолюючих дерев, і аномаліями виявляються точки, що значно віддалені від інших" [1].

Ціле сімейство перспективних і поширених [1] 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 [1], ефективних методів, що дозволяють визначати моменти часу, коли відбуваються суттєві зміни в часовому ряді [14].

На жаль, лімітований 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 таким 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. Доведеться 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, у роботі [1] автори пропонують та самі зосередилися на використанні згорткової глибинної нейронної мережі, (CNN) [15]. Глибинні нейронні мережі набули широкого розвитку і поширення в різноманітних сферах завдяки їх високій ефективності при рішенні багатьох задач, роботі із зображеннями та відео [1]. Якщо вдасться повторити експерименти цих дослідників, можна почати з цього методу.

Висновки

У результаті проведення даного дослідження було виконано таке:

1) проведено огляд основних сучасних систем детектування аномалій у відеоряді камер відеоспостереження. Зроблений висновок, що відмінності між собою систем пошуку аномалій у відеоряді камер відеоспостереження обумовлені вибором методів для обробки відеоінформації;

2) проведено аналіз методів виявлення аномалій у відеоряді камер відеоспостереження. Для цього розроблено класифікацію сучасних методів виявлення аномалій у відеоряді та розглянуто основи теорії глибинних нейронних мереж з точки зору можливості їх застосування для класифікації, локалізації, сегментації, виявлення, ідентифікації та трекінгу об'єктів у відеоряді камер спостереження;

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

Література

1. Рувінська В.М., Девятков В.В. Відеоспостереження для систем безпеки: моделі, методи та запропоновані рішення. *Інформатика та математичні методи в моделюванні*. 2021. Том 11. № 4. С. 331-342.
2. Відеоспостереження. URL: https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D1%81%D0%BF%D0%BE%D1%81%D1%82%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F (дата звернення: 01.11.2022).
3. Відеореєстратор. URL: https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D1%80%D0%B5%D1%94%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80 (дата звернення: 01.11.2022).
4. Роботизированная камера SpeedDome Hikvision DS-2DF8C448I5XS-AELW(T5) DarkFighter с лазерной подсветкой. URL: https://vario.com.ua/ptz-robotizirovannaya-kamera-speeddome-hikvision-ds-2df8c448i5xs-aelwt5-darkfighter-s-lazernoy-podsvetkoy/?gclid=Cj0KCQjw4omaBhDqARIsADXULuUk4Pc554R11Rizwk_Fe8MZ6JRxC8HQB-AIl-2Jn7yc-Jp0fShCu6QaAlqCEALw_wcB (дата звернення: 01.11.2022).
5. Особливості камер відеоспостереження. URL: https://worldvision.com.ua/ru/kak-vybrat-naruzhnuu-kameru-rabotaushchuu-ot-batarei/ (дата звернення: 01.11.2022).
6. Pedregosa F. Scikit-learn: Machine Learning in Python. *JMLR*. 2011. No.12. P. 2825-2830. URL: https://www.jmlr.org/papers/volume12/pedregosa

11a/pedregosa11a.pdf (дата звернення: 01.11.2022).
7. Відеоаналітика. URL: https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D1%82%D0%B8%D0%BA%D0%B0 (дата звернення: 01.11.2022).
8. Gorodnichy D.O., Mungham T. Automated video surveillance: challenges and solutions. *ACE Surveillance (Annotated Critical Evidence) case study NATO SET-125 Symposium Sensor and Technology for Defence against Terrorism*. Mainheim, 2008.
9. Мусієнко Д.І. Проблеми сучасних систем відеоаналітики. *Сучасна спеціальна техніка*. 2014. № 2 (37). С. 75-81.
10. Omar S., Ngadi A., Jebur H.H. Machine Learning Techniques for Anomaly Detection: An Overview. *International Journal of Computer Applications*. 2013. V.79. No.2. URL: https://research.ijcaonline.org/volume79/number2/pxc3891478.pdf (дата звернення: 01.11.2022).
11. Larose D. T. Discovering Knowledge in Data: An Introduction to Data Mining. NY, Wiley, 2014. 336 p.
12. Vapnik V.N. Statistical Learning Theory. NY, John Wiley & Sons, 1998. 312 p.
13. Liu F., Ting K., Zhou Z. Isolation Forest. *ICDM'08. Eighth IEEE International Conference on Data Mining*. 2008. P. 413-422.
14. Van den Burg, Gerrit J. J., Williams, C. An Evaluation of Change Point Detection Algorithms. Cornell Univercity Arxiv. 2020. No.06222. URL: https://arxiv.org/pdf/2003.06222.pdf (дата звернення: 01.11.2022).
15. Babcock B., Babu S., Datar M. Motwani R., Widom J. Models and issues in data stream systems. *Proceedings of the 21st ACM Sigmod-Sigact-Sigart Symposium on Principles of Database Systems*. 2002. P. 1–16. URL: https://www.researchgate.net/publication/221559970_Models_and_Isues_in_Data_Stream_Systems (дата звернення: 01.11.2022).

References

1. Ruvins'ka V.M., Devyatkov V.V. Videosposterezhennya dlya system bezpeky: modeli, metody ta zaproponovani rishennya [Video surveillance for security systems: models, methods and proposed solutions]. *Informatyka ta matematychni metody v modelyuvanni - Informatics and Mathematical Methods in Simulation*. 2021, vol.11, no.4, pp. 331-342.
2. Videosposterezhennya [Video surveillance]. Available at: https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D1%81%D0%BF%D0%BE%D1%81%D1%82%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F (accessed 01 November 2022).
3. Videoreyestrator [Video recorder]. Available at: https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D1%80%D0%B5%D1%94%D1%81%D1%82%D1%80%D0%B0%D1%82%D0%BE%D1%80 (accessed 01 November 2022).
4. Robotizirovannaya kamera SpeedDome Hikvision DS-2DF8C448I5XS-AELW(T5) DarkFighter s lazernoy podsvetkoy [Robotic camera SpeedDome Hikvision DS-2DF8C448I5XS-AELW(T5) DarkFighter with laser illumination]. Available at: https://vario.com.ua/ptz-robotizirovannaya-kamera-speeddome-hikvision-ds-2df8c448i5xs-aelwt5-darkfighter-s-lazernoy-podsvetkoy/?gclid=Cj0KCQjw4omaBhDqARIsADXULuUk4Pc554R11Rizwk_Fe8MZ6JRxC8HQB-AIl-2Jn7ycJp0fShCu6QaAlqCEALw_wc B (accessed 01 November 2022).
5. Osoblyvosti kamer videosposterezhennya [Features of video surveillance cameras]. Available at: https://worldvision.com.ua/ru/kak-vybrat-naruzhnuu-kameru-rabotaushchuu-ot-batarei/ (accessed 01 November 2022).
6. Pedregosa F. Scikit-learn: Machine Learning in Python. *JMLR*. 2011, no.12, pp. 2825-2830. Available at: https://www.jmlr.org/papers/volume12/ pedregosa11a/pedregosa11a.pdf (accessed 01 November 2022).
7. Videoanalityka [Video analytics]. Available at: https://uk.wikipedia.org/wiki/%D0%92%D1%96%D0%B4%D0%B5%D0%BE%D0%B0%D0%BD%D0%B0%D0%BB%D1%96%D1%82%D0%B8%D0%BA%D0%B0 (accessed 01 November 2022).
8. Gorodnichy D.O., Mungham T. Automated video surveillance: challenges and solutions. *ACE Surveillance (Annotated Critical Evidence) case study NATO SET-125 Symposium Sensor and Technology for Defence against Terrorism*. Mainheim, 2008.
9. Musiyenko D.I. Problemy suchasnykh system videoanalityky [Problems of modern video analytics systems]. Suchasna spetsial′na tekhnika - Modern Special Technics. 2014, no.2 (37), pp. 75-81.
10. .Omar S., Ngadi A., Jebur H.H. Machine Learning Techniques for Anomaly Detection: An Overview. *International Journal of Computer Applications*. 2013, vol.79. no.2. Available at: https://research.ijcaonline.org/volume79/number2/pxc3891478.pdf (accessed 01 November 2022).
11. Larose D. T. Discovering Knowledge in Data: An Introduction to Data Mining. New York, Wiley, 2014. 336 p.
12. Vapnik V.N. Statistical Learning Theory. New York, John Wiley & Sons, 1998. 312 p.
13. Liu F., Ting K., Zhou Z. Isolation Forest. *ICDM'08. Eighth IEEE International Conference on Data Mining*. 2008, pp. 413-422.
14. Van den Burg, Gerrit J. J., Williams, C. An Evaluation of Change Point Detection Algorithms. Cornell Univercity Arxiv. 2020, no.06222. Available

at: https://arxiv.org/pdf/2003.06222.pdf (accessed 01 November 2022).
15. Babcock B., Babu S., Datar M. Motwani R., Widom J. Models and issues in data stream systems. *Proceedings of the 21st ACM Sigmod-Sigact-Sigart Symposium on Principles of Database Systems*. 2002, pp. 1–16. Available at: https://www.researchgate.net/publication/22155 9970_Models_and_Isues_in_Da-ta_Stream_Systems (accessed 01 November 2022).

Симбірський Геннадій Дмитрович, к. т. н., доцент кафедри інформатики та прикладної математики, simbir.gd@gmail.com, тел. 066-129-04-75.
Харківський національний автомобільно-дорожній університет, 61002, Україна, м. Харків, вул. Ярослава Мудрого, 25.

Analysis of methods for detection of anomalies in video series of video surveillance camera on vehicles

Abstract. Problem. *Video surveillance is a process of monitoring various objects, which is implemented with the use of video cameras - optical-electronic and microprocessor devices, designed for visual control of the environment, with the aim of the safety of life, activity and property of a modern person. Such processes and objects can be, for example, cars moving at an intersection, on a street or on a country road, a road surface during the control of its condition and quality, a security system of any infrastructure object.* ***Goal.*** *The purpose of the study is the analysis of the technical composition of systems for detecting anomalies in the video of video surveillance cameras and a comparative review of computational methods for processing the results of this observation. To achieve the goal, it is necessary to research literary sources, that is, articles in scientific journals, reports at conferences, articles on non-thematic web portals, monographs and textbooks, the names of which indicate the possibility of finding information useful for this research.* ***Methodology****. As part of the research task, we are interested in the technologies, systems and methods that have been proposed and developed for obtaining, processing and analyzing video sequences and images, including machine vision tasks, image classification, object and anomaly detection, image segmentation, etc.* ***Results.*** *As a result of this research, the following was done: 1) An overview of the main modern systems for detecting anomalies in the video series of video surveillance cameras was conducted. It was concluded that the differences between the anomaly detection systems in the video series of video surveillance cameras are due to the choice of methods for processing video information. 2) An analysis of methods of detecting anomalies in the video series of video surveillance cameras was carried out. For this purpose, a classification of modern methods of detecting anomalies in the video series was developed and the basics of the theory of deep neural networks were considered in terms of the possibility of their application for classification, localization, segmentation, detection, identification and tracking of objects in the video series of surveillance cameras.* ***Originality.*** *An overview of the main modern systems for detecting anomalies in the video series of video surveillance cameras was conducted. It was concluded that the differences between the systems for searching for anomalies in the video series of video surveillance cameras are determined by the choice of methods for processing video information. An analysis of the methods of detecting anomalies in the video series of video surveillance cameras was carried out.* ***Practical value.*** *The developed information system is already used to provide students of all educational institutions of Ukraine of the III level of accreditation with the information about our university; regarding the specialties offered by the university and the corresponding professions; regarding open days, preparatory courses and much more.*

Key words: *video series anomalies, anomaly detection systems, classification of anomaly detection methods, intelligent video surveillance cameras, video analytics.*

Simbirsky Gennady, Ph.D., Assoc. Prof., Department of Informatics and Applied Mathematics, tel. +38 066-129-04-75, simbir.gd@gmail.com
Kharkov National Automobile and Highway University, 25, Yaroslava Mudrogo str., Kharkov, 61002, Ukraine