DOI 10.15276/imms.v11.no4.331
УДК 004.056

Informatics and Mathematical Methods in Simulation
Vol. 11 (2021), No. 4, pp. 331-342

ВІДЕОСПОСТЕРЕЖЕННЯ ДЛЯ СИСТЕМ БЕЗПЕКИ: МОДЕЛІ, МЕТОДИ ТА ЗАПРОПОНОВАНІ РІШЕННЯ

В.М. Рувінська, В.В. Девятков

Національний університет «Одеська політехніка»
пр. Шевченка, 1, Одеса, 65044, Україна;
e-mail: victoriya.ruvinskaya@gmail.com, wladdew2016@gmail.com,

Проведено аналіз історії розвитку систем відеоспостереження, а також моделей, методів та технічних засобів, що використовуються у сучасних системах та запропоновано нові підходи для їх удосконалення. Проведено огляд існуючих рішень в області систем відеоспостереження, а саме: технічного забезпечення, функцій, структури і особливостей сучасних систем. Проаналізовані сучасні моделі та методи, що можуть бути використані для відеаналітики в системах відеоспостереження, такі як: пошук аномалій у відеоряді, глибині нейронні мережі для класифікації, локалізації, сегментації, виявлення, ідентифікації та трекінгу об'єктів у відеоряді. У наш час відеоспостереження набуло широкого поширення у зв'язку з швидким розвитком як апаратного забезпечення такого роду систем, так і різноманітних моделей і методів комп'ютерного зору, методів штучного інтелекту, зокрема, машинного навчання на основі глибинних моделей. Останнє дає змогу проводити більш якісну відеоаналітику і, таким чином, зменшити число помилкових спрацьовувань, як і в випадках, коли не виявляються важливі об'єкти та події при відеоспостереженні, так і навпаки, коли надаються помилкові сигнали тривоги. Отже треба модернізувати сучасні системи відеоспостереження у зв'язку з новими можливостями. Запропоновано для аналізу відеоряду з метою пошуку небезпечних/підозрілих подій використовуватися згорткову нейронну мережу YOLO; щоб знизити навантаження на сервер від використання нейронної мережі система аналізуватиме зміну поточного відеокадру по відношенню до попереднього і для цього використовувати моделі і методи детектування аномалій, а також принцип локальності. В результаті досліджень запропоновано вимоги до систем безпеки на основі відеоспостереження та підходи до їх розробки. Спроектована клієнт-серверна структура і функції системи. Розроблено дві початкові версії системи відеоспостереження, на основі яких далі можливо запроваджувати різні рішення і проводити експерименти. Описані застосована апаратура, випробуване програмне забезпечення, результати роботи.

Ключові слова: відеоспостереження, глибинні нейронні мережі, пошук аномалій, відеоаналітика.

Вступ

Відеоспостереження — це процесс спостереження, що реалізується із застосуванням оптико-електронних пристроїв, призначених для візуального контролю та автоматичного аналізу [1]. Для контролю навколишнього середовища з метою безпеки життєдіяльності в даний час широко використовуються системи відеоспостереження – комплекс обладнання та програмного забезпечення, призначений для моніторингу поведінки, дій або інформації з метою збирання інформації, впливу, управління та координації [2].

Актуальність відеоспостереження безперечна, сьогодні за допомогою Інтернету і бездротового зв'язку можна перебувати в курсі всіх подій, стежити, налаштовувати і дивитися за потрібною ділянкою або людьми з будь-якого куточка земної кулі. Такого роду системи підвищують рівень безпеки, здійснюють контроль у сфері житлово-комунального господарства, тощо, що корисно як для особистого використання, так і в професійній діяльності. Таким чином, системи відеоспостереження мають вплив на різноманітні сфери життя, але найбільшою мірою вони здобули популярності у сфері

безпеки, що є пріоритетною для людей та бізнесу, і в наш час в цій сфері вони використовуються повсюдно. І зараз такі системи безпеки можуть вбудовуватися в Smart House наступним чином: датчики, які там є, використовувати і для детектування підозрілих подій.

Перші системи відеоспостереження з'явились в середині 20 сторіччя, швидко і широко розповсюдились по світу і за короткий час у зв'язку з технічним прогресом, зокрема, в сфері інформаційних технологій значно просунулися у своєму розвитку. Але в наш час, тобто за останні приблизно 20 років, апаратні можливості, Інтернет, моделі і методи штучного інтелекту, включаючи комп'ютерний зір, машинне навчання, включаючи глибинні моделі, засоби автоматичного пошуку аномалій та інші настільки швидко розвинулись, що необхідно їх своєчасно впроваджувати в прикладні системи, зокрема, і в області відеоспостереження.

Мета роботи

Метою роботи є підвищення якості систем відеоспостереження на основі їх модернізації у зв'язку з новими можливостями в апаратному, математичному, алгоритмічному та програмному забезпеченню.

Для досягнення поставленої мети необхідно вирішити наступні задачі:

- провести огляд історії розвитку систем відеоспостереження;
- виконати аналіз існуючих рішень в області відеоспостереження та суміжних областей, результати яких потенційно можуть застосовуватися для такого роду систем;
- запропонувати рішення по модернізації систем відеоспостереження;
- розробити початкові версії систем відеоспостереження, на базі яких далі запроваджувати різні рішення і проводити експерименти.

Історія розвитку систем відеоспостереження

Однією з перших систем відеоспостереження, під якою розуміється структура для передачі і аналізу зображення на відстані, з'явилася в Німеччині в 1942 р., використовувалися камери і монітори для моніторингу в реальному часі, але не було можливості записувати зображення. Перша система, задіяна в комерційних цілях, випущена в 1949 р., використовувала дроти замість радіохвиль. 50-ті роки ознаменувалися появою кольорових відеокамер. Вже до 1965 р. камери громадського спостереження стають все більш поширеними. 1968 р.: в американському штаті Нью-Йорк встановили відеоспостереження з метою охорони правопорядку, при цьому камери відсилали зображення в департамент поліції цілодобово. У 1969 р. з'являється перша офіційна система відеоспостереження від Марі Ван Бріттан Браун, механізм складався з чотирьох очок і камери, що передав зображення на монітор. Нова епоха історії відеоспостереження почалась з винаходом на початку 70-х побутових ві-деомагнітофонів, при цьому відеозапис став доступним приватним особам, а камери почали з'являтися повсюдно. Технологія пристроїв із зарядним зв'язком з'явилася в 1976 р, що призвело до створення камер, які можуть використовуватися в умовах низької освітленості [3].

Значний стрибок стався в 1990-х, коли мультиплексні рішення знайшли визнання, така технологія дозволила об'єднати відеосигнали з декількох камер і відображати їх на одному моніторі. Відеореєстратори оснащуються жорсткими дисками, і зображення записується по колу, коли самий «свіжий запис» затирає найбільш ранній, також включається запис при виявленні руху. У камерах стали також з'являтися CMOS-матриці, дешевші ніж CCD. Перші IP-камери випускається в 1996 р, вони могли відправляти або отримувати інформацію через комп'ютерні мережі, що призвело до появи веб-камер. У 1998 р. в лондонському бюро вперше розмістили систему розпізнавання осіб. Прогрес в області цифрових технологій з початку тисячоліття привів до подальших поліпшень. Аналогові відеомагнітофони замінялись цифровими (DVR), мультиплексори тепер вбудовані в усі подібні пристрої, що спрощує установку і експлуатацію. Цифрове спостереження також позбавило від необхідності відеокасет, зображення стало передаватися за допомогою IP-камери через локальну мережу або інтернет. Відеореєстратор може

бути розташований в будь-якій точці світу, або можна обійтися і без нього, використавши для зберігання записів персональний комп'ютер. Починає розвиватися відеоаналітіка, здатна розпізнавати об'єкти і події в кадрі, за рахунок чого спостереження і аналіз відеозапису спростився. Бурхливий розвиток хмарних технологій відбувався на початку 2010-х, і це позначилось на відеоспостереженні. Там, де раніше зводили велику інфраструктуру з відеореєстраторами та серверами, що використовують аналітику, тепер достатньо застосувати сучасні хмарні відеокамери і забезпечити швидкий канал зв'язку. Дана обставина змінила спосіб зберігання інформації – не треба утримувати великі сервера, все це є в «хмарі». У хмарному сховищі дані зарезервовані, зашифровані і доступні в будь-який час [4].

Технічне забезпечення систем відеоспостереження

Всі системи відеоспостереження, незалежно від виду, включають такі технічні компоненти: блок живлення, кабель, жорсткий диск (HDD) для запису і зберігання відео з камер, монітор або комп'ютер для підключення безпосередньо до відеореєстратора для локального перегляду відеозапису, Інтернет для використання відеореєстратора з хмарним сервісом при перегляді відеозапису в онлайн режимі.

Прийнято виділяти кілька типів класичних систем відеоспостереження в залежності від використовуваного технічного оснащення [2, 5]:

- Аналогові. Склад комплектуючих: AHD/HD-CVI/HD-TVI камера відеоспостереження, відеореєстратор DVR.

- Цифрові. В їх основу покладено IP-технології. Мається на увазі використання IP відеокамер спільно з мережевими комутаторами. Склад комплектуючих: IP камера відеоспостереження, відеореєстратор NVR, мережевий комутатор (світч) для підключення відеокамер і відеореєстраторів до мережі.

- Змішані (гібридні). Принцип їх роботи засновано на двох етапах: прийом відеозображення з аналогових камер; оцифрування зображення.

Аналогові системи вважаються морально застарілі, проте в деяких ситуаціях використання саме цього типу цілком обґрунтовано [2]. Цифрові системи в даний час є найперспективнішими. Їх переваги в порівнянні з аналоговими системами наступні: покращена якість відеозображення; гнучкість і легка масштабованість; можливість глибокого аналізу і віддаленого налаштування; легкість інтеграцій в існуючу мережу; перспективність і розвиток. Гібридні системи вважаються найбільш поширеними. У них якість одержуваної картинки істотно поступається цифрового формату, проте інші параметри роботи цього типу нічим не відрізняються від аналогічних характеристик цифрових систем, що дає можливість створювати надійні і багатофункціональні системи змішаного типу.

Системи нового покоління активно використовують Інтернет і з цією метою мають в своєму складі: або камери-відеореєстратори для запису і збереження відеозображення, а також виконання функцій маршрутизатора, управління всіма відеокамерами, обробки запитів користувачів; або одну мережеву IP-камеру, такий варіант оптимальний для невеликих територій; або декілька мережевих камер для передачі інформації одночасно з декількох пунктів.

Функції існуючих систем відеоспостереження

Системи відеоспостереження нового покоління користуються великим попитом. Основні можливості і переваги таких систем [5]: вести спостереження в режимі реального часу; віддалено отримувати доступ до налаштувань і функцій управління системами, в тому числі для зміни способів запису й передачі повідомлень; повна відсутність обмежень на кількість і тип використаної апаратури; підключення до системи будь-якого електронного пристрою, що має необхідне програмне забезпечення, тобто комп'ютера, ноутбука, смартфона тощо.

При цьому використовуються такі переваги комп'ютера як: можливість роботи без втоми, інфрачервоний спектр, термодетекція, потужна оптика та інша апаратура, що перевищує ресурси людини, уповільнення, оглядовість та інше.

У програмному забезпеченні систем відеоспостереження передбачені функції реагування на конкретні сигнали, щоб в потрібний момент включався запис одержуваного відеозображення, тобто система може автоматично включити запис, якщо, наприклад, перед камерами почався якийсь рух, тощо; далі запис може бути переглянутий для вивчення і аналізу ситуації. Такі програмні можливості є невід'ємною частиною такого роду систем [5].

У багатьох містах України в останні роки активно розвиваються і розширюються системи відеоспостереження. Так в Одесі проект міського відеоспостереження стартував в 2018 р в рамках програми «Безпечне місто», і був створений «Центр інтегрованої системи відеоспостереження та відеоаналітики Одеси», або «Центр-077» [6]. Крім панорамної зйомки, системи розпізнають обличчя (встановлені на вокзалах) і автомобільні номери, при цьому в нічний час пригнічується зустрічне світло фар (встановлені на всіх центральних автомагістралях), Все, що потрапляє в об'єктив камер, будь то обличчя або номерний знак, автоматично зберігається в єдиній базі: відеоматеріал – на 14 днів, фотофіксація і геодані – до року.

Структура і особливості сучасних систем відеоспостереження

Одним із самих простих підходів, що використовуються при відеоспостереженні, є відеодетекція. 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. Самими суттєвим недоліком відеодетекції є низька перешкодостійкість. Якщо у зоні відеодетекції знаходяться гілки, що гайдаються від вітру, то точність значно знижується. І це потребує безвідривного ручного контролю у реальному часі або тривалого перегляду відеоархівів, щоб відстежити важливі події.

Відеоаналітика порівнює не статичні картинки і не пікселі як такі, а зміна характеру активності. 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 наступає 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 – «короткий логічний виклад відеоінформації шляхом розкладання її на семантичні одиниці (відеосюжети), кожен з яких має свій закінчений зміст, що відрізняється від попереднього і наступного відеосегмента» [7].

Відеосемантика спрацьовує не при кожному хитанні гілочки, а тільки один раз, коли змінилася погода, ставши вітряною. При цьому технологія «коротких даних» вкорочує все, зокрема і перешкоди. У панелі видачі результатів буде про хитання гілочки, але один раз за час вітряної погоди, це в тисячі разів менше кількох годин постійного відеозапису, зав'язаного на стандартну відеодетекцію. Одна з перших систем відеоспостереження, що працювала по технології «коротких даних» була ACE Surveillance [8]. Вона займається вилученням та обробкою анотованих критичних ділянок відеоспостереження. ACE складається з ACE Capture модуля та ACE Browser модуля. ACE Capture працює наступним чином: відеосигнал з камери відправляється на комп’ютер, в результаті запуска програмного забезпечення звучить сигнал тривоги при виявленні нового об’єкта або активності. Критичні моментальні знімки даних (CES) автоматично виявляються і зберігаються. Кожний CES забезпечений візуальними та текстовими ано-

таціями, що допомагають зрозуміти дані та підвищують керованість архівними даними. Анотації CES включають: місцезнаходження та розмір об'єкта, що рухається; напрямок; звідки з'явився об'єкт; швидкість. Браузер ACE відповідає за підготовку, ефективний перегляд і пошук архівних даних CES. Така структура системи має за мету спростити виявлення аномальних подій в величезній кількості даних, що зберігаються.

Пошук аномалій у відеоряді

Природно розглядати відео як послідовність кадрів, і суттєві зміни від одного кадру до іншого зазвичай можуть вказувати на виникнення нових ситуацій, і це розглядається як вихід із стану стабільності, тобто як аномалія.

Розглядають два типи задач, пов'язаних з пошуком аномалій [9]:

1) Виявлення так званих викидів (Outlier detection), які визначаються як спостереження, що лежать далеко від інших. Алгоритми для детектування викидів намагаються знайти регіони, де зосереджена основна маса даних, ігноруючи аномальні спостереження, тобто нетипові приклади, які заважають надалі для використання цих даних, зокрема, перед машинним навчанням їх прибирають.

2) Визначення незвичайного явища або ситуації, зокрема, аномальної поведінки (Novelty detection), коли є спостереження, що описують різноманітні звичайні стани системи, а потім з'явились нові дані, і треба визначити, чи є вони аномальними. Очевидно, що саме такий підхід як Novelty detection найбільшою мірою підходить для аналізу відеоряду і встановлення, чи є аномалії в новому кадрі порівняно з попередніми.

Існують різноманітні методи пошуку аномалій, і їх модна поділити на два типи: Supervised Anomaly Detection (навчання зі вчителем) і Unsupervised Anomaly Detection (навчання без вчителя) [10].

Для методів першого типу на вхід навчанню надходять дані з мітками, що встановлюють, чи аномалії, чи ні. А саме методи являють собою такі розповсюджені підходи як: Support Vector Machines (SVM), k-Nearest Neighbors, Bayesian Networks, Decision Tree та інші [11]. Однак для них трудомісткою задачею та, часто, і проблемною є правильна установка міток. І в результаті датасет містить шум, що призводить до частих хибних спрацьовувань.

Розглянемо далі навчання без вчителя, коли для даних, що надходять для навчання, невідомо, які з них нормальні, а які аномальні (що характерно для аналізу відеоряді). В цьому випадку використовуються різноманітні підходи.

Найпростіше рішення: для більшості задач тільки невеликий процент даних аномальні, тоді використовують кластеризацію, в результаті великі по розміру кластери відповідають нормальним даним, а малі – аномальним.

Іншим рішенням є моделювання тільки нормальних даних, при цьому будуються їх профіль. Одним із прикладів є метод One Class SVM – одна із форм класичного алгоритму SVM [9, 12]. Як випливає із назви, для його навчання достатньо мати всього один клас – "чисті" спостереження без аномалій. Загальна ідея: перетворити ознаковий простір (за допомогою Kernel Trick [12]) і провести розділяючу гіперплощину так, щоб спостереження лягли як можна далі від початку координат. В результаті одержуємо кордон, по одну сторону якого максимально щільно упаковані спостереження із «чистої» тренувальної вибірки, а по іншу – аномальні, не схожі з тими, що алгоритм «бачив» під час навчання. І, таким чином, аномалії визначаються як ті екземпляри в наборі даних, що не відповідають нормальному профілю.

Ще один підхід будується на припущенні, що аномалії не тільки нечисленні, але й в них є значення атрибутів, що значно відрізняються від значень численних звичайних екземплярів. Одним із прикладів цього типу є метод Isolation Forest [13], у якому проводиться розбиття простору ознак у вигляді так званих ізолюючих дерев, і аномаліями виявляються точки, що значно віддаленні від інших.

Одним із перспективних напрямків в зв'язку з тим, що кадри відео змінюються за часом, є розгляд відео у вигляді часового ряду. Для аналізу часових рядів і, зокрема,

вирішення задачі пошуку в них аномалій, або точок зміни (Change Point Detection), розроблено достатньо багато ефективних методів, що дозволяють визначати моменти часу, коли відбуваються суттєві зміни в часовому ряді [14].

Якщо задача полягає в тому, щоб аналізувати відеоряд в реальному часі, це актуально для сучасних систем відеоспостереження, то необхідно використовувати так званий online Change Point Detection, що виявляє точки змін у вхідному потоці даних. При offline Change Point Detection припускається, що ряд доступний у повному обсязі до начала аналізу.

Для детектування точок змін у часовому ряді онлайн використовуються різні методи:

- Статистичний послідовний аналіз - розділ математичної статистики, який вивчає статистичні методи, основані на послідовній вибірці, що формується в ході статистичного експерименту, і на кожному етапі вирішується, необхідні чи ще спостереження для оцінки [15].

- Регресія часового ряду [15] – побудувавши такого роду модель із даних, можна спрогнозувати тенденції, а далі порівняти прогнозовані та фактичні показники; значна різниця указує на відхилення або аномалію.

- Поточні алгоритми (streaming algorithms) - для обробки послідовності даних в один або мале число проходіsв; вирішують задачі, в яких дані надходять послідовно та у великому обсязі [16].

- Стандартизована оцінка, z-оцінка (Standard score, z-score) - це міра відносного розкиду спостереженого чи виміряного значення [15]; чим z-оцінка більша, тим вище вірогідність того, що в потоці значень є відхилення. Щоб знайти аномалії, треба встановити границі z-оцінок, що прийняті за нормальні; всі z-оцінки, що виходять за задані межі, будуть вважатися аномальними. Однак із-за фіксованого порогу можливі численні хибні спрацьовування.

- Перестановочні мартингали аналізують, чи може кожне значення ряду бути виявлено з рівною вірогідністю (властивість комутативності); такого роду комутативний ряд стабільний; порушення комутативності вказує на аномалії; для аналізу використовується машинне навчання онлайн, тобто моделі, що дозволяють виявляти аномалії, будуються і корегуються в реальному часі по мірі надходження нових спостережень [17].

Примітно, що саме останнє рішення взято за основу при розробці сервісу для детектування аномалій (Anomaly Detection Service) в Azure Marketplace, і воно було випробувано для пошуку суттєвих змін яскравості в кадрах відеоряду [18, 19].

Глибині нейронні мережі для класифікації, локалізації, сегментації, виявлення, ідентифікації та трекінгу об'єктів у відеоряді

Сучасні системи відеоспостереження у великих кампаніях та у державних установах часто використовують так звані «розумні» інтелектуальні технології на основі моделей та методів комп'ютерного зору, що виявляють об'єкти у відеоряді, також можуть знаходити їх властивості як і в кожному кадрі окремо, так і в динаміці. Сучасними базовими моделями для комп'ютерного зору є згорткові глибинні нейронні мережі, CNN [20]. Глибині нейронні мережі мають більш одного прихованого шару, перша така успішна мережа AlexNet, що була створена в 2012 р., містила 8 прихованих шарів. З того часу глибинні нейронні мережі набули широкого розвитку та поширення в різноманітних областях в зв'язку з тим фактом, що ознаки в таких мережах виявляються автоматично, а також завдяки їх високій ефективності при рішенні багатьох задач при роботі з зображеннями і відео.

Класифікація – це визначення основного об'єкту на зображенні та його класу. Для аналізу зображення з декількома важливими об'єктами служать задачі локалізації (або сегментації) та виявлення. Локалізація – це обведення кожного об'єкту на зображенні прямокутними рамками, сегментація – обведення контуру об'єкту, а виявлення – кла-

сифікація кожного об’єкту, локалізованого або сегментованого. Існують моделі та методи, що дозволяють вирішувати одночасно декілька із перерахованих задач, зокрема, глибинна нейронна мережа OVERFEAT [21] проводить класифікацію, локалізацію та виявлення об’єктів на зображеннях.

Для більш складних задач аналізу зображень, а також відео, наприклад, в судово-медичному розслідуванні на основі даних відеоспостереження [22] використовуються:

- ідентифікація, зокрема, розпізнавання осіб;
- створення анотацій, тобто невеликих текстів з описами, щоб зафіксувати найбільш інформативну динаміку в відео [23];
- трекінг, що дозволяє простежити положення певних виявлених об’єктів у часі, тобто у різних кадрах відео [24].

В наш час для глибинних моделей широко використовується перенос навчання (transfer learning) [25]. Для вирішення конкретної задачі використовується так звана переднавчена мережа, навчена раніше для іншого завдання на великій кількості даних і, наприклад, для класифікації для великої кількості категорій. При цьому отримано високу точність. Нехай для конкретної нової задачі є невелика кількість даних, і категорій менше, і вони не повністю збігаються з категоріями передбачуваної мережі, але близькі до них. Ідея transfer learning - ознаки, які вийшли при навчанні одних категорій, перенести на інше завдання, донавчаючи переднавчену мережу на нових даних. При цьому точність отриманої після навчання моделі вище, ніж якби ми навчали мережу з нуля на новій невеликій кількості даних.

Система відеоспостереження, вимоги та запропоновані рішення

Для вирішення завдання збереження безпеки для об'єкту, що спостерігається, застосовують відеоспостереження, однак оскільки людина не в змозі постійно стежити за тим, що відбувається на багатьох моніторах, система повинна самостійно розпізнавати і виділяти небезпечні / підозрілі ситуації. Така система буде отримувати трансльований відеозапис з камер відеоспостереження і самостійно проводити аналіз того, що відбувається, що дозволить знизити навантаження на оператора, тим самим зменшивши ймовірність ігнорування небезпечної ситуації. Тобто пропонована система складається з однією або декількох відеокамер, що транслює те, що відбувається, а також програмного забезпечення, яке оброблятиме трансляцію на предмет пошуку ситуацій, на які треба акцентувати увагу оператора, за допомогою відеоаналітики.

Дуже цінною особливістю відеоспостереження буде можливість записувати відео навіть при вимкненій електриці, оскільки зловмисники, якщо спробують проникнути, наприклад, в приватний будинок, швидше за все, в першу чергу вимкнуть електрику. Відеокамера повинна бути обладнана акумулятором і картою пам'яті, щоб продовжити запис навіть у разі відключення зовнішнього джерела живлення, наприклад, якщо зловмисники спробують знеструмити квартиру. У разі відключення зовнішнього джерела живлення локального дискового простору та акумулятора вистачатиме як мінімум на добу відеозапису. Але використання акумулятора вимагає особливих економічних до витрат батареї алгоритмів обробки відеокадрів.

Відеокамера повинна мати хорошу якість запису в темний час доби, оскільки швидше за все зловмисники діятимуть саме в цей час доби. Доцільно також встановити датчик руху, тоді такий набір обладнання забезпечує максимально ефективний і точний аналіз інформації в нічний час доби.

Система буде виконувати інтелектуальну архівацію відеозаписів, оптимальна схема для економії пам'яті, займаної відеозаписами, полягає в тому, щоб зберігати повне відео за останню добу, а також окремі ділянки відео, в яких була помічена підозріла активність, за 10 секунд до початку активності і аж до моменту, плюс 10 секунд після завершення активності. Користувачам надсилаються повідомлення про підозрілі активності в реальному часі.

Система відеоспостереження розробляється як клієнт-серверна.

Сервер разом з основною програмною системою обробляє трансляцію на предмет пошуку підозрілих ситуацій, акцентуючи увагу оператора на тому, що відбувається.

Клієнт дозволяє будь-кому, хто пройшов авторизацію, побачити трансляцію з відеокамер, отримувати повідомлення у разі підозрілих подій, а також мати доступ до відеоархіву небезпечних ситуацій. У разі втрати з'єднання між відеокамерою та сервером на клієнтську програму має надходити повідомлення про можливу підозрілу активність.

Для сервера і клієнта потрібен доступ до Інтернет. Діаграма, що показує роботу запропонованої системи відеоспостереження, показана на рис. 1.

Пропонується відеоаналітику підключати у вигляді окремих модулів, кожен з яких повинен мати один і той же заздалегідь спроектований інтерфейс, і, таким чином, з'явиться можливість легко масштабувати систему поступово нарощуючи її інтелектуальність.

Порівняння запропонованої системи з аналогами наведено в таблиці 1.

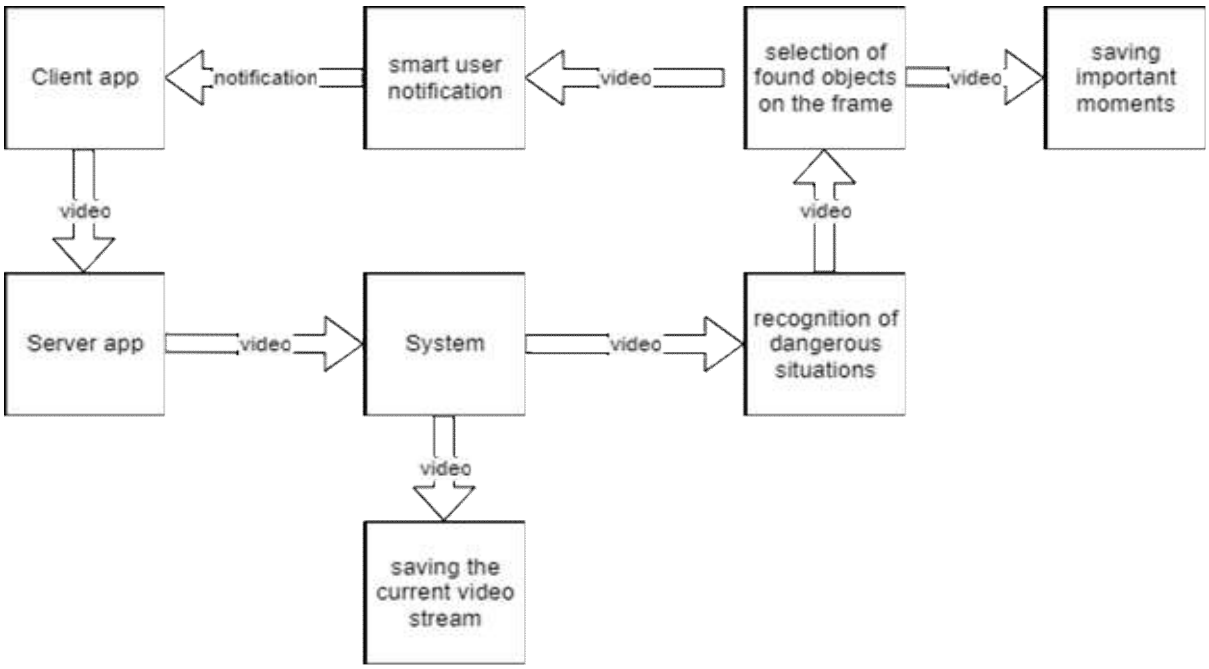

Рис. 1. Структура та функції пропонованої системи відеоспостереження

Було вирішено розробити початковий варіант системи відеоспостереження, на основі якої далі можливо запроваджувати різні рішення і проводити експерименти.

Застосована апаратура: процесор Intel Core I7, графічний адаптер NVIDIA GFORCE DX 1050.

Випробуване програмне забезпечення:

- Нейронна мережа YOLO (You Only Look Once) [26] версія v4 – архітектура CNN, що використовується для розпізнавання множинних об'єктів на зображеннях. Працює ефективніше, тобто швидше за інші архітектури завдяки роботі в один прохід по зображенню, що важливо для обробки відео.

- Бібліотека OpenCV [27], що застосовується для розробки та навчання нейронних мереж, версія 4.5.4. Вибрана, тому що показує більшу швидкодію порівняно з аналогами, наприклад, Tensorflow. Для зв'язку з YOLO використовується функція readNet from Darknet, що загружає YOLO в OpenCV.

Таблиця 1

Порівняльні характеристики розглянутих систем відеоспостереження

Характеристики розглянутих систем відеоспостереження	ACE Surveillance	Anomaly Detection Service	GoalCity	Запропонована система
Детектування аномалій для сусідніх кадрів	-	+	-	+
CNN	-	-	+	+
Короткі дані	+	-	+	+
Клієнт-серверна архітектура	+	-	+	+
Інтелектуальна архівація відеозаписів	+	-	+	+
Сповіщення користувача про підозрілі / небезпечні ситуації	+	-	+	+

Розроблена програма виводить вікно, в якому відтворюється відео і виділяються об’єкти тих класів, що може знаходити YOLO. Такі об’єкти виділяються рамочкою, і пишеться назва класу об’єкту, що розпізнано (рис. 2).

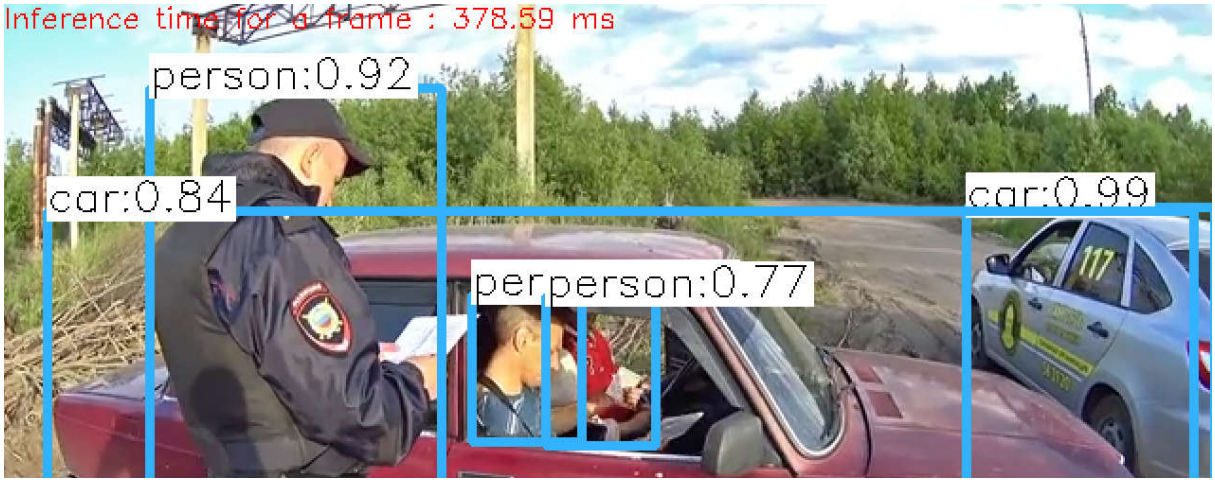

Рис. 2. Вікно системи відеоспостереження з локалізованими об’єктами та їх класами

В першій версії системи використовувався CPU. При запуску на відео, у якому роздільна здатність кадра 416*416, обробка здійснювалась з частотою кадра 1-1.5 кадрів в секунду, що занадто повільно, комфортна для людини частота - 30 кадрів в секунду.

В другій версії підключили GPU до OpenCV, для цього використовували декілька додаткових бібліотек:

- NVIDIA CUDA Toolkit для розробки середи для створення високо-ефективних застосувань на базі GPU [28];

- CUDA Deep Neural Network library (cuDNN) – бібліотека з GPU-прискоренням, що містить примітиви для глибинних нейронних мереж [29].

В результаті таких налаштувань обробка відео стала здійснюватися значно швидше з частотою 10-12 кадрів в секунду.

Надалі для аналізу відеоряду система буде використовуватися нейронну мережу YOLO. За її допомогою будуть вирішуватися наступні задачі:

1) Пошук на зображенні руху, виявлення людей, їх ідентифікацію, виділення небезпечних ситуацій, таких як відкритий вогонь або пожежа та інше.

2) Перенос навчання та донавчання глибинної нейронної мережі на нових даних (зображеннях, відео), що представляють нормальні ситуації для конкретного об'єкта, для якого потрібно забезпечити безпеку за допомогою відеоспостереження. І, таким чином, в результаті навчання нейронної мережі отримаємо на останньому шарі узагальнене графічне уявлення всіх нормальних ситуацій для конкретного об'єкта; далі пе-

ретворимо це на вектор ознак. При детектуванні поточну ситуацію (поточний кадр) порівнюємо з вектором ознак узагальненої нейронної мережі, що навчанна на прикладах нормальних ситуацій за допомогою введеної відстані.

Для того, щоб знизити навантаження на сервер від використання нейронної мережі і, таким чином, досягти комфортної для людини частоти кадрів в одиницю часу, система аналізуватиме зміну поточного відеокадру по відношенню до попереднього. Це дозволить істотно знизити навантаження на сервер, так як більшу частину часу, якщо система стоїть в режимі охорони, вона має справу зі статичним зображенням, на якому може змінюватися хіба що освітлення і тіні. Тобто, щоб довести обробку кадрів до прийнятної для людини частоти, треба обробляти не всі кадри, а частину з них, або в сусідніх кадрах обробляти не все зображення, а тільки ті об’єкти, що доцільно відслідковувати. Але треба мати на увазі, що не можна пропускати важливі для аналізу відеоспостереження кадри. Щоб це виявити, пропонується:

- по-перше, детектування аномалій за допомогою пошуку суттєвих змін або в яскравості кадрів відеоряду або в джерелах освітлення на базі різних методів, описаних вище, зокрема, перестановочних мартингалів;
- по-друге, використовувати принцип локальності, а саме, якщо знайдено важливий об’єкт на попередньому кадрі, то доцільно шукати його не по всьому зображенню поточного кадру, а десь поряд.

Висновки

Проведено огляд існуючих рішень в області систем відеоспостереження, а саме:

- технічного забезпечення,
- функцій,
- структури і особливостей сучасних систем.

Проаналізовані сучасні моделі та методи, що можуть бути використані для відеаналітики в системах відеоспостереження, такі як:

- пошук аномалій у відеоряді,
- глибині нейронні мережі для класифікації, локалізації, сегментації, виявлення, ідентифікації та трекінгу об’єктів у відеоряді.

Пред’явлені вимоги до системи відеоспостереження, що буде застосуватися для надання безпеки, спроектована клієнт-серверна структура і функції системи. Проведено порівняння з аналогами.

Розроблено дві початкові версії системи відеоспостереження, на основі яких далі можливо запроваджувати різні рішення і проводити експерименти. Описані застосована апаратура, випробуване програмне забезпечення, результати роботи.

Запропоновано для аналізу відеоряду з метою пошуку небезпечних/підозрілих подій використовувати згорткову нейронну мережу YOLO, для якої за допомогою переносу навчання провести донавчання на нових даних, що представляють нормальні ситуації для конкретного об'єкта, для якого потрібно забезпечити безпеку за допомогою відеоспостереження. При детектуванні для поточного кадру використовувати навчену узагальнену нейронну мережу.

Щоб знизити навантаження на сервер від використання нейронної мережі система аналізуватиме зміну поточного відеокадру по відношенню до попереднього і для цього використовувати моделі і методи детектування аномалій, зокрема перестановочні мартингали, а також принцип локальності.

Список літератури

1. Monahan T., Wood M., David. Surveillance Studies: A Reader. New York: Oxford University Press, 2018.
2. Актуальность и необходимость использования систем видеонаблюдения. URL: https://golossokal.com.ua/ru/cikavo/aktualnost-neobxodimost-ispolzovaniya-sistem-video.html
3. История видеонаблюдения Европы и США. URL: https://dneprsecurity.com/statji/ istorija-videonabljudenija.html
4. История видеонаблюдения: путь от телевизора и Третьего рейха до облаков и нейросетей. URL: https://habr.com/ru/company/ivideon/blog/313586
5. Особенности камер видеонаблюдения. URL: https://worldvision.com.ua/kak-vybrat-naruzhnuu-kameru-rabotaushchuu-ot-batarei/
6. В Одессе заработала муниципальная система видеонаблюдения «Безопасный город». URL: https://itc.ua/news/v-odesse-zarabotala-munitsipalnaya-sistema-videonablyudeniya-bezopasnyiy-gorod/
7. Система событийного видеонаблюдения GOALCity. URL: https://www.goal.ru/ videonabludenie/what-is_videoanalitika/
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.* 2008. URL: https://www.researchgate.net/publication/229040125_Automated_video_surveillance_challenges_and_solutions_ACE_Surveillance_Annotated_Critical_Evidence_case_study
9. Pedregosa. Scikit-learn: Machine Learning in Python. *JMLR.* 2011. No.12, P. 2825-2830.
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: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.402.6779&rep=rep1&type=pdf
11. Larose D. T. Discovering Knowledge in Data: An Introduction to Data Mining. 2014. P. 336. ISBN: 978-0-470-90874-7.
12. Vapnik V.N. Statistical Learning Theory. John Wiley & Sons, 1998.
13. Liu F.T., Ting K.M., Zhou Z.H. Isolation Forest. ICDM'08. *Eighth IEEE International Conference on Data Mining.* 2008. P. 413-422.
14. Van den Burg, Gerrit J. J., Williams, C.K.I. An Evaluation of Change Point Detection Algorithms. 2020. URL: https://arxiv.org/abs/2003.06222
15. Ивченко Г.И., Медведев Ю.И. Математическая статистика: Учебник. М.: Либроком, 2014. 352 с.
16. 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. doi:10.1145/543613.543615.
17. Fedorova V., Gammerman A., Nouretdinov I., Vovk V. Plug-in martingales for testing exchangeability on-line. *Proceedings of the 29th International Conference on Machine Learning (ICML-12).* 2012. P. 1639-1646.
18. Time Series Anomaly Detection. URL: https://docs.microsoft.com/en-us/azure/machine-learning/studio-module-reference/time-series-anomaly-detection
19. Рувинская В.М., Девятков В.В., Андросов А.Г. Поиск аномалий для систем видеонаблюдения. Інформаційні управляючі системи і технології. *Матеріали X Міжнародної науково-практичної конференції.* Одеса, 2021. С. 69 – 71.
20. Николенко А. Кадурин Е., Архангельская С. Глубокое обучение. Погружение в мир нейронных сетей. СПб.: Питер, 2018. 449с.

21. Sermanet P., Eigen D., Zhang X., Mathieu M., Fergus R., LeCun Y. OverFeat: Integrated Recognition, Localization and Detection using Convolutional Networks. 2014. URL: https://arXiv: 1312.6229.
22. Xiao J., Li S., Xu Q. Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation. *IEEE Access.* 2019, V.7, P. 55432-55442, DOI: 10.1109/ACCESS.2019.2913648.
23. Wu Z., Yao T., Jiang Y. Gang. Deep Learning for Video Classification and Captioning. *Frontiers of Multimedia Research*. 2016. URL: https://arxiv.org/abs/1609.06782
24. Luo W., Xing J., Milan A., Zhang X., Liu W., Kim T.K. Multiple object tracking: A literature review. *Artificial Intelligence.* 2021. V. 293. 103448.
25. Fuzhen Zhuang, Zhiyuan Qi, Keyu Duan, Dongbo Xi, Yongchun Zhu, Hengshu Zhu, Hui Xiong, Qing He. *A Comprehensive Survey on Transfer Learning*. 2020. URL: https://arxiv.org/abs/1911.02685
26. Bochkovskiy A., Wang C.Y., Liao H.Y.M. YOLOv4: Optimal Speed and Accuracy of Object Detection. 2020. URL: https://arxiv.org/pdf/2004.10934v1.pdf
27. OpenCV. Open-Source Computer Vision. URL: https://docs.opencv.org/4.x/
28. Nvidia Cuda Toolkit. Release Notes for CUDA 11.5.1. URL: https://docs.nvidia.com/cuda/ pdf/ CUDA_Toolkit_Release_Notes.pdf
29. NVIDIA cuDNN. URL: https://developer.nvidia.com/cudnn

VIDEO SURVEILLANCE FOR SECURITY SYSTEMS: MODELS, METHODS AND PROPOSED SOLUTIONS

V. Ruvinskaya, V. Devyatkov

National Odessa Polytechnic University,
1, Shevchenko Ave., Odessa, 65044, Ukraine; email: wladdew2016@gmail.com, victoriya.ruvinskaya@gmail.com

The history analysis of video surveillance systems, as well as models, methods and technical means used in modern systems were carried out and was proposed new approaches to improve them. A review of existing solutions in the field of video surveillance systems was carried out, namely: hardware, functions, structure and features of modern systems. Modern models and methods that can be used for video analytics in video surveillance systems are analyzed, such as: anomalies detection, deep neural networks for classification, localization, segmentation, detection, identification and tracking of objects in the video. Nowadays, video surveillance has become widespread due to the rapid development of both hardware and computer vision, methods of artificial intelligence, in particular, machine learning based on deep models. These achievements can be used for better video analytics and thus reduces the number of false alarms, as in cases where important objects and events are not detected during video surveillance, and vice versa, when false alarms are given. Therefore, modern video surveillance systems need to be modernized using new possibilities. It is proposed to use the YOLO convolutional neural network to analyze the video in order to search for dangerous / suspicious events; to reduce the load on the server from the use of the neural network, the system will analyze the change of the current video frame compared to the previous one and use models and methods to detect anomalies, as well as the principle of locality. As a result of research, the requirements for security systems based on video surveillance and approaches to their development are proposed. The client-server structure and functions of the system are designed. Two initial versions of the video surveillance system have been developed. On this basis it is possible to implement various solutions and conduct experiments. The applied equipment, tested software, results of work are described.

Keywords: video surveillance, deep neural networks, anomalies detection, video analytics