МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

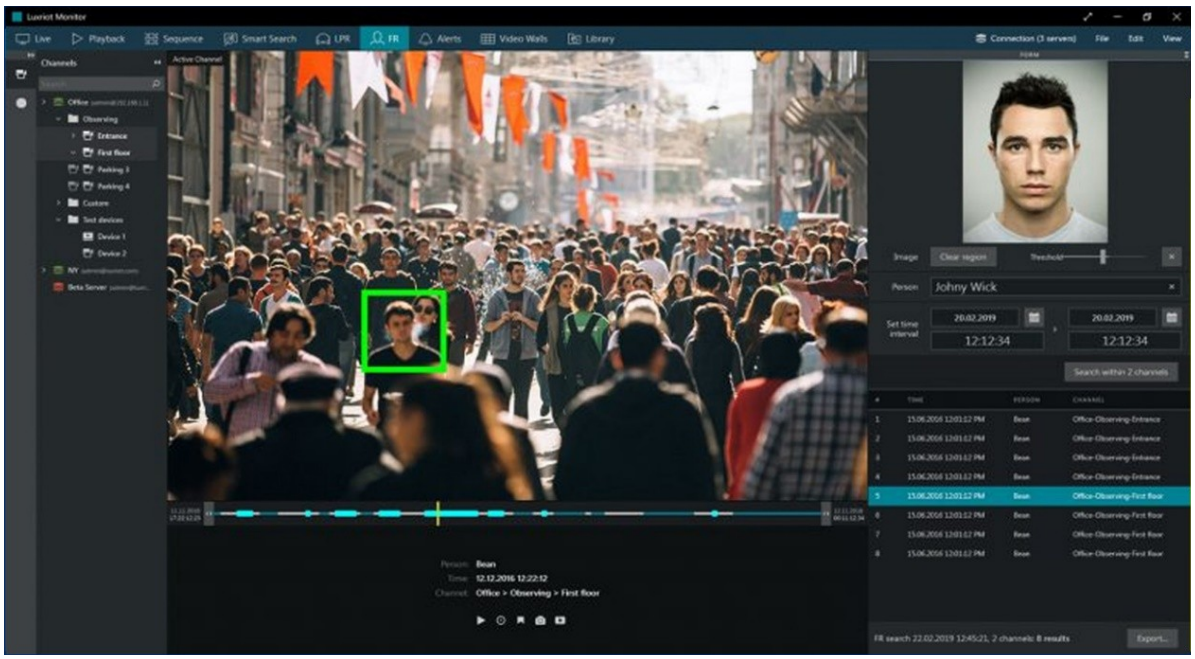
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ

ДЕПАРТАМЕНТ КРИМІНАЛЬНОГО АНАЛІЗУ

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІДЕОАНАЛІЗУ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З РОЗПІЗНАВАННЯ ОБЛИЧ ТА ІНШИХ ОБ'ЄКТІВ У КРИМІНАЛЬНОМУ АНАЛІЗІ

Методичні рекомендації



КИЇВ-2025

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ДЕПАРТАМЕНТ КРИМІНАЛЬНОГО АНАЛІЗУ

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІДЕОАНАЛІЗУ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З РОЗПІЗНАВАННЯ ОБЛИЧ ТА ІНШИХ ОБ'ЄКТІВ У КРИМІНАЛЬНОМУ АНАЛІЗІ

Методичні рекомендації

КИЇВ-2025

УДК 004.932+343.982.323+343.985.3
О-72

Авторський колектив:

Буренко О. В. (НАВС);
Бутко Р. Ю. (ДКА НП України);
Жадан Д. О. (ХНУВС);
Корнейко О. В., кандидат технічних наук, професор (НАВС);
Манжай О. В., кандидат юридичних наук, професор (ХНУВС);
Мордвинцев М. В., кандидат технічних наук, доцент (ХНУВС);
Овсянюк Д. І. (НАВС);
Пашнєв Д. В., кандидат юридичних наук, доцент (ХНУВС);
Сальніков І. І. (ДКА НП України);
Світличний В. А., кандидат технічних наук, доцент (ХНУВС);
Сивун А. С. (ДКА НП України);
Школьніков В. І., доктор філософії, доцент (НАВС).

Рецензенти:

Звєрєв В. П., кандидат технічних наук, старший науковий співробітник (Апарат Ради національної безпеки та оборони України);

Юдін О. К., доктор технічних наук, професор (Державний науково-дослідний інститут технологій кібербезпеки та захисту інформації).

Робота виконана відповідно до п. 2.9 Плану наукової роботи МВС України на 2024 рік, затвердженого наказом МВС України від 28.12.2023 № 108. Схвалено та рекомендовано до друку науково-методичною радою Національної академії внутрішніх справ 23 грудня 2025 року (протокол № 11).

О-72 Особливості використання технологій відеоаналізу та програмного забезпечення з розпізнавання облич та інших об'єктів у кримінальному аналізі : метод. реком. / за заг. ред. Р. Ю. Бутка та О. В. Корнейка. Київ : Вид-во НАВС, 2025. 86 с.

Розглянуті: системи відеомоніторингу, відеодані з яких можуть бути джерелами інформації для проведення відеоаналізу; теоретичні основи сучасних методів та технологій виявлення та розпізнавання на відеоданих фізичних осіб по їх фізичним, фізіологічним чи поведінковим ознакам, а також транспортних засобів та інших об'єктів. Наведені приклади щодо використання відповідного програмного забезпечення з розпізнавання облич та інших об'єктів у правоохоронній сфері.

Призначено для практичних працівників підрозділів кримінального аналізу Національної поліції України. Може бути корисним для здобувачів вищої освіти, наукових та науково-педагогічних працівників закладів вищої освіти системи МВС України.

УДК 004.932+343.982.323+343.985.3

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АРП	–	автоматичне регулювання підсилення
БпЛА	–	безпілотний літальний апарат
ГПК	–	Господарський процесуальний кодекс
ІАК	–	інформаційно-аналітичний комплекс
ІТТ	–	ізолятор тимчасового тримання
ЗНМ	–	згорткова нейронна мережа
КАС	–	Кодекс адміністративного судочинства
КПК	–	Кримінальний процесуальний кодекс
ЛБШ	–	локальні бінарні шаблони
МГК	–	метод головних компонент
НП	–	Національна поліція
ОРД	–	оперативно-розшукова діяльність
ПЗЗ	–	прилади із зарядовим зв'язком, англ. Charge Coupled Device, CCD
ТЗ	–	транспортний засіб
ЦПК	–	Цивільний процесуальний кодекс
CCTV	–	англ. Closed Circuit TeleVision, замкнута телевізійна система
CMOS	–	англ. Complementary-symmetry/Metal-Oxide Semiconductor, технологія побудови логічних електронних схем
DCT	–	англ. Discrete-Cosine Transformation, перетворення дискретного косинуса
IP	–	англ. Internet Protocol, Інтернет-протокол
KLT	–	англ. Karhunen-Loeve Transform, перетворення Кархунена-Лоева
MJPEG	–	англ. Motion Joint Photographic Experts Group, стандарт покадрового цифрового стиснення відеосигналів
MPEG-4	–	стандарт цифрового стиснення аудіо- і відеосигналів, прийнята експертами MPEG (англ. Moving Picture Experts Group)
H.264	–	стандарт розширеного стиснення відеофайлів, ще має назву MPEG-4/AVC (англ. Advanced Video Coding)
H.265	–	стандарт високоефективного стиснення відеофайлів, ще має назву HEVC (англ. High Efficiency Video Coding)
USB	–	англ. Universal Serial Bus, універсальний стандарт для передачі даних

ВСТУП

На даний час кримінальний аналіз є сучасним, швидким та дієвим механізмом допомоги в розкритті та попередженні злочинів, який доповнює роботу оперативників і слідчих [1]. За своєю суттю кримінальний аналіз є складною сферою діяльності, яка охоплює інформаційно-пошукову та аналітичну роботу й містить елементи оперативно-розшукової діяльності [2-4].

Основне завдання працівників підрозділів кримінального аналізу – «оперативне» надання ініціаторам (керівництву, підрозділам кримінальної поліції та досудового розслідування) достовірної, актуальної, об'єктивної і повної інформації з метою ефективного виконання завдань, визначених ст. 2 Закону України «Про Національну поліцію» [1].

Важливою підтримкою цієї роботи підрозділами кримінального аналізу є успішне використання можливостей різноманітних систем відеомоніторингу по отриманню відеоданих щодо відповідних подій та об'єктів, проведення їх аналізу за рахунок використання сучасних технологій на програмного забезпечення, що дозволяє своєчасно виявити та розпізнати відповідних осіб, їх дії, транспортні засоби, зброю та інші об'єкти.

Тому володіння працівниками підрозділів кримінального аналізу відповідними теоретичними знаннями щодо цієї сфери діяльності, методично правильне використання засобів та програмного забезпечення відеоаналізу є важливим фактором успішного виконання ними службових завдань.

Саме цим питанням і присвячене відповідне науково-методичне видання, що підготовлено авторським колективом фахівців Національної академії внутрішніх справ (НАВС), Харківського національного університету внутрішніх справ (ХНУВС) і Департаменту кримінального аналізу Національної поліції України (ДКА НП України) за результатами виконання відповідної науково-дослідної роботи.

У розділі 1 використані матеріали, що підготовлені науковцями ХНУВС та НАВС. Матеріали розділу 2 підготовлені науковцями НАВС (О. Буренко за участю О. Корнейка). Матеріали розділу 3 підготовлені науковцями НАВС (О. Корнейко, Д. Овсянюк, В. Школьніков) з використанням матеріалів наданих науковцями ХНУВС (М. Мордвинцев, Д. Пашнєв). Матеріали розділу 4 підготовлені фахівцями ДКА НП України за участю науковців ХНУВС і НАВС. Упорядкування матеріалів роботи здійснив О. Корнейко, а загальне редагування матеріалів видання – начальник ДКА НП України Роман Бутко за участю професора НАВС Олександра Корнейка.

Підготовлена авторським колективом робота призначена, насамперед, для практичних працівників підрозділів кримінального аналізу Національної поліції України, а також може бути корисною для здобувачів вищої освіти, наукових та науково-педагогічних працівників закладів вищої освіти системи МВС України.

1. СИСТЕМИ ВІДЕОМОНІТОРИНГУ ЯК ДЖЕРЕЛА ОТРИМАННЯ ВІДЕОДАНИХ ПРО ОСІБ ТА ІНШІ ОБ'ЄКТИ ПІДРОЗДІЛАМИ КРИМІНАЛЬНОГО АНАЛІЗУ

1.1. Загальні принципи побудови систем відеомоніторингу

Відеомоніторинг є сучасним і ефективним засобом забезпечення безпеки та контролю, що здійснює безперервний систематичний процес збору та обробки даних щодо стану публічної безпеки, який здійснюється засобами відеомоніторингу, що є технічними засобами, які призначені для обробки даних (камери з функціями детектування обличчя, охорони периметру, керування трафіком, визначення задимлення, вибухів, несанкціонованого залишення предметів тощо) [5].

Відповідно до [5] в інтересах забезпечення публічної безпеки відеомоніторинг повинен здійснюватися цілодобово та автоматично за:

– інформаційними об'єктами, до яких належать фізичні особи, а також транспортні засоби;

– публічними місцями;

– об'єктами критичної, соціальної, економічної, житлово-комунальної, транспортної, інженерної та іншої інфраструктури, а саме:

– парками, рекреаційними зонами, садами, скверами та майданчиками;

– пам'ятками культурної та історичної спадщини;

– вулицями, дорогами, провулками, пішохідними та велосипедними доріжками;

– автомобільними стоянками та майданчиками для паркування транспортних засобів;

– іншими територіями загального користування;

– об'єктами міської інфраструктури (соціальними, інженерними та транспортними);

– засобами організації дорожнього руху;

– будівлями, спорудами, в яких розташовані органи державної влади або органи місцевого самоврядування, підприємства, установи та організації державної, комунальної форми власності;

– територіями, будівлям, спорудами закладів освіти, охорони здоров'я та приміщень в них;

– об'єктами підвищеної небезпеки;

– речами і предметами.

Відеомоніторинг передбачає широке використання технічних засобів відеореєстрації (камер відеоспостереження) разом з відповідним

телекомунікаційним, серверним обладнанням, аналітичними технологіями для відстеження подій на перелічених вище об'єктах моніторингу в реальному часі.

Структурно система відеомоніторингу зазвичай складається з таких складових:

– засобів відеофіксації (аналогових та цифрових відеокамер);

– програмно-апаратного комплексу відеореєстрації, обробки та зберігання даних, що розміщається в центрі обробки даних;

– каналів передачі даних від засобів відеофіксації до обладнання програмно-апаратного комплексу відеореєстрації, обробки та зберігання даних, включаючи необхідне мережеве обладнання (пасивне та активне);

– автоматизованих робочих місць адміністратора системи та автоматизованих робочих місць користувачів інформації в системі відеомоніторингу;

– моніторингового центру, який забезпечує відображення відеоданих, що надходять до центру обробки даних, віддалених автоматизованих робочих місць (ситуаційних центрів, оперативних штабів тощо);

– відповідної комплексної системи захисту інформації, що є взаємопов'язаною сукупністю організаційних та інженерно-технічних заходів, засобів і методів захисту інформації в системі відеомоніторингу;

– платформи збору та аналітичної обробки даних – сукупності, серверного обладнання та програмного забезпечення, яке забезпечує обробку та аналіз даних в системі;

– інших технічних засобів.

Тобто структурно систему відеомоніторингу можна представити як сукупність системи відеоспостереження, яка здійснює фіксацію, обробку та зберігання відеозображень (відеоданих), та системи відеаналітики, що здійснює автоматизований аналіз цих відцифрованих відеозображень (відеоданих) з використанням спеціального програмного забезпечення з метою відеомоніторингу стану публічної безпеки.

На даний час системи відеомоніторингу вже широко застосовуються для забезпечення громадської безпеки та порядку на місцевому рівні, в системах охорони банків, торговельних центрів, розважальних закладів, промислових підприємств, інших комерційних і некомерційних організацій, а також володінь громадян. Вони надають змогу здійснювати швидке реагування на небезпечну ситуацію, спостереження за персоналом та відвідувачами, мають широке застосування та перспективи в області контролю за дорожнім рухом тощо [6].

Відповідно до [7] станом на вересень 2024 року на території України працює понад 60 тисяч камер відеоспостережень, які функціонують у понад 600 системах відеомоніторингу, що належать суб'єктам різних форм власності. Тільки у Києві на 1 тисячу населення встановлено 2 камери відеоспостереження, а на автодорогах державного значення функціонують 244 комплекси автофіксації.

На теперішній час найбільше застосування в системах відеомоніторингу знаходить технологія побудови систем відеоспостереження за схемою «замкнутої телевізійної системи» (Closed Circuit TeleVision, CCTV).

Іншими словами CCTV – це система відеоспостереження, де відеосигнали передаються між спеціальними пристроями, такими як (рис. 1.1):

– відеокамери;
– комутаційні пристрої;
– пристрої відображення (монітори);
– пристрої документування та зберігання (відеореєстрації);
– канали передачі відеосигналу.

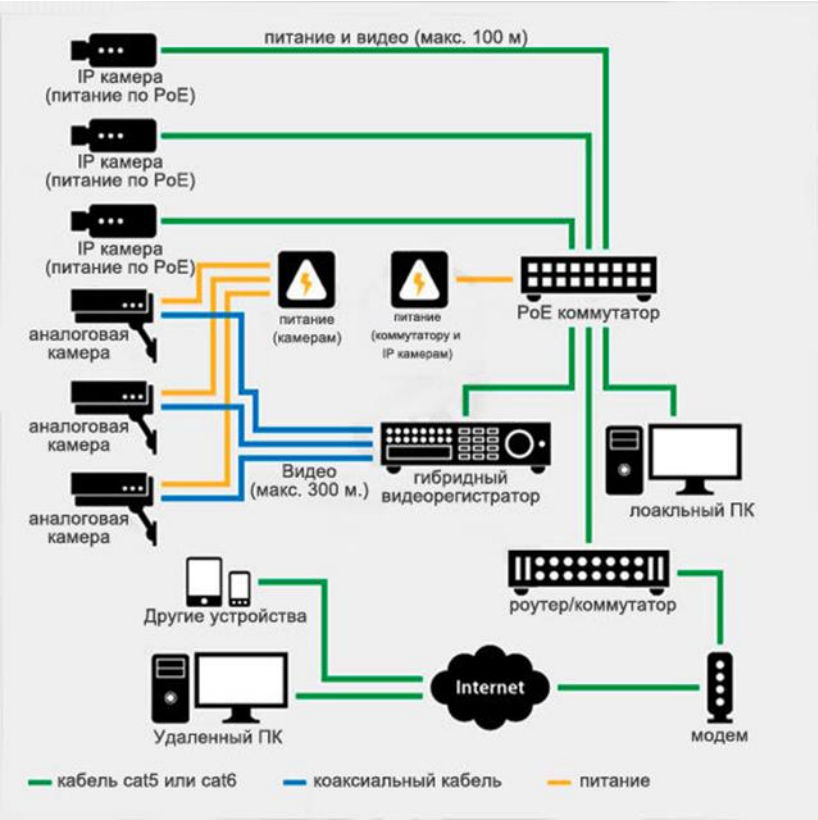


Рисунок 1.1 – Спрощена структура системи відеоспостереження

Відеокамера – це пристрій, який перетворює оптичне зображення об'єкта (сцени), що спостерігається, в електричний відеосигнал певного стандарту (набору вимог до структури і характеру складових відеосигналу, що дозволяє стандартизувати процес прийому/передачі відеозображень) (рис. 1.2). Відеокамера є найважливішим елементом системи відеомоніторингу, оскільки саме з неї до системи відеоаналізу надходить первинна інформація про об'єкт і саме її характеристиками визначається якість зображення загалом.

Відеокамера складається з електронною плати, на якій розміщений чутливий елемент – матриця та інші електронні компоненти. Крім того до складу камери входить вбудований або змінний об’єктив.

Рисунок 1.2 – Різноманіття конструкцій відеокамер систем відеоспостереження

Головною частиною відеокамери є світлочутлива матриця. Матриці бувають двох типів:

– прилади із зарядовим зв'язком (ПЗЗ або англ. CCD, Charge Coupled Device);

– металоокисні (CMOS).

ПЗЗ-матриця складається з безлічі чутливих до світла елементів, які називають фотоелементами. Кожен з них перетворює світло в електричний заряд. Потім відбувається зчитування аналогового значення заряду з усіх фотоелементів. У ПЗЗ-матриці перетворення електричного заряду з кожного фотоелемента в цифрову форму відбувається за допомогою аналогово-цифрового перетворювача. Для спрощення будемо вважати фотоелемент одним пікселем. ПЗЗ-матриці формують високоякісні, малозашумлені зображення.

CMOS-пристрої використовують для передачі сигналу більш придатну для обробки форму. У них можливе безпосереднє визначення цифрового значення освітленості від кожного окремого пікселя. CMOS-пристрої, більш схильні до колірного шуму. Особливості використовуваної в них технології вимагають наявності в безпосередній близькості від пікселя декількох фототранзисторів (фотоелектричних перетворювачів-підсилювачів електричних сигналів).

Еенергоспоживання CMOS-пристроїв майже в 100 разів менше, ніж у конкуруючої ПЗЗ-технології. ПЗЗ-матриці виробляються та використовуються порівняно давно, вони дозволяють одержувати високоякісні зображення з великою роздільною здатністю. CMOS-пристрої майже завжди мають меншу розрізняльну здатність, меншу чутливість і, в цілому, видають відеосигнал набагато гіршої якості. Однак цифрові технології розвиваються стрімко, і цілком можливо, що незабаром технології CMOS має належати пріоритет на ринку якісних відеокамер, принаймні, південно-східні виробники активно над цим працюють.

Простіші (і, відповідно, дешевші) камери оснащуються, як правило, найпростішими вбудованими об'єктивами, дорожчі – змінними об'єктивами з покращеними характеристиками та широкими функціональними можливостями.

Основними елементами та характеристиками відеокамер є:

1. Об'єктив – це пристрій, що формує зображення об'єкта у площині матриці. Він може бути вбудованим чи змінним.

2. Фокусна відстань (об’єктиву) f (мм) – характеризує величину кута зору за певного оптичного формату камери (тобто визначає масштаб зображення).

3. Трансфокатор – пристрій, що дозволяє змінювати фокусну відстань у широких межах (ZOOM-функція).

4. Відносний отвір (об’єктиву) F визначає освітленість на матриці.

5. Оптичний формат – розмір фоточутливої області матриці в дюймах.

6. Роздільна здатність (дозвіл) – максимальна кількість телевізійних ліній, що розрізняються візуально у вихідному сигналі камери при мінімально допустимій глибині модуляції 10%. Роздільна здатність по горизонталі визначає максимальну кількість градацій від чорного до білого або назад, які можуть бути отримані від камери в центральній частині екрана.

7. Порогова чутливість (чутливість) – мінімальна освітленість на матриці, при якій камера зберігає працездатність.

8. Синхронізація – прив'язка відеосигналу до фази мережевого напруги або зовнішнього джерела синхроімпульсів або іншого відеосигналу.

9. Електронний «затвор» – елемент електронної частини матриці, що забезпечує можливість зміни часу накопичення електричного заряду (витримки). Електронний «затвор» дозволяє отримати прийнятну якість зображення об'єктів, що швидко рухаються, і забезпечує працездатність камери в умовах високого освітлення.

10. Електронна діафрагма (автоматичний електронний «затвор», електронний ірис) – елемент електронної частини матриці, що забезпечує автоматичне регулювання витримки в залежності від рівня освітленості.

11. Автоматичне регулювання підсилення (АРП) – властивість електронної частини камери змінювати коефіцієнт підсилення у відеотракті залежно від рівня відеосигналу. АРП згладжує зміни рівня сигналу та дозволяє отримати прийнятну «картинку» на моніторі при недостатній освітленості об'єкта.

12. Відношення сигнал/шум. Дозволяє враховувати, коли потрібна висока якість телевізійного сигналу – чим вона вища, тим вища якість зображення.

13. Автоматичний баланс білого (для кольорових камер) – здатність камери забезпечувати правильну кольору при зміні умов освітленості об'єктів, що спостерігаються.

Камери для відкритого внутрішнього спостереження розміщуються в захисних корпусах (кожухах), які мають різну форму (сфера, напівсфера і т. д.), габарити, конструкцію кріплення (стельова, настінна, кутова) і дозволяють вибрати оформлення, що найбільше підходить до конкретного інтер'єру.

Камери для використання на відкритому повітрі поміщаються у захисні кожухи, обладнані підігрівом – термокожухи. Термокожухи призначені для роботи в широкому діапазоні кліматичних умов та дозволяють використовувати різноманітні комбінації телекамер та об'єктивів. Кожух забезпечений сонцезахисним козирком (або фільтром), платою для встановлення камери,

термостатом та комутаційною панеллю. Деякі термокожухи мають додаткове обладнання – вентилятори, двірники, омивачі скла.

Поворотні пристрої призначені для відеокамер з дистанційним керуванням. Вони забезпечують поворот у горизонтальній (до ±365°) і вертикальній (до ±183°) площинах або лише у горизонтальній.

Як правило, разом з поворотними пристроями поставляються пульти керування, за допомогою яких можна маніпулювати також трансфокатор об'єктивів, якщо потрібно отримати укрупнене зображення.

Відеоспостереження, як правило, здійснюється відеокамерами, які підключають:

1) до сервера системи відеоспостереження;

2) по локальній мережі чи мережі Internet.

Камери підключаються до комп'ютерної техніки за допомогою наступного обладнання:

- плати відеовводу;
- порти USB;
- локальна мережу чи мережа Internet – (для IP-камер).

Робота системи відеоспостереження можлива в наступних конфігураціях:

1) шляхом підключення аналогових камер до плат відеовводу;

2) шляхом підключення IP-камер по мережі Internet.

Допускається побудова систем комбінованого типу (аналогові камери та IP-камери).

У будь-якому випадку в системі відеоспостереження може бути кілька серверів і кілька приймачів, з'єднаних по мережі Internet. Також до системи може підключатися додаткове обладнання (сповіщувачі охоронної та пожежної сигналізації, мікрофони, поворотні пристрої тощо).

Можливості відеоплат з перетворення аналогового сигналу на цифровий залежать від потужності комп'ютерного обладнання, параметрів відеозображення (наприклад, кількість кадрів в секунду, роздільна здатність, колір) і пропускної спроможності локальної мережі.

Аналогові камери передають аналоговий відеосигнал на плату відеозахоплення, де він оцифровується. IP-камера має схему цифрової обробки, компресії та передачі зображення. Воно передається від такої камери до локальної мережи або мережи Internet. Кожна камера має IP-адресу та вбудоване програмне забезпечення, що дозволяє їй функціонувати як WEB-сервер.

USB камера передає зображення через USB-порт. Продуктивність відеосервера системи оцінюють у сумарному числі кадрів в секунду, які здатний обробити сервер і в числі кадрів в секунду для одного каналу. При цьому швидкість захоплення-відображення на екрані, швидкість запису в архів і швидкість передачі по мережі можуть бути різними.

Наприклад, плата відеозахоплення захоплює «живе» відео зі швидкістю 25 кадрів в секунду, на екран відображається також 25 кадрів в секунду, швидкість запису в архів встановлено 8 кадрів в секунду, а по мережі віддаленому клієнту повільним каналом передається один кадр в секунду.

Максимальна швидкість захоплення та відображення відео обмежується смугою пропускання комп'ютерної шини даних конкретного обладнання та визначається наступними факторами:

- кольоровість зображення;
- роздільна здатність зображення.

Кольорове зображення займає вдвічі більше місця, ніж чорно-біле і, відповідно, швидкість його захоплення, стиснення та передачі мережею значно нижче.

Плати відеозахоплення, що оцифровують сигнал із відеокамер, видають строго певний набір дозволів, заданий форматом відеосигналу PAL. Повний кадр відеосигналу має роздільна здатність 768 x 576. При цьому він формується з двох полів, кожне з яких має роздільну здатність 768 x 288. Поля містять «черезрядкову» інформацію – «парне» поле містить парні рядки кадру, а «непарне» – непарні. Якщо відбувається відеозйомка об'єкта, що рухається, то зображення в цих двох полях виявляється зміщеним і при їх складанні в повний кадр утворюється ефект «гребінки». Таким чином, для отримання повного кадру 768x576 відеосистема повинна скласти два поля та за допомогою математичного алгоритму усунути ефект гребінки.

Типове програмне забезпечення дозволяє записувати в архів «живе» відео з тією ж швидкістю, з якою зображення відображається на екрані. Ця можливість обмежується лише потужністю процесора. Але для більшості випадків немає необхідності записувати відео з такою швидкістю, оскільки для цього потрібний потужніший сервер і великий розмір дисків. Виходячи з досвіду вважається, що швидкість 4 кадри в секунду цілком достатня для аналізу ситуацій з відеоархіву, а швидкість 8 кадрів в секунду при перегляді архіву рівносильна «живому» відео. За замовчуванням для всіх каналів встановлюється швидкість запису в архів 4 кадри на секунду.

Типове програмне забезпечення дозволяє використовувати декілька алгоритмів стиснення відеопотоку, з різними опціями. Зазвичай використовуються MJPEG, MPEG-4 або H.264 формат стиснення відеоінформації.

Кожен з цих форматів має свої особливості.

MJPEG – це один з перших форматів запису відеозображення, заснований на покадровому методі відеостиснення. Запис, зроблений в цьому форматі, займає більший обсяг дискового простору. Відеореєстратори, що використовують MJPEG, мають застарілу елементну базу, тому на ринку їх вартість нижча.

MPEG-4 – це більш сучасний формат, призначений для стиснення потоку аудіо- та відеоінформації. Запис, зроблений відеореєстратором, що використовують MPEG-4, займає приблизно в 10 разів менше місця дискового простору. Такі відеореєстратори мають більш сучасну елементну базу, отже, їх ціна вища.

H.264 – цей формат використовує новітні алгоритми стиснення аудіо- та відеоінформації і є логічним продовженням розвитку формату MPEG-4. Відмінними особливостями цього стандарту від MPEG-4 можна назвати поліпшену передачу кольору, підвищену чіткість зображення; відеоінформація, що записується в H.264, займає приблизно в 2 рази менше місця на диску, ніж попередній формат. Вартість відеореєстраторів з H.264 вище, ніж на основі MPEG-4.

Найбільш новим є формат відеостиснення H.265 (HEVC), призначений для ще більш ефективного стиснення даних, більш високої пропускної спроможності, що дозволяє зберігати більший розмір файлів. Але він достатньо повільно впроваджується у сучасні системи відеоспостереження й мабуть єдина причина цього полягає в тому, що він вимагає значно більшої обчислювальної потужності, ніж H.264. Рішення, які пропонують необхідний рівень обробки, є достатньо дорогими та ресурсомісткими. Незважаючи на це, застосування H.265 кожен рік зростає.

Коли формат H.265 охопить всю галузь відеоспостереження передбачити складно. Значною мірою це залежить від успіху 4K Ultra HD та інших форматів високої роздільної здатності. Якщо 4K отримають широке поширення в вистемах відеоспостереження, то формат H.265 буде за ними.

Існує також і інший формат відеостиснення, що розробила компанія Hikvision Digital Technology як власний алгоритм стиснення на базі стандарту H.265/High Efficiency Video Coding (HEVC). Новий формат стиснення має назву H.265+. Варто зазначити, що це не перший досвід компанії в доробці відеокодека: Hikvision вже вела поліпшення в H.264, назвавши його вдосконалений стандарт H.264+.

Розглянемо основні переваги H.265+.

1.Розподілене інтелектуальне кодування. Воно передбачає в H.265+ поділ фону (тобто реального фізичного об'єкта) та відвідувачів. Створення моделі з одного або декількох раніше закодованих відеокадрів дозволяє здійснювати «міжкадрове передбачення» та «прогнозування всередині кадру», де зразки макроблоків (блок обробки) передбачається за допомогою інформації про передані макроблоки одного і того ж кадру. Таким чином, стиснення відеопотоку може здійснюватися за рахунок трансляції лише динамічної складової кадру. Оскільки більшість об'єктів відеоспостереження мають статичний фон, подібне доопрацювання може суттєво покращити кодек H.265.

2. Придушення цифрового шуму. Інтелектуальний алгоритм аналізу H.265+ розрізняє фонові зображення і об'єкти, що рухаються таким чином, що кожен з них може бути закодований з різними стратегіями кодування. Фонове зображення кодується з високим ступенем стиснення для зменшення шуму. Модуль також кодує візуальний шум у сцені. В результаті виходить висока якість зображення об'єктів, що рухаються при невеликих розмірах відеопотоку.

3. Довгостроковий контроль бітрейту. Hikvision вводить поняття Long-Term Average Bitrate (довгостроковий середній бітрейт), щоб повною мірою використовувати можливості пропускного каналу. Long-Term Average Bitrate розраховує ставки протягом певного періоду часу (зазвичай 24 години). При середній швидкості передачі даних, можливо призначити більш високі бітрейти для часів з високою активністю відвідувачів, при одночасному їх зниженні під час простою. Наприклад, для відеоспостереження офісу очевидно, можна зменшити бітрейт у нічний час. Таким чином, можна декларувати значні переваги H.265+ для реального об'єкту відеоспостереження.

Компанія Hikvision Digital Technology провела порівняльне тестування форматів стиснення для реального об'єкту відеоспостереження цілодобового відеоспостереження – невеликого кафе. Випробування проводилося на основі камер з роздільною здатністю 1080p при 25 кадрах за секунду.

Середній бітрейт між форматами H.264 та H.265+ зменшився на 83%, а різниця між стандартним H.265 та H.265+ склала 67%. Порівняння 24-годинних фрагментів відеоархіву також демонструє істотні відмінності: для кодека H.264 розміри файлу склали в середньому 22,7 ГБ, для H.265 – 11,8 ГБ, а для H.265+ лише 3,9 ГБ. Друге порівняльне тестування проводилося для цілодобового відеоспостереження за транспортною розв'язкою. Тут відмінність 24-годинних фрагментів відео також виявилася відчутною: розміри файлу для H.264 в середньому займали 36,4 ГБ, для H.265 – 21,1 ГБ, а для H.265+ – лише 7,5 Гб.

Типове програмне забезпечення відеоаналізу використовується для аналізу подій у місцях спостереження. Для цього спільно використовуються детектори руху та детектори звуку. Детектори руху проводять аналіз зображення, а детектори звуку – аналіз звуку. Це дозволяє підвищити надійність відеоаналізу, скоротити час для ухвалення рішення у разі виникнення небезпечних ситуацій.

Детектор руху – це елемент програми, що аналізує зображення. Якщо виявляється рух, то детектор може увімкнути запис та/або змінити швидкість запису зображення. Детектор руху має широкий діапазон налаштувань, що дозволяє користувачеві вибрати оптимальні умови роботи. Індивідуально налаштовується розмір та положення зон контролю, чутливість та інші.

Зображення на моніторі можна умовно розділити на області. Найбільш інформативними є ті, в яких можливий рух. Але й сам рух може бути різним за темпом. Наприклад, порушник може бігти, повзти, повільно переміщатися. Тому області, у яких темпи руху не змінюється, можна об'єднати в зони і призначити їм однакові параметри детектора.

Основними параметрами кожної зони є чутливість та поріг спрацьовування. Кількість зон та областей, їх положення та розмір задаються користувачем.

Принцип роботи детектора руху заснований на постійному порівнянні сусідніх відеокадрів: попереднього та поточного. Зображення складається з так званих «фасет». Спрацьованими вважаються ті фасети, у яких зафіксовано зміну більше заданого.

«Чутливість» – параметр, що дозволяє налаштувати мінімальну зміну фасети, при якому фасета буде визнана спрацювала. Даний параметр вимірюється у відносних величинах, тому налаштування слід проводити, враховуючи умови відеоспостереження та перешкода захищеність відеосигналу.

«Поріг спрацьовування» – параметр, що дозволяє налаштувати мінімальну кількість фасет, що спрацювали, яке призводитиме до спрацювання детектора руху. Значення цього параметра підбирається досвідченим шляхом, враховуючи при доборі параметри відеокамери, об'єктива, освітлення і т. д. Також різних ділянках одного кадру можуть переміщатися об'єкти різної величини – наприклад, пішохід і автомобіль.

Для унеможливлення перешкод від певних зон кадру використовується редагування зон. Кожній зоні окремо задаються розміри, параметри чутливості та порога спрацьовування.

Одним із призначень типового програмного забезпечення є збереження відеоінформації (відеоданих) у вигляді архівних записів на жорсткому диску відеореєстратора. Але постійний запис веде до швидкого заповнення жорстких дисків, тому програма передбачає включення запису до архіву у деяких випадках: за командою оператора; за розкладом; зі спрацьовування детекторів руху та звуку; із спрацьовування тривожного датчика.

При будь-якому з цих варіантів включення каналу на запис відбувається затримка в часі, внаслідок якої може статися втрата інформації.

Часто буває важливо зафіксувати кілька миттєвостей, що передували події включення запису. Для цього і створено попереднього-тривожний запис. При подачі команди на запис програма спочатку архівує вміст буфера, потім кадри поточного зображення, до команди зупинки запису в архів.

У налаштуваннях відеоканалів плат конкретного обладнання можна включати попереднього-тривожний запис встановленої кількості кадрів з різною частотою. Наприклад, спочатку зі встановленою для даного каналу швидкістю стиснення, а потім – зі встановленою під час редагування детектора руху.

У програмному забезпеченню може бути передбачено «Режим з підвищеної пильності», що дозволяє виводити на екран монітора лише ті вікна, на яких зафіксовано рух. За відсутності руху на екран будуть виведені всі відеоканали заданої конфігурації.

1.2. Системи відеомоніторингу, відеодані з яких можуть бути джерелами інформації для проведення відеоаналізу підрозділами кримінального аналізу Національної поліції України

Як вже зазначалася раніше, на даний час системи відеомоніторингу вже широко застосовуються для забезпечення громадської безпеки та порядку на місцевому рівні, а також для відеомоніторингу подій на підприємствах, установах, організаціях (незалежно від форм власності) та володіннях фізичних осіб, які повністю або частково здійснюють відеомоніторинг публічних місць.

Основними серед них є наступні.

Місцеві системи відеомоніторингу, побудовані за концепцією «Безпечне місто», є інформаційно-аналітичними комплексами (ІАК), що на даний час найбільш технологічно розвинені та розповсюджені не тільки в мегаполісах, а й в багатьох містах і селищах України (рис. 1.3).

Рисунок 1.3 – Загальна структура ІАК «Безпечне місце»

ІАК «Безпечне місто» – це можливість всебічного віддаленого моніторингу поточної ситуації в місті або селищі. Основними об’єктами відеоспостереження є транспортні, соціальні, житлово-комунальні, економічні та інші інфраструктурні місця (парки, сквери, пам’ятки, площі, вулиці тощо). Концепція «Безпечне місто» обов’язково включає можливість накопичення, об’єднання, аналізу, групування масивів різноманітних даних, отриманих з різних джерел у реальному часі чи ретроспективно. Це єдиний інформаційний простір системи безпеки, реалізований як комплекс інноваційних рішень, що забезпечує відеофіксацію транспортного та пішохідного трафіку, дозволяє здійснювати моніторинг та управління діяльністю комунальних служб, поліції та підрозділів ДСНС у відповідному населеному пункті.

Тільки столична система «Безпечне місто» налічує понад 8 тисяч відеокамер комунальної власності, серед яких 198 розташовані у метро та мають функцію розпізнавання облич [8]. За допомогою цих встановлених камер правоохоронні органи мають можливість розшукувати людей, автомобілі, розкривати злочини тощо. Наприклад, стосовно задач відеоаналізу в інтересах правоохоронних органів Київський ІАК «Безпечне місто» має наступні можливості щодо моніторингу осіб та інших об'єктів [9]:

1) дозволяє розпізнавати та ідентифікувати осіб, що знаходились поряд із особою, що складає предмет зацікавленості правоохоронних органів (пошук здійснюється по фото об'єкта камерами, що технічно мають можливість пошуку по обличчям);

2) дозволяє здійснювати пошук осіб по фото- і відеозображенню (камерами, що технічно мають можливість пошук по обличчям);

3) дозволяє здійснювати пошук місць, де об'єкт зацікавлення знаходиться найчастіше (може використовуватись для встановлення місця перебування, роботи тощо);

4) дозволяє відслідковувати кількість разів знаходження особи в радіусі дії певної камери;

5) дозволяє встановлювати місце перебування транспортного засобу (ТЗ) по заданих даних (час, місце перебування, номер, вид, модель, колір транспортного засобу тощо) та будувати та відображати на карті маршрут руху певного ТЗ;

7) дозволяє при накладенні двох або більше областей (територій) пошуку на карті встановлювати закономірності пересування останніми певного транспортного засобу (засобів);

8) дозволяє здійснювати пошук місць, де ТЗ зацікавлення знаходиться найчастіше (може використовуватись для встановлення місця перебування, роботи тощо);

9) дозволяє встановлювати місце перебування ТЗ по заданих архівних даних (час, місце перебування, номер, вид, модель, колір транспортного засобу тощо);

10) показує розміщення камер спостереження на місцевості, їх вид та орієнтовний напрямок зйомки (в деяких випадках зображений напрям зйомки камери не відповідає фактичному);

11) дозволяє виявляти ТЗ, що могли «супроводжувати» об'єкт зацікавленості;

12) дозволяє здійснювати пошук автомобіля на визначеному маршруті;

13) дозволяє відслідковувати знаходження певного ТЗ в радіусі дії певної камери;

14) дозволяє здійснювати аналіз відео високої якості (в т.ч. завантаженого користувачем самостійно) на предмет виявлення номерів автомобілів, осіб тощо.

Системи відеоспостереження та моніторингу підприємств, установ, організацій. Ці системи побудовані та використовуються на підприємствах, установах та організаціях різної сфери діяльності (незалежно від форм власності) в населених пунктах або навіть місцевостях. Сучасні технології, наприклад, аналітика руху, розпізнавання облич та інші, є нормою і роблять ці системи відеоспостереження потужним інструментом для підвищення ефективності та контролю безпеки на виробництві і офісі. Ресурси деяких з них інтегровані з ІАК «Безпечне місто».

Системи відеоспостереження окремих колективних домогосподарств та приватних будинків фізичних осіб. Системи відеоспостереження, встановлені у багатоквартирних домах, житлових комплексах та у приватних будинках, допомагають запобігати хуліганству, вандалам чи злодіям, та підвищують рівень суспільної безпеки. Кожен мешканець багатоквартирного будинку може отримати віддалений доступ до перегляду відео з камер спостереження, навіть перебуваючи далеко від будинку.

Як правило, грамотно спроєктована та якісно встановлена система відеоспостереження дозволяє мешканцям контролювати: автомобільну стоянку та паркінг; дитячий майданчик; двір; входи до під'їздів; сходовий майданчик; ліфт; підвали та горищні приміщення; автономну котельню та ін. А, отже, за рахунок цих систем можна отримати відповідні відеозображення осіб, транспортних засобів та інших об’єктів, які попали в поле зору цих систем.

Засоби відеофіксації, що застосовуються громадянами. На даний час посадовими особами державних та місцевих органів влади, підприємств, установ і організацій (незалежно від форм власності) при виконанні ними службових обов’язків, а також фізичними особами в особистих цілях широко використовуються різні технічні засоби, за допомогою яких можна зробити відповідні відеозаписи. Насамперед, це, як правило, смартфони, цифрові фото- і відеокамери, відеореєстратори, що встановлені на транспортних засобах.

Отже, і вони можуть бути джерелами відеоданих, що можуть бути отримані представниками правоохоронних органів.

Порядок отримання інформації, використання технологій доступу, типів наборів даних, обсяг і структура даних, до яких надається доступ з автоматичної фото- і відеотехніки, що знаходиться у приватному володінні, відповідно до потреб Національної поліції України визначаються згідно із законодавством України.

Серед відомчих інформаційних систем Національної поліції, які можуть задіюватися для отримання відеоданих з метою проведення подальшого відповідного відеоаналізу підрозділами кримінального аналізу НП України, є наступні.

Підсистема відеоспостереження системи централізованого управління нарядами поліції («ЦУНАМІ»). Система «ЦУНАМІ» – це комплекс апаратних та програмних засобів, а також персоналу, призначений для управління силами й засобами органів та підрозділів НП України [10]. Мета впровадження системи «ЦУНАМІ» була обумовлена необхідністю вдосконалення процесу організації діяльності з управління силами й засобами Національної поліції для ефективного реагування на повідомлення про злочини та події.

Однією зі складових системи «ЦУНАМІ» є підсистема відеоспостереження, яка отримає відеодані в тому числі з ІАК «Безпечне місто», і яка, у свою чергу, пов'язана із системою колективного відображення (рис. 1.4). Метою впровадження такої системи є необхідність оперативного візуального контролю за основними криміногенними місцями, вулицями, площами, транспортними потоками, а також перегляд записаної інформації під час розкриття злочинів [10].

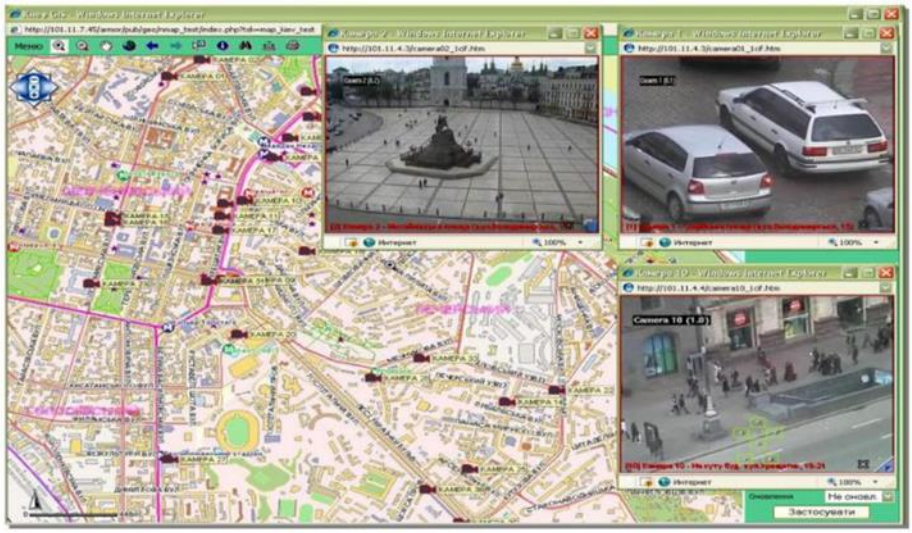


Рисунок 1.4 – Відеовідображення об'єктів в системі «ЦУНАМІ»

Інформаційна підсистема «Гарпун» (ІП «Гарпун») інформаційно-комунікаційної системи «Інформаційний портал Національної поліції України» (система ІПНП), призначена для обробки відомостей про транспортні засоби (ТЗ) усіх типів (автомобілі, автобуси, мотоцикли всіх типів, марок і моделей, самохідні машини, причепи та напівпричепи до них, мотоколяски, інші прирівняні до них ТЗ та мопеди) та номерні знаки ТЗ, що розшукуються у рамках кримінального, виконавчого проваджень, проваджень у справах про адміністративні правопорушення, оперативно-розшукової діяльності, а також за ухвалою слідчого судді, суду [10].

Спеціалізоване програмне забезпечення ІП «Гарпун», створене для: формування та ведення, аналітичної обробки й інформування про розшук ТЗ або номерного знаку ТЗ для запобігання вчиненню правопорушень; аналізу тимчасового набору даних про номерні знаки, що надходять із систем

відеофіксації, на предмет їх розшуку; одночасного перебування на різних ТЗ номерних знаків – двійників, використання знищених знаків, а також для автоматизованого інформування про такі факти диспетчерів, оперативних чергових, нарядів поліції органів (підрозділів) поліції та ініціаторів розшуку.

Для аналітичної обробки цих даних в ІП «Гарпун» використовується фото- і відеоінформація, отримана з технічних засобів і технічних приладів відеофіксації (відеоспостереження), закріплених поліцією на службових ТЗ, розміщених по зовнішньому периметру доріг і будівель, а також інформація, отримана з автоматичної фото- і відеотехніки, що знаходиться у приватному володінні [10].

Система «Custody Records» є сучасною системою відеоспостереження, що обладнана в приміщеннях ізоляторів тимчасового тримання (ІТТ), у приміщеннях територіальних органів поліції та в спеціальному автотранспорті, для перевезення затриманих і взятих під варту осіб. Система передбачає відеофіксацію, передачу, відображення та архівацію всього, що відбувається в службових та камерних приміщеннях ІТТ, а також в спеціальному автотранспорті, під час їх використання [10].

Отже, система надає можливість, у разі необхідності, отримати цілісну і хронологічну відео- та аудіо інформацію про доставлення й увесь час перебування затриманих осіб в ІТТ та поводження з ними посадових осіб поліції. У разі необхідності ці дані можуть бути відповідним джерелом відеоданих.

Персональні відеореєстратори посадових осіб патрульної поліції. Всі працівники патрульної поліції, які знаходяться на чергуванні, оснащені нагрудними камерами (відеореєстраторами), наявність яких призначена для фіксації протиправних діянь осіб, які перевіряються, та ходу виконання поліцейськими службових обов’язків і розглядається як засіб захистити їх від упереджених заяв щодо їхньої неправомірної поведінки [11]. Відеореєстратор є засобом об’єктивного контролю за місцем подій, відеозапис з місця події – це рівною мірою контроль дій патрульного та документальне підтвердження правомірності його вимог і вжитих заходів.

Тобто ці засоби також можуть бути ще одним із джерел відеоданих.

Засоби відеозапису, що застосовуються під час організації діяльності чергової служби органів (підрозділів) поліції. Діяльність чергової служби органів (підрозділів) Національної поліції України забезпечується засобами відеоспостереження. Зокрема, старший інспектор-черговий для забезпечення публічної безпеки та порядку, попередження і припинення правопорушень, встановлення осіб, які підозрюються в їх вчиненні, ліквідації наслідків надзвичайних подій має право проводити відеозйомку осіб, затриманих за підозрою у вчиненні правопорушень (затриманих згідно з дорученнями органів правопорядку, затриманих органами досудового розслідування, адміністративного арешту, домашнього арешту), відповідно до законодавства України [11].

При цьому, камери для затриманих оснащуються засобами відеонагляду, а перед поміщенням до камери затриманої особи черговий зобов’язаний проінформувати її про наявність системи відеоспостереження.

Засоби відеозапису на безпілотних літальних апаратах. На даний час працівниками поліції активно використовуються безпілотні літальні апарати (БпЛА) [11]. Особливо масовий характер це прийняло зараз, під час повномасштабного вторгнення російського агресора на територію України.

Основними напрямками використання БпЛА підрозділами поліції під час виконання завдань є [11]:

– висотне спостереження під час проведення культурно-масових, суспільно-політичних і спортивних заходів, а також під час припинення масових заворушень і загрози блокування об’єктів;

– супроводження розслідування в межах єдиного реєстру досудових розслідувань;

– виявлення злочинів та адміністративних правопорушень, фото- та відеодокументування, забезпечення зв’язку й управління наземними нарядами поліції, їх взаємодія з іншими силовими підрозділами;

– моніторинг для забезпечення безпеки дорожнього руху;

– повітряна розвідка, відстеження оперативної обстановки під час виконання службових (поліцейських) завдань;

– порятунок і пошук зниклих людей.

У будь-який час, у складних умовах і в максимально короткі терміни застосування БпЛА дає можливість здійснювати відеомоніторинг обстановки в режимі реального часу, а, отже, відеодані, отримані цими засобами, також можуть бути джерелом для систем відеоаналітики.

Система прикордонного контроля «Гарт-1» інтегрованої міжвідомчої інформаційно-комунікаційної системи контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон («Аркан»). Розпорядником системи «Аркан» є Адміністрація Державної прикордонної служби України (Держприкордонслужби), що є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через міністра внутрішніх справ України. Одним із суб’єктів, який має право в установленому порядку користуватися інформаційними ресурсами системи «Аркан», є Міністерство внутрішніх справ України (а отже і Національна поліція України) [10].

Система «Аркан» створена з метою своєчасного, достовірного та функціонально повного інформаційно-аналітичного забезпечення діяльності суб'єктів системи стосовно здійснення ними заходів із запобігання і недопущення в'їзду в Україну або виїзду з України осіб, яким згідно із законодавством не дозволяється в'їзд в Україну або яких тимчасово обмежено в праві виїзду з України, у тому числі згідно з дорученнями правоохоронних органів, розшуку в

пунктах пропуску через державний кордон осіб, які переховуються від органів дізнання, слідства та суду, ухиляються від відбуття кримінальних покарань, припинення протиправної діяльності фізичних і юридичних осіб, які незаконно переправляють мігрантів в Україну або транзитом переміщують їх через територію України, посилення контролю за додержанням правил в'їзду, виїзду, перебування в Україні іноземців та осіб без громадянства, а також виконання інших завдань у правоохоронній сфері згідно із законодавством [10].

Система прикордонного контролю «Гарт-1» – це інтегрована міжвідомча автоматизована система обміну інформацією щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон України, обслуговується Державною прикордонною службою України та є складовою частиною інтегрованої системи «Аркан» [10].

З метою фіксації діяльності посадових осіб Держприкордонслужби, осіб, ТЗ і вантажів, які перетинають держаний кордон, а також в інтересах функціонування інформаційних баз системи «Аркан» система «Гарт-1» здійснює:

– цілодобове відеоспостереження за територією та об'єктами в пунктах пропуску, відеозапис, детектування руху по кожному з відеоканалів, ведення циклічного відеоархіву та здійснення пошукових функцій по ньому;

– обробку відеозображень та розпізнавання державних номерних знаків автотранспорту та перевірки зчитаних номерних знаків за базами даних викраденого автотранспорту.

Таким чином, у цьому розділі роботи розглянуті загальні принципи побудови та функціонування систем відеомоніторингу та їх складових елементів. Крім того, проаналізовані системи відеомоніторингу, відеодані з яких можуть бути джерелами інформації для проведення відеоаналізу підрозділами кримінального аналізу Національної поліції України.

Отримані від цих систем відеомоніторингу відеодані є електронним представленням послідовності візуальних зображень у формі закодованих цифрових даних, що складається з серії цифрових зображень, які відображаються у швидкій послідовності, а також можуть бути поєднані (супроводжуватись) з аудіоданими [5].

В наступному розділі розглянемо правові засади поводження з цими відеоданими працівниками правоохоронних органів.

2. ПРАВОВІ ЗАСАДИ ОТРИМАННЯ ТА ПОВОДЖЕННЯ ПОСАДОВИМИ ОСОБАМИ ПРАВООХОРОННИХ ОРГАНІВ З ВІДЕОДАНИМИ У ЯКОСТІ ЕЛЕКТРОННИХ ДОКАЗІВ ТА ОПЕРАТИВНОЇ ІНФОРМАЦІЇ

Електронні докази — це докази, які можна отримати в електронній формі [12]. В Україні електронні докази як юридичну категорію започатковано в 2017 році у Цивільному процесуальному кодексі (ЦПК) України [13], Господарському процесуальному кодексі (ГПК) України [14] та Кодексі адміністративного судочинства (КАС) України [15].

Так, відповідно до [13-15] електронними доказами є «інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі інтернет)».

Нажаль, на даний час стосовно кримінальних проваджень в Кримінальному процесуальному кодексі (КПК) України [16] досі так і не надано визначення поняття електронних доказів. Хоча відповідно до ст. 99 КПК України, коли вводиться поняття документа як речового доказу, визначено, що до документів можуть належати: матеріали відеозапису та інші носії інформації (у тому числі електронні), а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії.

Електронні докази належать до категорії документів, а матеріальні носії, на яких вони розміщені, визнаються речовими доказами. Тобто відповідно до [16] матеріали фотозйомки, відеозапису, електронні носії цієї інформації відносяться до речових доказів у якості документів і де юро (стосовно КПК) все ж є електронними доказами.

Відповідно до [16] оригіналом електронного документа є його відображення, якому надається таке ж значення, як і документу (ч. 3 ст. 99 КПК України). При цьому дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа (ч. 4 ст. 99 КПК України).

Електронні докази отримують за допомогою різноманітних електронних пристроїв (аналогових і цифрових). Стосовно фото- і відеозаписів електронні докази в аналоговій формі – це кіно-, фото-, відеоматеріали, зроблені за допомогою аналогової електронної техніки. Електронні докази у цифровій формі: кіно-, фото-, мультимедійні тощо матеріали, зроблені за допомогою цифрових (комп'ютеризованих) засобів, що наявні у цифровій формі на комп'ютерних носіях інформації, а також в комп'ютерних мережах, у тому числі в мережі Інтернет [12]. Вони стають доступними для сприйняття людиною після їх обробки засобами комп'ютерної техніки.

До електронних доказів, які містять відеозображення в цифровій формі, належать:

– відеозаписи, що зроблені за допомогою камер спостереження, та зберігаються в їх відповідних структурних частинах (відеосерверах тощо);

– відеозаписи, що зроблені за допомогою переносних і стаціонарних цифрових відео- і фотозасобів, зберігаються безпосередньо в них або їх зйомних носіях;

– файли, які записані безпосередньо на мобільний телефон, призначений для роботи в мережах стільникового зв'язку;

– дані систем обміну миттєвими повідомленнями (месенджери), зокрема мобільних додатків, вебсервісів, систем, інтегрованих в соціальні мережі (скайп, вайбер, телеграм, фейсбук тощо);

– вебсайти в мережі Інтернет;

– скріншот (відображення електронного документа незалежно від електронної чи паперової форми);

– файли, які є додатками до протоколів слідчих дій і містять відомості про хід їх проведення, записані на знімні носії інформації.

Як і збір звичайних доказів збирання електронних доказів повинно здійснюватися процесуально правильно. Відповідно до ст. 93 КПК України про збирання доказів зазначено наступне [16]:

1. Збирання доказів здійснюється сторонами кримінального провадження, потерпілим, представником юридичної особи, щодо якої здійснюється провадження, у порядку, передбаченому цим Кодексом.

2. Сторона обвинувачення здійснює збирання доказів шляхом проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій, витребування та отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових та фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій та актів перевірок, проведення інших процесуальних дій, передбачених цим Кодексом.

3. Сторона захисту, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, здійснює збирання доказів шляхом витребування та отримання від органів державної влади, органів місцевого самоврядування,

підприємств, установ, організацій, службових та фізичних осіб речей, копій документів, відомостей, висновків експертів, висновків ревізій, актів перевірок; ініціювання проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших процесуальних дій, а також шляхом здійснення інших дій, які здатні забезпечити подання суду належних і допустимих доказів.

Ініціювання стороною захисту, потерпілим, представником юридичної особи, щодо якої здійснюється провадження, проведення слідчих (розшукових) дій здійснюється шляхом подання слідчому, прокурору відповідних клопотань, які розглядаються в порядку, передбаченому статтею 220 цього Кодексу. Постанова слідчого, прокурора про відмову в задоволенні клопотання про проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій може бути оскаржена слідчому судді.

4. Докази можуть бути одержані на території іноземної держави в результаті здійснення міжнародного співробітництва під час кримінального провадження.

На відміну від звичайних доказів (паперових документів, предметів, засобів тощо), характеристики та просторові межі яких можна бачити, електронні докази мають іншу природу і вирізняються такими характеристиками [12]:

– електронні докази невидимі «неозброєним оком» (без спеціального інструментарію) і для їх сприймання та дослідження використовують спеціальні технічні або програмно-технічні засоби;

– вони можуть бути легко змінені, пошкоджені або знищені в процесі експлуатації пристрою користувачем чи під впливом фізичних чинників (високий рівень вологості, висока температура, електромагнітні випромінювання тощо);

– електронний доказ не може існувати без носія інформації. При цьому набувають значення ідентифікаційні ознаки носія інформації (зокрема найменування типу, марки моделі, індивідуального машинного носія, на якому записаний документ тощо);

– за стадіями виготовлення електронні докази (документи), як і звичайні, поділяють на оригінали, дублікати, копії й виписки.

Під час роботи з електронними доказами слід дотримуватися наступних принципів [12]:

1. Законність. Працівники підрозділів, що провадять розслідування і досліджують докази в електронній формі, зобов’язані дотримуватися чинного законодавства, загальних процесуальних та криміналістичних принципів.

2. Документування процесу. Документують будь-які дії, виконувані стосовно електронних доказів, і зберігають ці документи на випадок перевірки, щоб незалежна третя сторона могла повторити ці дії та отримати аналогічний результат.

3. Цілісність даних. Дії фахівця не повинні призводити до матеріальних змін даних, електронних пристроїв чи носіїв інформації, які можуть використовуватись як докази.

4. Експертна підтримка. Якщо передбачається, що при огляді (обшуку) можуть бути виявлені електронні докази, отримують підтримку фахівців (спеціалістів), забезпечивши, за можливості, їх присутність на місці події.

5. Відповідна фахова підготовка. Якщо при огляді (обшуку) відсутні фахівці з електронних доказів, першочергові дії на місці події здійснюють особи, які мають необхідні знання та навички для виявлення і збирання доказів.

6. Розумна обережність. Уникають будь-яких навмисних або ненавмисних дій, які можуть призвести до пошкодження потенційних доказів, представлених у цифровій формі.

Пошук та вилучення доказів в електронній формі можуть здійснюватися під час кримінального провадження відповідно до КПК шляхом здійснення таких дій [16]:

– обшук (ст. 234 КПК України) на підставі ухвали слідчого судді (ст. 235 КПК України);

– огляд (ст. 237 КПК України);

– проведення негласних слідчих (розшукових) дій (глава 21 КПК України);

– тимчасовий доступ до речей і документів на підставі ухвали слідчого судді, суду (ст. 159 КПК України);

– зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України);

– зняття інформації з електронних інформаційних систем (ст. 264 КПК України);

– дослідження інформації, отриманої при застосуванні технічних засобів (ст. 266 КПК України);

– зняття показань технічних приладів та засобів, що мають функції фото-, кінозйомки, відеозапису, чи таких засобів (ст. 245^{1} КПК України).

Відповідно до с. 298-1 КПК України процесуальними джерелами доказів у кримінальному провадженні про кримінальні проступки, крім визначених статтею 84 цього Кодексу, також є пояснення осіб, результати медичного освідування, висновок спеціаліста, показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису [16].

Такі процесуальні джерела доказів не можуть бути використані у кримінальному провадженні щодо злочину, окрім як на підставі ухвали слідчого судді, яка постановляється за клопотанням прокурора.

Відповідно до проведеного у п. 1.2 цієї роботи аналізу, відеоданими, як джерелами електронних доказів, що зроблені засобами кіно-, відеозйомки можуть бути:

1. Відеодані з Єдиного інформаційного простору системи безпеки громад «Безпечне місто».

2. Відеодані з відомчих систем відеомоніторингу Національної поліції України, до яких належать:

2.1. Відеодані з портативних відеореєстраторів.

2.2. Відеодані з відеореєстраторів, встановлених на службових транспортних засобах для максимальної фіксації навколишньої обстановки та/або внутрішньої частини салону.

2.3. Відеодані з автомобільних систем, встановлених на службових транспортних засобах ситуаційних центрів, командно-штабних автомобілях, спеціальному автотранспорті для перевезення затриманих та взятих під варту осіб.

2.4. Відеодані з стаціонарних систем органів, підрозділів поліції.

2.5. Відеодані з безпілотних літальних апаратів.

3. Відеодані з систем відеомоніторингу підприємств, установ, організацій (незалежно від форм власності).

4. Відеодані з систем відеомоніторингу фізичних осіб, які повністю або частково здійснюють відеомоніторинг публічних місць.

5. Відеодані з систем відеомоніторингу транспортних засобів юридичних та фізичних осіб.

Збирання електронних (цифрових) доказів з кіно-, фототехніки, систем відеоспостереження під час процесуально-кримінальних дій проводиться шляхом [16]:

1. Тимчасового доступу до речей і документів на підставі ухвали слідчого судді, суду (ст. 159 КПК України) та ст. 245-1 КПК України;

2. Огляду (ст. 237 КПК України) та Обшуку (ст. 234 КПК України) на підставі ухвали слідчого судді (ст. 235 КПК України);

3. Проведення негласних слідчих (розшукових) дій (глава 21 КПК України).

Згідно ст. 159 КПК України тимчасовий доступ до речей і документів полягає у наданні стороні кримінального провадження особою, у володінні якої знаходяться такі речі і документи, можливості ознайомитися з ними, зробити їх копії та вилучити їх (здійснити їх виїмку).

Тимчасовий доступ до електронних інформаційних систем, комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку здійснюється шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах, комп'ютерних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення.

Забороняється вилучення (виїмка) матеріальних носіїв інформації, пов'язаних із веденням Центральним депозитарієм цінних паперів та депозитарними установами системи депозитарного обліку цінних паперів, облікової системи часток товариств з обмеженою відповідальністю та товариств з додатковою відповідальністю (далі - облікова система часток) і внесенням змін до них.

Тимчасовий доступ до речей і документів здійснюється на підставі ухвали слідчого судді, суду.

Відповідно до вимог ст. 168 КПК України тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку для вивчення їх фізичних властивостей, які мають значення для кримінального провадження, здійснюється лише у разі, якщо вони безпосередньо зазначені в ухвалі суду.

Відповідно до ст. 237 КПК України про огляд зазначено наступне [16]:

1. З метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів та комп'ютерних даних.

2. Огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі).

3. Для участі в огляді може бути запрошений потерпілий, підозрюваний, захисник, законний представник та інші учасники кримінального провадження. З метою одержання допомоги з питань, що потребують спеціальних знань, слідчий, прокурор для участі в огляді може запросити спеціалістів.

5. При проведенні огляду дозволяється вилучення лише речей і документів, які мають значення для кримінального провадження, та речей, вилучених з обігу. Усі вилучені речі і документи підлягають негайному огляду і опечатуванню із завіренням підписами осіб, які брали участь у проведенні огляду. У разі якщо огляд речей і документів на місці здійснити неможливо або їх огляд пов'язаний з ускладненнями, вони тимчасово опечатуються і зберігаються у такому вигляді доти, доки не буде здійснено їх остаточні огляд і опечатування.

У ст. 234-236 КПК України про общук встановлено наступне: правоохоронець має можливість отримання електронних документів у разі невиконання власником ухвали про тимчасовий доступ до речей і документів – у примусовому порядку, шляхом виконання ухвали слідчого судді, суду про дозвіл на проведення обшуку [16].

Ч. 7 ст. 236 КПК України зазначає, що при обшуку слідчий, прокурор має право проводити вимірювання, фотографування, звуко- чи відеозапис, складати плани та схеми, виготовляти графічні зображення обшуканого житла чи іншого володіння особи або окремих речей, виготовляти відбитки та зліпки, оглядати й вилучати документи, тимчасово вилучати речі, які мають значення для кримінального провадження [16].

Вилучені речі та документи, які не входять до переліку, щодо якого прямо надано дозвіл на відшукання в ухвалі про дозвіл на проведення обшуку, та не відносяться до предметів, які вилучені законом з обігу, вважаються тимчасово вилученим майном. Відповідно до ч. 5 ст. 171 КПК України, клопотання слідчого, прокурора про арешт тимчасово вилученого майна повинно бути подано не

пізніше наступного робочого дня після вилучення майна, інакше майно має бути негайно повернуто особі, у якої його було вилучено [16].

Відтак, вилучення електронного документа (матеріалів відеозйомки за допомогою камери спостереження) можливе також шляхом вилучення матеріального об'єкта – носія такої інформації (жорсткий диск комп'ютера, зовнішні носії інформації, CD-диски тощо) під час проведення обшуку на підставі ухвали слідчого судді.

Зміни від 15.03.2022 року до чинного КПК України, яким доповнено ст. 245^1 закріплює нову слідчу (розшукову) дію, а саме зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису. Дана слідча (розшукова) дія була закріплена з метою забезпечення повноти імплементації Конвенції про кіберзлочинність та щодо підвищення ефективності досудового розслідування за «гарячими слідами» та протидії кібератакам.

Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису чи засобів фото-, кінозйомки, відеозапису як слідча (розшукова) дія відповідає ознакам, що притаманні таким дія, а саме: бути законодавчо регламентованою; спрямованою на отримання (збирання) доказів або перевірку вже отриманих доказів у конкретному кримінальному провадженні; яка суттєво зачіпає права і законні інтереси людини; здійснюється компетентною посадовою особою; пов'язана з можливістю застосування заходів державного процесуального примусу.

Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису як слідча (розшукова) дія має бути спрямована на формування або дослідження доказової основи правової позиції певного суб'єкта доказування, тобто показання технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису мають бути визнаними процесуальними джерелами, щоб застосовувати цю дію.

Відповідно до ст. 84 КПК України доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів.

Серед суб'єктів проведення такої слідчої (розшукової) дії як зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису визначено слідчого, прокурора [17].

Ця слідча дія полягає в одержанні копій фото, кінозйомки, відеозапису, здійснених у публічно доступних місцях. Зокрема, кінозйомка й відеозапис можуть проводитися в автоматичному режимі.

Раніше (до появи в КПК України ст. 245[1]) для проведення зняття показань потрібна була обов'язкова ухвала слідчого судді, а тепер підставою може бути постанова слідчого або прокурора. За необхідності до проведення слідчої дії можна залучати спеціаліста. Копіювання інформації проводиться або на надані слідчим чи прокурором носії, або на носії власника. Обов'язково складається протокол.

В [18] наголошується, що ця нова слідча дія не може стосуватися записів, які були проведені у місцях, що відносяться до приватних помешкань осіб.

Як процесуальна дія зняття показань з технічних засобів, як здійснювали відеозапис, полягає в копіюванні візуальної чи аудіовізуальної цифрової (електронної) інформації, а також, ймовірно, інших похідних метаданих з оригінального носія інформації, що міститься чи використовувався у відповідному приладі, на окремий носій інформації, який надалі долучається до матеріалів досудового розслідування.

Отримані в ході здійснення цієї процесуальної дії відомості можуть надалі бути використаними як докази, оскільки джерело походження даних і правомірність процесу копіювання зафіксовані як у постанові слідчого, прокурора про зняття показань техприладів і техзасобів, так і в протоколі процесуальної дії.

Згідно з нормами, що містяться в абз.1 ч.1 ст. 298-1, ст. 300 КПК, результатом зняття показань засобів, як здійснювали відеозапис, є, власне, «показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису» як окреме процесуальне джерело доказів, яке може бути отримане (створене) та використане (за загальним правилом) лише у кримінальних провадженнях про кримінальні проступки [16].

Ця слідча дія полягає в одержанні копій фото, кінозйомки, відеозапису, здійснених у публічно доступних місцях. Зокрема, кінозйомка й відеозапис можуть проводитися в автоматичному режимі.

Раніше для проведення зняття показань потрібна була ухвала слідчого судді, а тепер підставою може бути постанова слідчого або прокурора. За необхідності до проведення слідчої дії можна залучати спеціаліста. Копіювання інформації проводиться або на надані слідчим чи прокурором носії, або на носії власника. Обов'язково складається протокол.

Згідно ст. 264 КПК України стосовно зняття інформації з електронних інформаційних систем зазначено наступне [16]:

1. Пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в електронній

інформаційній системі або її частині, що має значення для певного досудового розслідування.

2. Не потребує дозволу слідчого судді здобуття відомостей з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту.

3. В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки електронної інформаційної системи, в якій може здійснюватися втручання у приватне спілкування.

Відповідно до 265 КПК України, щодо фіксації та збереження інформації, отриманої з електронних комунікаційних мереж за допомогою технічних засобів та в результаті зняття відомостей з електронних інформаційних систем встановлено [16]:

1. Зміст інформації, що передається особами через електронні комунікаційні мережі, з яких здійснюється зняття інформації, зазначається у протоколі про проведення зазначених негласних слідчих (розшукових) дій. При виявленні в інформації відомостей, що мають значення для конкретного досудового розслідування, в протоколі відтворюється відповідна частина такої інформації, після чого прокурор вживає заходів для збереження знятої інформації.

2. Зміст інформації, одержаної внаслідок здійснення зняття відомостей з електронних інформаційних систем або їх частин, фіксується на відповідному носієві особою, яка здійснювала зняття у спосіб, що забезпечує обробку, збереження або передання інформації.

Згідно ст. 266 КПК України стосовно дослідження інформації, отриманої при застосуванні технічних засобів зазначено наступне [16]:

1. Дослідження інформації, отриманої при застосуванні технічних засобів, у разі необхідності здійснюється за участю спеціаліста. Слідчий вивчає зміст отриманої інформації, про що складається протокол. При виявленні відомостей, що мають значення для досудового розслідування і судового розгляду, в протоколі відтворюється відповідна частина інформації, після чого прокурор вживає заходів для збереження отриманої інформації.

2. Носії інформації, на яких зафіксовані відомості, отримані в результаті проведення зазначених негласних слідчих (розшукових) дій, повинні зберігатися у стані, придатному для їх дослідження, до набрання законної сили вироком суду.

3. Носії інформації, на яких зафіксовані відомості, отримані в результаті проведення зазначених негласних слідчих (розшукових) дій, можуть бути предметом дослідження відповідних спеціалістів або експертів у порядку, передбаченому цим Кодексом.

Що стосується слідчих (розшукових) дій під час досудового розслідування кримінальних проступків в ст. 300 КПК України встановлено [16]:

1. Для досудового розслідування кримінальних проступків дозволяється виконувати всі слідчі (розшукові) дії, передбачені цим Кодексом, та негласні слідчі (розшукові) дії, передбачені частиною другою статті 264 та статтею 268 цього Кодексу, а також відбирати пояснення для з'ясування обставин вчинення кримінального проступку, отримувати висновок спеціаліста, що має відповідати вимогам до висновку експерта, знімати показання технічних приладів і технічних засобів у провадженнях щодо вчинення кримінальних проступків, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису, вилучати знаряддя і засоби вчинення кримінального проступку, речі і документи, що є безпосереднім предметом кримінального проступку, або які виявлені під час затримання особи, особистого огляду або огляду речей, до внесення відомостей про кримінальний проступок до Єдиного реєстру досудових розслідувань.

Відповідно до КПК України передбачено наступні форми отримання електронного документа (матеріалів фото- та відеозйомки) з приміщення, що належить суб'єкту господарювання (юридичній чи фізичній особі) [16]:

– отримання копії електронного документа (матеріалів фото- та відеозйомки) за згодою та участю власника на підставі постанови слідчого, прокурора;

– отримання копії електронного документа (матеріалів фото- та відеозйомки) під час виконання ухвали слідчого судді, суду про тимчасовий доступ до речей і документів;

– вилучення матеріального носія інформації під час обшуку або огляду житла чи іншого володіння особи на підставі ухвали слідчого судді, у разі, якщо вилучення таких матеріальних носіїв прямо вказано в ухвалі слідчого судді, або з наступним протягом 24 годин поданням клопотання про арешт такого майна як тимчасово вилученого;

– отримання копії електронного документа під час обстеження шляхом таємного проникнення до публічно недоступних місць, житла чи іншого володіння особи, яке проводиться на підставі ухвали слідчого судді.

Відповідно до ст. 2 Закону України «Про оперативно-розшукову діяльність» «оперативно-розшукова діяльність – це система гласних і негласних пошукових, розвідувальних та контррозвідувальних заходів, що здійснюються із застосуванням оперативних та оперативно-технічних заходів» [19]. А ст. 1 цього Закону України наголошує, що «завданнями оперативно-розшукової діяльності є пошук і фіксація фактичних даних про протиправну діяльність окремих осіб та груп, розвідувально-підривну діяльність спеціальних служб іноземних держав та організацій з метою припинення правопорушень та в інтересах кримінального судочинства, а також отримання інформації в інтересах суспільства і держави» [19].

Отже робота оперативних підрозділів правоохоронного органу пов'язана, в першу чергу, з виявленням, попередженням, розкриттям і розслідуванням злочинів, а оперативно-розшукова діяльність (ОРД) здійснюється ними також з метою отримання інформації, її накопичення, обробки, аналізу і висновків та вжиття відповідних заходів [20]. Для цього ними проводиться комплекс заходів по збиранню, обробці, аналізу та видачі інформації оперативного та оперативно-розшукового призначення, яка використовується, зокрема, при розкритті та розслідуванні злочинів.

Отримання оперативної інформації – це одна із форм інформаційно-аналітичної роботи в ОРД, у межах якої відбувається пошук і фіксація відомостей про протиправні діяння окремих осіб та груп, з використанням наявних сил, засобів і методів ОРД, в інтересах ОРД та досудового розслідування [21].

Оперативна інформація може бути первинною, перевіреною (достовірною), тотальною (повною, вичерпною) або частковою, поточною, конкретною, загальною або деталізованою, відкритою (доступною), закритою (таємною, особливо таємною, конфіденційною, для службового користування), оціночною, програмною, прямою і непрямою [20]. При всій розбіжності характеристик інформації чи при її наявності в достатніх обсягах, працівники оперативних підрозділів не можуть нехтувати будь-якою додатковою інформацією, яка б вона не була початковою чи загальною.

Збирання інформації, її накопичення та обробка є безперервним і трудомістким процесом, який складає основну форму оперативно-розшукової роботи, головним напрямком якої є збирання конфіденційної інформації негласними методами. Отримана оперативна інформація дозволяє орієнтуватись в ситуаціях, планувати подальші дії, відслідковувати результативність здійснюваних заходів, ухилятися від випадковостей і уникати помилок, прийняти тактичні і стратегічні рішення, ставити нові завдання по збору додаткової інформації [20].

Переваги, що характерні для ОРД при зборі інформації про злочин, більш успішно можуть бути реалізовані тільки в межах процесу доказування, який встановлений законом, тобто, за рахунок послідовного їх «включення» до процедур, що передбачені КПК. Оперативні підрозділи вирішують завдання щодо надання юридичної чинності отриманій оперативній інформації за рахунок тих дій, що здійснюються до моменту передачі її слідчому (а у відповідних випадках – і прокурору чи суду), а слідчий від моменту надходження до нього таких даних і до закінчення розслідування.

Отже, отримані відеодані під час здійснення ОРД оперативними підрозділами гласними чи негласними діями також відноситься до оперативної інформації і слугують одним із важливих джерел здійснення оперативно-розшукової ідентифікації відповідних осіб, транспортних засобів або інших об'єктів.

Оперативно-розшукова ідентифікація – це форма інформаційно-аналітичної роботи в ОРД, спрямована на встановлення тотожності об’єкта або особи за сукупністю загальних і окремих ознак шляхом їх порівняльного дослідження з використанням сил, засобів і методів ОРД [21].

Таке оперативне ототожнення осіб та інших об’єктів при здійсненні ОРД проводиться у випадках, коли пред’явлення для впізнання, передбачене КПК, неможливо здійснити з різних обґрунтованих причин, але сам акт пізнавання можливий, доцільний, необхідний і здійснимий лише оперативно-розшуковим шляхом [21].

Механізм оперативно-розшукової ідентифікації охоплює низку послідовних дій суб’єкта його застосування: роздільне дослідження ознак вже ідентифікованої та ідентифікуючої особи чи об’єкта; їх порівняльне дослідження; оцінку результатів порівняння; прогноз подальших дій, ухвалення рішення. Метою оперативно-розшукової ідентифікації є емпіричне виявлення за заздалегідь відомими загальними ознаками осіб і об’єктів ідентифікації, а також отримання нових знань про ці об’єкти з метою припинення правопорушень та в інтересах кримінального судочинства, безпеки громадян, суспільства і держави [21].

Для підрозділів кримінального аналізу Національної поліції України наведені вище заходи є дуже важливими. Адже разом з іншими напрямами діяльності окремими завдання кримінального аналізу є забезпечення аналітичного супроводження заходів ОРД та досудового розслідування шляхом: здійснення виявлення та ідентифікації осіб та об’єктів розслідування; напрацювання детального аналітичного продукту щодо цих осіб та об’єктів; оброблення великого обсягу здобутої інформації, що унеможливлює відстеження та пов’язування фактів без застосування спеціальних аналітичних методів; аналізу складної і розгалуженої структури зв’язків об’єктів оперативно-розшукової справи або кримінального провадження тощо [1-4].

Таким чином, все наведене у цьому розділі роботи показує, що відеодані, що отримані відповідно до КПК у якості речового доказу (електронного доказу), а також у якості оперативної інформації за рахунок здійснення відповідних заходів ОРД, можуть мати правове підґрунтя (у разі дотримання вимог законодавства) і займати важливе місце в діяльності підрозділів кримінального аналізу Національної поліції України. А, отже, вони можуть бути правомірно використані щодо завдання здійснення виявлення та ідентифікації на отриманих відеоданих фізичних осіб по їх фізичним, фізіологічним чи поведінковим ознакам, а також транспортних засобів та інших об’єктів, що є однією із важливих задач кримінального аналізу.

У наступному розділі роботи проаналізуємо за рахунок яких методів та технологій можливо забезпечити виявлення і розпізнавання фізичних осіб та інших об’єктів на відеоданих, що отримані правоохоронними органами для аналізу.

3. ТЕОРЕТИЧНІ ОСНОВИ СУЧАСНИХ МЕТОДІВ ТА ТЕХНОЛОГІЙ ВИЯВЛЕННЯ ТА РОЗПІЗНАВАННЯ НА ВІДЕОДАНИХ ФІЗИЧНИХ ОСІБ ПО ЇХ ФІЗИЧНИМ, ФІЗІОЛОГІЧНИМ ЧИ ПОВЕДІНКОВИМ ОЗНАКАМ, А ТАКОЖ ТРАНСПОРТНИХ ЗАСОБІВ ТА ІНШИХ ОБ'ЄКТІВ

3.1. Огляд основних методів і технологій виявлення та розпізнавання на відеоданих облич людей

Процесом виявлення та розпізнавання обличчя прийнято називати набір різних операцій для ідентифікації людини по цифровому зображенню, отриманого з відео потоку.

У загальному вигляді цей процес виглядає наступним чином: після того, як система отримала зображення з камери, здійснюється пошук області особи на зображенні та за допомогою алгоритмів визначаються межі обличчя (етап виявлення). Тобто система має знайти де саме на зображенні знаходиться об'єкт ідентифікації, визначити його точні або приблизні координати.

Виявлення особи чи осіб – це визначення кількості облич, присутніх на зображенні, і виявлення їх положення. Загалом, процес виявлення осіб складається з двох етапів, на першому з яких зображення сканується цілком для виявлення області (функцій), які можуть бути ідентифіковані як обличчя. Далі йде локалізація, яка дає більш точну оцінку розмірів і положення облич.

Відома з [22] класифікація методів виявлення людських облич представлена на рис. 3.1.

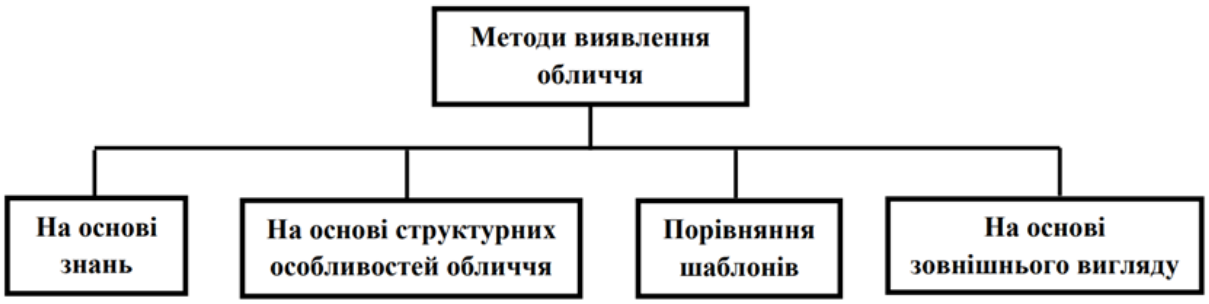


Рисунок 3.1 – Класифікація методів виявлення обличчя

Ці методи поділяються на наступні чотири категорії [23].

1 категорія. Методи на основі знань використовують для виявлення облич накопичені знання. Зрозуміло, що кожне людське обличчя має ніс, очі та рот, які розташовані на певній відстані між собою. Найважливішим у цій групі методів є вибір відповідного набору правил. Такий підхід не може знайти багато облич у кількох зображеннях.

2 категорія. Методи з використанням функцій полягають у знаходженні облич, використовуючи різні структурні особливості обличчя. В першу чергу створюють класифікатор структурних особливостей, а потім використовують його для розмежування частин обличчя та не обличчя. Основна ідея полягає у тому, щоб перейти межу інстинктивного знання облич. Цей підхід розділений на кілька частин і є успішним для більшості фотографій (відеокадрів) з великою кількістю облич.

3 категорія. В методах порівняння шаблонів використовуються наперед визначені і параметризовані шаблони для знаходження облич. В цьому випадку основним є співвідношення вхідними зображеннями і існуючими шаблонами облич. Взагалі кажучи, людське обличчя поділяється на чотири частини – очі, ніс, рот і контур обличчя. Інший спосіб визначення обличчя використовує технологію виявлення ребер. Такий підхід є простим, проте недостатнім для виявлення обличчя. Однак для вирішення таких проблем можна використати шаблони, які деформуються.

4 категорія. Методи, що використовують зовнішній вигляд, орієнтовані на зовнішній вигляд і залежить від набору делегатів зображень обличчя, що навчаються для з’ясування моделі обличчя. Для пошуку відповідних характеристик зображень обличчя використовуються машинне навчання і статистичний аналіз.

Методи на основі зовнішнього вигляду, в свою чергу поділяється на такі похідні методи [23]:

– на основі власних поверхонь, що використовується для виявлення облич за допомогою аналізу основних компонентів;

– на основі розподілу, які можуть бути використані для визначення підпростору, що представляє схеми обличчя;

– з використанням нейронних мереж, дозволяють виявити об'єкти, обличчя, емоції та розпізнати обличчя;

– підтримки векторних машин, що використовують лінійні класифікатори, які максимально збільшують можливість отримання правильного рішення на основі навчальних наборів;

– використання Байєвих класифікаторів, які обчислюють ймовірність наявності обличчя на фотографії (відеокадрі), обчислюючи частоту серії рисунків в навчальних зображеннях;

– використання прихованої моделі Маркова та Марківських випадкових полів, у яких є варіанти рис обличчя, які зазвичай характеризують смужками пікселів;

– на основі індуктивного навчання, що використовують відповідні алгоритми.

Алгоритми виявлення об’єктів на відео розділені на чотири основні категорії: відстеження областей, відстеження по активному контуру, відстеження за характерними признаками, відстеження по моделі [24].

Алгоритми виявлення областей застосовуються для відстеження об'єктів в відповідно до змін областей зображення, відповідних рухомих об'єктів.

Алгоритми відстеження по активному контуру відстежують об'єкти шляхом подання їх обрисів у вигляді обмежуючих контурів і динамічного оновлення цих контурів на наступних кадрах. Ці алгоритми мають своєю метою пряме вилучення форми об'єктів і дають більш повний опис об'єктів в порівнянні з алгоритмами відстеження областей.

Алгоритми виявлення за характерними ознаками виконують розпізнавання і відстеження об'єктів шляхом вилучення елементів зображення, їх об'єднання в характерні ознаки більш високого рівня і наступного порівняння з характерними ознаками інших зображень.

Щоб підвищити ефективність якості виділення облич і подальшого їх розпізнавання, в системах розпізнавання облич проводять для вхідних зображень етапи попередньої обробки. Зображення після визначення обличчя на кадрі і визначення положення голови, розміру, пози і ключових особливостей воно відображається шляхом нормалізації: масштабоване, закодоване, перетворене в горизонтальну лінію, що з’єднує центри очей. Для зменшення рівня шуму під час попередньої обробки використовуються різні фільтри (гауссовський, медіанний та ін.).

Методи попередньої обробки досить різноманітні і залежать від завдань досліджень. Найчастіше зустрічаються [22]:

– нелінійні фільтри – фільтри, що використовують для видалення імпульсного шуму (окремих точок з максимальною (білої) чи мінімальної (чорної) яскравістю) на зображенні;

– фільтр Гауса (Gauss) – фільтр розмиття зображення, найчастіше використовують, якщо зображення має шум і дрібні деталі, які не вимагають відділення від фону, і їх можна розмити, що приглушує шум;

– медіанні фільтри – фільтри, що використовують для збереження перепадів яскравості контурів і придушення імпульсних шумів.

Далі йде саме етап розпізнавання, на якому обличчя трансформується (змінюється його яскравість, воно вирівнюється, масштабується, і т.д.) і приводиться до деякого заданого виду. Після чого, відбувається обчислення ознак і безпосередньо порівняння їх із закладеними в базу даних еталонами.

В загальному вигляді загальний алгоритм розпізнавання облич можна представити наступним чином (рис. 3.2).

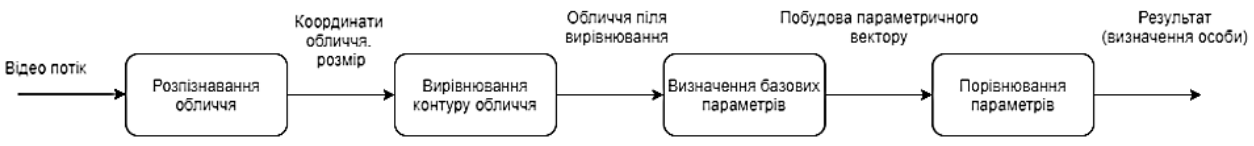


Рисунок 3.2 – Загальний алгоритм розпізнавання облич

Заключний етап порівняння параметрів називається ідентифікація або верифікація, в залежності від застосованої системи.

Верифікація – це порівняння зразків за схемою «1:1». Тобто для визначення особистості система порівнює біометричний зразок з одним із біометричних шаблонів, що зберігається в базі даних, і дає відповідь на питання «Чи є ця людина тією людиною, з якою ми порівнюємо (на шаблоні)?».

Ідентифікація – це порівняння зразків за схемою «1:N». Для визначення особистості система порівнює біометричний зразок з усіма наявними шаблонами обличь, що зберігаються в базі даних, і дає відповідь на питання «Хто це?».

Коли зображення у вигляді цифрових даних з камер передається на комп'ютер – воно обробляється за допомогою спеціального методу, який визначає розташування області обличчя за її основними рисами (очей, рота, брів, носа і т. д.). Таких методів виявлення осіб існує багато і більшість з них в реальних системах ідентифікації осіб представляють собою комбінацію різних методів.

Основними такими найбільш відомими методами розпізнавання обличь є [25-32]:

- геометричний;
- головних компонент;
- гнучкого порівняння на графах;
- прихованої марковської моделі;
- Віоли-Джонса;
- нейромережеві;
- бінарних шаблонів.

Розглянемо їх докладніше.

Геометричний метод був одним із перших методів розпізнавання обличчя, що полягає у виборі ключових антропометричних точок на обличчі особи й формуванні набору ідентифікаційних ознак. Дані точки являють собою губи, ніс, кутики очей, центр ока, вуха тощо (рис. 3.3).

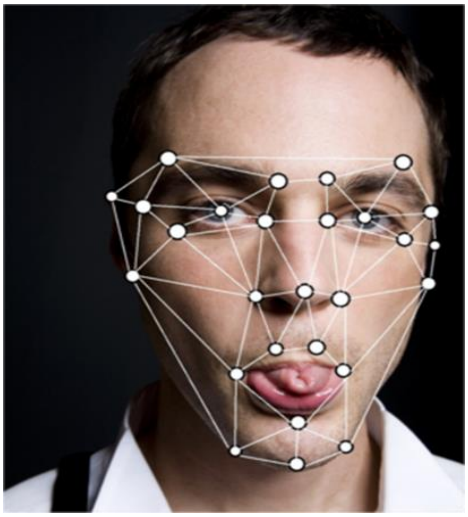


Рисунок 3.3 — Ключові антропометричні точки та лінії між ними на фронтальній проекції обличчя людини

Як правило, ідентифікаційними антропометричними точками на обличчі людини обираються (рис. 3.3): центри брів, центри зіниць, верхні крайні точки вух, правий кут правого і лівого ока, ліві кути очей, кінець мочок вух, крайні точки носа по горизонталі, кінчик носа, кути рота, центр рота — як точка перетину лінії, яка розділяє верхню та нижню губу об’єкта, та перпендикуляра опущеного із точки, що позначає кінчик носа, кінчик підборіддя.

За результатами визначення цих точок вимірюються відстані (рис. 3.3): між центрами сітківки очей; між внутрішніми куточками очей; між центром сітківки ока і центром брови; між центром сітківки ока і серединою лінії змикання губ; між центром сітківки ока і нижньою точкою носа; максимальна ширина носа; між центром сітківки ока і підборіддям; між серединою лінії змикання губ і підборіддя; між кінчиком носа і підборіддя; ширина роту; ширина лиця на рівні лінії очей; ширина лиця на рівні нижньої точки носу; ширина лиця на рівні лінії змикання губ; між зовнішнім краєм ока і верхньою точкою вуха; між верхніми точками вух; між нижніми точками вух; між верхніми і нижніми точками вуха.

Саме ці дані є ідентифікаційними ознаками кожної людини. Введення цих ознак у форматі відносини для ідентифікаційних одиниць робить їх масштабно незалежними від відстані, із якої виконується фотографія (відеозйомка) людини.

Геометричні методи забезпечують достатньо низьку достовірність, але для їх використання не потрібно дорого обладнання.

Метод головних компонент (МГК, англ. *Principal Component Analysis*, PCA) базується на процесі розпізнавання, що будує для вхідного зображення певної кількості базових компонент зображень. Цей метод застосовується для того, щоб стиснути інформацію без важливих втрат інформативності.

В задачі розпізнавання осіб його використовують, першочерговим чином, для представлення зображення особи вектором малої розмірності або ж головних компонентів, що порівнюється потім вже із еталонними векторами, що є закладеними в базу даних. Головним завданням методу головних компонент є значне зменшування розмірів простору ознак таким чином, щоб б він найкраще описував «типові» образи, які належать певній множині осіб.

Застосовуються даний метод для того, щоб виявити різні мінливості у навчальній вибірці зображень обличь та виконати опис цієї мінливість в базисі декількома ортогональних векторів, що називаються власними (eigenface). Отриманий один раз на навчальній вибірці зображень обличь набір власних векторів застосовується для кодування усіх інших подальших зображень обличь, що будуть представлені зваженою комбінацією даних власних векторів.

Суть цього методу зображена на рис. 3.4: першочергово увесь навчальний набір осіб перетворюється на одну загальну матрицю даних. У цій матриці кожен рядок – це один екземпляр зображення обличчя, що розкладений у рядок. Усім особам навчального набору необхідно обов'язково надати єдиний розмір. Вони всі також повинні бути з нормованими гістограмами.

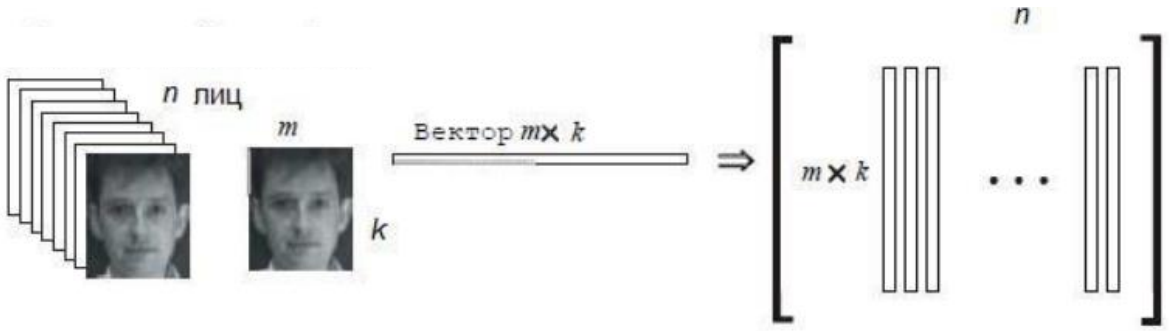
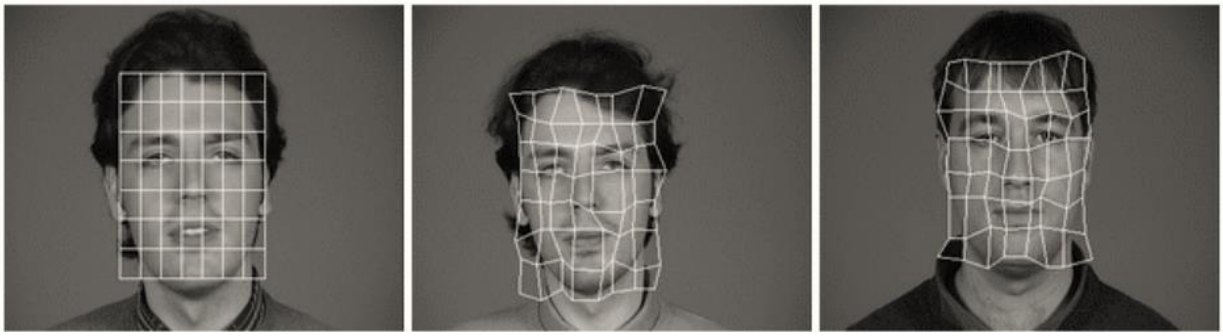


Рисунок 3.4 – Перетворення навчального набору осіб в одну загальну матрицю

Цей метод чудово зарекомендував себе у практичних додатках. Проте, недоліком даного методу є чутливість до освітлення. В тих випадках, коли на зображенні обличчя є певні зміни у освітленості або ж виразі обличчя, ефективність методу значною мірою зменшується.

Метод гнучкого порівняння на графах. Суть даного методу полягає у порівнянні графів, які описують зображення обличчя особи. Зображення, що представлені у вигляді графів (решітки) із зваженими вершинами і ребрами (рис. 3.5).



а б в

Рисунок 3.5 — Деформація графа у вигляді регулярної решітки

Для розпізнавання графи на обличчі можуть бути представлені як у вигляді прямокутної решітки (рис. 3.5а), так і структуру, що утворена антропометричними точками особи (рис. 3.3).

На етапі розпізнавання один із графів, а саме — еталонний (що зроблений заздалегідь для особи), буде незмінним (рис. 3.5а), а у той час як інші (3.5б, в) деформуються із метою найоптимальнішої підгонки відповідно до першого.

Для вдосконалення цього методу на вершинах графа для обрахування значення ознак найчастіше всього застосовують комплексні значення фільтрів Габора (Gabor) чи їх впорядкованих наборів — Габоровських вейвлетів (або ж строїв Габора), що обчислюються у певній локальній області вершини графа локально, шляхами згортки значення яскравості пікселів із фільтрами Габора.

Ребра графа зважуються (обчисляються) відстанями між суміжними вершинами. Різниця — відстань, дискримінаційна характеристика між двома графами вираховується за допомогою певної цінової функції деформації, яка враховує як відмінність між значеннями ознак, що обчислені в вершинах, так й ступінь деформації ребер графа (рис. 3.5).

Деформація графа відбувається зміщенням кожної із його ж вершин на певну відстань у потрібних напрямах щодо її вихідного місця розташування та вибору її такої позиції, завдяки якій різниця між значеннями ознак на вершині деформованого графа та тій, що відповідає їй вершині еталонного графа буде максимально мінімальною.

Така операція робиться по черзі для усіх вершин графа до тих пір, коли не буде досягнуто найменшої сумарної відмінність між ознаками деформованого та еталонного графів. Значення такої цінової функції деформації при такому положенні деформованого графа й буде мірою відмінності між вхідним зображенням обличчя та еталонним графом.

Даний метод забезпечує високий відсоток точності розпізнавання й низьку чутливість до освітлення. Проте метод гнучкого порівняння є повільним та затратним в плані споживання ресурсів, а також таким, що має властивість нелінійності залежності часу роботи від розміру бази даних.

Методи, що основані на використанні прихованої марковської моделі. Марковська модель — це математична модель, що використовується для описання переходів від одного стану системи в інший, яка має властивість, названу ім’ям математика Андрія Маркова, тобто якщо наступний стан залежить тільки від теперішнього і ніяк не залежить від послідовності станів. Марковські моделі задаються скінченим числом станів, яка є в доступності у системи, а також матрицею переходів, де визначена ймовірність переходів від одного стану до іншого.

На основі моделі ставиться задача знаходження невідомих параметрів на основі параметрів, за якими ведеться спостереження. Отримані параметри можуть бути використані в подальшому аналізі для розпізнавання обличь.

Адже з точки зору розпізнавання – зображення це двомірний дискретний сигнал. Важливу роль в побудові моделі зображення грає вектор спостереження, тобто обхід зображення. Для того, щоб уникнути розбіжностей в описах, зазвичай використовують прямокутне вікно для розпізнавання. Щоб не втрачати області даних, прямокутні вікна мають перекривати одне інше. Значення для перекривання, як і області розпізнавання підбираються експериментально.

Після зняття блоку виконують його перетворення в цифровий блок за одним з двох методів: Кархунена-Лоева (Karhunen-Loeve Transform, KLT) або дискретного косинуса без конверсії (Discrete-Cosine Transformation, DCT).

Метод KLT в базовому вигляді дає не надто хороші результати, хоча модифікації методів, які вимагають значних затрат обчислювальних ресурсів, цього недоліку позбавлені.

Натомість DCT простіший і більш стійкий до шумів, трансформації, спотворень.

Після отримання блоку пікселів його переводять у вектор, який містить лише значимі елементи. Значимі – це якась кількість перших коефіцієнтів DCT.

Після цього отримані вектори розподіляють по станах моделі. Стани моделі представляють певні класи об'єктів. В загальному це 5 суперстанів, що відповідають областям обличчя – лобова частина, очі, ніс, рот, підборіддя. Перехід в наступний стан відбувається після попереднього, в наступний суперстан – після завершення попереднього.

Вважається, що обличчя зберігаються в базі даних на різних рівнях абстракції. На найнижчому рівні – це набір пікселів. Цей рівень – просто для відштовхування, адже його використання в обчислення вимагає дуже великих обчислювальних ресурсів. Саме тут вводиться поняття сигнатури – числового дескриптора, який описує візуальні характеристики певної області. Користь використання сигнатур зрозуміла, вони вимагають набагато менших затрат на оновлення конфігурацій обчислювальної техніки. Пошук здійснюється саме на основі порівнянь наборів сигнатур. Пошук ведеться поки міра схожості наборів сигнатур не буде відповідати заданим вимогам точності.

Практично, тобто програмно реалізація здійснюється на основі трикутного дерева (*Really Fixed Query Tree*) – структури для пошуку співпадінь в залежності від критеріїв пошуку (рис. 3.6).

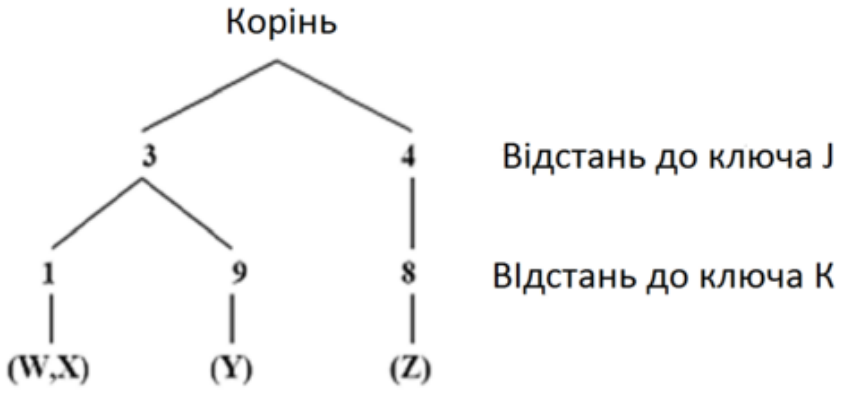


Рисунок 3.6 – *Really Fixed Query Tree* (W, X, Y, Z – елементи; J, K – ключі)

Компоненти цього дерева – міра відстані, набір ключових зображень і набір елементів бази даних. Ребра від кореня до листя визначають індекс листя, листя дерева в своє чергу містять елементи бази даних. Шлях від кореня до листя – це відстань від елемента бази даних до кожного з ключів.

Основна проблема методів на основі моделі Маркова – це робота, власне, з моделями, тобто алгоритм визначає, яка з моделей краще підходить для характеристики цього зображення. Основним недоліком є необхідність підбирати параметри моделі для кожної бази даних.

Також, алгоритм навчання здатний максимізувати відгук кожного зображення на свою модель, а от мінімізувати відгук на інші моделі він не може. Фактично, цей алгоритм зручно використовувати на перших етапах розпізнавання.

Метод Віоли-Джонса та ознаки Хаара (*Viola-Jones Object Detection*)**.** Метод, запропонований Полом Віолою і Майклом Джонсом в 2001 році, став справжнім проривом в цій області. Цей метод набув великої популярності завдяки високій точності і серйозної теоретичної основі.

Основні принципи, на яких базується метод [25-29]:

– використовуються зображення в інтегральному уявленні, що дозволяє швидко обчислювати необхідні об’єкти;

– використовуються ознаки Хаара, за допомогою яких відбувається пошук потрібного об’єкта (в цьому контексті, обличчя і його рис);

– використовується бустінг для вибору найбільш підходящих ознак для шуканого об’єкта на цій частині зображення;

– всі ознаки надходять на вхід класифікатора, який дає результат «так» або «ні»;

– використовуються каскади ознак для швидкого відкидання вікон, де не знайдено обличчя.

Найбільш популярний цей метод для пошуку об’єктів у відеопотоці. Також цей детектор має вкрай низьку ймовірністю помилкового виявлення обличчя. Алгоритм навіть добре працює і розпізнає риси обличчя під невеликим кутом, приблизно до 30 градусів. При куті більше 30 градусів точність різко падає.

Для того, щоб проводити будь-які дії з даними в методі Віоли-Джонса, використовується інтегральне представлення зображень. Однією з корисних особливостей інтегрального представлення є можливість дуже швидко вирахувати суму пікселів довільного прямокутника (або будь-який інший фігури, яку можна апроксимувати декількома прямокутниками).

Інтегральне представлення зображення – це матриця, що збігається за розмірами з вихідним зображенням. У кожному елементі її зберігається сума інтенсивності яскравості всіх пікселів, що знаходяться лівіше і вище даного елемента. Розрахунок матриці займає лінійний час, пропорційне числу пікселів в зображенні, тому інтегральне зображення прораховується за один прохід.

Інтегральне представлення зображення використовується для обчислення ознак Хаара. Ознаки Хаара (*Haar-Like Features*) – ознаки цифрового зображення, використовувані в розпізнаванні образів.

Ознака Хаара складається з суміжних прямокутних областей (рис. 3.7).

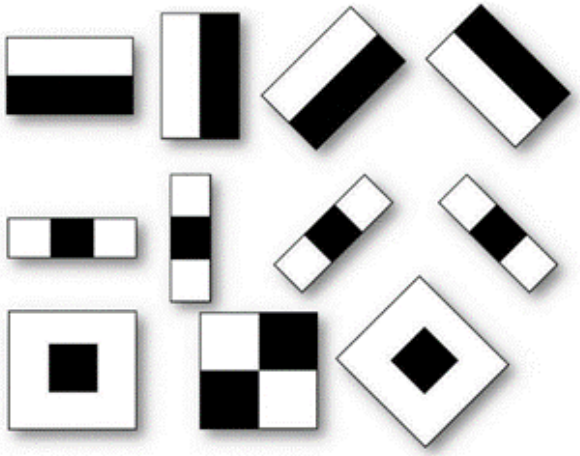


Рисунок 3.7 – Стандартні ознаки Хаара

Найпростішу прямокутну ознаку Хаара можна визначити як різницю між сумою пікселів двох суміжних областей всередині прямокутника, який може займати різні положення і масштаби на зображенні. Такий вид ознак називається 2-прямокутним. Алгоритм Віоли-Джонса визначає також 3-прямокутні і 4-прямокутні ознаки, які складаються із трьох чи чотирьох областей відповідно. Крім того, є похилі ознаки Хаара, які мають кут 45°. Це дозволяє максимально покрити простір ознаки та покращити якість розпізнавання.

Кожна ознака може показати наявність (або відсутність) будь-якої конкретної характеристики зображення, такий як кордону або зміна текстур. Наприклад, 2-прямокутна ознака може показати, де знаходиться межа між темним і світлим регіонами.

Вони позиціонуються на зображенні, далі сумуються інтенсивності пікселів в областях, після чого обчислюється різниця між сумами. Ця різниця і буде значенням певної ознаки, визначеного розміру, певним чином позиційованої на зображенні. Загальним для всіх зображень є те, що область в районі очей темніше, ніж область в районі щік. Отже загальною ознакою Хаара для облич є два суміжних прямокутних регіони, що лежать на очах і щоках (рис. 3.8).

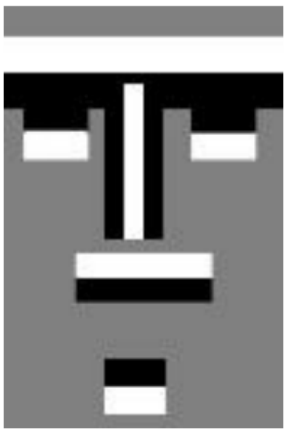


Рисунок 3.8 – Приклад розташування ознак Хаара на обличчі людини

Ключовою особливістю ознак Хаара є найбільша, в порівнянні з іншими ознаками, швидкість. Обчислюється значення такої ознаки за формулою: F =X-Y, де X – сума значень яскравості точок закриваються світлою частиною ознаки, Y – сума значень яскравості точок що закриваються темною частиною ознаки. Ознаки Хаара дають точкове значення перепаду яскравості по осі X і Y відповідно.

Алгоритм сканування вікна з ознаками виглядає так [23]:

– обирається вікно сканування та використовувані ознаки для основних рис обличчя;

– вікно сканування послідовно просувається по зображенню з кроком в 1 клітинку вікна (припустимо, розмір самого вікна 24x24 клітинки);

– при скануванні зображення в кожному вікні обчислюється приблизно 200 тис. варіантів розташування ознак, за рахунок зміни масштабу ознак і їх положення в вікні сканування;

– сканування проводиться послідовно для різних масштабів скануючого вікна;

– всі знайдені ознаки потрапляють до класифікатору, який фіксує наявність рота, носа, та іншої ознаки певної розмірності у певному регіоні і знаходить найближчий зразок у базі.

Для поліпшення точності використовується технологія так званого бустінга. Бустінг (англ. boosting) – комплекс методів підсилення у машинному начанні, що сприяють підвищенню точності аналітичних моделей [25, 26]. В його основі лежить побудова каскаду класифікаторів, кожен з яких (крім першого) навчається на помилках попереднього. Наприклад, один з перших алгоритмів бустінга використовував каскад з 3-х моделей, перша з яких навчалася на всьому наборі даних, друга – на вибірці прикладів, в половині з яких перша дала правильні відповіді, а третя – на прикладах, де «відповіді» перших двох розійшлися. Таким чином, має місце послідовна обробка прикладів каскадом класифікаторів, причому так, що завдання для кожного наступного стає важче. Результат визначається шляхом простого голосування: приклад відноситься до того класу, який виданий більшістю моделей каскаду.

Хоч він і має нижчу точність за сучасніші методи, такі як згорткова нейронна мережа (ЗНМ), його ефективність і компактний розмір (лише близько 50 тисяч параметрів у порівнянні з мільйонами параметрів для типових ЗНМ) означають, що його все ще використовують у випадках з обмеженою обчислювальною потужністю.

Методи, що основані на використанні нейронних мереж дають одні з найкращих результатів розпізнавання образів [32-34]. Основною особливістю таких мереж є їх здатність до навчання на наборі готових прикладів заздалегідь занесених в базу даних. Під час навчання нейронних мереж, мережа автоматично витягує ключові ознаки і будує взаємозв'язок між ними.

Після цього, для того щоб розпізнати до цього невідомий об'єкт, навчена нейронна мережа застосовує отриманий досвід.

Головним компонентами нейромережі є нейрони, що поєднані зв’язками. По суті, нейрон — це закінчений елемент програмного коду, який формує нейронну сітку. Кожен нейрон може сприймати вхідні дані, працювати з ними ну і також ще передати далі із допомогою синапсу. Або ж по-іншому, нейрон — це є базовою одиницею штучного інтелекту. А нейронна мережа — комп’ютерна реалізація людського мозку. Сигнали виконують передачу по зваженим зв’язкам, із кожним з яких зв’язаний ваговий коефіцієнт або ж вага.

Штучний нейрон може імітувати у першому наближенні властивості біологічного нейрона. На вхід штучного нейрона буде подаватися множина сигналів, що являються виходами інших нейронів. Кожен із входів множиться на відповідну вагу, таку ж як його синаптична сила зв’язку з іншими нейронами, ну і всі виходи тоді підсумовують, при цьому визначаючи рівень активації нейрона.

Найкращі результати в області розпізнавання облич показала згорткова нейронна мережа (ЗНМ, англ. *Convolutional Neural Network, CNN*). Відмінними рисами ЗНМ є локальні рецепторні поля (забезпечують локальну двовимірну зв'язність нейронів), загальні ваги (забезпечують детектування деяких рис в будь-якому місці зображення) і ієрархічна організація з просторовим семплінгом (прикладами, англ. *Spatial Subsampling*). Завдяки цим нововведенням ЗНМ забезпечує часткову стійкість до змін масштабу, зсувів, поворотам, зміні ракурсу і іншим спотворень (рис. 3.9).

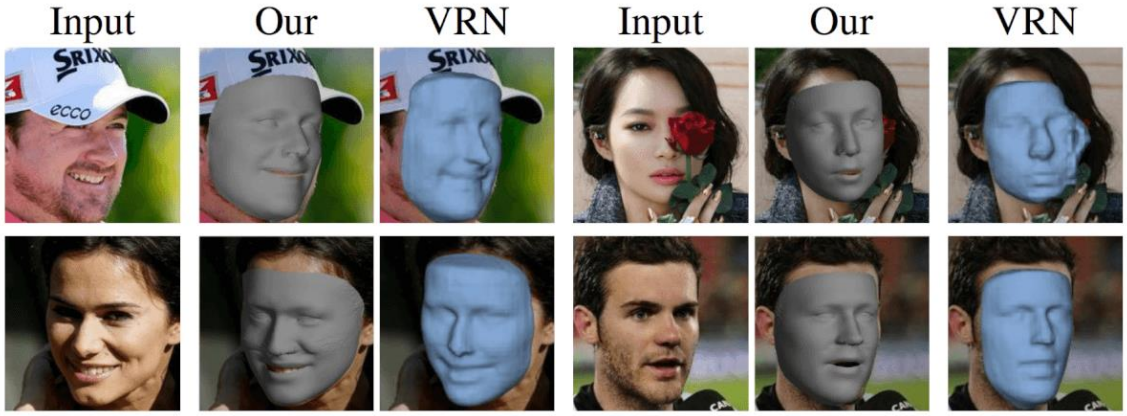


Рисунок 3.9 – Тривимірна реконструкція облич по зображенню
за допомогою згорткових нейронних мереж

Нейромережні методи показують одні з найкращих результатів в області розпізнавання, але вважаються найбільш складними для реалізації, якщо не застосовувати готові рішення. Дані методи характеризується стійкістю до змін масштабу, зсувів, поворотам, переміні ракурсу тощо. Результати тестувань показують рівень успішного розпізнавання та правильності рішення на рівні 96% при дії спотворюючих факторів.

Основними недоліками цих методів є необхідність тренування нейронної мережі кожен раз коли необхідно додати нову особу для розпізнавання. Час тренування збільшується пропорційно кількості осіб в базі облич. Хоча недолік необхідності тренування мережі іноді є значущим, попри це даний метод являється одним з найефективніших на даний час.

Метод локальних бінарних шаблонів (ЛБШ, англ. *Local Binary Pattern*, LBP), являє собою метод, що описує межі приймаючи значення інтенсивності пікселя зображення у двійковій формі при аналізі текстури півтонових зображень.

Оператор, що застосовується до пікселя зображення використовує вісім пікселів околу, приймаючи центральний піксель у якості порогу. Пікселі, які мають значення більші, ніж центральний піксель (чи дорівнюють йому), приймають значення «1», а ті, які, менше центрального, приймають значення «0». Таким чином утворюється 8-розрядний бінарний код, який описує окіл пікселя.

Описаний вище приклад роботи оператора ЛБШ над зображенням показано на рис. 3.10.

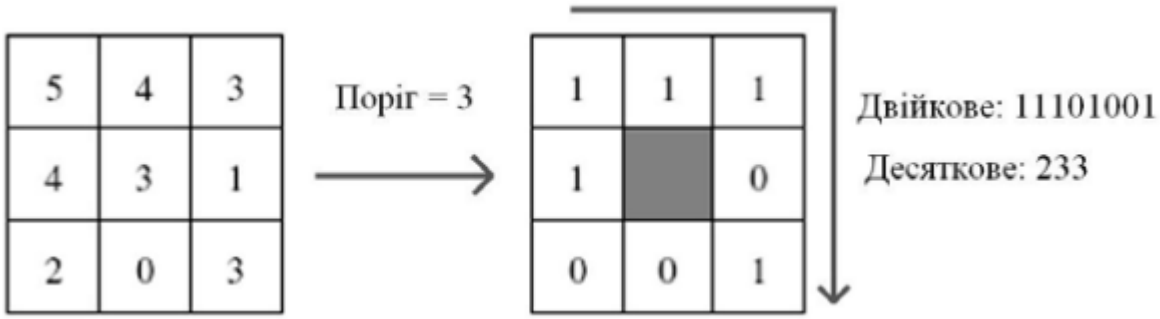


Рисунок 3.10 – Приклад роботи ЛБШ оператора

В подальшому зображення обличчя розбивається на k*k областей. Потім у кожній області для кожного пікселя зображення обчислюється свій бінарний код значень околу пікселя. При цьому збільшується на одиницю значення стовпчика, який відповідає за цей код. Потім будується гістограма, яка графічно представляє ці дані і де кожному коду в гістограмі відповідає окремий стовпчик. Після цього для представлення глобального опису зображення обличчя всі гістограми областей об’єднують в одну гістограму. Ця гістограма і формуватиме вектор ознак обличчя.

Приклад поділу зображення обличчя на області та відповідні цим областям гістограми зображено на рис. 3.11.

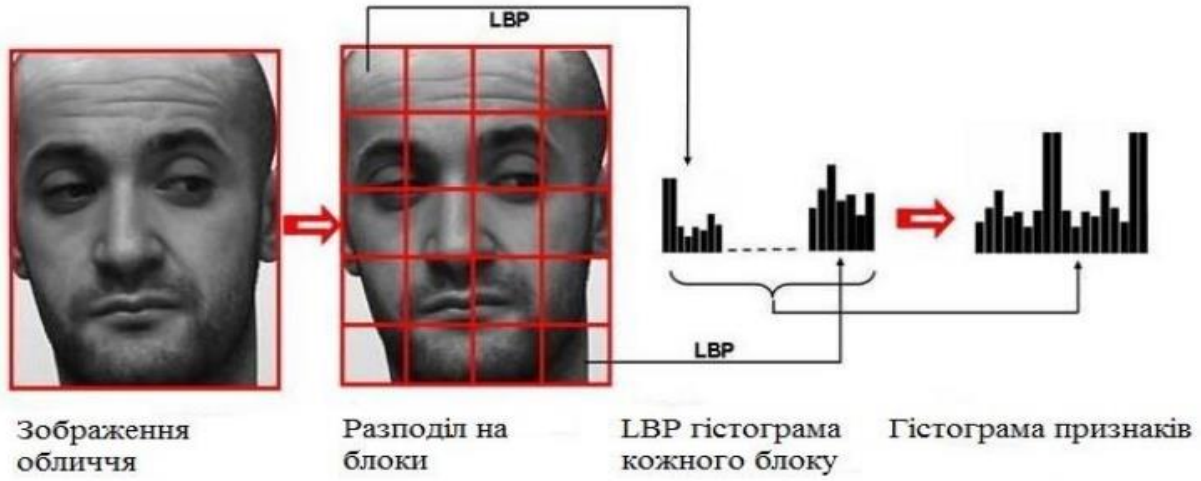


Рисунок 3.11 – Розбивка зображення на прямокутні області й формування гістограми

При класифікації зображень облич розраховуються відстані між гістограмами для різних облич, а для знаходження найменшої відстані між гістограмами, що представляють обличчя, використовуються відповідні статистичні показники (хі-квадрат). При цьому, оскільки деякі області облич (наприклад, область очей) можуть нести більш важливу інформацію, ніж інші області, кожній області в залежності від її важливості для розпізнавання можуть бути присвоєні відповідні ваги.

Розрізняють три основні алгоритми ЛБШ перетворення [35, 36]:

– класичний алгоритм ЛБШ (LBP) – суть якого полягає в застосуванні до пікселів зображення порогового перетворення, в якому значення яскравості оброблюваного пікселя порівнюється з значеннями яскравості пікселів його оточення;

– рівномірний ЛБШ (Uniform-LBR) – алгоритм скорочує розмірність гістограми, пояснюючи це тим, що істотну інформацію про форму об'єктів на зображенні містить тільки частина з локальних бінарних шаблонів;

– центрально-симетричний ЛБШ (CS-LBP) – суть модифікації полягає в тому, що в якості порогового значення для кожного пікселя оточення приймається не значення яскравості центрального пікселя оточення, а значення яскравості протилежної щодо центру оточення пікселя.

Методи розпізнавання облич, які використовують для виокремлення ознак ЛБШ та їх модифікації показують високі результати, як за швидкістю, так і за точністю розпізнавання. Такі методи робастні (незалежні впливу результатів різноманітних викидів, стійкі до перешкод) при використанні зображень облич із різною мімікою, різним освітленням, поворотами голови.

Серед недоліків – необхідність якісної попередньої обробки зображень через високу чутливість до шуму, оскільки за його присутності зростає кількість помилкових бінарних кодів.

На даний час існує багато готових програмних рішень для виявлення та розпізнавання на відеозображеннях облич людини, що застосовують розглянути вище алгоритми та методи.

В першу чергу це широко відома, найбільш використовувана у світі величезна бібліотека комп'ютерного зору OpenCV (Open Source Computer Vision Library), що ліцензована як безкоштовне програмне забезпечення з відкритим вихідним кодом згідно з ліцензією Apache License 2. Бібліотека містить понад 2500 оптимізованих алгоритмів та підтримує платформи глибокого навчання для обробки зображень та відео. Ці алгоритми можна використовувати для виявлення та розпізнавання облич, ідентифікації об'єктів, класифікації дій людей у відео, відстеження рухомих об'єктів, пошук подібних зображень у базі даних зображень, стеження за рухами очей, розпізнавання пейзажу та встановлення маркерів для накладання на нього доповненої реальності, і т.д. Написана на C++, але підтримує також Python, JavaScript, Ruby та інші мови програмування. Саме бібліотека OpenCV використовується на даний час Google, Yahoo, Microsoft, Intel, IBM, Sony, Honda, Toyota та іншими технологічними компаніями для вирішення різноманітних завдань комп'ютерного зору, в тому числі на мобільних платформах та пристроях.

Існують також інші, не так відомі бібліотеки, які також можна застосувати в системах розпізнавання облич для навчання по готовим наборам даних. Серед них, наприклад, CelebFaces, Tufts Face, UMDFaces, UTKFace, MORPH та інші.

На сьогоднішній день розробкою програмного забезпечення розпізнавання осіб займаються сотні компаній по всьому світу. За оцінками аналітиків, у 2020 році міжнародний ринок подібних технологій становив приблизно 10 млрд доларів.

В березні 2022 року, після повномасштабного вторгнення російських окупаційних військ, уряд України оголосив про співпрацю з американською компанією Clearview AI щодо запровадження їх відповідного програмних комплексів розпізнавання обличчя для ідентифікації жертв війни та окупантів. Ця система ідентифікує людей за допомогою зображень, які раніше були зібрані в Інтернеті з платформ соціальних мереж (таких як Google, Facebook, Twitter, Vkontakte тощо) і має понад 50 мільярдів загальнодоступних зображень людей.

Якщо говорити про готове комп'ютерне забезпечення, що розроблено українськими фірмами і застосовує бібліотеки OpenCV та інші, то як приклад можна навести програмний комплекс виявлення та розпізнавання облич ZetPro VMS української компанії «Kobi software». Це програмне забезпечення з інтелектуальними модулями, розроблене для роботи з різними виробниками систем відеоспостереження (камери, мережеві реєстратори та ін.).

3.2. Особливості технологій та застосованих методів розпізнавання на відеозображеннях емоційно-психологічного стану людини, її статі та інших ознак

Емоції – це особливий вид психічних процесів людини, які відображають її переживання до самої себе та ставлення до навколишнього світу. Емоції займають та відіграють велику роль в житті людини та в її спілкуванні з іншими. Тому виявлення збудженого та агресивного стану людини на відеозображенні є важливим завданням відеоаналізу, що проводиться правоохоронними органами.

Людина може виражати емоції різними способами: мімікою, позою, рухами, голосом і вегетативними реакціями (пульс, частота дихання). Однак найвиразнішим і зрозумілим для інших є обличчя людини.

Розпізнавання емоцій людини за виразом її обличчя (*Facial Expression Recognition*, *Face Computing*) є однією з технологій обробки відеозображень та є однією з найскладніших проблем комп'ютерного зору [37].

У технологіях розпізнаванні емоцій людини за виразом обличчя найчастіше використовується категоріальне подання емоцій, що включає нейтральне стан та шість базових емоцій, детально досліджених Полом Екманом [38]: гнів, огида, страх, щастя, смуток, подив, нейтральність. Іноді у існуючих наборах даних додається ще одна емоція, наприклад, спокій або зневага.

Іншим дискретним способом представлення емоцій людини за виразом її обличчя при розпізнаванні є модель Facial Action Coding System (FACS) [38]. Вона описує рухи м’язів обличчя, які відповідають за вираження емоцій та настрою. У FACS виділено більше 40 мускулатурних дій на обличчі людини та дано їх числовий код, що дозволяє квантифікувати відмінності у вираженні емоційних станів між людьми.

В даний час практично всі сучасні методи розпізнавання емоцій із зображення обличчя використовують глибоке навчання та нейронні мережі. При цьому згорткова нейронна мережа і її модифікації вважаються кращими алгоритмами по точності й швидкості знаходження емоцій людини на відеофрагменті [37]. Незважаючи на великий розмір, ці мережі мають невелику кількість параметрів, що можна налаштовувати в порівнянні зі звичайними нейронними мережами. Згорткові нейронні мережі забезпечують часткову стійкість до змін масштабу, зсувів, поворотів, змін ракурсу й інших деформацій зображень.

Більш детально алгоритм застосування технологій нейронних мереж, що здійснюють розпізнавання емоцій людини за виразом її обличчя, можна описати наступними етапами (рис. 3.12).

а б в г д е

Рисунок 3.12 – Етапи аналізу зображень для розпізнавання емоцій за виразами обличчя людини

Перше завдання, яке ставиться перед нейронною мережею для вирішення задачі розпізнавання емоцій людини – це попередня обробка отриманого зображення (рис. 3.12а) і локалізація (виділення) області обличчя (рис. 3.12б), обрізання та масштабування знайденої області (рис. 3.12в), вирівнювання обличчя (рис. 3.12г) та регулювання контрастності (рис. 3.12д). Після того як обличчя людини було виділено, необхідно визначити його елементи. Людина, загалом, проявляє емоції за допомогою брів, очей і рота. Тому наступним кроком є знаходження ключових точок виділених елементів особи (рис. 3.12е). Останнім кроком розв'язання задачі – є класифікація емоцій на основі аналізу декількох ключових точок, що знайдені на обличчі людини.

Етап локалізації області обличчя (рис. 3.12б) дозволяє визначити розмір та місцезнаходження особи на зображенні. Найчастіше використовують наступні методи локалізації [37]:

- розглянутий раніше метод Віоли-Джонса;
- метод Single Shot Multibox Detector (SSD) [39];
- гістограма спрямованих градієнтів (Histogram of Oriented Gradients, HOG) [40];
- метод Max Margin Object Detection (MMOD) [41].

Етап обрізання та масштабування знайденої області особи (рис. 3.12в) здійснюється згідно з координатами, отриманими методами локалізації області особи. Так як знайдені області особи мають різний розмір, то необхідно виконувати масштабування зображення, тобто приведення всіх зображень до одному розміру.

Етап вирівнювання обличчя (рис. 3.12г) дає змогу зменшити внутрішньокласові відмінності. Так, наприклад, для кожного вираз обличчя вибирається опорне зображення, яке поділяється за кольоровими компонентами або найбільш інформативним областям особи (наприклад, лоб, очі), інші зображення вирівнюються щодо опорних зображень.

Етап регулювання контрастності (рис. 3.12д) дозволяє згладжувати зображення, зменшувати шум, підвищувати контрастність зображення обличчя та покращувати насиченість, що дозволяє впоратися, наприклад, із проблемою освітленості.

Наступним етапом є вилучення знайдених ознак обличчя (рис. 3.12е, 3.13).

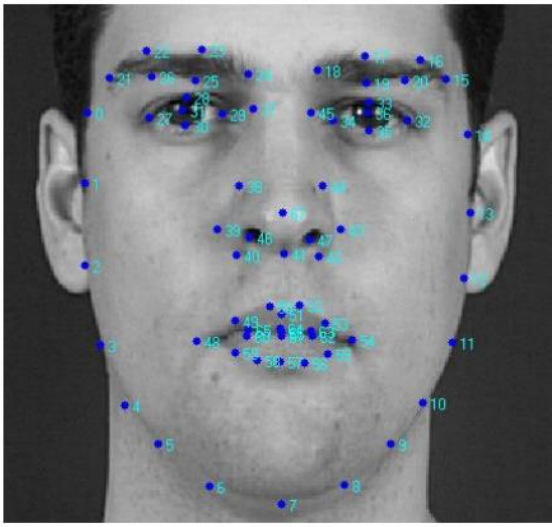


Рисунок 3.13 – Визначені ознаки на обличчі для оцінки емоції людини

На цьому етапі здійснюється точне місце знаходження елементів на обличчі людини, які є найінформативнішими для подальшої обробки. Залежно від виконуваних функцій методи отримання інформативних візуальних ознак поділяються на кілька основних типів [37]:

1) методи на основі геометричних об’єктів, що дозволяють витягувати інформацію про геометричні об’єкти обличчя, такі як рот, ніс, брови та інші об'єкти, та визначати їхнє місце розташування. Маючи інформацію про геометричні об’єкти та точне місце їх розташування на обличчі, можна розрахувати відстань між об’єктами. Ці отримані відстані та координати положень об’єктів і є ознаками для подальшої класифікації емоцій;

2) методи на основі моделей зовнішнього вигляду, що дозволяють отримувати інформацію про текстурні особливості обличчя. Наприклад, різна кількість зморшок в області очей говорить про різні вирази обличчя, тому застосування методів на основі моделей зовнішнього вигляду є найбільш інформативним для завдань класифікації емоцій;

3) методи на основі глобальних та локальних векторних об'єктів. Наприклад, метод основних компонентів (Principal Component Analysis, PCA) витягує відмінні ознаки виразів особи, зменшуючи розмірність отриманих векторів, а лінійний дискримінантний аналіз (Linear Discriminant Analysis, LDA) шукає вектори, які мають кращі відмінності між класами та групує ознаки одного і того ж класу.

З наведених методів вилучення ознак, методи на основі зовнішнього вигляду є найкориснішими, тому що вони дозволяють витягувати текстурні особливості зовнішнього вигляду, які є важливими параметрами для розпізнавання виразу облич, але вони значно менш адаптовані до графічних оклюзій (коли два об’єкти розташовані приблизно на одній лінії і один з них, розташований декілька ближче до місця візуалізації, частково або повністю закриває видимість іншого об’єкта).

Методи на основі геометричних об’єктів краще адаптовані до оклюзій, відстань між лицьовими орієнтирами більше характеризують міжкласові відмінності. А використання гібридних методів для вилучення ознак виразів обличчя підвищує точність класифікації.

Алгоритми комп’ютерного зору фіксують основні точки людської особи: очі, кінчик носа, брови, куточки рота — і відстежують рух для розшифровки емоцій. Порівнюючи зібрані дані із зразками з бази зображень, програма для розпізнавання може визначати почуття людини щодо поєднання виразів його обличчя.

Класифікація емоцій на основі аналізу декількох ключових точок є останньою стадією в розпізнування емоційного стану людини по відеозображенню. На цій стадії здійснюється класифікація витягнутих ознак на вираз обличчя: щастя, здивування, гнів, страх, огида, сум і нейтральність. На даний момент при достатньому наборі навчальних даних найкращим методом класифікації є технологія глибоких нейронних мереж, так як вони автоматично вивчають і витягують ознаки з вхідних зображень, і виявляють емоції на обличчі з більш високою точністю та швидкістю в порівнянні з іншими методами [37].

На жаль, навіть наведені сучасні підходи до розпізнавання емоцій з зображення обличчя показують не дуже достану точність на різних набори даних. Наприклад, для відомого набору даних Ryerson Audio-Visual Database of Emotional Speech and Song (RAVDESS) точність розпізнавання дорівнювала не більше 80 % [37]. Найкраща точність 77,62 % була отримана при використанні нейронної мережі EmotiEffNet-B0 для отримання ознак і self-attention моделі для класифікації емоцій. Хоча після донавчання мереж під конкретних користувачів точність може значно зрости і в деяких випадках досягти майже 100% [37].

Задачі визначення статі (гендерної приналежності) людини по відеозображенню відіграють також важливу роль в завданнях правоохоронної системи.

Існують особливості у розпізнаванні обличчя особи та її статі. У [42] вказано, якщо для ідентифікації обличчя людини потрібна інформація, яка робить його унікальним, то щоб розпізнати стать обличчя, закодована інформація потрібна бути спільною для групи різних облич (чоловічого чи жіночого). З точки зору даних складності, гендерна класифікація є проблемою двох класів із зазвичай великою кількістю зображення облич різних людей у класі, що призводить до рідкісних класів.

Коли люди виконують завдання розпізнавання статі значна кількість труднощів, що виникають при класифікації обличчя за статтю, людиною залишаються непоміченими. Люди ненавмисно стикаються з обличчями різних розмірів, та в різних ракурсах, а тому людина може розпізнавати стать осіб, обличчя яких бачить поблизу або на відстані, та в різних ракурсах. Крім того, люди добре розпізнають стать, коли пропорції обличчя не такі як очікують, що раніше бачили.

Наприклад, ми все одно можемо визначити стать людини, навіть якщо він або вона має більший ніс або менші очі, ніж обличчя, які ми зазвичай бачимо. Освітлення, ракурс, пропорції тіла або обличчя, масштаб є незначними проблемами для розпізнавання людьми, однак автоматичні системи зазвичай потребують спеціальних методів щоб успішно вирішувати проблеми гендерної класифікації в таких ситуаціях.

На даний час існує достатньо багато готових програмних рішень, що реалізують розглянуті вище методи та дозволяють визначити емоційно-психологічний стан людини по відеозображенню. Програмні продукти представлені багатьма компаніями та в різному вигляді: від коробкових версій програмного забезпечення до багатоплатформних веб-рішень.

На наш погляд, найбільш досконалим та цікавішим для розгляду в контексті завдання розпізнавання емоцій на сьогоднішній день є продукт FaceReader голландської компанії Noldus Information Technology (рис. 3.14).

Програма застосовує технології нейронних мереж і може чітко інтерпретувати такі вирази обличчя, як «щасливе», «сумне», «сердите», «здивоване», «злякане», «невдоволене» і «нейтральне». Крім того, FaceReader здатний по особах людей визначати їх вік, стать і навідь етнічну приналежність. Можливості програми FaceReader:

– середній відсоток розпізнавання емоцій дорівнює 89 %. Для деяких емоцій він вищий, для декого нижче;

– нахил обличчя може бути будь-яким у площині, його система виявить;

– програма працює із завантажуваним відео у форматах з кодеками MPEG1, MPEG2, XviD, DivX4, DivX5, DivX6, DV-AVI та uncompressed AVI, причому визначати емоції можна пофреймно, або повністю при перегляді всього відео. Також FaceReader може працювати зі статичними зображеннями, а також у реальному часі, якщо у користувача підключена веб-камера.

Рисунок 3.14 – Інтерфейс програмного продукту FaceReader (версії 4.0)

Але існуюча версія FaceReader поки ще не натренована для розпізнавання дітей віком до 5 років, а також якщо людина в окулярах, то розпізнавання емоцій досить неточне.

Іншими відомими програмними продуктами, що дозволяють достатньо вдало розпізнати емоції та інші ознаки людини по відеозображенню, є, наприклад, eMotion Software фірми Visual Recognition, MMER_FEASy (the FacE Analysis System) фірми MMER-Systems, FaceSecurity фірми Cognitec та багато інших.

Відомі методи розпізнавання статі людини схожі з розглянутими вище методами розпізнавання облич та емоційно-психологічного стану людини [43].

Зазвичай зображення обличчя людини попередньо обробляються, з кольорових зображень перетворюються на монохромні з сірою шкалою, далі застосовується гістограмне вирівнювання для кращої роботи із зображеннями в умовах з різним освітленням. Вирівнювання гістограми – це техніка для посилення контрастності шляхом рівномірного використання кожного сірого рівня у повному діапазоні.

На рисунку 3.13 зображення двох осіб різних рас (чоловіка європеоїдної раси та афроамериканки) показані до та після застосування вирівнювання гістограми. Як можна побачити на рис. 3.14а деякі плями на обличчі жінки сяють (наприклад, ніс і щоки), а на обличчі чоловіка їх немає. Після вирівнювання гістограм (див. рис 3.14б), на обох обличчях видно світліші ділянки навколо щік і носа разом із зображення з вищим контрастом, завдяки чому деталі виділяються.

а- до гістограмного вирівнювання

б- після гістограмного вирівнювання

Рисунок 3.14 – Зображення двох осіб (чоловіка та жінки) до та після застосування вирівнювання гістограми

Гістограмне вирівнювання за шкалою сірого є важливим для гендерного розпізнавання. Знаходження зображень обличчя в форматі RGB у градаціях сірого покращує контрастність зображення та покращує гендерну класифікацію.

Далі знаходять орієнтири обличчя. Для цього використовуються відомі методи визначення орієнтиру. При цьому існує шість орієнтирів для кожного ока, 14 орієнтирів для губ, 17 орієнтирів для бічного контуру, три орієнтири для кожного верхнього та нижнього зубів, дев'ять орієнтирів для цілого носа та п'ять орієнтирів для кожної брови. Таким чином загалом є 68 орієнтирів. Такі орієнтири необхідні також як для обрізання зображення так і для геометричної інформації. Для розпізнавання необхідно поєднувати ряд відомих методів розпізнавання обличчя, що розглянуті вище.

На рис. 3.15 приведено результати оцінювання орієнтирів на кількох гранях зразків.

Рисунок 3.15 – Знайдені орієнтири для різних зразків обличчя

Для того щоб виключити додаткову інформацію про довге волосся для розпізнавання статі обличчя слід використовувати виключно центральну частину обличчя. Тому з всього зображення вирізається тільки інформативний центр обличчя людини.

На завершальному етапі попередньої обробки, виконується передискретизація обрізаних центральних граній до рівномірної сітки (наприклад, 30x30) за двома причинами: знайдені обрізані центральні грані не обов'язково можуть мати однаковий розмір на різних зображеннях; дуже висока розмірність вектора ознак із-за великої кількість пікселів.

В зображенні, яке використовує система розпізнавання є не тільки саме обличчя, а і інші фонові елементи зображення. Тому першим кроком системи розпізнавання статі є знаходження на вхідному зображенні локальних областей обличчя, в першу чергу очей людини, а потім по ньому меж обличчя (рис. 3.16).

Виконуючи крок перевизначення на основі положень очей можливо отримати більш точну оцінку області обличчя.

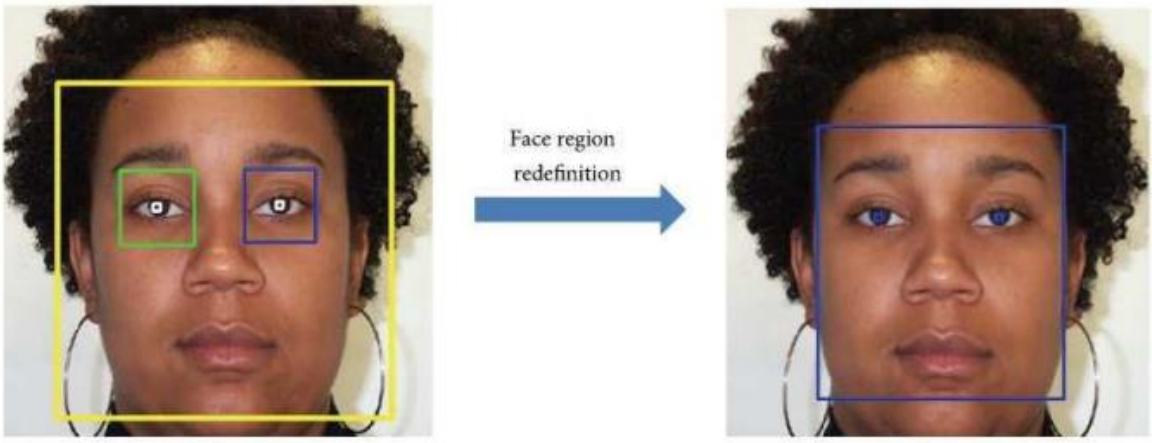


Рисунок 3.16 – Локалізація меж обличчя перевизначенням локальних областей

Далі, застосовуючи розглянутий нами раніше метод локальних бінарних шаблонів (LBP) будують гістограми векторів ознак обличчя людини (рис. 3.11). Для кожного окремого локального регіону (області) виконується знаходження ознак за допомогою фільтрації Габора.

Глобальні характеристики, що отримано за допомогою метода LBP, та локальні характеристики, що отримано за допомогою фільтрації Габора, використовуються для побудови остаточного вектору ознак статі за рахунок об'єднання двох нормалізованих ознак, що використовує так звану z-оцінку нормалізації, що відома з літератури [42]. Розпізнавання статі виконувалось із застосуванням класифікатору SVM за парою зображень елементів обличчя: очі, ніс, рот, підборіддя, внутрішнє зображення зовнішнє зображення та повне зображення.

Застосовуються також різні методи та технології визначення людини та її статі по стилю ходьби. Наприклад, в [44] представлена комп'ютерна система GaitNet, що за рахунок застосування технологій нейронних мереж і відповідним методом маркуванням за «скелетними» рухами ходьби людини дозволяє ідентифікувати основні характеристики, які відрізняють ходу чоловіків і жінок (рис. 3.17).

У наш час дуже важливим стає питання моніторингу поведінки людей у громадських місцях та попередження злочинних дій. Тому розпізнавання пози людини (наприклад, лежить без ознак життя тощо) або її аномальної поведінки з ознаками насильства також є важливою задачею систем відеоспостереження правоохоронних органів.

Через це з кожним роком зростає кількість безпілотних технологій, технологій віртуальної реальності і доповненої реальності, які використовують інформацію про положення тіла людини у просторі [45]. Також розроблено багато методів визначення пози або активності людини по відеозображенню, що застосовують нейронні мережі, серед яких, наприклад, бібліотеки OpenPose, DeepCut, AlphaPose, Mask R-CNN та інші.

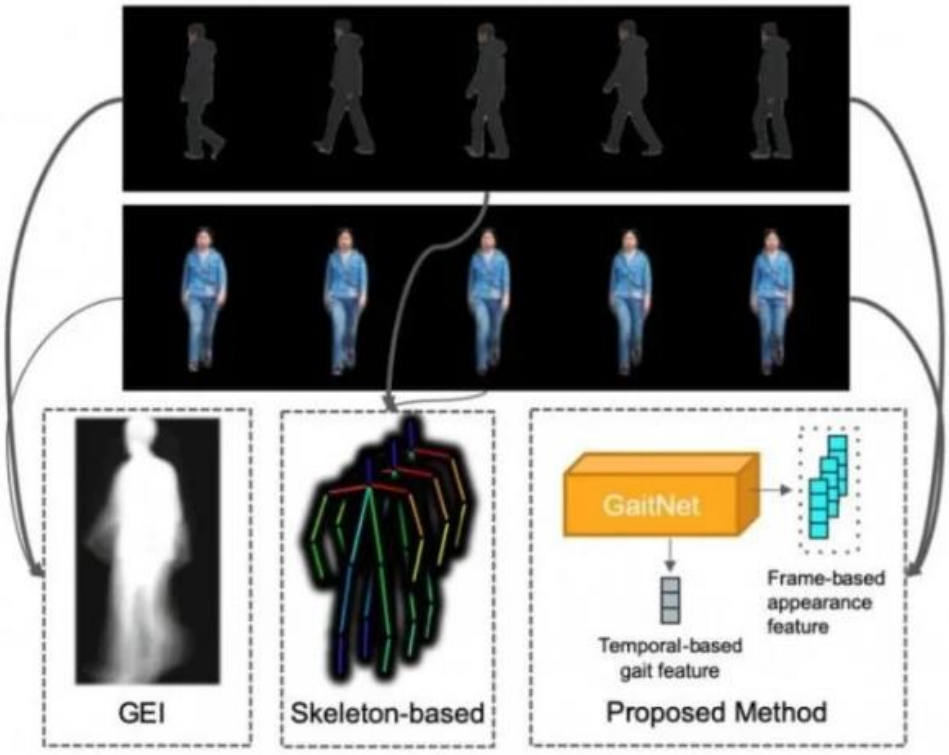


Рисунок 3.17 – Принципи гендерної визначеності людини за її ходою [44]

В [46] наводяться приклади, а в [47] проаналізовані можливі підходи використання технологій машинного навчання у сукупності зі згортковими нейронними мережами щодо визначення насильницьких дій на відеозображеннях.

Широке поширення у світі вірусу COVID-19 порушили також питання автоматичної ідентифікації (верифікації) правоохоронними органами людини та її статі в умовах пандемії, оскільки тепер у громадських місцях люди змушені були носити захисні маски, що собою закривали частину обличчя. Таким чином, стало неможливо достеменно встановлювати особистість людини, яка перебуває в аеропорту, банку, кафе чи просто ходить вулицею

З цією метою були розроблені нові системи, в яких широко застосовуються технології нейронних мереж та розглянуті раніше різні методи розпізнавання особистості (рис. 3.18). Адже системам потрібно точно визначити, які частини обличчя є видимими, тобто вихідними даними для подальшого процесу розпізнавання, а які закритими, тобто, потребують відновлення зображення обличчя, що досягається завдяки технологіям штучного інтелекту [48].

Загальна методологія роботи цих систем в першу чергу базується на широко прийнятих моделях глибокого навчання (VGGFace, FaceNet, OpenFace і DeepFace) для вивчення відмінних характеристик облич у масках. Бібліотеки MaskTheFace, MaskedFace-Net, глибока згорткова нейронна мережа (DCNN), CYCLE-GAN, Identity Aware Mask GAN (IAMGAN) та starGAN є одними з найбільш популярних застосованих технологій для визначення масок на обличчі та їх власників.

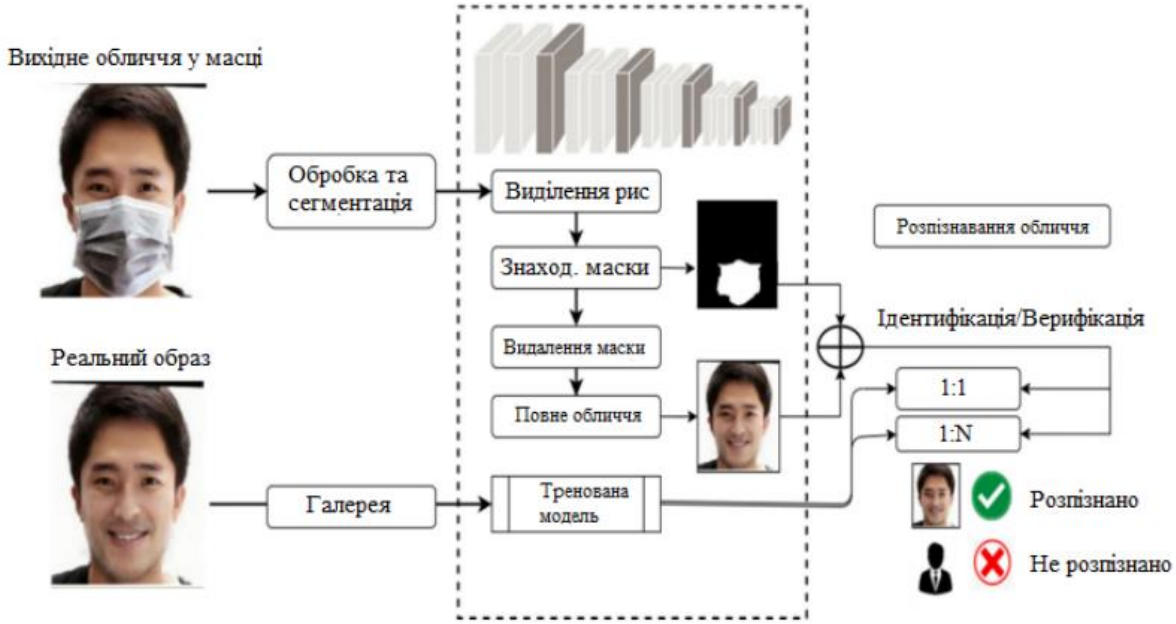


Рисунок 3.18 – Схематичне зображення процесу розпізнавання облич у масці

Широке поширення нової субкультури квадроберами, частіше підлітками, які наслідують поведінку тварин, носять маски та розмальовують під тварини свої обличчя, наявність інших неформальних течій молоді, нанесення ними та зловмисниками камуфляжних масок на обличчя, вимагають від правоохоронних органів також наявності відповідних технологій розпізнавання осіб в таких умовах.

Тому на даний час вже розроблені та наявні на ринку програмні системи, що широко застосовують технології нейронних мереж, що застосовуються розпізнавання осіб з відповідним камуфляжним розмалюванням обличчя (рис. 3.19).

Рисунок 3.19 – Етап локалізації меж обличчя у камуфляжній масці

Окремою проблемою з початком російсько-української війни стає актуальне питання виявлення зброї в руках людини та ідентифікація як типу зброї, так і того, хто її тримає. Однак, застосування камер без спеціальних інтелектуальних систем обробки відео не забезпечує достатню ефективність виявлення зброї. Тому для підвищення ефективності такого моніторингу потрібні системи штучного інтелекту для автоматизованої обробки відео з камер спостереження з метою виявлення зброї. Загальний алгоритм цих систем такий – система штучного інтелекту отримує відео з камери спостереження, перевіряє відео на наявність зброї і якщо зброя наявна, то вона виділяється і виводиться оператору для прийняття відповідного рішення.

В [46, 49, 50] наведені приклади застосування технологій машинного навчання та згорткових нейронних мереж для виявлення озброєних людей у відеопотоці.

Наприклад, в [49] показано, що для виконання поставленої задачі найкраще підходить згорткова нейронна мережа YOLO. Особливістю даної мережі є застосування спеціальної операції – згортки, яка дозволяє зменшити кількість інформації, що зберігається в пам’яті. За рахунок цього мережа краще справляється із зображеннями високої роздільної здатності і виділяє опорні ознаки зображення, такі як ребра, контури або грані.

Технологія виявлення озброєних людей у відеопотоці складається з таких етапів [49]:

1) розбиття відеопотоку на кадри;

2) подання кадрів на вхід нейронної мережі;

3) розпізнавання нейронною мережею об’єктів на зображенні, схожих на зброю;

4) виділення кожного розпізнаного об’єкта прямокутником відповідного розміру (рис. 3.20);

5) підпис виділеного об’єкта назвою виду зброї (пістолет, гвинтівка та ін.);

6) виведення результатів виявлення на екран оператора для прийняття відповідного рішення.

Рисунок 3.20 – Приклад виявлення системою зброї та визначення її класу [49]

Відповідно до результатів тестування, система, що використовує ЗНМ YOLO має достовірність виявлення озброєних людей 98,51 % [49]. Ці результати вказують на можливість практичного використання з подальшим покращенням програми в майбутньому.

В [50] також наведені приклади визначення місцезнаходження озброєних людей та виявлення різних типів зброї та ножів (рис. 3.21) у реальному часі, засновані на ресурсно-обмеженій та легкій згортковій нейронній мережі.

Рисунок 3.21 – Приклад виявлення системою зброї та визначення її класу [50]

На даний час існує багато готових програмних засобів виявлення на відеозображеннях різних видів зброї та озброєних ними людей, що широко застосовують системи штучного інтелекту, технології нейронних мереж тощо. Серед них, наприклад, SafePointe фірми SoundThinking, OpenData Weapon Detection, системи фірми Securitas Technology, Gun Detection System фірми ScyllaAI та інші.

3.3. Особливості технологій та застосованих методів виявлення та розпізнавання на відеоданих транспортних засобів та їх номерних знаків

Окремим важливим завданням, який виникає в процесі здійснення правоохоронними органами відеоаналізу є виявлення на відеозображенні відповідних транспортних засобів, ідентифікація їх за кольором, моделлю, а також визначення їх автомобільних номерів для ідентифікації їх власників.

Знаходження транспортних засобів на зображенні чи в відеопотоці це завдання з області комп’ютерного зору, яка розв’язується різними підходами, але найчастіше за допомогою технології вже розглянутих раніше згорткових нейронних мереж. Потрібно знайти не просто область, в якій зустрічається шуканий об’єкт, але і відокремити всі його точки від інших об’єктів або фону.

При цьому на відеозображеннях транспортні засоби не тільки стоять припаркованими або зупинились на світлофорі, але і досить швидко рухаються. Тому зазвичай досить складно створити універсальну систему для розпізнавання різних типів таких об'єктів та подальшого їх аналізу. Вузькими місцями подібної системи також є обчислювальні можливості комп'ютерів та недосконаліть самих алгоритмів.

Загальний процес виявлення та розпізнавання такого класу об'єктів у відеопотоці може буди розділений на наступні етапи, кожен з яких має свої задачі і проблеми, що потрібно вирішувати [51]:

Етап 1. Порівняння кадрів у відеопотоці серед проблем, які виникають на цьому етапі, слід зазначити незмінність кадрів. Частіше за все відеопотік має 16-30 кадрів у секунду, часто виникають ситуації, коли кадри ідентичні, або мають незначні відмінності. Існують три основних підходи до вирішення такої проблеми: порівняння значення хеш-функцій двох кадрів, які змінюються; обчислення коефіцієнту кореляції; побудова та аналіз так званих SURF-дискриптів (пошук особливих точок зображення, інваріантних до масштабу і обертанню).

Етап 2. Оцінка якості зображення – серед проблем, які виникають на цьому етапі, слід зазначити розмиття, наявність шумів та засвічення кадрів. З багатьох причин зображення у кадрі може бути пошкоджено або змазано через атмосферні явища тощо, іноді якість кадру може бути дуже низькою і не придатною до розпізнавання, такі кадри слід відкинути. На цьому етапі слід провести оцінку контрастності, різкості та чіткості. Можна також підвищити різкість або компенсувати недоліки якості зображення.

Етап 3. Зменшення розмірності зображення – серед проблем, які виникають на цьому етапі, слід зазначити вхідні кадри високої розмірності. Кадри надходять у вигляді матриці пікселів, чим більша розмірність, тим більше операцій буде виконано і більше часу на розпізнавання буде витрачено. Тому потрібно зменшити розмірність зображення, при цьому залишивши достатньо даних для обробки.

Етап 4. Сегментація об’єктів на зображені – виділення окремих областей на відеозображенні в чорно-білому та кольоровому спектрах, де знаходяться об’єкти.

Етап 5. Безпосередньо розпізнавання об'єктів на зображенні – серед проблем, які виникають на цьому етапі, слід зазначити розглянутий у попередньому розділі ефект оклюзії та трансформацію. Іноді об'єкти повертаються, віддаляються або перекриваються іншими об'єктами.

Сьогодні розроблено низку методів розпізнавання такого класу об’єктів на відеозображеннях, в яких використані методи машинного навчання. Серед них можна виокремити наступні [52]:

– метод бінарної класифікації ознак зображення – вирішує завдання класифікації, що є предметом розгляду в машинному навчанні. Це здійснюється навчанням з учителем – метод, в якому категорії відомі, полягає у визначенні цих категорій для нових спостережень;

– метод опорних векторів ознак зображення – це метод аналізу даних для класифікації та регресійного аналізу за допомогою моделей з керованим навчанням із пов'язаними алгоритмами навчання, які називаються опорно-векторними машинами (ОВМ). Для заданого набору тренувальних зразків, кожен із яких виокремлено як належний до однієї чи іншої з двох категорій, алгоритм тренування ОВМ будує модель, яка зараховує нові зразки до однієї чи іншої категорії, роблячи це неймовірнісним бінарним лінійним класифікатором;

– метод штучної нейронної мережі (ШНМ) ознак зображення – ґрунтується на сукупності з'єднаних вузлів, що називають штучними. Кожне з'єднання (аналогічне синапсові) між штучними нейронами може передавати сигнал від одного до іншого. Штучний нейрон, що отримує сигнал, може обробляти його й потім сигналізувати штучним нейронам, приєднаним до нього. Використання штучних нейронних мереж для класифікації зображень – один із доволі ефективних методів. Проте така класифікація ускладнюється, насамперед, великим розміром вектора вхідних зображень нейронної мережі, кількістю нейронів у проміжних шарах, і, як наслідок, великими обчислювальними витратами на навчання і виконання мережі;

– метод згорткової нейронної мережі (ЗНМ) вхідного зображення – це клас глибинних штучних нейронних мереж прямого поширення, який успішно застосовувався до аналізу візуальних зображень.

В [52] визначено, що порівняльний аналіз переваг та недоліків розглянутих методів дає змогу встановити, що для вирішення завдання з пошуку і розпізнавання об'єктів, що можуть досить швидко рухатись, доцільно використовувати ЗНМ.

Сьогодні існує багато ЗНМ, які застосовуються для виявлення та розпізнавання об'єктів, що рухаються у відеозображеннях. До найпоширеніших можна зарахувати такі [52, 53]:

– R-CNN (Regions with CNN). Працює як звичайний класифікатор зображень. На вхід мережі подають різні регіони зображення і для них роблять передбачення. У результаті процедура дуже повільна, оскільки проганяє одне зображення кілька тисяч разів;

– Faster R-CNN. Цей алгоритм відомий своєю швидкістю та точністю в виявленні об'єктів на зображеннях. Він використовує комбінацію ЗНМ для визначення регіонів і рекурентних нейронних мереж (РНМ, англ. *Recurrent Neural Networks*, RNN) для точного визначення об'єктів. Спочатку все зображення подають на вхід згорткової нейронної мережі, потім з отриманого внутрішнього представлення генерують регіони;

– Mask R-CNN. Ця модель, основана на Faster R-CNN, додатково включає сегментацію об'єктів, дозволяючи виділяти області, де знаходиться об'єкт, та сегментувати їх. Кожен алгоритм та архітектура мають свої переваги та обмеження, і вибір залежить від конкретного завдання та вимог щодо продуктивності;

– ResNet (Residual Network). Відома своєю глибиною та впровадженням концепції «резидуальних блоків». Замість того, щоб намагатися навчати точну функцію, ResNet навчається різниці між вхідним і вихідним значеннями (резидуальні блоки). Це допомагає уникнути проблем градієнта, що зазвичай виникають при навчанні дуже глибоких мереж. ResNet здатна до розрізнення тонких деталей на зображеннях і використовується для багатьох завдань від класифікації до сегментації;

– Inception (GoogLeNet). Відома своєю архітектурою, що використовує блоки Inception з різними розмірами фільтрів одночасно. Це дозволяє ефективно виявляти різні властивості на зображенні на різних шарах мережі. Inception здатна до зменшення кількості параметрів та при цьому забезпечує високу продуктивність;

– YOLO (You Only Look Once). Використовує зовсім інший принцип роботи порівняно з попередніми системами. Тоді як більшість систем використовують згорткову нейронну мережу декілька разів із різними регіонами зображення, YOLO використовує її лише один раз до всього зображення. Мережа ділить зображення на сітку і передбачає розташування потрібного об’єкта для кожної ділянки. YOLO є швидким та легким алгоритмом для виявлення об'єктів в реальному часі. Має багато реалізацій у вигляді бібліотек, таких як Keras;

– SSD. За принципом схожа на YOLO. Теж доволі швидка і придатна для роботи в реальному часі, проте розмір вихідної моделі істотно більший, ніж у YOLO.

Застосування розглянутих вище типів нейронних мереж дозволяє створити відповідні алгоритми виявлення на відеозображеннях транспортних засобів, а також здійснити їх сегметацію на зображенні (рис. 3.22).

Подібні алгоритми визначення типу транспортного засобу, його кольору та моделі також здійснюються за рахунок широкого застосування технологій нейронних мереж.

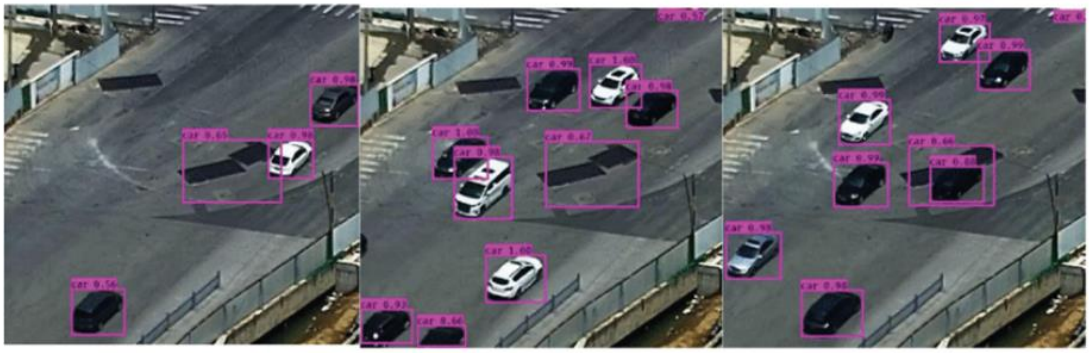


Рисунок 3.22 – Результат виявлення транспортних засобів на відеозображенні

Окремими завданнями, що виникають у відеоаналізі, є визначення швидкості транспортного засобу та його номерного знаку за даними відеоспостережень. Для цих завдань також використовують технології нейронних мереж.

В [54] зазначається, що в деяких системах для виміру швидкості транспортного засобу на основі відеоданих аналізують послідовні відеокадри, щоб відстежити транспортний засіб і таким чином виміряти його швидкість. Послідовними етапами при цьому є: локалізація кадрів зображення, виявлення транспортного засобу, що рухається, міжкадрове стеження за транспортним засобом. Також зустрічаються системи, де для автоматичної обробки відеозапису розпізнається транспортний засіб та фіксується час його перебування в зоні його розпізнавання.

Швидкість транспортного засобу також може вимірюватися на основі порівняння двох послідовних кадрів відеозапису та визначення зміщення транспортного засобу між послідовними кадрами [54]. За величиною зміщення швидкість автомобіля визначалася на основі відомих розмірів об’єкту, до якого виконана прив’язка. Але при використанні даної технології зроблені звичайною відеокамерою зображення можуть виявитися надмірно розмитими, що завадить процедурі визначення зміщення пікселів, тому така система вимагає використання дорогих камер високої роздільної здатності.

Але для розрахунків швидкості руху за результатами обробки відеозапису в основному визначають час проходження транспортними засобами деякої мірної ділянки відомої довжини. Мірний відрізок як правило, виявляє собою два перерізи дороги, які можна прив’язати до деяких нерухомих стаціонарних об’єктів (рис. 3.23) [54]. Такими об’єктами можуть бути елементи дорожніх споруд, опори освітлення, технічні засоби регулювання руху, тощо. Вибрані маркери мають розташовуватись на приблизно однаковій відстані від краю проїжджої частини дороги. У якості маркерів, за можливості, доцільно обирати лінії дорожньої розмітки.

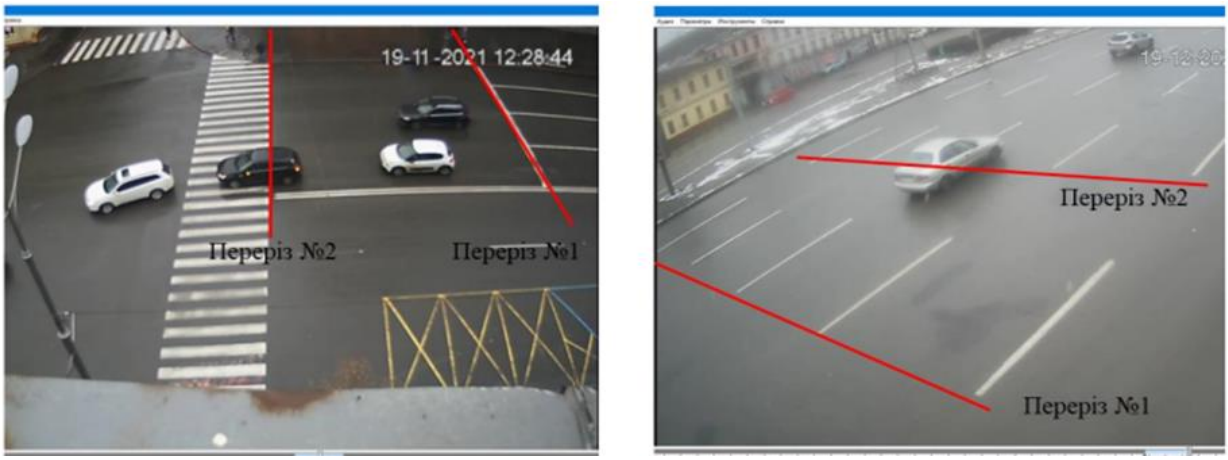


Рисунок 3.23 – Виявлення швидкості транспортних засобів на відеозображенні за допомогою маркерних ліній [54]

Для розпізнавання атрибутів транспортних засобів (їх типу, марки, моделі та кольору) також широко застосовуються технології нейронних мереж і методів машинного навчання. З цією метою, наприклад, може застосовуватися набір даних The Comprehensive Cars (CompCars) dataset, де представлені фотографії 163 марок автомобілів, а загальна кількість моделей на фотографіях є рівною 1716. Загальна кількість фотографій в наборі сягає 160 тис., з яких 136 726 фотографій є повними фотографіями машин, а 27 618 включають в себе часткові фото автомобілів.

Розглянуті вище технології та методи застосовують і для розпізнавання номерних знаків транспортних засобів.

Зараз в Україні існує 15 типів реєстраційних знаків транспортних засобів [55]. Знаки мають різні геометричні розміри і форми, колір, в них можуть використовуватися українські літери, літери латиниці, цифри, а також малюнки. Крім того, в сучасних умовах важливим є задачі розпізнавання автомобілі з іноземними номерами, в тому числі країни-агресора (росії) та її сателітів (рис. 3.24). Тому така різноманітність автомобільних номерів потребує їх детального аналізу системами розпізнавання.

Рисунок 3.24 – Різновиди номерних знаків транспортних засобів

Загальний підхід до розпізнавання автомобільних номерів на зображенні складається з таких етапів (рис. 3.25) [56]: попередня обробка зображення, отриманого з відопотоку; пошук області з зображенням номеру, потім нормування номеру для знаходження чітких меж та регулювання контрасту, безпосередньо розпізнавання символів на автомобільному номері; постобробка (постпроцесінг). Тому кожен з етапів має різні підходи до рішення проблеми, які мають свої характерні особливості, переваги і недоліки.

Рисунок 3.25 – Етапи процесу розпізнавання номерних знаків транспортних засобів

Першим етапом є попередня обробка зображень. Цей процес включає фільтрацію, яка дозволяє видалити шум з зображення, покращуючи його якість. Один із найбільш розповсюджених методів – Гаусів фільтр, який згладжує зображення і зменшує дрібні артефакти. Наступним кроком є корекція освітлення, що допомагає усунути проблеми, пов'язані з нерівномірним освітленням. Це забезпечує кращу видимість символів на номерному знаку, що є критично важливим для подальшого розпізнавання.

На другому етапі виявлення знаку (пошуку області з зображенням номеру) зазвичай застосовують детально розглянутий вище метод Віоли-Джонса, який добре працює в реальних умовах відеозображень транспортних засобів. Адже бруд, сніг, пил – ті супутники, без яких автомобільні номери рідко зустрічаються. На цьому етапі також можуть використовуватися алгоритми комп'ютерного зору, такі як детектори країв, зокрема алгоритм Кенні, каскади Хаара (Haar Cascades) і HOG (Histogram of Oriented Gradients) [56, 57]. Цей етап допомагає виділити область розташування (контури) номерного знаку, що є важливим для наступної сегментації символів (рис. 3.26а).

а б в, г

Рисунок 3.26 – Виявлення та обробка номерного знаку транспортного засобу

На третьому етапі здійснюється нормування, сегментація та регулювання контрасту зображення номеру. Після попереднього етапу на вихід подається рамка зображення автомобільного номера (рис. 3.26а), але цьому зображенню притаманне: можливий градус нахилу і бруд на номері, розмиття зображення.

Це лише частина проблем, які необхідно вирішити для подальшої роботи системи. Для визначення кута нахилу зображення номеру найбільш простим в реалізації є перетворення методом Хафа (англ. *Hough Transform*) – обчислювальним алгоритмом, який застосовується для параметричної ідентифікації геометричних елементів растрового зображення. Цей метод знаходить прямі лінії на зображенні (рис. 3.26б). Надалі виконується поворот на знайдений у попередньому етапі кут. Крім цього, можна відразу за отриманими після перетворення Хафа лініях обрізати зображення (рис. 3.26в).

Після виділення, необхідно зробити зображення більш контрастним. Для цього можна лінійно розтягнути гістограму зображення. Потім здійснюється накладення фільтра LoG (англ. *Laplacian of Gaussian*) для зменшення шуму зображення. Цей процес передбачає бінаризацію зображення, що перетворює його в чорно-біле, полегшуючи подальше виділення символів на номерному знаку.

Контурна детекція є ще одним важливим аспектом цього етапу, оскільки вона дозволяє точно сегментувати кожен символ, що є ключовим для їх подальшого розпізнавання [56]. Після цього етапу контури букв чітко видно на зображенні (рис. 3.26г).

Надалі виконуються етапи безпосереднього розпізнавання символів на виявленому номері та їх постобробка [56, 57].

На етапі розпізнавання використовуються методи машинного навчання, зокрема розглянуті вище згорткові нейронні мережі, які навчаються на великих наборах даних номерних знаків. Це дозволяє досягти високої точності розпізнавання навіть у складних умовах. Альтернативно, метод шаблонного порівняння може бути використаний для порівняння сегментованих символів із заздалегідь визначеними шаблонами.

Потім, зазвичай, здійснюється постобробка розпізнаних номерів [56, 57]: виконується перевірка формату, що забезпечує відповідність розпізнаних номерів певним критеріям (наприклад, кількість цифр і літер); крім того, порівняння з базами даних дозволяє виявити підроблені або викрадені автомобілі, що підвищує загальну ефективність відеоаналізу.

На даний час існують багато програмних і системних рішень, у тому числі української розробки, що реалізують розглянуті вище методи і технології розпізнавання транспортних засобів, їх атрибутів та номерних знаків (рис. 3.25).

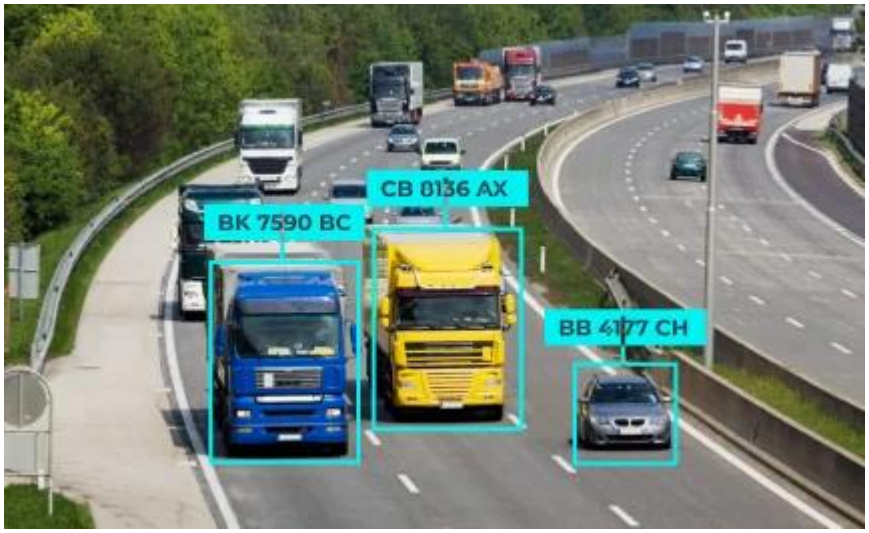


Рисунок 3.27 – Приклад розпізнавання транспортних засобів та їх номерних знаків

Наведемо тільки деякі із таких прикладів.

Наприклад, розроблене і впроваджене програмне забезпечення українською фірмою «Kobi software» дозволяє розпізнавати номерні знаки автомобілів на швидкості до 260 км/год і для номерів 50 країн світу. Також здійснюється розпізнавання атрибутів автотранспорту – їх тип, марка, модель та колір.

Програмне забезпечення Nomeroff Net є бібліотекою автоматичного розпізнавання автомобільних номерів, яка створена програмістами української компанії «AUTO.RIA» і написана на мові програмування Python v3 із архітектурою ЗНМ YOLOv8. Ця програма поширюється за відкритою ліцензією GNU General Public License v3 і містить натреновані моделі номерів України, країн Європейського Союзу, росії, Білорусі, Молдови, Грузії, Вірменії, Азербайжану, Казахстану та Киргизстану.

А програмні рішення, що реалізовані українською компанією «Восток-Дніпро» у вигляді продукту AutoTRASSIR LPR, дозволяють розпізнавати номери автомобілів, що їдуть зі швидкістю до 30 км/год.

Таким чином, розглянути у цьому розділі роботи теоретичні основи сучасних методів та технологій виявлення та розпізнавання на відеоданих фізичних осіб по їх фізичним, фізіологічним чи поведінковим ознакам, а також транспортних засобів, їх номерних знаків та зброї, а також наведені деякі приклади їх реалізації програмно чи апаратно-програмно, дозволяють зробити висновок про реальність і доцільність виявлення та розпізнавання відповідних осіб і об’єктів відповідними програмними комплексами відеоаналітики правоохоронних органів.

4. ВИКОРИСТАННЯ ПРАВООХОРОННИМИ ОРГАНАМИ ПРОГРАМНИХ ЗАСОБІВ РОЗПІЗНАВАННЯ ЛЮДЕЙ ТА ІНШИХ ОБ'ЄКТІВ У КРИМІНАЛЬНОМУ АНАЛІЗІ

Кримінальний аналіз становить собою дії, спрямовані на ідентифікацію і точне визначення взаємозв'язків між відносинами, які стосуються подій злочинного характеру, осіб, пов'язаних з ними та даними, що походять з різних джерел, і в подальшому їх використання слідчими органами, прокуратурою та судами. Цілями кримінального аналізу є: розробка гіпотези (припущення), реконструкція ходу здійснення правопорушення, визначення, чи було воно здійснене одним злочинцем, встановлення злочинця, зв'язків, інформації, важливої для доказування скоєння злочину, розуміння функціонування злочинної мережі, дослідження масштабу і характеристики злочинної діяльності.

Кримінальний аналіз за специфікою своєї роботи накопичує велику кількість даних пов'язаних зі злочином, до яких також відносяться відеодані про обличчя людей, що потрапили в об'єктив камери відеоспостереження. В свою чергу, у криміналістичній практиці, використання даних про зовнішність людини полягає у її розшуку та ідентифікації (ототожненні) [58]. В цьому випадку для ідентифікації особи за її обличчям необхідно провести її розпізнання з наявних фото та відео даних. Ототожнення проводиться методом порівняння зовнішнього вигляду певної людини з зображенням розшукуваної особи (фото знімків, відео відзнятих камерами відеоспостереження, опису свідків тощо). У залежності від типу зображень що використовувались для розшуку особи ототожнення проводять з фото- чи відеозаписом, рисунком, суб'єктивним портретом, словесним портретом або з уявним образом у пам'яті свідка.

В кримінальному аналізі використання програм відеоаналізу для швидкої ідентифікації людей, об'єктів та транспортних засобів може сприяти прискоренню розкриттю злочинів. В цьому випадку сортування ідентифікованих об'єктів за багатьма категоріями, такими як колір, розмір, модель транспортного засобу, напрям руху підозрюваного або транспортного засобу та інші може покращити можливості кримінального аналізу та допомогти правоохоронним органам в пошуку всіх причетних до скоєного злочину.

На теперішній час прикладами програмного забезпечення, що використовуються правоохоронними органами для ідентифікації людей за обличчям є: Veritone Identify [59], Clearview AI [60], Corsight [61] та BriefCam [62] від закордонних розробників, а також, наприклад, ТиХто [63] та Artellence [64] від вітчизняних розробників.

З представлених програмних засобів кожен має свої особливості та переваги у їх застосуванні. Veritone Identify розроблена спеціально для правоохоронних органів та має функціонал пошуку та ідентифікації людей за

обличчям з відео знятих камерами відеоспостереження. Clearview AI створена для пошуку людей за обличчям у відкритих базах даних, такими як соціальні мережі. Corsight також має можливості ідентифікації людей за обличчям з відеоматеріалів відзнятих камерами відеоспостереження, але на додачу вона може відслідковувати переміщення людей, обличчя котрих потрапляє в об'єктив камери спостереження. Вітчизняні розробки ТиХто та Artellence проводять ідентифікацію людей за допомогою фотографій.

З перелічених вище продуктів розглянемо, наприклад, детальніше програму Veritone Identify [59]. Veritone Identify це розумна та швидка система ідентифікації підозрюваних для правоохоронних органів. Ця система дозволяє проводити пошук правопорушників за відео та фото даними, фільтрувати знайдених правопорушників (вік, стать, зріст, колір волосся, колір очей та етнічна приналежність), об'єднувати потенційних підозрюваних для подальшого розслідування, ділитися списками підозрілих осіб всередині підрозділу та установами (включно з даними: фото, ім'я, остання відома адреса), об'єднувати інформацію про підозрюваних у централізованій веб-платформі (докази, фотографії, остання відома адреса, тощо), упорядковувати докази за справами включно з деталями як приклад: ідентифікатор справи, відділ, офіцер, опис, місцезнаходження, час і доступні примітки.

Система Veritone Identify складається з таких розділів: управління справами, подробиці справи, дії, докази, обробка, підозрювані, примітки. Розглянемо функціональні можливості цієї системи.

Робота з програмою Veritone Identify розпочинається зі створення нової справи, для цього натиснувши на кнопку «new case», на панелі управління справами, (рис. 4.1а) відкриється форма (рис. 4.2), котру необхідно заповнити. В формі зазначається ідентифікатор справи (id), дата та час, назва, опис, до якого відділку належить, відповідальний, адреса. Панель «Управління» справами надає можливості переглядати справи за трьома категоріями: активні справи, закриті справи або архівовані справи.

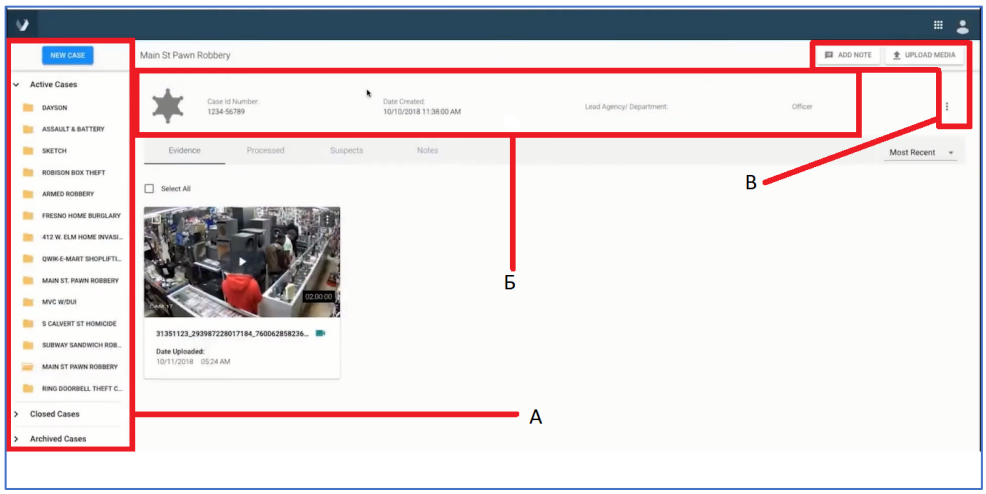


Рисунок 4.1 – (А) панель управління справами, (Б) – вкладка подробиці справи, (В) – дії.

Розділ «Подробиці» містить всі зібрані докази та інформацію про справу, що додані до справи, та зображений на рис. 4.1б. Тут також можна завантажити та обробити додаткові докази, відредагувати деталі справи, додати примітки, обмінюватись інформацією між підрозділами та підтвердити збіг обличчя. Основна інформація про справу відображається у верхній частині сторінки з інформацією про справу.

Розділ «Дії», що зображений на рисунку 4.1в, надає можливості створення приміток, для додавання інформації до справи. Також, в цьому розділі, можна завантажити відео та фото дані як докази до справи, поширити справу колегам в інші підрозділи за допомогою електронної пошти, дізнатися інформацію про справу, редагувати матеріали справи, закрити справу, архівувати справу, видалити справу, повторно відкрити справу.

Рисунок 4.2 – Форма для створення нової справи

У розділі «Докази» (рис. 4.3), містяться всі медіафайли завантажені у справу, що впорядковані в форматі галереї. В цьому розділі можна провести додаткові дії над файлами, як приклад: обітнути відео або обробити, зазначається довжина відеофайлу.

Також тут можна запустити процес розпізнавання обличчя. Для цього натиснувши на відеофайл потрібно натиснути на кнопку «process» в верхньому лівому кутку відкритого вікна, далі з’явиться вікно з вибором бази даних з зображеннями, що будуть порівнюватись, та можна вказати особу, яка займається цією справою. Також тут можна видаляти відео та фотодані.

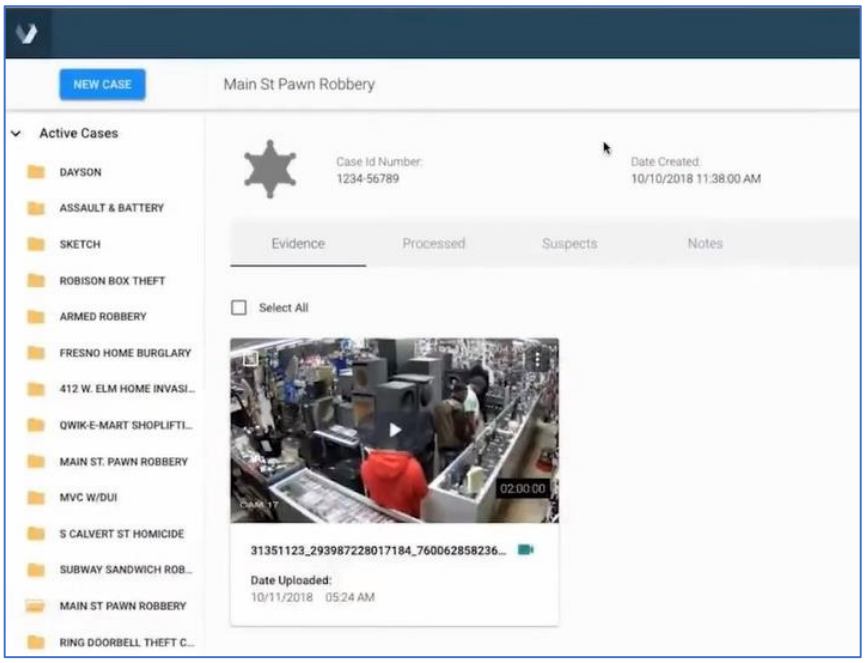


Рисунок 4.3 – Розділ докази

Розділ «Обробка» містить список файлів відео та фото даних що пройшли розпізнавання облич. Тут, навівши курсор миші на відеофайл з потенційним зловмисником та натиснувши на кнопку «view matches», можна переглянути обличчя, що збігаються з базою даних злочинців та невпізнаних людей (рис. 4.4). Тут же за допомогою фільтрів можна сортувати ідентифікованих людей за віком, расою та статтю.

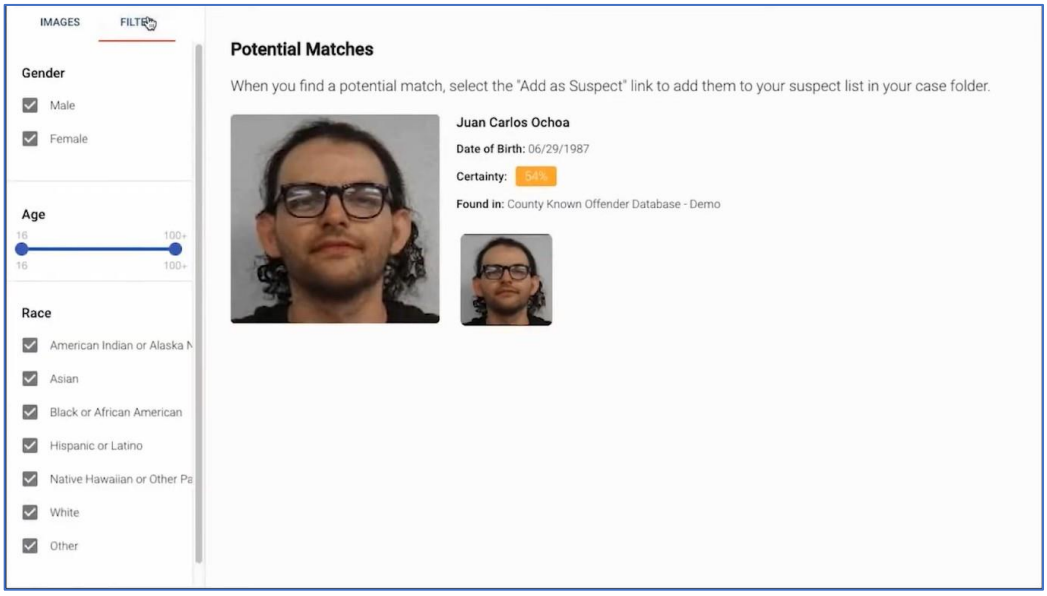


Рисунок 4.4 – Вікно з ідентифікованими підозрюваними

Якщо обличчя підозрюваного не знайшлося в жодній з баз даних, його можна зберегти в базі даних неідентифікованих обличь, щоб в подальшому, якщо виникне така необхідність, швидко знайти цю людину.

Для того щоб додати невпізнану людину в базу з невпізнаними обличчями необхідно у вікні з виявленими обличчями (рис. 4.5) обрати пункт меню з невпізнаними обличчями. Далі навівши курсор миші на обличчя, що не було ідентифіковано (рис. 4.6), потрібно натиснути кнопку додати. Після чого з’явиться форма, після заповнення котрої обличчя невпізнаної людини буде додано в базу.

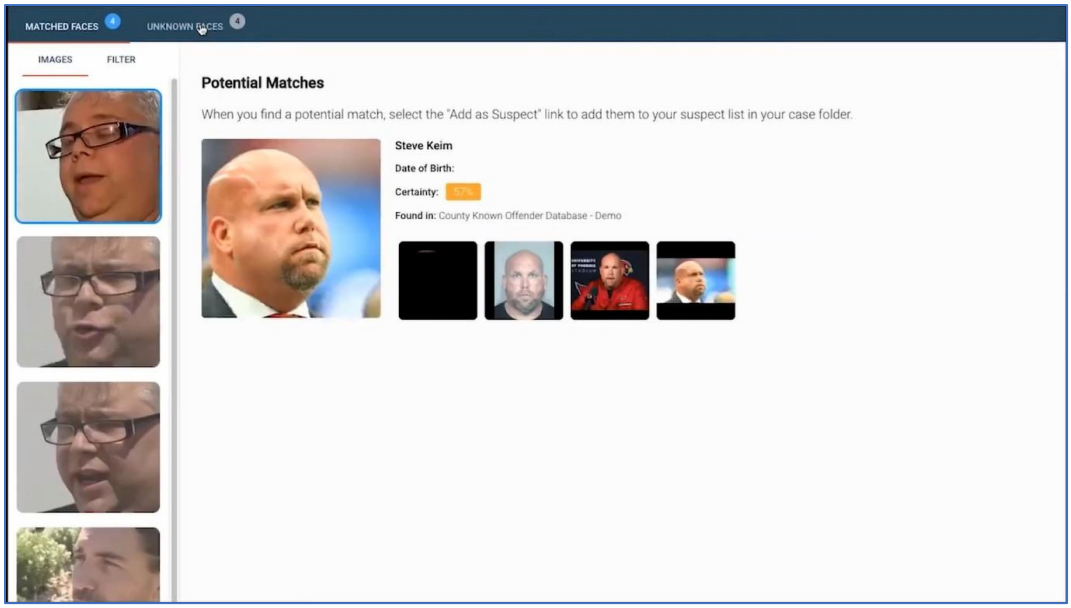


Рисунок 4.5 – Вікно з ідентифікованими обличчями

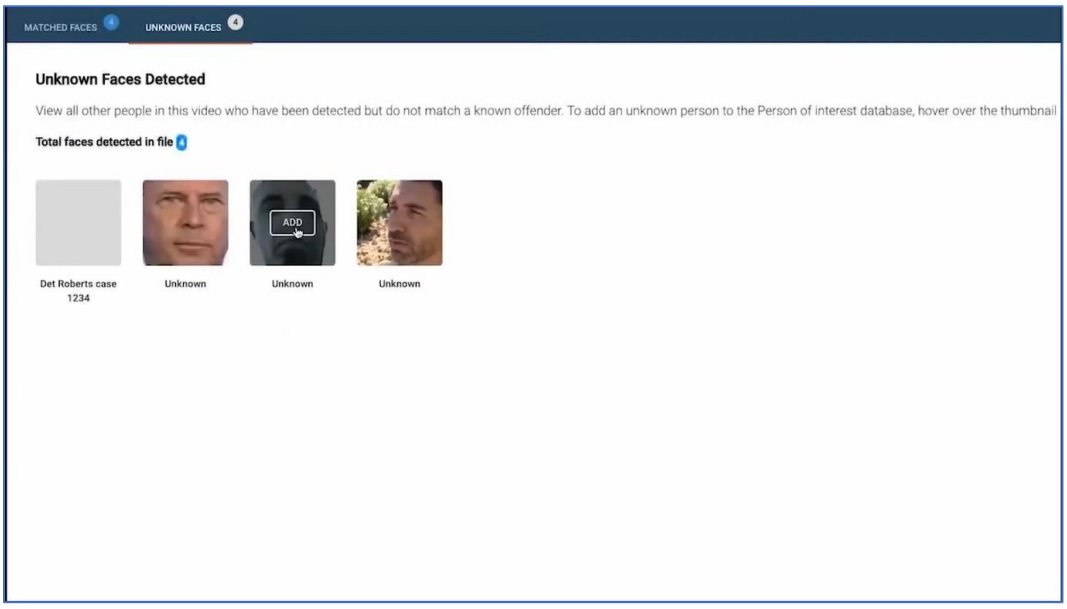


Рисунок 4.6 – Вікно з невпізнаними обличчями

Як приклад одних з найкращих продуктів, здатних аналізувати відеодані та широко використовуваних правоохоронними органами, можна назвати програмні продукті від ізраїльської компанії BriefCam [62, 65]. Це програмне забезпечення здатне аналізувати необроблений відеофайл та «розуміти» контекст всієї сцена та фон, виявляти, відстежувати та класифікувати кожен об’єкт та створювати структуровану базу даних з відеоданих, що полегшує обробку відеоконтенту.

Наприклад, програмний продукт BriefCam Investigator – це готове до роботи універсальне рішення для відеоаналітики правоохоронних органів, призначене для завантаження відео на основі файлів, яке поступово перетворює відео на корисну інтелектуальну інформацію [65]. BriefCam Investigator прискорює розслідування, підвищує продуктивність відео-дослідників та забезпечує швидке досягнення цілей.

BriefCam Investigator являє собою унікальне поєднанням комп'ютерного зору та технологій глибокого навчання разом із запатентованим додатком VIDEO SYNOPSIS®, що дозволяє правоохоронцям швидко визначати на відео, людей та об’єкти, що представляють оперативний інтерес, переглядати години відео за лічені хвилини та ефективно працювати у кримінальних справах для їх швидкого вирішення [65].

Рішення BriefCam Investigator включає в себе наступні можливості: швидкий пошук та фільтрація цікавих об’єктів та подій по чоловікам, жінкам, дітям, транспортним засобам та змінам освітлення зі швидкістю та точністю, використовуючи 27 класів та атрибутів; доповнення до розпізнавання облич, зовнішньої подібності, кольору, розміру, швидкості, шляху, напрямку, та час очікування, забезпечуючи постійно зростаючий та потужний набір різноманітних пошукових комбінацій [65].

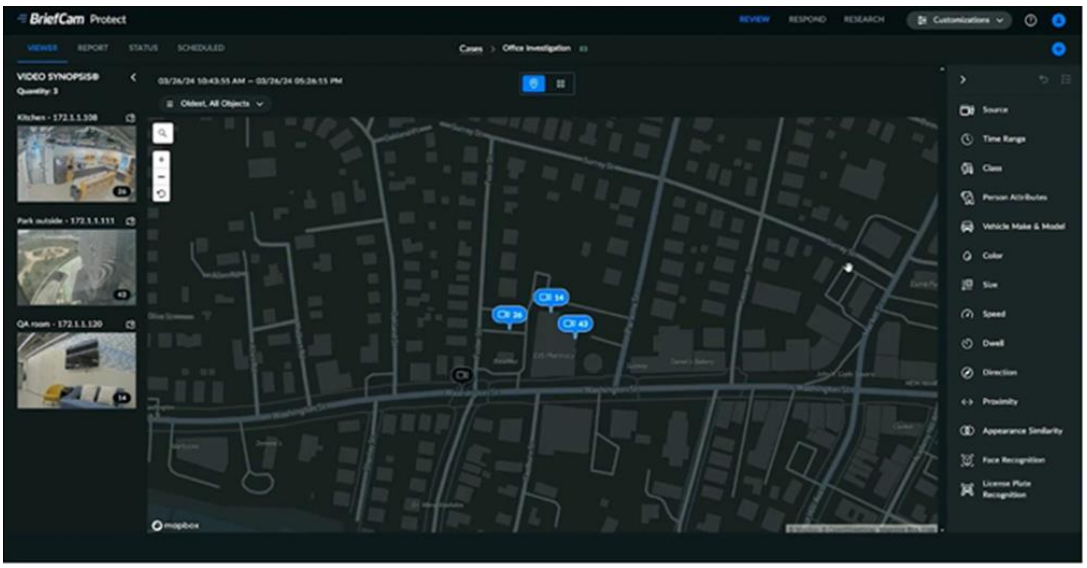
Основне керування програмою розташоване в таких розділах:

– перелік відеофайлів в котрих буде проводитись розпізнавання;

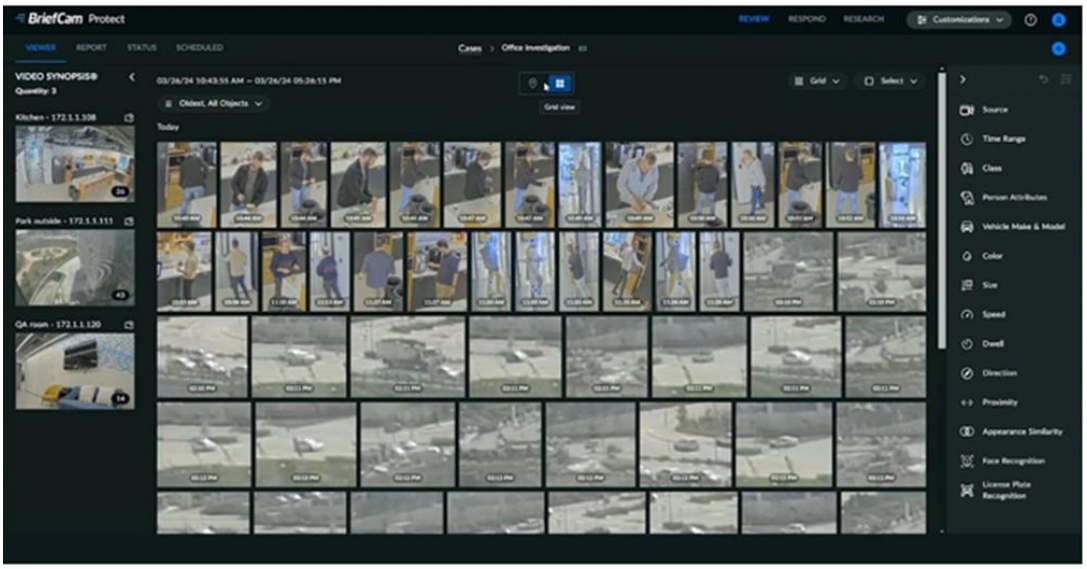
– мапа, з місцем розташування камер відеоспостереження підключених до програми, та всіма ідентифікованими об’єктами, що потрапила в об’єктив камери відеоспостереженн;

– дії, в якому можна відсортувати ідентифіковані об’єкти за різними властивостями, ідентифікувати людину, що була знята відеокамерою та розпізнати номерний знак на транспортному засобі.

Для аналізу відеоданих в програмі BriefCam їх необхідно додати в програму. Це можна зробити, обравши відповідну камеру спостереження на мапі (рис. 4.7а) або просто завантажити відео для обробки. Після ідентифікації всіх об’єктів та людей, що потрапили в об’єктив камер відеоспостереження, вони будуть показані як на рис. 4.7б.



(А)

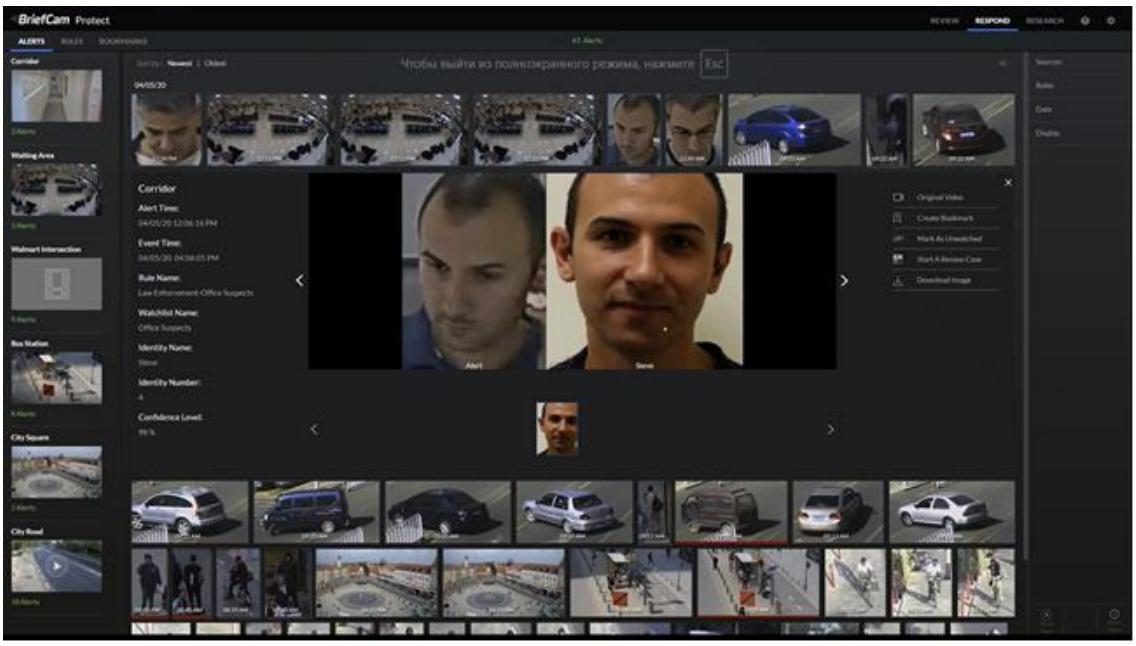


(Б)

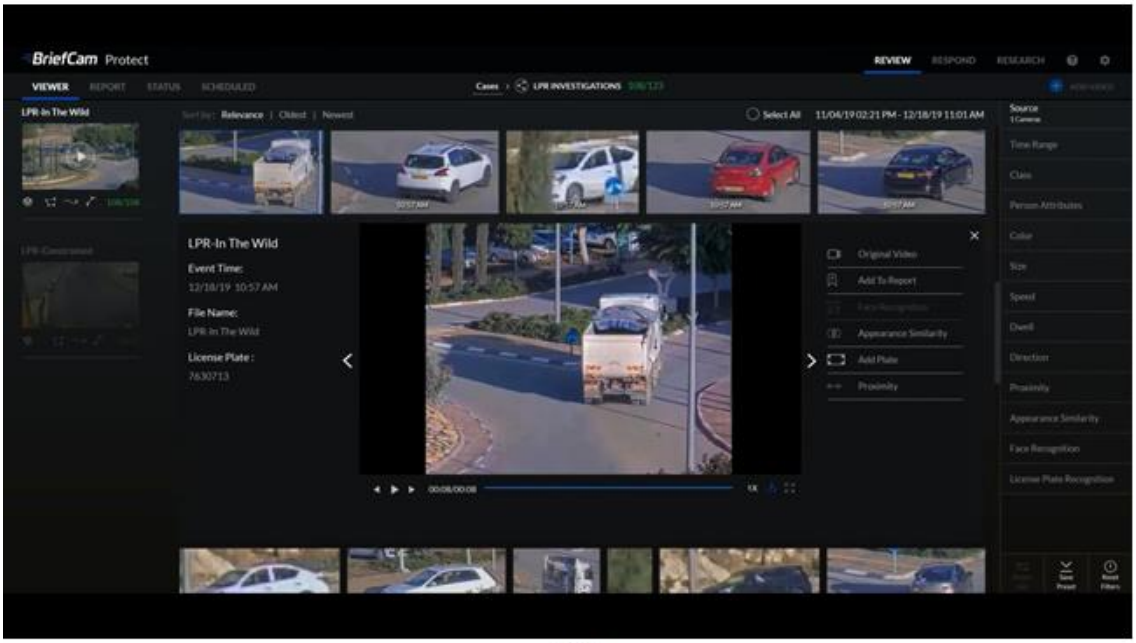
Рисунок 4.7 – Інтерфейс програми аналізу відеоданих BriefCam: А – мапа з зображеними камерами відеоспостереження, Б – ідентифіковані з відео об’єкти

Далі, для того щоб ідентифікувати особу треба натиснути на її фото, після чого з’явиться інформація про цю людну (рис. 4.8а). В разі, якщо людина не впізнана, її можна додати до бази для подальшого розслідування.

Окрім впізнання людей невід’ємною частиною кримінального аналізу є також ідентифікація об’єктів, що можуть стосуватися злочину. Сюди можна також віднести ідентифікацію транспортного засобу та його номерних знаків, що можливо був залучений до вчинення злочину (рис. 4.8б). Можливості програмного забезпечення BriefCam дозволяють швидко аналізувати відеодані на присутність різноманітних транспортних засобів, визначати їх колір, швидкість та напрям руху.



(А)



(Б)

Рисунок 4.2 – Приклад ідентифікації BriefCam людини за обличчям (А) та приклад ідентифікації транспортного засобу (Б)

Таким чином, сучасні програмні засоби реалізують розглянуті раніше (в розділі 3) новітні технології розпізнавання людей по зображенню облич, одягу, їх статі, ходьби та інших ознак, а також відповідних транспортних засобів та інших об’єктів.

Отже, їх застосування підрозділами кримінального аналізу дозволяє швидко визначати на відео людей та об'єкти, що представляють оперативний інтерес, переглядати години відео за лічені хвилини та ефективно працювати для швидкого вирішення інформаційно-аналітичних завдань у сфері кримінального аналізу.

ВИСНОВКИ

У кримінальному аналізі використання програмних засобів відеоаналізу для швидкої ідентифікації людей, транспортних засобів та інших об’єктів може сприяти прискоренню розкриттю злочинів. У цьому випадку сортування ідентифікованих об’єктів за багатьма категоріями, такими як стать та вік особи, колір, розмір, модель транспортного засобу, напрям руху підозрюваного або транспортного засобу та інші може покращити можливості кримінального аналізу та допомогти правоохоронним органам в пошуку всіх причетних до скоєного злочину.

Тому наявність знань працівників підрозділів кримінального аналізу щодо джерел отримання відеоданих, сучасних технологій та програмних засобів здійснення відеоаналітики є важливим елементом підвищення їх підготовки до вирішення практичних завдань у сфері кримінального аналізу.

Саме тому у цьому виданні надані відомості щодо:

– загальних принципів побудови систем відеомоніторингу, відеодані з яких можуть бути джерелами інформації для проведення відеоаналізу підрозділами кримінального аналізу Національної поліції України;

– правових засад отримання та поводження посадовими особами правоохоронних органів з відеоданими у якості електронних доказів та оперативної інформації;

– теоретичних основ сучасних методів та технологій виявлення та розпізнавання на відеоданих фізичних осіб по їх фізичним, фізіологічним чи поведінковим ознакам, а також транспортних засобів та інших об’єктів, включно зброю;

– прикладів використання правоохоронними органами програмних засобів розпізнавання людей та інших об’єктів у кримінальному аналізі.

Підготовлене видання призначене, насамперед, для практичних працівників підрозділів кримінального аналізу Національної поліції України, а також може бути корисною для здобувачів вищої освіти, наукових та науково-педагогічних працівників закладів вищої освіти системи МВС України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бутко Р. Ю. Імплементація моделі поліцейської діяльності, керованої аналітикою в Україні. Розвиток підрозділів кримінального аналізу в умовах сьогодення / Р. Ю. Бутко // Імплементація ILP моделі в Україні: матеріали круглого столу (15 березня 2023 р.). Одеса : ОДУВС, 2023. С. 8-12.

2. Основи кримінального аналізу : навч.-метод. реком. / уклад. О. А. Балтовський, В. Ю. Калугін. Одеса : ОДУВС, 2023. 84 с.

3. Основи кримінального аналізу : навч. посіб. Львів : Львівський держ. Ун-т внутрішніх справ, 2021. 288 с.

4. Корнієнко М. В. Кримінальний аналіз у діяльності Національної поліції України / М. В. Корнієнко // Право і суспільство. № 1, Т. 2. 2024. С. 397-402.

5. Проект Закону України «Про єдину систему відеомоніторингу стану публічної безпеки» від 20.02.2024 № 11031.

6. Мирошниченко В. О. Використання відеоаналітики у роботі Національної поліції : метод. реком. / В. О. Мирошниченко, І. Б. Кочеткова, О. В. Махницький. Дніпро : ДнДУВС, 2020. 34 с.

7. Леонід Тимченко: Користувачі систем відеомоніторингу нестимуть відповідальність за незаконне розповсюдження даних. [Електронний ресурс]. – Режим доступу: https://mvs.gov.ua/news/leonid-timcenko-koristuvaci-informaciyi-z-kamer-videosposterezennia-nestimut-vidpovidalnist-za-nezakonne-rozpovsiudzennia-danix

8. У Києві запрацює Єдина система відеонагляду, що охопить тисячі камер спостереження у метро та навчальних закладах [Електронний ресурс]. – Режим доступу: http://kmr.ligazakon.ua/SITE2/l_docki2.nsf/alldocWWW/C1A12C3D23D6ADEC22582D600687956?OpenDocument

9. Встановлення місцеперебування осіб з використанням інформаційно-аналітичного комплексу «Безпечне місто» : практ. посібн. / [В. Школьніков, О. Корнейко, С. Тіхонов, Р. Білоус, Д. Круглій, Д. Овсянюк]. К. : Вид-во Нац. акад. внутр. справ, 2020. 68 с.

10. Використання єдиного інтегрованого інформаційного простору МВС України щодо забезпечення публічної безпеки та профілактики правопорушень : метод. реком. / Ю. І. Ігнатушко та ін. ; за заг. ред. О. В. Корнейка. Київ : Вид-во НАВС, 2022. 178 с.

11. Застосування органами та підрозділами поліції технічних приладів і технічних засобів фото- і кінозйомки, відеозапису. Аналіз закордонного досвіду : методичні матеріали для працівників підрозділів поліції / [уклад. В. А. Коршенко, М. В. Мордвинцев, Ю. В. Гнусов, В. В. Чумак, В. А. Світличний] ; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. 44 с.

12. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.] ; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

13. Закон України «Цивільний процесуальний кодекс України» № 1618-IV від 18 березня 2004 р. (зі змінами та доповненнями) // Урядовий кур'єр. 2004, Липень. № 130.

14. Закон України «Господарський процесуальний кодекс України» (зі змінами та доповненнями) Закон України № 1798-XII від 6 листопада 1991 р. // Відомості Верховної Ради України (ВВР). 1992. № 6. ст. 56.

15. Закон України «Кодекс адміністративного судочинства України» (зі змінами та доповненнями) № 2747-IV від 6 липня 2005 року // Відомості Верховної Ради України (ВВР). 2005. № 35-36, № 37. ст. 446.

16. Кримінальний процесуальний кодекс України (зі змінами та доповненнями) № 4651-VI від 13 квітня 2012 року // Відомості Верховної Ради України (ВВР). 2013. № 9-10, № 11-12, № 13. ст. 88.

17. Зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису чи засобів фото-,кінозйомки, відеозапису А.М. Соцький, Юридичний науковий електронний журнал. 2022. № 4. С. 384-386.

18. Дар’я Березина. Новий закон змінює механізм огляду електронних даних. URL: https://tokar.ua/read/47992/novyy-zakon-zminiuie-protseduru-rovedennia-slidchykh-diy-z-elektronnymy-danymy/.

19. Закон України «Про оперативно-розшукову діяльність» (зі змінами та доповненнями) № 2135-XII від 18 лютого 1992 року // Відомості Верховної Ради України (ВВР). 1992. № 22. ст. 303.

20. Греченко С. Ю. Отримання та використання оперативної інформації / С. Ю. Греченко // Юридичний часопис Національної академії внутрішніх справ. 2015. № 1. С. 203-213.

21. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник / А. В. Мовчан. Львів: ЛьвДУВС, 2017. 244 с.

22. S. Z. Li , Anil K. Jain Handbook of face recognition (The Second Edition). Springer Science & Business, 2005. 395 p.

23. Курта І. В. Розроблення системи розпізнавання людських облич для відеоспостереження / І. В. Курта, А. Е. Лагун // Автоматика, вимірювання та керування. Національний університет «Львівська політехніка». 2020. № 1(2). Т. 2. С. 57-66.

24. Лебедєва О. Ю. Розробка алгоритму пошуку та відстеження об’єктів на відео / О. Ю. Лебедєва, Т. О. Бирченко, В. М. Лебіга // Informatics and Mathematical Methods in Simulation. Vol. 9 (2019). No. 1-2. pp. 59-68.

25. Голуб`як І. Методи розпізнавання облич: короткий огляд / І. Голуб`як // Матеріали міжнародної науково-практичної конференції «Інформаційні технології та комп`ютерне моделювання». 2017. С. 78-81. URL: http://itcm.comp-sc.if.ua/2017/Holubiak.pdf.

26. Ділай В. І. Огляд методів розпізнавання облич для використання в системах контролю і управління доступом // Матеріали VII Міжнародної студентської науково-технічної конференції / Тернопіль: Тернопільський національний технічний університет ім. І. Пулюя (28-29 листопада 2018 р.). 2018. 212 с. С. 48-49.

27. Левенець Т. В. Дослідження методів розпізнавання облич при використанні мобільних технологій / Т. В. Левенець, І. О. Кравець // Наукові праці : наук.-метод. журн. Миколаїв : Вид-во ЧНУ ім. Петра Могили. 2016. Т. 283. Вип. 271. С. 28-34.

28. Ляшенко Г. Є. Дослідження методів розпізнавання облич / Г. Є. Ляшенко, О. І. Даниленко // НІСТ'2019: Міжнародна науково-практична конференція «Наукоємні технології в інфокомунікаціях»: Матеріали ІІІ Міжнародної науково-практичної конференції. Мадрид, Харків. 2019. С. 85-86.

29. Кюппєр П. Б. Методи розпізнавання облич / П. Б. Кюппєр, О. А. Галуза, О. А. Тевяшева // MicroCAD: Міжнародна науково-практична конференція «Інформаційні технології: наука, техніка, технологія, освіта, здоров'я» : Матеріали Міжнародної науково-практичної конференції. 2021. Ч. IV. С. 262.

30. Мрак В. Методи розпізнавання обличчя у системах відеоспостереження з використанням машинного навчання / В. Мрак // Інфокомунікаційні технології та електронна інженерія. 2023. Вип. 3. № 2. С. 33-42.

31. Данченко О. Б. Розробка системи розпізнавання обличчя людини у відеопотоці з доповненою реальністю / О. Б. Данченко, О. Є. Іларіонов, Г. В. Красовська, Т. С. Короткова // Вісник Черкаського державного технологічного університету. 2020. № 3. С. 75-84.

32. Дигодій В. І. Нейромережева технологія виявлення і розпізнавання людей у відеопотоці / В. І. Дигодій, Т. Б. Мартинюк, М. А. Очкуров // Матеріали LIII науково-технічної конференції підрозділів ВНТУ (20-22 березня 2024 р.). Вінниця. 2024. С. 75-84.

33. Кушнір Н. О. Використання згорткових нейронних мереж у задачах розпізнавання та класифікації об'єктів зображень / Н. О. Кушнір, Т. М. Локтікова, А. В. Морозов, В. О. Юрченко // Технічна інженерія. 2022. №1 (89). С. 93-100.

34. Синєглазов В. Глибокі нейронні мережі для вирішення завдань розпізнавання і класифікації зображення / В. Синєглазов, О. Чумаченко // «Інформаційні технології та комп'ютерне моделювання» : матеріали Міжнар. наук.-практ. конф. (15-20 трав. 2017 р.). Івано-Франківськ, 2017. С. 274–277.

35. Маслій Р. В. Використання локальних бінарних шаблонів для розпізнавання облич на напівтонових зображеннях / Р. В Маслій // Інформаційні технології та комп'ютерна техніка. Наукові праці ВНТУ. 2008, № 4. С. 1-6.

36. Гришанов Д. Ю. Дослідження ефективності локальних бінарних шаблонів / Д. Ю. Гришанов // Наукове мислення: Збірник статей учасників двадцятої всеукраїнської практично-пізнавальної інтернет-конференції «Наукова думка сучасності і майбутнього» (3-11 травня 2018р.). Дніпро : Вид-во НМ, 2018. С. 34.

37. Facial expression recognition based on adaptation of the classifier to videos of the user / E.N. Churaev 1, A.V. Savchenko // Computer Optics. 2023. Vol. 47(5). pp. 806-815.

38. Ekman P. Basic emotions. In Book: Dalgleish T, Power MJ, eds. Handbook of cognition and emotion. New York: John Wiley & Sons; 1991. pp. 45-60.

39. Liu W., Anguelov D., Erhan D., Szegedy C., Reed S., Fu C.-Y., Berg A.C. SSD: single shot multibox detector // Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 2016. V. 9905. pp. 21-37.

40. Déniz O., Bueno G., Salido J., De la Torre F. Face recognition using histograms of oriented gradients // Pattern Recognition Letters. 2011. V. 32. № 12. pp. 1598-1603.

41. King D. Max-margin object detection URL: https://arxiv.org/pdf/1502.00046.pdf.

42. X. Geng, Z.-H. Zhou, and K. Smith-Miles. Automatic age estimation based on facial aging patterns // Pattern Analysis and Machine Intelligence, IEEE Transactions. 2007. vol. 29. no. 12. pp. 2234-2240.

43. C. Shan, S. Gong, and P. W. McOwan. Facial expression recognition based on local binary patterns: A comprehensive study // Image and Vision Computing. 2009. vol. 27. no. 6. pp. 803-816.

44. М. Андерсон. Визначення статі за допомогою стилю ходьби за допомогою машинного навчання URL: https://www.unite.ai/uk/determining-gender-through-gait-with-machine-learning/.

45. Фастовець В. І. Аналіз підходів виявлення аномальної поведінки людини в реальному часі у відеопослідовності / В. І. Фастовець, Т. А. Радівілова // Матеріали Всеукраїнської науково-практичної Internet-конференції «Моделювання та інформаційні технології в науці, техніці, кібербезпеці та освіті» (15-16 листопада 2022 р.). м. Харків, 2022. С. 43-46.

46. Жадан Д. О., Мордвинцев М. В., Пашнєв Д. В. Відстеження протиправних дій за допомогою систем відеоспостереження: огляд сучасного стану досліджень / Д. О. Жадан, М. В. Мордвинцев, Д. В. Пашнєв // Право і безпека. 2024. № 1 (92). С. 78-89.

47. Vijeikis R., Raudonis V., Dervinis G. Efficient Violence Detection in Surveillance. Sensors. 2022. Vol. 22. Iss. 6. URL: доступу: https://www.researchgate.net/publication/359215233_Efficient_Violence_Detection_in_Surveillance.

48. Masked face recognition: Human versus machine / N. Damer та ін. IET Biometrics, 2022. URL: https://digital-library. theiet.org/doi/10.1049/bme2.12077

49. Колесницький О.К. Виявлення озброєних людей у відеопотоці з використанням згорткових нейронних мереж.// О. К. Колесницький, Є. В. Янковський, І. К. Денисов, І. Р. Арсенюк // Оптико-електронні інформаційно-енергетичні технології. 2023 р. № 2 (46). С. 76-83.

50. Ingle P. Y., Kim Y.-G. Real-Time Abnormal Object Detection for Video Surveillance in Smart Cities. Sensors. 2022. Vol. 22. Iss. 10. URL: https://www.researchgate.net/publication/360748771_Real-Time_Abnormal_Object_Detection_for_Video_Surveillance_in_Smart_Cities

51. Губаренко Є. В. Розпізнавання об'єктів у відеопотоці / Є. В. Губаренко, М. С. Губаренко, М. В. Антонюк // АСУ та прилади автоматики : всеукраїнський міжвідомчий науково-технічний збірник. Харків : ХНУРЕ, 2021. Вип. 177. С. 18-28.

52. Кушнір Д. О. Методи пошуку та розпізнавання об'єктів у відеозображеннях на мобільній платформі IOS в реальному часі / Д. О. Кушнір, Я. С. Парамуд // Computer Systems and Networks. 2019. Т. 1. № 1. С. 24-33.

53. Жеребух О. Використання нейронних мереж для визначення об’єктів на зображенні /О. Жеребух, І. Фармага // Комп’ютерні системи проектування. Теорія і практика. Науковий журнал НУ «Львівська політехніка», Львів. 2024. Вип. 6, № 1. С. 232-240.

54. Рябушенко О. Дослідження швидкостей руху транспортних засобів з використанням даних відеоспостереження / О. Рябушенко, С. Данець, М. Скляров // Сучасні технології в машинобудуванні та транспорті. 2022. 2(19). С. 182-190.

55. ДСТУ 4278:2012. Управління безпеки дорожнього руху. URL: http://www.sai.gov.ua/uploads/filemanager/file/zmina-1-dstu-4278.pdf

56. Ківа А. О. Пайплайн методів обробки зображень у системах розпізнавання номерних знаків / А. О. Ківа, С. М. Коваленко // Матеріали XVII Міжнародної науково-практичної конференції «Інформаційні технології і автоматизація» (31 жовтня – 1 листопада 2024 р.). м. Одеса, 2024. URL: https://www.researchgate.net/publication/385751264_Pajplajn_metodiv_obrobki_zobrazen_u_sistemah_rozpiznavanna_nomernih_znakiv

57. Волошин Н. Методи автоматичного розпізнавання автомобільних номерних знаків / Н. Волошин, П. Федорів // Матеріали III Всеукраїнської науково-технічної конференції «Теоретичні та прикладні аспекти радіотехніки і приладобудування» (8-9 червня 2017 року). Тернопіль : ТНТУ, 2017. С. 137-138.

58. Криміналістика: криміналістична техніка : навч. посіб. / Р. Л. Степанюк, В. О. Гусєва, В. В. Кікінчук та ін. ; МВС України, Харків. нац. ун-т внутр. справ. Харків : ХНУВС, 2023. 388 с

59. Intelligent, rapid suspect identification. URL: https://www.veritone.com/applications/identify

60. Clearview AI. URL: https://www.clearview.ai/

61. Face Recognition Technology In Law Enforcement. URL: https://www.corsight.ai/law-enforcement/
62. Video analytics for law enforcement. BriefCam. URL: https://www.briefcam.com/video-analytics-for-law-enforcement/
63. Перевірка особи — просто, як ніколи. ТиХто. URL: https://tyhto.com/
64. Artellence розробляє унікальні AI технології для вирішення OSINT задач на основі аналізу big data з відкритих джерел. URL: https://artellence.com/ua
65. BriefCam Datasheet Investigator. URL: https://ukrinfosystems.com.ua/images/docs/BriefCam/BriefCam_datasheet_investigator.pdf

Науково-методичне видання

БУРЕНКО Олег Володимирович
БУТКО Роман Юрійович
ЖАДАН Дмитро Олегович
КОРНЕЙКО Олександр Васильович
МАНЖАЙ Олександр Володимирович
МОРДВИНЦЕВ Микола Володимирович
ОВСЯНЮК Дмитро Іванович
ПАШНЄВ Дмитро Валентинович
САЛЬНІКОВ Ігор Іванович
СВІТЛИЧНИЙ Віталій Анатолійович
СИВУН Андрій Сергійович
ШКОЛЬНІКОВ Владислав Ігорович

ОСОБЛИВОСТІ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ВІДЕОАНАЛІЗУ ТА ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ З РОЗПІЗНАВАННЯ ОБЛИЧ ТА ІНШИХ ОБ'ЄКТІВ У КРИМІНАЛЬНОМУ АНАЛІЗІ

Методичні рекомендації

Відповідальний за випуск та комп'ютерна верстка: О. В. Корнейко

Відділ підготовки навчально-наукових видань
Національної академії внутрішніх справ.
03035, м. Київ, пл. Солом'янська, 1.
Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців, виготовників і розповсюджувачів видавничої продукції ДК № 4155 від 13.09.2011.
Підписано до друку 30.12.2025. Формат 60х84/16. Папір офсетний.
Ум.-друк. арк. 5,08. Тираж 50 прим.

Друк: ФОП Поліщук О. В.
Свідоцтво суб'єкта видавничої справи ДК № 2142 від 31.03.2015.
07400, м. Бровари, вул. Незалежності, 2, кв. 148.
тел. (044) 592-13-49