**МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН
АЛМАТИНСКАЯ АКАДЕМИЯ МВД РЕСПУБЛИКИ КАЗАХСТАН
ИМЕНИ МАКАНА ЕСБУЛАТОВА**

Кафедра уголовного процесса и криминалистики

Стамбеков О.Е.,
Кудайбергенов Е.Б.,Сарсенбаева Б.Б.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

НА ТЕМУ: «ПРАВОВЫЕ ОСНОВЫ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ ВИДЕОАНАЛИТИКИ, В ТОМ ЧИСЛЕ С ПРИМИНЕНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ХОДЕ РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ»

Алматы 2024

Методические рекомендации обсуждены и одобрены на заседании кафедры уголовного процесса и криминалистики Алматинской академии МВД Республики Казахстан им. Макана Есбулатова Протокол № ____ от «___» _____2024 г.

Методические рекомендации обсуждены и одобрены на научно-методическом заседании Алматинской академии МВД Республики Казахстан им. Макана Есбулатова. Протокол № ____ от «___» _____2024 г..

Рецензенты:

Коржумбаева Т.М. – начальник кафедры административно-правовых дисциплин Алматинской академии МВД Республики Казахстан им. Макана Есбулатова, к. ю.н., ассоциированный профессор (доцент), полковник полиции.

Аубакирова А.А. - Директор Алматинского филиала Санкт-Петербургского гуманитарного Университета профсоюзов, д.ю.н, профессор

Стамбеков О.Е. старший криминалист Управления организационно-методической работы ОКД МВД, Кудайбергенов Е.Б. главный криминалист Управления криминалистического обеспечения досудебного расследования ОКД МВД, Б.Б.Сарсенбаева, профессор кафедры уголовного процесса и криминалистики Алматинской академии МВД Республики Казахстан им. Макана Есбулатова, «Правовые основы использования системы видеоаналитики, в том числе с применением искусственного интеллекта в ходе расследования уголовных дел: Методические рекомендации. – Алматинская академия МВД Республики Казахстан имени Макана Есбулатова, ООНИиРИР, г. Алматы 2024 г. – 68 с.

Методические рекомендации подготовлены в соответствии с Планом НИД Алматинской академии позиция 7 Правовые основы использования системы видеоаналитики, в том числе с применением искусственного интеллекта в ходе расследования уголовных дел (2024г.), и разработаны с учетом современных требований криминалистики, уголовного и уголовно-процессуального законодательства. Отражают основные понятия, стандарты видеоаналитики. в практике сотрудниками правоохранительных органов.

Методические рекомендации предназначены для сотрудников правоохранительных органов, а также научных и практических работников системы ОВД, преподавателей и обучающихся ведомственных и иных юридических учебных заведений.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Вы когда-нибудь задумывались, что происходит с записями с камер видеонаблюдения на вокзалах, в аэропортах, магазинах, заправочных станциях и любых других заведениях, которые вы видите каждый день?

Кроме того, что произойдет с этими многочасовыми кадрами видеонаблюдения позже? Их когда-нибудь увидит кто-нибудь?

Записи видеонаблюдения являются важным инструментом в руках следователей по уголовным делам. В случае совершения преступления или подозрения, что преступление вот-вот будет совершено, правоохранительные органы будут использовать все улики, включая записи камер наблюдения, сделанные в различных учреждениях, для установления личности преступников. В случае возникновения угрозы, независимо от того, является ли она реальной, проводится анализ записей видеонаблюдения для установления, устранения или предотвращения угрозы.

Человеческий анализ записей видеонаблюдения

До появления компьютерного анализа видеоматериалов основную работу приходилось выполнять людям. Необходимо было просмотреть многочасовые видеоданные, оценить любую связанную с ними информацию и затем передать на следующий уровень с целью установления факта преступления.

Процесс был утомительным и громоздким. Не говоря уже о неотъемлемых проблемах, возникших из-за того, что весь процесс был подвержен человеческим ошибкам или оплошностям. В ходе исследования, проведенного с целью оценки способности человека концентрироваться при просмотре видеозаписей с камер видеонаблюдения, было обнаружено, что в среднем человек не может концентрироваться на экране более 20 минут.

Кроме того, просмотр прямых потоков данных, поступающих из нескольких источников с камер, требовал дополнительных усилий со стороны любого сотрудника стойки регистрации или специальной зоны безопасности.

Таким образом, группы наблюдения по очереди выполняли работу круглосуточно. Простая идея заключалась в том, что две пары глаз лучше, чем одна. Тем не менее, существовала необходимость исключить вмешательство человека при обработке данных наблюдения. Машины стали быстрее и выполняли гораздо более эффективную работу по оценке текущих данных, а также тщательному анализу исторических данных, записанных за определенный период времени. Естественным переходом было цифровизировать весь процесс, чтобы сделать его быстрее и эффективнее. Так родилась компьютеризированная видеоаналитика.

Эффективность компьютерной видеоаналитики

Процесс анализа записей видеонаблюдения, сбора на их основе разведданных и установления связи между преступлением и исполнителями известен под различными названиями. В ходе любого исследования вы можете поочередно слышать «видеоаналитику», или «анализ видеоконтента», или «компьютерную видеоаналитику». По сути, все они указывают на одно и то же. Применение видеоаналитики в системе распознавания преступников в правоохранительной деятельности имеет ряд эффективных преимуществ:

1. Повышение точности и скорости идентификации. Современные алгоритмы распознавания лиц, основанные на машинном обучении, способны сравнивать изображения с базами данных гораздо быстрее и точнее, чем человек.

2. Обработка большого объема данных. Видеоаналитика позволяет анализировать одновременно множество камер видеонаблюдения, что значительно расширяет возможности по сбору и обработке информации.

3. Непрерывность мониторинга. Компьютерные системы могут вести постоянное наблюдение, в отличие от человека, что повышает эффективность обнаружения преступников или других интересующих событий.

4. Объективность и беспристрастность. Алгоритмы видеоаналитики принимают решения исключительно на основании данных, что исключает человеческий фактор и предубеждения.

5. Возможность автоматического реагирования. Системы могут самостоятельно подавать сигналы тревоги при обнаружении подозрительных лиц или событий, что ускоряет реакцию правоохранительных органов.

Таким образом, применение видеоаналитики значительно повысит эффективность работы правоохранительных органов в вопросах распознавания и поиска преступников.

ИСТОРИЯ РАЗВИТИЯ, СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ВИДЕОАНАЛИТИКИ С ПРИМЕНЕНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА.

Видеоаналитика - это технология, использующая методы компьютерного зрения для автоматизированного получения различных данных на основании анализа последовательности изображений, поступающих с видеокамер в режиме реального времени или из архивных записей.

Видеоаналитика представляет собой программное обеспечение (ПО) для работы с видеоконтентом. В основе программного обеспечения лежит комплекс алгоритмов машинного зрения, позволяющих вести видеомониторинг и производить анализ данных без прямого участия человека. Алгоритмы видеоаналитики могут быть интегрированы в различные бизнес-системы, чаще всего используются в видеонаблюдении и других сферах безопасности.

Определения

Видеоаналитика – компьютеризированная обработка и автоматический анализ видеоконтента, который поступает на видеосервер от видеокамер, носимых устройств и устройств Интернета, оснащённых веб-камерами.

– Видеоаналитика - это технология, использующая методы компьютерного зрения для автоматизированного получения различных данных на основании анализа последовательности изображений, поступающих с видеокамер в режиме реального времени или из архивных записей.

– Видеоаналитика представляет собой программное обеспечение (ПО) для работы с видеоконтентом. В основе программного обеспечения лежит комплекс алгоритмов машинного зрения, позволяющих вести видеомониторинг и производить анализ данных без прямого участия человека.

– Традиционное решение, включающее в себя функции какой-либо видеоаналитики строится по схеме: камера + back-end аналитика. Т.е. камера просто гонит поток видео на сервер, а специальное ПО на сервере уж делает весь видеоанализ.

Во время видеонаблюдения в промышленности, городском и жилищном хозяйстве, а также в различных социальных медиа, генерируется огромное количество видеоданных, для которых требуется системы хранения данных (СХД) с высокой ёмкостью.

Разрешающая способность видеоизображений всё время возрастает, и количество хранимого контента растёт экспоненциально.

Видеоаналитика в последние годы набирает всё большую популярность по многим причинам. Она позволяет гибко управлять видеопотоками при анализе их контента «на лету», при автоматизации аналитических функций.

Это позволяет персоналу концентрироваться на определённых инцидентах на видеозаписи, а не тратить время на просмотр длинных однообразных видеопотоков, что позволяет сократить затраты и численность персонала. Интеллектуальные системы безопасности с видеоаналитикой могут начинать запись, например, только при начале какого-то движения в зоне обзора камеры. При этом снижается нагрузка на сеть и экономится пространство в системе хранения.

Системы видеоаналитики не требуют чрезмерно громоздкой инфраструктуры и даже небольшие предприятия, магазины и пр. вполне могут себе позволить её использование. Интенсивность использования функций видеоаналитики можно гибко регулировать по мере потребностей, выбирая именно те функции, которые нужны в конкретном случае. Это позволяет создавать кастомизированные решения.

Типовая системная архитектура ВИДЕОАНАЛИТИКА показана на рисунке ниже.

Рис. 1- 1. Типовая системная архитектура видеоаналитики

Видеоаналитика автоматизирует процесс видеонаблюдения, делает его удобным в использовании и значительно сокращает затраты на мероприятия, в которых используется видеонаблюдение. Потребность в видеоаналитике растет в различных отраслях экономики, таких как финансовый сектор и услуги, розничная торговля, транспорт, добыча и транспортировка ископаемых, производство и др.

К тому же, рост требований к IP-системам безопасности и их инфраструктуре, а также повышение важности безопасности в повседневной жизни, также приводит к росту рынка видеоаналитики.

Существует также термин «компьютерное зрение» («машинное зрение«, техническое зрение»). Эту технологию часто путают с видеоаналитикой. Однако, они неравнозначны. Можно сказать, что видеоаналитика является составной частью компьютерного зрения в части анализа изображения.

Компьютерное зрение (Computer Vision) - это технология (а также область исследований) по автоматизации понимания того, что мы видим в окружающем мире.

Видеоаналитика – это частные приложения компьютерного зрения,
которые извлекают информацию и знания из видеоконтента, то есть дают ответы на вопросы:

- ***Кто:*** распознавание и идентификация людей;
- ***Что:*** объекты, действия, события, поведение, взаимоотношения;
- ***Где:*** геолокация, пространственная (3D) и планарная (2D) локация;
- ***Когда:*** маркировка даты и времени, сезона.

Три основных типа приложений видеоаналитики:

- **Ретроспектива:** что уже случилось, т.е. управление архивами видеозаписей, поиск, сортировка, получение юридических доказательств;
- **Настоящий момент:** что происходит сейчас, т.е. контроль ситуации, получение предупреждений в реальном времени, кодирование, компрессия видеопотока;
- **Взгляд в будущее:** что может или скорее всего произойдёт, т.е. предсказания на основе событий прошлого и настоящего, прогнозирование событий или активности, детектирование намечающихся аномалий.

Типы платформ видеоаналитики

Видеоаналитика на выделенном сервере

Например, это может быть сервер интеллектуального видеонаблюдения IVS (Intelligent Video Surveillance) и сервер автоматического распознавания номеров

автомашин ALPR (Automatic License Plate Recognition). Такой сервер хорошо масштабируется при увеличении числа камер и позволяет ввод новых функции анализа видеоизображений. Видеоданные в этом случае хранятся на сервере и могут быть извлечены через удалённую программу-клиент.

Видеоаналитика на сетевом видеорекордере NVR

Сетевой видеорекордер NVR (Network Video Recorder) может обладать некоторыми встроенным функциями видеоаналитики. Однако, ввод новых аналитических функций в этом случае либо невозможен, либо сложен. Такое решение выгодно использовать если число камер невелико и функции фиксированы. Данные в этом случае хранятся на видеорекордере и могут быть извлечены через удалённую программу-клиент.

Видеоаналитика на камерах

Камеры видеонаблюдения могут также обладать встроенными функциями видеоаналитики. Преимуществом здесь является то, что такие возможности аналитики в таких камерах не зависят от полосы пропускания сети и времени отклика сервера. Такое решение выгодно там, где требуется высокая оперативность и немедленный отклик, например при слежении через купольные камеры PTZ. Видеоданные в этом случае хранятся на самих видеокамерах и могут быть извлечены через удалённую программу-клиент.

История развития

Существует легенда, что при помощи больших зеркал, установленных на верхней площадке Александрийского маяка, древние греки могли наблюдать корабли далеко в море.

С появлением первых казино, их службы безопасности использовали сложные системы зеркал, чтобы вести наблюдение за игровыми комнатами. Можно сказать, что они были прототипами систем видеонаблюдения. Однако, развитие настоящих систем видеонаблюдения началось с появления иконоскопа – электронного устройства для передачи изображений.

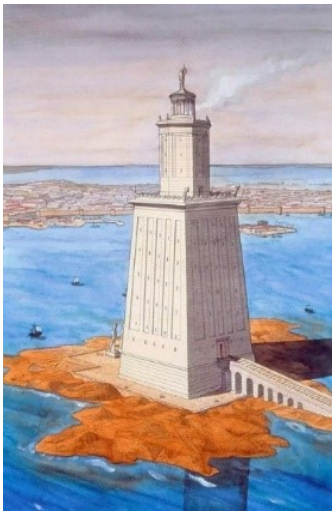


Рис. Александрийский маяк

Отцом современных видеосистем и изобретателем иконоскопа, устройства для захвата видеоизображений, считается ***Виктор Кузьмич Зворыкин,*** русский инженер, выпускник с отличием Санкт-Петербургского Технологического института 1911 года, ветеран Первой Мировой войны и офицер Белой Армии. Однако, работая в России, он успел лишь провести фундаментальные исследования в области удалённой передачи изображений, а само изобретение иконоскопа было сделано в США, куда Зворыкин эмигрировал после победы большевиков, куда был послан командованием Белой армии для закупки радиостанций).

Во время научной работы в Санкт-Петербургском Технологическом институте, он вёл исследования вместе с профессором ***Борисом Розингом***, создавшим неэлектронный вариант кинескопа, на который в то время удавалось передавать лишь самые простые изображения. Профессор Розинг умер в 30-х годах, находясь в ссылке в Архангельске, не имея возможности продолжать научные разработки.

Первой точкой телепередачи изображения стал 103-этажный небоскрёб Эмпайр Стейт Билдинг в Нью-Йорке в 1932 году. Видеосигнал с иконоскопа передавался

передатчиком мощностью 2,5 кВт и был принят на кинескоп конструкции Розинга, находящийся на расстоянии 100 км в здании RCA (Radio Corporation of America).

Таким образом, началом эры телевидения считается 1932 г., однако, это относится и к началу развитию систем видеонаблюдения.

Первое практическое использование «закрытой системы телевидения» CCTV (closed curcuit television), было осуществлено германским инженером Вальтером Брухом в 1941 году в Пенемюнде, во время испытаний ракеты «Фау-2». Это первый известный в истории случай использования видеонаблюдения на практике. Оператор должен был неотлучно сидеть перед монитором, наблюдая за происходящим на стартовой площадке, т.к. видеозапись тогда ещё не была реализована. Так продолжалось до 1951 года, пока не появились первые видеомагнитофоны VTR (Video Tape Recorder).

Рис. В.К. Зворыкин демонстрирует первую в мире видеокамеру

С тех пор, системы видеонаблюдения совершенствовались практически каждые 10 лет.

- Начало 1950-х годов: появление устройств, позволяющих передавать изображение на магнитной ленте;
- Конец 1950 – начало 1960х: использование видеокамер для наблюдения на дорогах, важных объектах и в местах массового скопления людей;
- 1970-е годы: появление в продаже домашних видеомагнитофонов и видеокамер;
- 1990-е годы: появление цифровых видеосистем (DVR);
- 2000-е годы: появление сетевых систем видеонаблюдения;
- 2010-е годы: разработка и применение облачных видеокамер, которые могут работать без периферийного оборудования (серверов видеоаналитики, рекордеров, IP-систем) на площадке предприятия, отправляя видеоданные в облако.

Технологии продолжают развиваться, и в период 2023-2030 годов могут появиться алгоритмы и системы, которые будут способны различать объекты и даже события непосредственно в видеопотоке. Камеры будут способны распознавать нестандартные ситуации и предпринимать соответствующие действия – информировать оператора, самостоятельно вызывать спецслужбы и пр.

Современные технологии видеонаблюдения и нейросети взаимосвязаны, так как последние значительно усиливают возможности анализа видеоинформации. Нейросети позволяют обрабатывать большие объемы данных, распознавать объекты и лица, а также выявлять аномалии в поведении. Это делает системы видеонаблюдения со встроенной видеоаналитикой более интеллектуальными и эффективными в реальном времени.

Краткая история развития нейросетей

В 1950-е - 1960-е годы: Первые идеи о нейронных сетях появились с

работами таких ученых, как Фрэнк Розенблатт, который разработал перцептрон — простую модель нейронной сети.

В 1943 году американские учёные: нейропсихолог, нейрофизиолог, один из основателей кибернетики Уоррен Маккалох и нейролингвистик, логик и математик Уолтер Питтс изобрели первое устройство, которое можно было назвать нейросетью, работавшее по принципу «пороговой логики» (Threshold Logic) для имитации элементарных операций нейронов человеческого мозга.

Warren McCulloch and Walter Pitts (source)

Рис. Уоррен Маккалох и Уолтер Питтс

В начале 60-х годов, Генри Келли, профессор Политехнического института штата Вирджиния, разработал модель обратного распространения (Back Propagation Model) для обучения нейросети. Примерно в тоже время японский учёный Кунихико Фукушима разработал концепцию свёрточной нейросети CNN (Convolutional Neural Network), разновидности DNN. В конце 1970-х годов Фукушима разработал первую иерархическую многослойную нейросеть, под названием Neocognitron которая могла распознавать визуальные образы.

В разработке учёных из Института когнитивной науки университета Калифорнии в Сан-Диего, Дэвида Румельхарта и Рональда Уильямса, а также Джеффри Хинтона из Университета Карнеги-Меллона из Филадельфии в 1989 году был впервые на практике использован алгоритм обратного распространения (Back Propagation), теоретически предложенный ещё в начале 60-х.

В 1980-е годы: Появление методов обратного распространения ошибки (backpropagation) сделало обучение многослойных нейронных сетей более эффективным и привело к возрождению интереса к нейросетям.

В 1990-е годы: Исследования в области нейросетей замедлились, однако технологии развивались, и началось применение нейросетей в практических задачах, таких как распознавание речи и обработка изображений.

В 1997 году Зепп Хохрайтер и Юрген Шмидхубер из Университета Иоганна Кеплера в Австрии разработали «длинную кратковременную память» LSTM (Long Short-Term Memory) для рекурсивных нейросетей RNN (Recurrent Neural Network).

В настоящее время сделано множество изобретений и усовершенствований в архитектурных моделях нейросетей, активационных функциях нейронов и пр., что привело к взрывному росту развития глубоких нейросетей. Сыграли свою роль и сопутствующие технологии, концепции и вклад многочисленных учёных и разработчиков, что привело к синергетическому развитию области нейросетей применительно к видеоаналитике.

В 2000-е годы: Появление больших объемов данных и мощных вычислительных ресурсов (графических процессоров) способствовало бурному развитию глубокого обучения. Нейросети стали основой для многих прорывных технологий, включая распознавание лиц и объектов.

В 2010-е годы - настоящее время: Нейросети становятся стандартом в области искусственного интеллекта, активно применяются в видеонаблюдении, медицине, финансах и других сферах, обеспечивая высокую точность и эффективность.

Анализ больших данных, искусственный интеллект

Технологии Искусственного Интеллекта (ИИ) быстро распространяются по всему миру. Возможности искусственного интеллекта, в частности, широко применяются в видеоаналитике.

Технологии ИИ (AI) – по сути являются другим названием нейросетей с возможностью обучения.

Существует три основных метода обучения нейросетей: с учителем, без учителя, с подкреплением.

При обучении с учителем нейронная сеть обучается на предварительно размеченном наборе данных для получения ответов, которые используются для оценки точности алгоритма на обучающих данных. При обучении без учителя модель использует неразмеченные данные, из которых алгоритм самостоятельно пытается извлечь признаки и зависимости.

Обучение с частичным привлечением учителя представляет собой нечто среднее. Оно использует небольшое количество размеченных данных и большой набор неразмеченных данных. А обучение с подкреплением тренирует алгоритм при помощи системы поощрений.

Поэтому, когда мы говорим об использовании ИИ в видеонаблюдении, мы фактически имеем в виду использование нейросетей с возможностью обучения без учителя.

Использование ИИ в видеонаблюдении

В университете Карнеги (США) в 2019 году было проведено исследование использования ИИ для видеонаблюдения и был разработан Глобальный Индекс использования ИИ для видеонаблюдения AIGS (AI Global Surveillance), который показывает степень использования ИИ для видеонаблюдения в 176 странах мира (без различия легитимности такого использования)[20].

Исследование показало, что в настоящее время технологии ИИ для видеонаблюдения распространяются быстро. По крайней мере, 75 из 176 стран в мире активно используют ИИ для целей видеонаблюдения и видеоаналитики. Наиболее часто ИИ используется в таких приложениях видеоаналитики, как платформы Умного или Безопасного Города (56 стран), системах распознавания лиц (64 страны), а также в системах Умной охраны правопорядка, Smart Police (52 страны).

Наиболее бурно технологии ИИ для видеонаблюдения развиваются в *Китае,* благодаря разработкам таких компаний как Huawei, Hikvision, Dahua и ZTE.

Компании США также активно работают в этой области. Наиболее крупными американским игроками в этой области являются компании IBM (11 стран), Palantir (9 стран) и Cisco (6 стран). Важную роль также играют разработки компаний из Франции, Германии, Израиля и Японии.

В исследовании приводится карта происхождения используемых технологий ИИ для видеонаблюдения.

СТАНДАРТЫ ВИДЕОАНАЛИТИКИ

20 июля 2020 года В России разработан Национальный стандарты в области Искусственного интеллекта (далее - ИИ) для ситуационной видеоаналитики. Документ, подготовленный ООО «Видеоинтеллект» (развивает системы компьютерного зрения для использования в сложных условиях, общественных местах с большим скоплением людей, на объектах промышленности), представил технический комитет по стандартизации ТК «Искусственный интеллект».

Ситуационная видеоаналитика. «Термины и определения» является первым в группе стандартов, устанавливающих нормативные требования в области ситуационной видеоаналитики. Они должны регламентировать эксплуатационные характеристики, методики испытаний и оценки качества и требования к размещению оборудования технических систем интеллектуального видеонаблюдения.

В России разработан первый национальный стандарт в области искусственного интеллекта для ситуационной видеоаналитики

Предполагается, что принятие стандарта в качестве национального позволит упорядочить нормативное регулирование в области ситуационной видеоаналитики и, в последующем, устранить технические барьеры при применении подобных «умных» информационных систем.

Современные системы видеонаблюдения все применяют интеллектуальные технологии обработки данных, позволяющих в реальном времени анализировать не только отдельные изображения, но и целые последовательности динамических событий и сцен Отечественные и зарубежные разработчики предлагают целый спектр решений подобного рода. Однако отсутствие *терминологического единства* в этой области зачастую ставит заказчиков и интеграторов систем в сложное положение, затрудняя выбор решения, оптимального в каждом конкретном случае

По мнению специалистов, введение стандарта, устанавливающего единые термины и определения в области ситуационной видеоаналитики будет способствовать росту эффективности применения подобных систем и, в конечном счете, – повышению заинтересованности рынка в использовании технологий искусственного интеллекта.

Функциональные возможности

На рисунке ниже показаны базовые функции видеоаналитики. На основе этих базовых функций и их комбинацией, могут быть созданы разнообразные услуги и новые функции аналитики.

Улучшение изображений

В компьютерном зрении и в компьютерной графике применяются различные методы и алгоритмы восстановления и улучшения изображений, такие как шумоподавление (denoising) и устранение размытости (deblurring).

Кроме того, используются методы повышения чёткости изображений при помощи нейросетей: «супер-разрешение» SR (Super Resolution) на базе нескольких изображений объекта, а также супер-разрешение на базе единственного изображения SISR (Single Image Super Resolution).

Рис. Базовые функции видеоаналитики

Детектирование движения

Детектирование движения – процесс обнаружения изменения положения объекта относительно его окружения или изменения окружения относительно объекта. При сравнении нескольких последовательных изображений сцены, система видеоаналитики может распознать начало движения какого-либо объекта внутри сцены.

Распознавание лиц

Распознавание лиц – практическое приложение теории распознавания образов, в задачу которого входит автоматическая локализация лица на неподвижном или движущемся изображении и, в случае необходимости, идентификация личности по характерным параметрам лица. Распознавание лиц людей и определение личности человека – одна из самых употребительных функций видеоаналитики, которая используется практически во всех современных системах безопасности на базе интеллектуального видеонаблюдения.

Распознавание бесцельного поведения (Loitering)

«Бесцельное поведение», праздношатание (Loitering) – это нахождение на одном месте или в пределах одной сцены в публичном пространстве в течение продолжительного времени без определённой цели.

В ряде стран такое поведение запрещено законодательно. В любом случае, оно может косвенно свидетельствовать о противозаконных намерениях, поэтому лиц, проявляющих признаки такого поведения, бывает необходимо выявлять при видеонаблюдении. Системы видеоаналитики имеют гибко настраиваемые алгоритмы, определяющие **бесцельное** поведение субъектов.

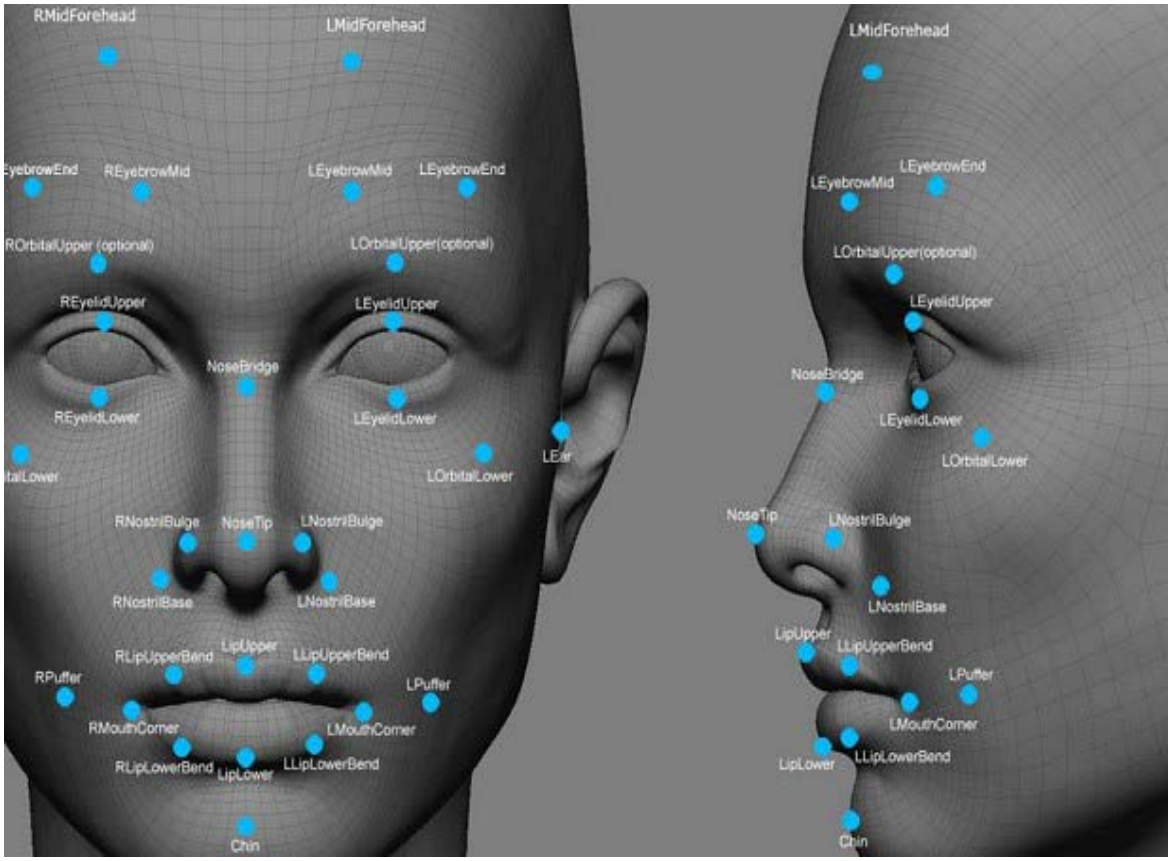


Рис. Определение личности человека по расстоянию между характерными точкам

На рисунке ниже показан пример **Распознавание бесцельного поведения** с отслеживанием перемещения субъекта (белая пунктирная линия).

Распознавание пропажи, либо оставленных без присмотра объектов

На рисунке выше также показан пример подозрительного объекта, оставленного без присмотра *(Abandoned object).*

Такие объекты в системах видеоаналитики обычно выделяются рамками с соответствующим пояснением. Это может быть признаком готовящегося теракта, поэтому на основе данных видеоаналитики необходимо как можно быстрее задержать подозрительного субъекта, оставившего предмет, и выяснить, что именно он оставил в нём.

Рис. Пример распознавания бесцельного поведения.

Аналогично может распознаваться пропажа (исчезновение) объекта, например, музейного экспоната. В этом случае система видеоаналитики немедленно выдаёт предупреждение тем или иным образом.

Закрытая зона

Примеры разграничения закрытых зон показаны на рисунке ниже. При проникновении людей в закрытую зону система выдаёт предупреждение, например выделяет нарушителя рамкой.

Детектирование проникновения

Детектирование проникновения – часть сервиса «Закрытая зона», пример показан на рисунке выше)

Распознавание автомобильных номеров

Автоматическое распознавание номерных знаков — это технология видеоаналитики, которая использует оптическое распознавание символов на изображениях для считывания регистрационных знаков транспортных средств для получения информации о местонахождении транспортных средств.

На рисунке ниже показан процесс распознавания номера автомобиля, состоящий трёх стадий: обнаружение номера (License Plate Detection), Обнаружение символов на номере (Character Detection) и распознавание символов (Character Recognition), при котором используются методы машинного обучения системы видеоаналитики.

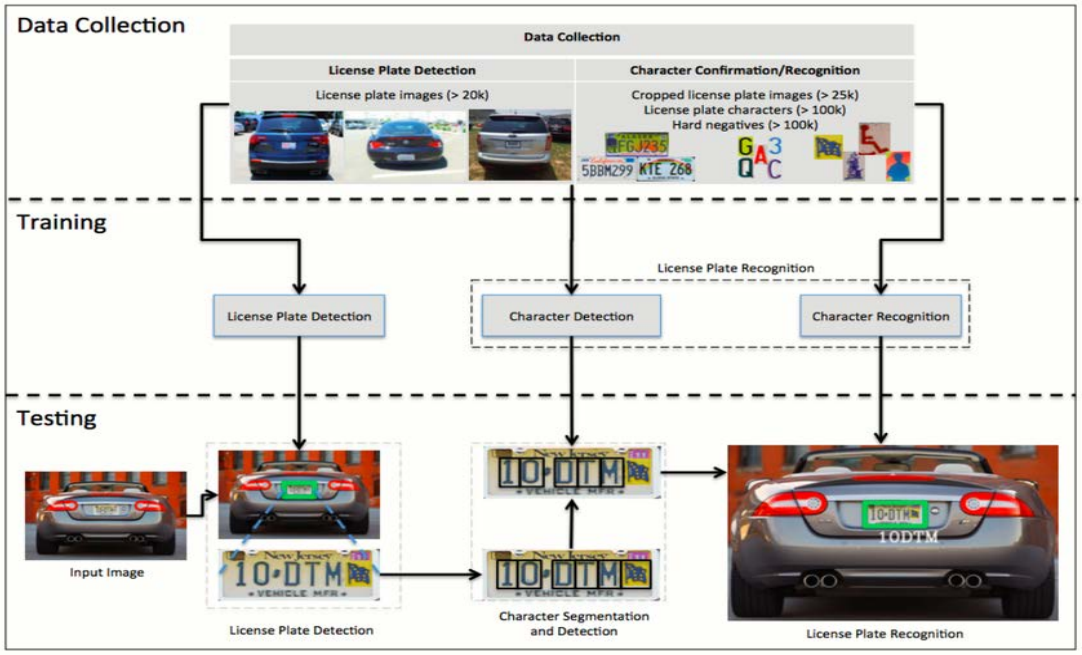


Рис. Оптическое распознавание символов на автомобильных номерах

Слежение за объектами

Слежение за объектами – вспомогательный сервис для услуги распознавания «бесцельного поведения» (Loitering), однако, он может использоваться и для иных целей. На рисунке ниже показан пример такого распознавания. Изображение посередине показывает подозрительное поведение, человека, идущего сзади. Обычно люди так («след в след») не ходят, и система видеоаналитики обучена производить распознавание такого поведения субъектов, с выдачей предупреждения о подозрительном поведении.

Интеграция функций

Многие функции видеоаналитики часто представляют собой интеграцию нескольких базовых функций. Например, аналитика парковки автомобилей может включать в себя следующие функции:

– Проникновение в закрытую зону;
– Оставление объектов без присмотра в течение определённого времени;
– Распознавание движения объектов;
– Распознавание номеров.

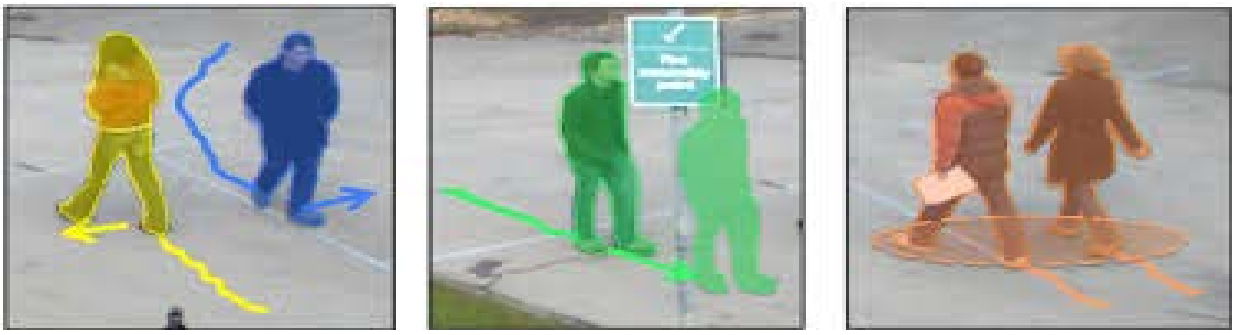


Рис. Слежение за объектами

Рис. Аналитика парковки автотранспорта

Сферы использования видеоаналитики

Рассмотрим некоторые практические применения вышеперечисленных базовых функций видеоаналитики. Заметим, что многие более сложные функции, описанные ниже, фактически являются интеграцией базовых функций.

Системы видеоаналитики - Каталог систем и проектов видеоаналитики

Системы Умного Города - одна из самых перспективных областей применения систем видеоаналитики.

Подсчёт людей и транспорта

Функция подсчёта людей, пересекающих заданную линию, предоставляет ценную информацию для принятия бизнес-решений, в таких сферах, как:

– Торговля: информация о количестве посетителей магазинов, торговых центров, а также отдельных зон магазинов и торговых центров;

– Банки: получение информации о количестве посетителей отделений;

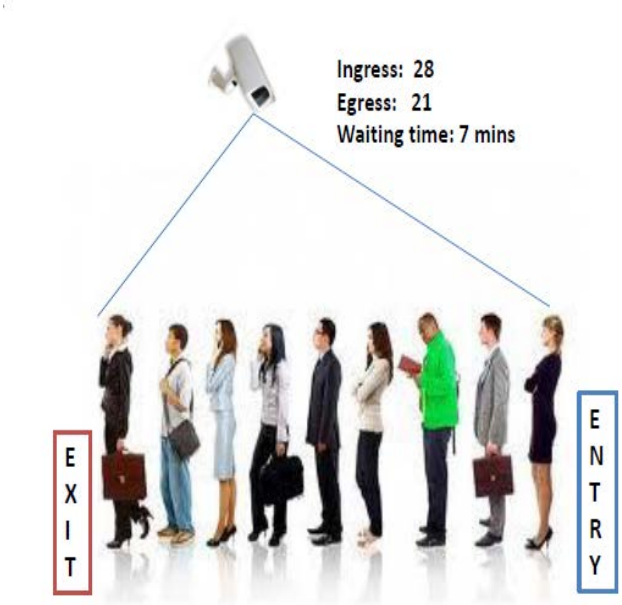
– Гостиницы и туризм: получение информации о количестве посетителей ресторанов, кинотеатров, турагентств и пр.

– Обладая этой информацией, руководство предприятия может:

– оценить общую эффективность работы компании;
– оценить эффективность проводимых маркетинговых акций;
– оценить загруженность площадей;
– улучшить сервис путём регулирования рабочих графиков персонала в соответствии с данными о посещаемости.
– Отдельно необходимо отметить выгоды использования системы подсчёта посетителей для арендодателей торговых площадей:
– оценка популярности и прогнозирование развития торгового центра;
– оценка привлекательности отдельных площадей и корректировка арендных ставок.

Системы подсчёта также могут анализировать маршруты и поведение покупателей в торговых центрах. Например, путём подсчёта покупателей в зоне наружной рекламы можно оценить её эффективность, а также можно оценивать покупательский спрос на различные виду товара.

Рис. 10. Подсчёт количества людей в очереди



Аналогично, для транспортных средств можно получить следующую ценную информацию:
– Количество машин, проезжающих по улице за определённый промежуток времени, в зависимости от времени суток, дня недели и сезона;
– Количество машин, скапливающихся у светофора и среднее время ожидания проезда перекрёстка;
– Количество машин, проезжающих через КПП в закрытую зону и выезжающих из неё;
– Заполняемость уличных парковок и её зависимость от времени;
– А также другую информацию, необходимую для планирования развития транспортной системы города.

Функционал подсчёта количества людей и транспортных средств имеет важное значение для работы автоматизированных интеллектуальных транспортных систем (ИТС), которые могут улучшить транспортную ситуацию в городе, повысить пропускную способность дорог, оптимизировать работу светофоров и пр.

По собранной информации можно рассчитать макроскопические характеристики транспортного потока, а именно такие показатели как:
– средняя скорость потока;
– объем потока (количество транспортных средств в час);
– плотность потока (количество транспортных средств на км);
– средняя занятость полосы;
– длина транспортных средств (для решения задачи классификации транспортных средств);
– длина очереди перед перекрёстком;
– детектирование выезда на встречную полосу.

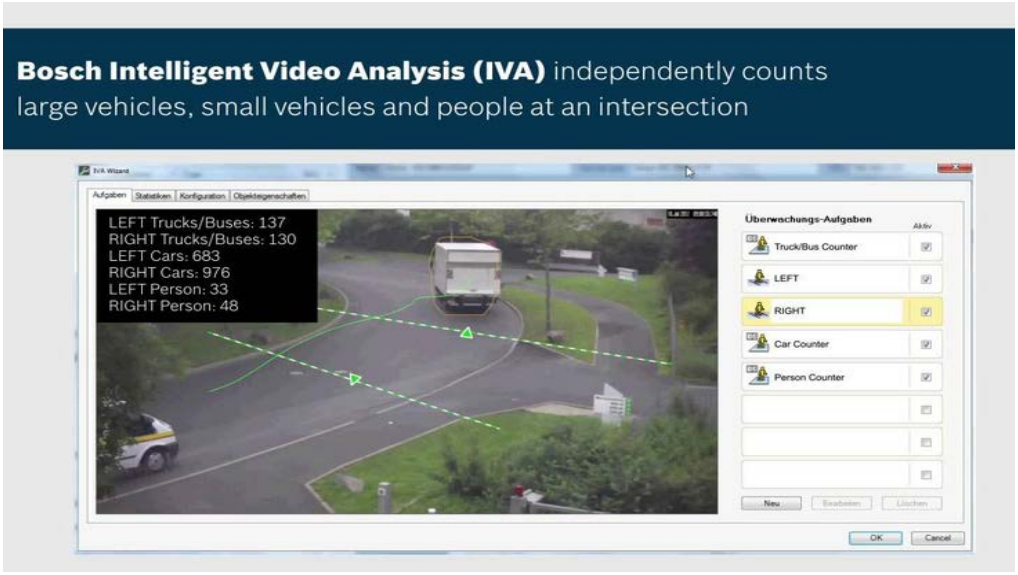


Рис. Работа системы подсчёта транспортных средств и людей на перекрёстке

Анализ видеонаблюдения ограниченной зоны и периметра

Аналитика систем видеонаблюдения для охраны закрытых зон и периметров предназначена для выявления попыток несанкционированного проникновения в закрытую зону, даже в отсутствие физического ограждения. Основные сервисы аналитики систем для охраны закрытых зон следующие:

- выявление потенциальных угроз объекту в закрытой зоне;
- определение вероятностей реализации потенциальных угроз;
- определение уязвимых зон объекта в закрытой зоне;
- обнаружение факта пересечения периметра закрытой зоны;
- информирование о наличии потенциальных угроз или фактов проникновения;
- рассылка извещений и изображений инцидента дежурному персоналу безопасности объекта, включая носимые устройства.
- Типовыми задачами видеоаналитики уязвимых зон охраняемых объектов являются:
- поиск, обнаружение и распознавание подозрительных предметов и людей;
- выявление и распознавание изменений видеоизображений определённых зон во времени.

Для наблюдения за периметром закрытой зоны используются направленные всепогодные видеокамеры, в т.ч. с функцией инфракрасного видения, с защитой от погодных воздействий (дождь, снег, наледь, туман). Для наблюдения внутри закрытой зоны чаще всего используются купольные видеокамеры типа PTZ, с возможностью поворота объектива в нужном направлении.

Рис. Пример системы видеоаналитики охраны периметра и закрытой зоны

Распознавание лиц

В настоящее время для распознавания лиц может подойти любая коммерческая камера с разрешением не менее Full-HD. Поэтому практически любой магазин, торговый центр или офис, где находятся люди, может позволить себе установить камеру для распознавания лиц, детекции очереди и других функций.

Многие камеры для домашнего видеонаблюдения содержат встроенные функции распознавания лиц, что позволяет их владельцу создавать базы данных членов семьи и друзей, которые регулярно посещают его. Систему охраны дома можно настроить на открывание двери для разрешённых лиц из базы данных, а также выдачи предупреждений, при визите неизвестных или нежелательных лиц. При этом система может учитывать множество факторов: таких как наличие или отсутствие очков, макияж, и многое другое.

В распознавании лиц могут использоваться разные технологии, но основные шаги процесса, следующие:

1. Из фото-картинки или видеозаписи извлекается изображение лица (детекция лица). Лицо может быть как одиноким, так и находится в окружении многих лиц. Поворот головы не оказывает решающего влияния на этом шаге.

2. Приложение распознавания лиц считывает геометрические параметры лица: такие как расстояние между глазами, расстояние от лба до подбородка и др. Всего могут учитываться до 100 и более подобных геометрических параметров. На основе этих данных составляется цифровая сигнатура лица (facial signature).

3. Сигнатура лица сравнивается с другими сигнатурами из базы данных известных лиц. По данным на май 2018 г. Федеральное Бюро Расследований США (FBI) имеет доступ к 412 миллионам изображений лиц. Изображения лиц по крайней мере 117 млн. американцев имеются в различных базах данных полиции США.

4. Определение личности человека с достаточно высокой точностью, превышающей 90%.

Некоторые аэропорты США (Нью-Йорк, Атланта, Миннеаполис, Солт-Лейк Сити и др.) используют функцию распознавания лиц при регистрации на рейс вместо посадочного талона (с согласия пассажира).

В маркетинге и рекламных кампаниях используется т.н. анонимное (без установления личности) распознавание лиц, поскольку для маркетинговых мероприятий очень полезной бывает информация о том, сколько времени человек смотрит на ту или иную рекламу и какое при это эмоции выражает его лицо. При этом могут использоваться следующие метрики:

- Заметность (сколько людей обратили внимание на рекламу);
- Демография (возраст и пол обративших внимание);
- Время просмотра (сколько в среднем времени смотрят на рекламу);
- Время дня (в какие часы больше всего внимания обращают на рекламу)

При этом значительно сокращаются затраты и время изучения и анализа данных по сравнению с ручными методами.

Существует много практических применений распознавания лиц при помощи видеоаналитики, ниже перечислены некоторые из них:

- **Безопасность в аэропортах.** Департамент внутренней безопасности США (The Department of Homeland Security) использует видео-аналитику для распознавания лиц людей, входящих и выходящих из зданий аэропортов, чтобы определять тех, людей с просроченной визой или находящихся в розыске или под расследованием.
- **Распознавание лиц для доступа к мобильным устройствам.** Компания Apple впервые использовала распознавание лиц для разблокировки смартфонов iPhone X (Face ID). По заявлению Apple, шансы неверной разблокировки составляют один на миллион,

однако, СМИ сообщали о случаях разблокировки смартфонов родителей их детьми в Китае.

– **Контроль на экзаменах в учебных заведениях.** Это является эффективным средством против попыток сдачи экзаменов подставными лицами вместо неуспевающих студентов.

– **Социальные веб-медиа.** Facebook использует алгоритм для нахождения лиц при загрузке фото на платформу, при этом выдаётся запрос, хотите ли вы отметить друзей на фото. При утвердительном ответе на вопрос, создаётся линк на страницы отмеченных друзей. Точность распознавания лиц на Facebook составляет 98%.

– **Контроль на входе организаций.** Некоторые компании заменяют сканеры служебных бейджиков на устройства распознавания лиц.

– **Религиозные сообщества**. В церквях используется распознавание лиц для контроля тех, кто регулярно ходит на службы, чтобы отслеживать активность верующих, а также вносящих пожертвования.

– **Розничные продавцы в торговых центрах.** Видеоаналитика может использоваться для распознавания подозрительных лиц, чтобы выявлять потенциальных воров.

– Индустриальное применение
– Производство
– На производстве видеоаналитика используется для следующих основных целей:
– Контроль качества продукции;
– Помощь в управлении технологическими процессами;
– Обеспечение безопасности работающих;
– Предотвращение хищений или других злонамеренных действий.

Уже несколько десятков лет видеоаналитика («машинное зрение», «техническое зрение») используется в производственных процессах для обнаружения дефектов, загрязнений, и других отклонений в производимых изделиях. На рисунке ниже показана простейшая система видеоаналитики для сортировки изделий на конвейерной ленте.

Рис. 14. Производственная линия с машинным зрением

ПРИМЕР ИСПОЛЬЗОВАНИЯ ВИДЕОАНАЛИТИКИ

Сервер системы видеоаналитики воспринимает сигналы предупреждения от программы видеоаналитики, которая работает со множеством видеокамер, установленных на территории предприятия химического производства. Возможные действия реакции на предупреждающие сигналы:

- Управление камерами (движение, запись и пр.);
- Предоставление новой видео- и аудиоинформации для операторов и персонала предприятия, например, изменение точки обзора, включение дополнительных микрофонов;
- Команды для других подключённых устройств или программ через протокол HTTP

- Команды через интерфейс пользователя (Windows) для запуска и настройки других устройств или ПО;
- Запуск SNMP-ловушек (SNMP traps) для индикации состояние ПО мониторинга под управлением протокола SNMP;
- Журналирование (Logging) предупреждающих сообщений и сохранение их в базах данных для последующего анализа.

Использование видео для анализа событий на сложных производственных площадках часто означает многие часы напряженной работы по просмотру и классификации событий на видеозаписях с многих сотен камер. Тем не менее, при этом нет полной гарантии, что проблема будет правильно идентифицирована.

Применение IP-видеокамер с хорошей разрешающей способностью, инфракрасным видением и защитой от погодных условия, работающих вкупе с платформой видеоаналитики, даёт возможность адекватного анализа событий и реакции на них в реальном масштабе времени.

Качественное и эффективное видеонаблюдении позволяют значительно повысить эффективность видеонаблюдения. Особенности использования решений видеонаблюдения и аналитики:

- необходимость адаптации к суровым условиям окружающей среды;
- высокая стоимость обслуживания энергетических объектов;
- совместимость с окружающей средой и другими оборудованиями;

Обеспечение безопасности

Видеонаблюдение – основное средство предотвращения и расследование случаев воровства, несанкционированного проникновения, вандализма, терроризма и других нежелательных действий.

Важной частью системы видеоаналитики является способность проактивно извещать сотрудников правоохранительной системы ***о вторжениях на*** территорию, для быстрого реагирования, и предотвращения преступлений и возникновения ущерба. Видеозаписи произошедших инцидентов также помогают при расследовании преступлений.

В транспортно-логистической отрасли и на дорогах наибольшее применение получили следующие функции видеоаналитики:

Рис. Основные функции видеоаналитики

Распознавание номеров автотранспорта

Основные функции:

– Добавление номеров в черные и белые списки;

– Быстрая регистрация и пропуск автотранспорта, с записью эпизода проезда через ворота и по территории и фиксацией времени;

– Загрузка данных в формате XLS или CSV.
– Преимущества:
– Предотвращение проезда неавторизованных транспортных средств;
– Автоматический подъём шлагбаума при въезде и выезде.

Поиск и отслеживание подозрительных лиц

При выборе подозрительного персонажа на записи с камеры, платформа видеоаналитики может выполнить следующие действия:

– Сделать стоп-кадр и создать видеоклип с изображениями похожих людей на записях с других камер в хронологическом порядке;
– Построить траекторию движения объекта на плане помещения.
– Возможен поиск объектов в видеоархиве с использованием загруженных изображений в соответствии со следующими параметрами:
– Форма; Цвет; Размер;
– Положение в кадре.

Используя функцию поиска подозрительных лиц (Suspect Search) можно реконструировать маршрут объекта в течение минуты. Это позволяет быстро найти подозреваемого и задержать нарушителя.

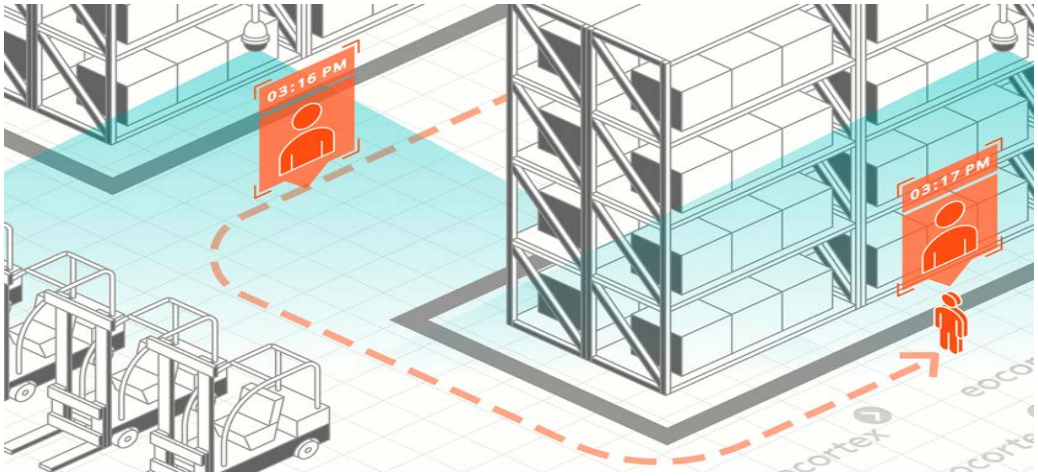


Рис. Поиск и отслеживание подозрительных лиц Suspect Search.

Управление камерами PTZ

Основные функции:

– Поворот камер PTZ в желаемом направлении при помощи джойстика или клавиатуры;
– Масштабирование изображения при помощи оптического зума;
– Управление фокусировкой камеры в автоматическом или ручном режимах;
– Задание сценария автоматической работы камер PTZ.
– Преимущества:
– Возможность замены нескольких стационарных камер одной камерой PTZ с расширением возможностей обзора;
– Регистрация мельчайших деталей на изображении;
– Фокусировка камеры на желаемом объекте и слежение за ним.

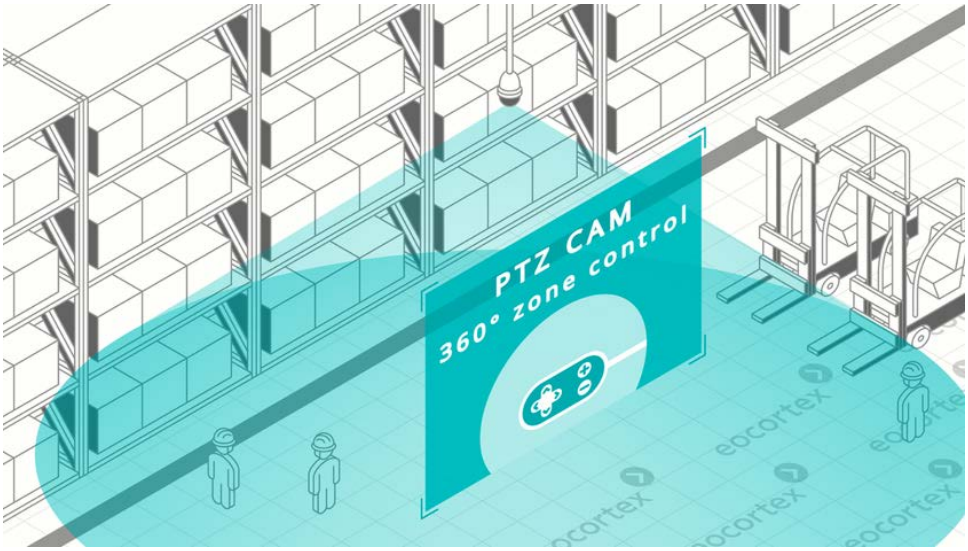


Рис. Управление камерой PTZ

Трекинг объектов

Основные функции:

– Установка минимального размера объекта, перемещения которого должны быть отслежены;

– Получение немедленного извещения тревоги на монитор, телефон или электронную почту;

– Пересечение объектом заданной линии (вторжение на территорию и пр.);

– Перемещение объекта по заданной зоне;

– Долгое нахождение объекта на одном месте (Loitering).

– Преимущества:

– От персонала не требуется внимания на мониторах 24 часа в сутки;

– Охрана собственности, грузов и инфраструктуры логистического центра;

– Обеспечение безопасности логистического центра и его персонала;

– Предотвращение возможных террористических атак.

Рис. Трекинг объектов

Распознавание саботажа

Функция позволяет предотвратить следующие виды саботажа:

– Расфокусировка видеокамеры;

– Поворот камеры в сторону от установленного для неё направления съёмки;

– Длительное ослепление камеры;
– Перегораживание вида камеры.

Функция обеспечивает выдачу немедленного извещения ALARM о всех перечисленных действиях на монитор, телефон или электронную почту.

Рис. Распознавание саботажа

Развёртывание изображения с панорамной камеры типа «рыбий глаз»

Возможно получение «плоского» изображения с панорамной камеры типа «рыбий глаз», которая обычно сильно искажает перспективу изображения. При этом становится возможным заменить несколько обычных камер на одну панорамную с более широким функционалом, и контролировать несколько зон при помощи одной камеры.

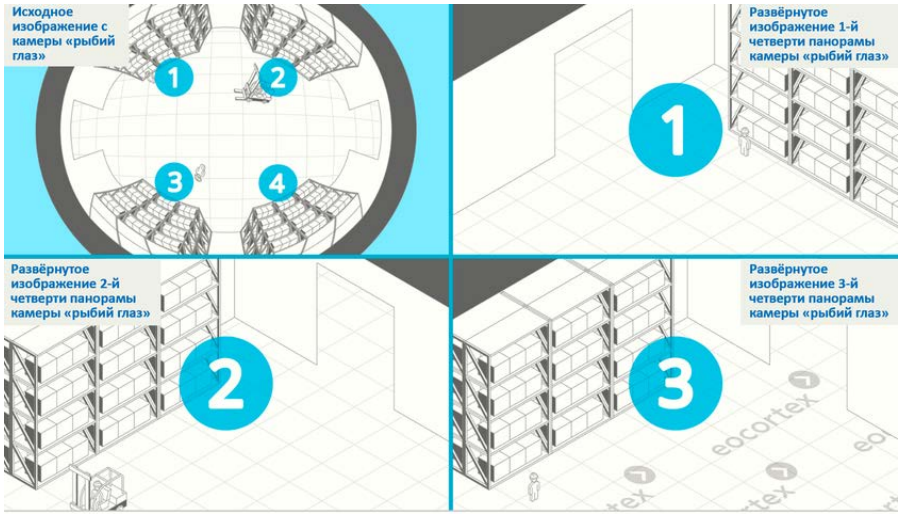


Рис Развёртывание изображения с панорамной камеры типа «рыбий глаз»

Видеоаналитика в банках используется прежде всего для подсчета посетителей, выдачи талонов раннее распознанным клиентам, идентификации новых клиентов, а так же для:

– обеспечения безопасности в операционном зале и переговорных комнатах
– обеспечения безопасности в зонах самообслуживания и банкоматах
– обеспечения безопасности в рабочей зоне банковских служащих и клерков
– предотвращения проникновения на территорию банка грабителей и злоумышленников
– оповещения сотрудников службы безопасности о появлении мошенников из «чѐрного списка» и других нежелательных личностей

- предотвращения терактов (обнаружение оставленных бесхозных предметов)
- предотвращения появления и скапливания различных маргинальных личностей в зонах самообслуживания
- предотвращения актов вандализма, ведущих к повреждению банкоматов

Рис Преимущества для торговых предприятий при использовании видеоаналитики

В современных системах видеоаналитики могут использоваться интеллектуальные камеры со встроенной обработкой видео или специальные аналитические программные платформы, работающие на удалённом сервере.

В таких платформах всё чаще используются алгоритмы *машинного обучения*, чтобы облегчить интерпретацию и анализ данных во всё более увеличивающихся объёмах потоков видео-контента.

Использование нейросетей и глубокого обучения

Использование высокоточных нейросетей в видеоаналитике позволило значительно расширить функционал систем безопасности предприятий.

Нейросети получили широкую известность с 2012 года. С этого времени всё больше компаний, как известных, так и начинающих, стали широко использовать технологию нейросетей для точного и достоверного распознавания изображений.

Нейросети используют такие Интернет-компании, как Microsoft, Facebook, Google, Amazon, Instagram, Яндекс и другие, например:

- Яндекс предоставляет функцию распознавания марки автомобиля для портала Auto.ru;
- Приложение CaptionBot компании Microsoft автоматически предлагает подпись для изображения;
- Приложение WhatDog распознаёт породы собак.

Для этих целей в настоящее время используются нейросети с глубоким обучением DNN (Deep Neural Network), или просто глубокие нейросети.

Глубокие нейросети используются для создания систем, которые могут распознавать объекты и их свойства из объёмных массивов неразмеченных данных. В последнее время для целей глубокого обучения нейросетей все большее применение находят графические процессоры GPU, которые позволяют обучить огромные массивы данных за относительно короткое время.

Модели на основе DNN используются для распознавания образов «на лету», в тех случаях, где скорость распознавания очень важна для того, чтобы оперативно выполнить какие-то действия. Однако, время обучения может занять большое время. Поэтому, стандартные DNN не всегда удовлетворяют требованиям задержки для некоторых приложений реального времени. Хорошо «обученные» DNN могут иметь высокую точность распознавания образов, что очень важно для развития видеонаблюдения.

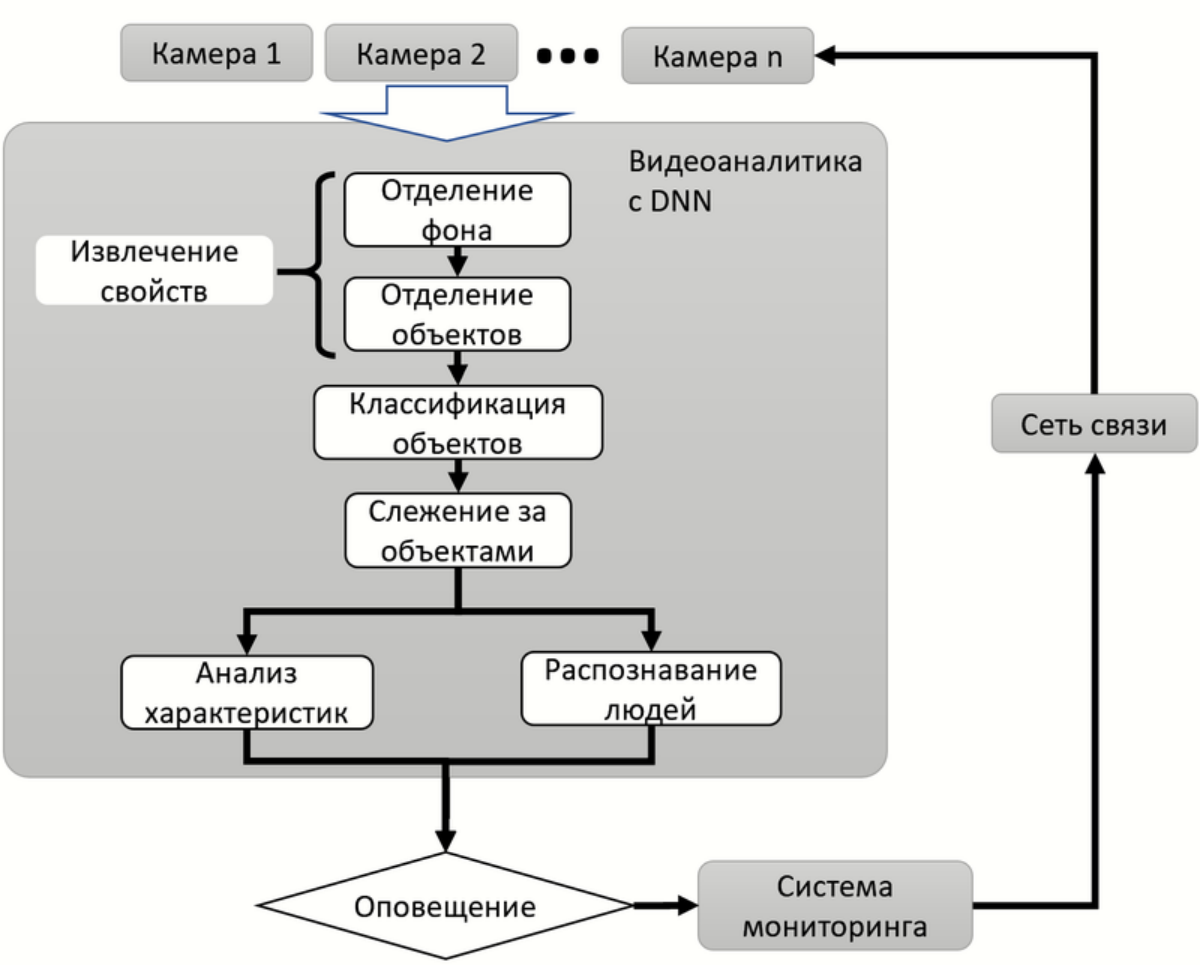


Рис. Структура системы видеоаналитики с нейросетью DNN

Некоторое число камер следят за определённой областью с целью отслеживания траекторий движения людей и объектов. *Нейросеть DNN предварительно обучена распознаванию объектов, определению направления и скорости их движения*.

На основании этой информации осуществляется анализ характеристик объекта (*например, тип и марка транспортного средства, распознавание лиц людей и пр.*).

Это может быть сложной задачей, особенно в условиях ограниченности наличных вычислительных ресурсов. Технология очистки данных на основе взаимоотношений RelDC (Relationship-Based Data Cleaning) может повысить качество распознавания, даже в условиях видео не очень высокого качества.

Обычные нейросети состоят из взаимосоединённых вычислительных узлов, называемых нейронами, каждый из который активирует узлы соседнего слоя с установленным весом (величиной) сигнала. Активация начинается на входных нейронах, и затем внутренние «слои» нейронов активируются под воздействием присоединённых к ним нейронов в соответствии с коэффициентами передачи сигнала. Обычные нейросети работают с использованием простого механизма распространения сигнала со входа на выход и имеют не больше 2-3 внутренних слоёв нейронов.

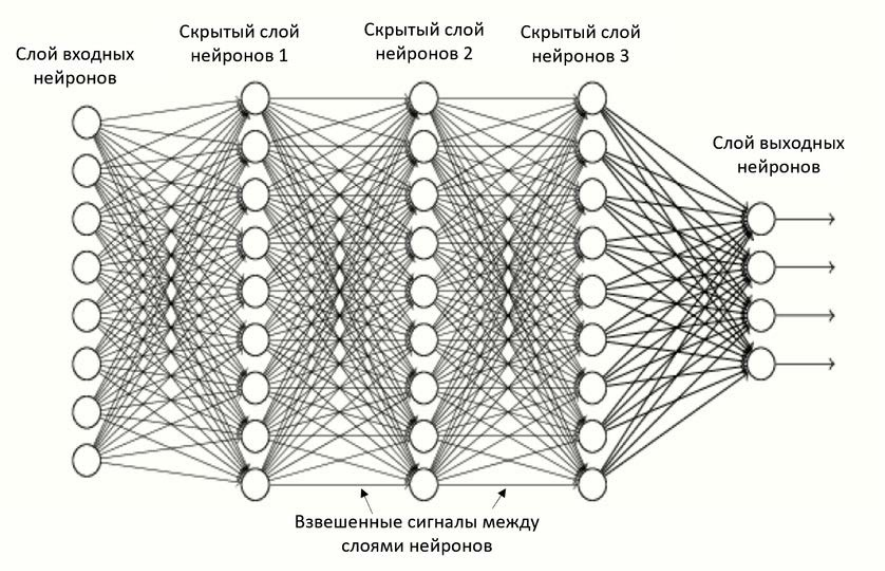


Рис. Структура нейросети

В зависимости от числа скрытых слоёв нейронов для обучения, нейросети классифицируются как «мелкие» (shallow) и «глубокие» (deep), DNN.

Мелкие нейросети обычно содержат 1-3 скрытых слоя, в то время как число слоёв в глубоких сетях DNN – от трёх и более. Увеличение числа слоёв повышает эффективность обучения нейросети и точность распознавания образов.

DNN могут иметь различную сетевую архитектуру, «модель» (model), которая также существенно влияет на процесс обучения.

Рис. Пример модели свёрточной интеллектуальной нейронной сети СИНС

Глубокое обучение DL (Deep Learning), как разновидность машинного обучения ML (Machine Learning), использует различные алгоритмы для обработки данных и имитации процесса мышления, чтобы делать различные умозаключения, заключающиеся в распознавании объектов и их поведения.

При этом становится возможным распознавать рукописный текст (даже в том случае, если DNN никогда раньше не «видела» почерк данного человека), понимать живую речь (без необходимости предварительной биометрии голоса), и распознавать различные объекты, например, класс «животные», а внутри него – подклассы: «собака», «кошка», «корова» и пр.

Информация в DNN передаётся и обрабатывается последовательно со слоя на слой, когда выходной сигнал после обработки в нейроне предыдущего слоя служит входным сигналом для всех, либо части нейронов последующего слоя, причем сила величина

(амплитуда) сигнала определяется «весом» данного линка от нейрона предыдущего слоя к нейрону следующего слоя.

В зависимости от получаемого результата на выходе слоя выходных нейронов, может производиться последовательная коррекция весов отдельных линков между нейронами соседних слоёв. Этот итерационный процесс коррекции весов линков называется «обучением» (Learning) нейросети.

ИНТЕЛЛЕКТУАЛЬНОЕ ВИДЕОНАБЛЮДЕНИЕ В «УМНОМ ГОРОДЕ»: КОНТРОЛЬ И ЗАЩИТА ВИЗУАЛЬНЫХ ПЕРСОНАЛЬНЫХ ДАННЫХ

В настоящее время одной из передовых является технология «умного города», которая получила развитие во многих странах мира. «Умный город» призван в первую очередь повысить качество жизни граждан, сделать проживание в городе безопасным и комфортным. Для обеспечения реализации данных критериев используется видеонаблюдение, позволяющее осуществлять мониторинг общественной, экологической безопасности на определенной местности с оперативным реагированием. Главным элементом «умного города» является автоматизированная система, основанная на анализе потоков данных от различных источников информации, которая позволяет производить обработку полученных сведений в реальном времени, осуществлять многофакторный анализ и инициировать оперативное реагирование как в режиме поддержки принятия решений с участием человека, так и в полностью автоматическом режиме.

Системы интеллектуального видеонаблюдения являются неотъемлемой частью «умных городов», что обусловлено широким кругом решаемых ими задач. Видеоаналитика включает в себя обнаружение и распознавание людей, сопровождение их перемещения на видео, повторную идентификацию (реидентификацию) людей в мультикамерных системах видеонаблюдения, определение нехарактерного поведения людей. В динамично развивающемся мире должен соблюдаться баланс интересов человека и государства.

С технической точки зрения должна быть обеспечена безопасность и непрерывность функционирования таких систем.

С правовой стороны: человек должен иметь возможность защищать свое право на неприкосновенность частной жизни. Следует учитывать интересы всех сторон и предложить сбалансированные решения, содействующие распространению новых технологий и обеспечивающие их надежность и безопасность.

Необходимо создать республиканскую систему мониторинга общественной безопасности» (далее – РСМОБ) которая по единым техническим стандартам, будет повышать уровень общественной безопасности Система должна объединяет на одной платформе локальные системы видеонаблюдения, специальные детекторы, каналы связи, центр обработки данных, а также иные системы и информационные ресурсы. При этом обработка и хранение информации в системе мониторинга должна осуществляться посредством программной платформы и аппаратного комплекса республиканского центра обработки данных.

При практической реализации алгоритмов обработки видео

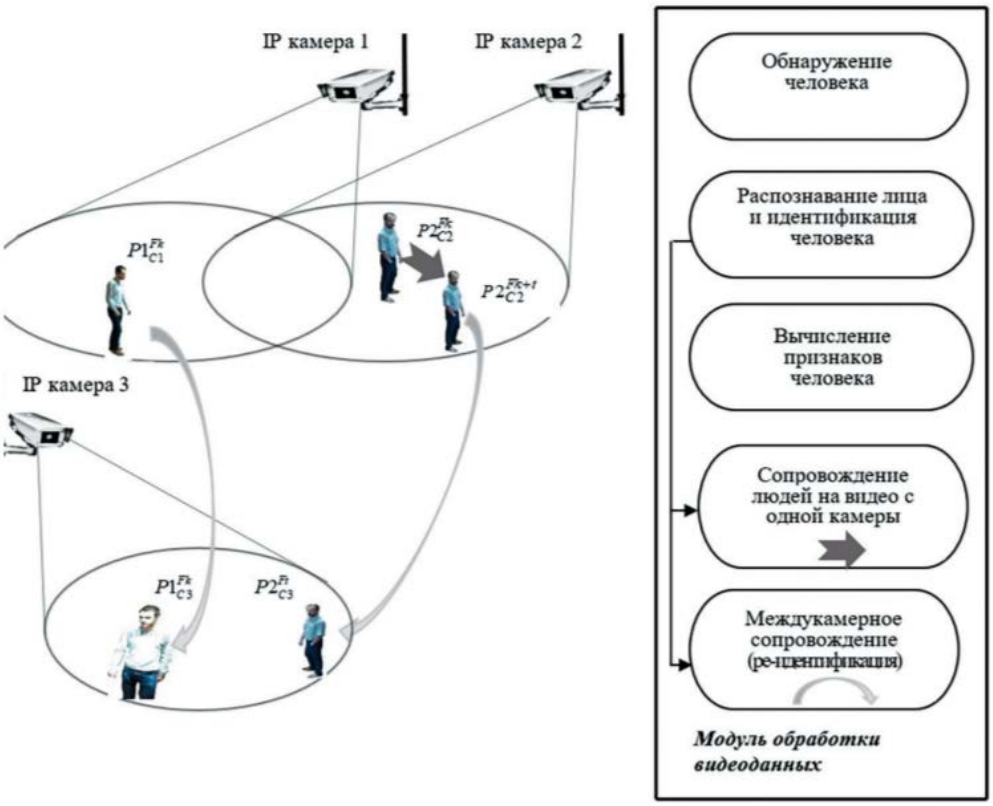
– на первом шаге должно выполнятся обнаружение объектов и их локализация или же детектирование областей-кандидатов, которые могут быть отнесены к объектам интереса

– следующий этап требует вычисления признаков выделенных фрагментов (лица), на основе которых выполняется анализ и конечная их классификация.

Технология видеонаблюдения с функциями обнаружения, идентификации, отслеживания и реидентификации людей

Система видеонаблюдения должна состоять из территориально разнесенных IP-камер и организована на основе единого центра обработки данных.

На рисунке показана упрощенная структура пространственно распределенной видеосистемы с функциями обнаружения и отслеживания людей для трех IP-камер.



На каждом кадре P k - – номер видеокамеры.

С помощью детектора выполняются обнаружение всех людей, попадающих в поле зрения камер, формирование ограничительных рамок, которые описывают прямоугольником обнаруженные фигуры для них. Эти изображения людей размещаются в галерее, и для каждого из них с помощью ***сверточных нейронных сетей (далее – СНС)*** определяются векторы СНС-признаков (СНС-дескрипторы), формирующие общее пространство СНС-признаков, которое представляется в виде таблицы, где каждая строка является СНС-дескриптором для одного изображения. В каждой обнаруженной области выполняется поиск лица человека и распознавание по признакам лиц

В системах видеонаблюдения для обнаружения и контроля передвижения людей можно выделить следующие основные задачи:

– обнаружение человека на видео;

– распознавание человека по лицу;

– сопровождение передвижения человека на видео, полученного с одной камеры;

– идентификация человека с определением всех его персональных данных;

– повторная идентификация людей, изображения которых получены с разных камер или с одной, но в различное время.

Первой задачей, которую необходимо решить, является обнаружение людей на изображении или видео.

Основные методы, которые могут использоваться для обнаружения движущихся людей

– межкадровой разности (frame difference);
– вычитания фона (background subtraction)
– на основе анализа оптического потока (optical flow).

После того как человек обнаружен и выделен на изображении, необходимо выделить и распознать его лицо. Разработано и используется много алгоритмов для выделения лица человека на изображении (face detection).

Распознавание лица человека по цифровому изображению – одна из ключевых задач идентификации человека. Схожей задачей является поиск местоположения человека в пространстве по его цифровой фотографии, а также его сопровождение по набору признаков, который включает, кроме признаков лица, общие признаки человека, позволяющие отследить его движение даже при невозможности распознавания лица, например, когда оно скрыто капюшоном или расположено относительно видеокамеры под значительным углом, который не позволяет выполнить идентификацию по лицу.

Далее следует поиск лиц в сопровождаемых областях. Выделение области поиска лица выполняется на основе анализа размеров детектированного фрагмента. Если его ширина меньше его высоты более чем в три раза, то анализируется только верхняя часть этого фрагмента, иначе анализируется вся область, описывающая человека.

Для обнаружения областей, содержащих лица, применяется мультизадачная трехкаскадная СНС MTCNN. Признаки лица используются для установления соответствия людей на кадрах. Это позволяет повысить эффективность сопровождения при анализе траекторий движения людей, долговременного скрытия их за объектами фона, высокой схожести внешних признаков людей. Полученная на предыдущем шаге область кадра, содержащая лицо, поступает для распознавания. Для этого этапа применяется может применятся СНС MobileFaceNet, которая характеризуется значительно меньшими вычислительными затратами и обеспечивает при этом высокую точность работы (например, на базе данных LFW точность составляет 99,5%, а для СНС LResNet100E-IR – 99,77%).

Сопровождение людей (одного или нескольких человек) – одна из наиболее актуальных задач для систем видеоаналитики, однако в настоящее время она не решена в полной мере.

На сегодняшний день наиболее результативным является сопровождение через обнаружение. Широкое развитие и применение для обнаружения объектов получили алгоритмы классификации с применением СНС, которые устойчивы к изменениям освещенности, динамическому заднему фону и позволяют осуществлять детектирование даже в случае частичных перекрытий, что повышает качество сопровождения.

Если лицо не распознано с использованием базы данных, то должно выполнятся сравнение признаков обнаруженного лица с соответствующими данными составного дескриптора.

Составной дескриптор изображения каждого человека включает признаки лиц, вычисленные на основе СНС, и комплекс признаков изображения человека, что позволяет сопровождать людей даже при дальнейшей невозможности идентификации лиц.

рисунок . Примеры сопровождения множества людей вне помещения

В случаях невозможности обнаружения или распознавания лиц сопровождение выполняется на основе алгоритма, включающего: оценку наличия всей фигуры человека; формирование CHC-признаков для всей области и для верхней ее части и их накопление; формирование пространственных признаков и фильтрацию по:

- расстоянию и размерам;
- вычисление схожести между всеми сопровождаемыми и обнаруженными на текущем кадре людьми и установление соответствия между ними;
- индексацию людей; определение их видимости на кадре;
- выделение рамкой человека при его присутствии в кадре.

Данная методика дает возможность идентифицировать человека по лицу и затем сопровождать его передвижение при сложной траектории движения.

После того как лицо человека распознано, наступает этап полной идентификации человека с установлением всех его персональных данных. Это выполняется посредством поиска лица по базам данных, имеющим изображения лиц, например, «Образ +++».

Биометрические персональные данные

Использование технологий видеоаналитики предоставляют большие возможности для обеспечения общественной безопасности.

Риски

Могут возникнуть риски и угрозы как для человека в частности, так и для общества в целом. Распознавание человека по лицу можно использовать не только как инструмент для идентификации людей и отслеживания местоположения, но и для получения информации об их социальной активности (с кем и где они проводят время).

Полиция города Чжэнчжоу, использует очки с системой распознания лиц, выдающие имя и адрес человека за 2-3 минуты]. При этом если у человека есть профиль в социальных сетях (база его снимков разного возраста), то точность распознавания повышается.

Проведя анализ использования видеоаналитики в разных странах, можно прийти к выводу, что применять данные технологии пытаются все без исключения, однако многие страны, в частности страны Европейского союза, соотносят использование видеонаблюдения со встроенной видеоаналитикой с единым актом в сфере защиты персональных данных General Data Protection Regulation.

Следует отметить, что единого подхода к регулированию использования систем видеоаналитики и распознавания лиц в этих странах не выработано.

В некоторых городах США существует запрет применения технологии распознавания лиц при видеонаблюдении. Однако в КНР практикуется широкомасштабное использование как видеонаблюдения, так и технологии распознавания

лиц с полной идентификацией и даже с правовыми последствиями (штраф, социальный рейтинг и др.).

Мировой опыт внедрения и распространения технологий интеллектуального видеоаналитики для обеспечения общественной безопасности «умного города» свидетельствует о неоднозначном отношении к нему общества. Применение систем действительно приводит к положительной динамике сокращения преступности, предотвращению крупных аварий и т. д., однако не каждое общество отдельно взятой страны готово к тотальному контролю со стороны государства и небезосновательно видит в этом посягательство на тайну частной жизни.

Вместе с тем, все большее распространение получает **добровольное согласие на так называемое «отслеживание»** путем использования различных приложений, определяющих и использующих геолокацию .

Закон «О защите персональных данных» (далее – Закон), должен внести определенную ясность в данную сферу. В Законе даются следующее определения:

- «Биометрические данные» – персональные данные, которые характеризуют физиологические и биологические особенности субъекта персональных данных, на основе которых можно установить его личность;
- «Персональные данные» – сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и (или) ином материальном носителе.
- Однако отсутствует понятие «Идентификация физического лица»

«Идентификация физического лица» – это когда физическое лицо может быть прямо или косвенно определено, например, через фамилию, собственное имя, отчество, дату рождения, идентификационный номер либо через один или несколько признаков, характерных для его физической, психологической, умственной, экономической, культурной или социальной идентичности.

Преимущество определении заключается в том, что они четко описывает основные признаки персональных данных и позволяет относить к таким данным информацию, косвенно идентифицирующую субъектов персональных данных.

Законом, в частности, определяются биометрические персональные данные – информация, характеризующая физиологические и биологические особенности человека, которая используется для его уникальной идентификации (отпечатки пальцев рук, ладоней, радужная оболочка глаза, характеристики лица и его изображение, голос и другое).

Таким образом, биометрических и физиологических данных большое количество, причем далеко не все активно используются с точки зрения сбора и последующей обработки. Во многих странах осуществляется сбор биометрических данных, таких как распознавание голоса и лица. Применение данных технологий возможно и в рамках электронного правительства при получении электронных услуг.

К примеру, в России принят Федеральный закон **«Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных…»,** который регулирует отношения, возникающие при осуществлении идентификации с использованием биометрических персональных данных, что подчеркивает внимание к данной проблеме со стороны государства.

В рамках данного исследования полагаем возможным выделить изображение (фотографию или видеосъемку) человека как визуальные персональные данные, как подвид биометрических персональных данных, так как именно эти данные используются как государством, так и бизнесом. Сбор, обработка, хранение и даже передача этих данных, в том числе трансграничная, осуществляются повсеместно, начиная со

сканирования и распознавания лица при использовании смартфона до полной идентификации человека на улице камерами видеонаблюдения.

Визуальные персональные данные становятся таковыми только после идентификации личности человека. Результаты видеосъемки в общественных местах или на охраняемой территории до установления личности не считаются биометрией. Только после распознавания и идентификации личности человека они становятся визуальными персональными данными.

Следует отметить, что использование систем видеонаблюдения возможно и без идентификации человека, в целом это касается общего мониторинга ситуации в городе. В случае выявления определенных отклонений от нормы (скопление людей, девиантное поведение, совершение противоправных действий) применяется технология распознавания лиц.

Контроль и защита визуальных персональных данных

Контроль и защита должна осуществляться со стороны оператора персональных данных

Изображение лица человека, распознанное системами видеоаналитики, может храниться в различных базах данных. При утечке сведений из таких баз в Интернет они становятся доступными для всеобщего пользования. Люди должны быть уверены, что их визуальные персональные данные не будут использованы в противоправных целях.

Персональные данные человека должны быть **защищены.** Такая защита включает целую группу мер:

– меры программного-технического характера (криптографическая защита, регламентация права на доступ и др.).

– меры организационно-правового характера: принятие нормативно-правовых актов, определяющих политику оператора в отношении обработки персональных данных, и ознакомление с ними сотрудников оператора,

– определение порядка доступа, внесение изменений в должностные обязанности лиц, обрабатывающих персональные данные, обучение сотрудников, назначение структурного подразделения или лица, ответственного за осуществление внутреннего контроля за обработкой персональных данных,

– введение режима и охраны помещений, эффективного делопроизводства по электронным документам].

Обнародовать изображение гражданина – значит впервые сделать изображение доступным для всеобщего сведения (опубликование, публичный показ, размещение в Интернете или любой другой способ). Однако обнародование изображения (в том числе размещение его самим гражданином в Интернете) и его общедоступность не дают иным лицам права его свободно использовать без получения согласия изображенного лица.

Отдельной проблемой является использование баз изображений лиц и людей для обучения нейронных сетей. При использовании существующих наборов данных, имеющихся в Интернете, для обучения СНС приходится сталкиваться с проблемой защиты персональных данных, и некоторые наборы данных являются закрытыми, так как авторы предоставляют для исследований не изображения, а только извлеченные из изображений людей признаки.

Некоторые наборы данных можно использовать с ограничениями, потому что при публикации исследований оператор просит соблюдать конфиденциальность студентов, изображения которых использовались для создания, при этом распространение этих наборов данных возможно только при согласовании с авторами. Некоторые наборы данных могут быть отозваны. Например, система DukeMTMC-ReID была отозвана и его использование не рекомендуется из-за нарушений гражданских прав, прав людей и частной жизни студентов университета Duke, изображения которых использовались при

формировании набора данных. Если базу данных, содержащую фото людей, планируется кому-то передать и использовать, то необходимо, чтобы оператор выставил, а принимающая сторона подписала и соблюдала следующие условия:

• база данных не будет публиковаться, копироваться или распространяться каким-либо образом или в какой-либо форме, независимо от того, был изменен набор данных или нет;

• вся база данных будет использоваться только в целях научных исследований;

• изображения из базы данных не могут быть опубликованы или показаны в какой-либо форме для публикации, документа или демонстрации.

Для возможности использования изображений людей в исследовательских целях при формировании базы данных, содержащей их фото, у всех участников необходимо получать разрешения на включение фото в базу. И такое разрешение должно быть в ***письменном виде***. Чтобы запросить и получить базу изображений для исследований, необходимо отправить подписанное соглашение держателям базы.

Контроль со стороны гражданина С точки зрения гражданина важным является вопрос сбора, использования и дальнейшего распространения видео с его участием. Открытым остается вопрос присутствия человека в различных базах данных и **возможности от этого отказаться.**

Согласие субъекта персональных данных на обработку персональных данных, за исключением специальных персональных данных, не требуется: для целей ведения административного и (или) уголовного процесса, осуществления оперативно-розыскной деятельности; для исполнения правосудия, судебных постановлений и иных документов; в целях осуществления контроля (надзора) в соответствии с законодательными актами; для защиты жизни, здоровья или иных жизненно важных интересов субъекта персональных данных или иных лиц, если получение согласия субъекта персональных данных невозможно.

Основное требование законодателя к допустимости видеозаписи и фотосъемки заключается в том, что обе стороны должны быть осведомлены о ее проведении. Однако гражданин не знает, каким образом будет использована видеосъемка в последующем и будет ли произведена идентификация личностей. Использование и интегрирование такой информации, в базы данных будут признаваться *нарушением прав и свобод граждан*.

В рамках Закона о национальной безопасности Республики Казахстан, от 6 января 2012 года № 527-IV., информационная безопасность определена как – состояние защищенности информационного пространства Республики Казахстан, а также прав и интересов человека и гражданина, общества и государства в информационной сфере от реальных и потенциальных угроз, при котором обеспечивается устойчивое развитие и информационная независимость страны;. Таким образом, информационная безопасность личности является составной частью информационной безопасности.

В связи этим необходимо соблюдать баланс интересов государства с точки зрения обеспечения общественной безопасности с использованием видеонаблюдения и последующей видеоаналитики и интересов человека, так как затрагиваются вопросы неприкосновенности частной жизни и персональных данных.

В соответствии с Законом любой человек вправе ***отозвать согласие***, а оператор обязан прекратить обработку и удалить информацию. Но данное право может быть реализовано только если этому ***предшествовало само согласие***.

Человек может требовать удаления своих данных, если их собрали или обработали без законных оснований. Остается открытым вопрос реализации данного права в части определения оператора. Если видео размещено в сети Интернет, то найти автора или первоисточник практически невозможно для простого пользователя. Если в результате опубликования фотографий или видеозаписи возникает *реальная угроза жизни и здоровью*

гражданина либо ему наносятся моральные страдания, то на основании его мотивированного обращения распространение (демонстрация) данной информации должно быть прекращено.

Однако существует необходимость в разработке подзаконных актов, строго регламентирующих данную процедуру. На основании анализа зарубежного опыта выявляются следующие случаи использования изображения физического лица без его согласия:

– изображение человека относится к его публичной деятельности либо официальной должности;

– предоставление изображения человека по запросу правоохранительных органов;

– фиксация изображения человека в общественных местах.

Помимо указанных случаев использования изображения человека без его согласия, выявляется ограничительный принцип: использование изображения не должно унижать честь, достоинство и деловую репутацию человека, нарушать его половую неприкосновенность, противоречить моральным устоям. Таким образом, необходимо разграничивать интересы государства в рамках обеспечения общественной безопасности и интересы личности в рамках защиты неприкосновенности частной жизни. Считаем, что на сегодняшний день существуют предпосылки для дальнейшего развития законодательства в сфере защиты персональных данных в части видеонаблюдения и выделения отдельного подвида биометрических персональных данных – визуальных персональных данных.

АРХИТЕКТУРЫ СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ И ВИДЕОАНАЛИТИКИ

Все перечисленные технологические тенденции открывают много новых возможностей для систем видеоаналитики. Однако, системные архитекторы и разработчики должны реализовать функционал этих технологий в конкретных разработках и системах. Поэтому, в первую очередь, очень важно разработать и реализовать соответствующую архитектуру систем видеонаблюдения и видеоаналитики, для того чтобы эти возможности можно было реализовать и использовать в синергетическом взаимодействии.

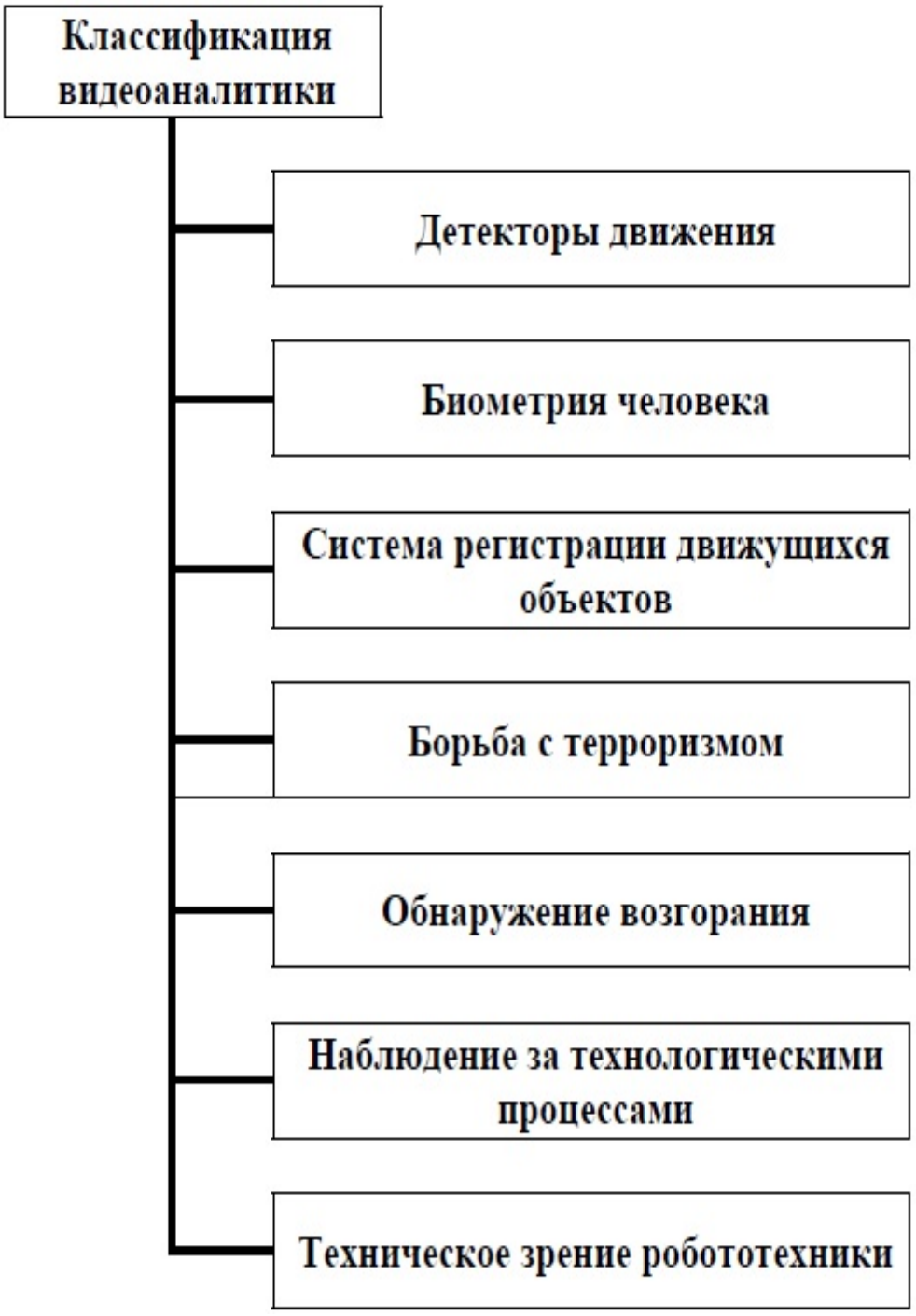
В современных системных архитектурах для видеонаблюдения активно используются облачные технологии, а также концепция граничных вычислений (edge/fog computing) для того, чтобы обрабатывать видеоданные в непосредственной близости от места их генерации и использования. Это позволяет получать значительную экономию на полосе пропускания сети и достичь высокой оперативности систем мониторинга безопасности за счёт снижения задержек при передаче видеопотоков по сети.

Камеры, разворачиваемые на границе сети, являются частью узлов видеоаналитики, которые способны обрабатывать видеокадры в режиме реального времени, без передачи их в удалённое центральное облако. Граничные узлы также способны интеллектуализировать сбор данных за счёт гибкой настройки частоты кадров в зависимости от контекста событий перед видеокамерой.

Если на сцене ничего особенного не происходит, то частота кадров может быть снижена. Если в кадре начинается движение, видеокамера увеличивает частоту кадров, а если распознан инцидент – включает съёмку с высокой скоростью и в высоком разрешении. Это позволяет не только сэкономить полосу пропускания, но и вычислительные ресурсы, а также сократить требуемый объём систем хранения.

Открытые стандарты, которым следуют основные вендоры систем видеонаблюдения и аналитики, также помогают значительно упростить архитектуры систем и сделать их независимыми от решений конкретных вендоров.

КЛАССИФИКАЦИЯ ПРОГРАММНЫХ СРЕДСТВ АНАЛИЗА ВИДЕОИЗОБРАЖЕНИЯ ПО ТИПАМ



РАСШИРЕННАЯ КЛАССИФИКАЦИЯ ВИДЕОАНАЛИТИКИ

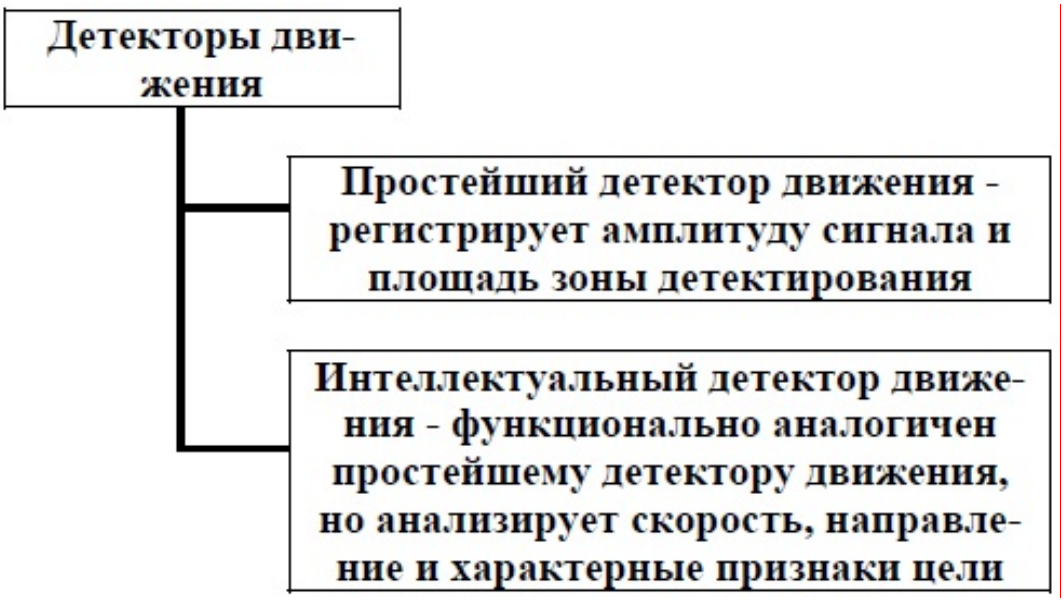


Рис. Детекторы движения (Расширенная классификация видеоаналитики)

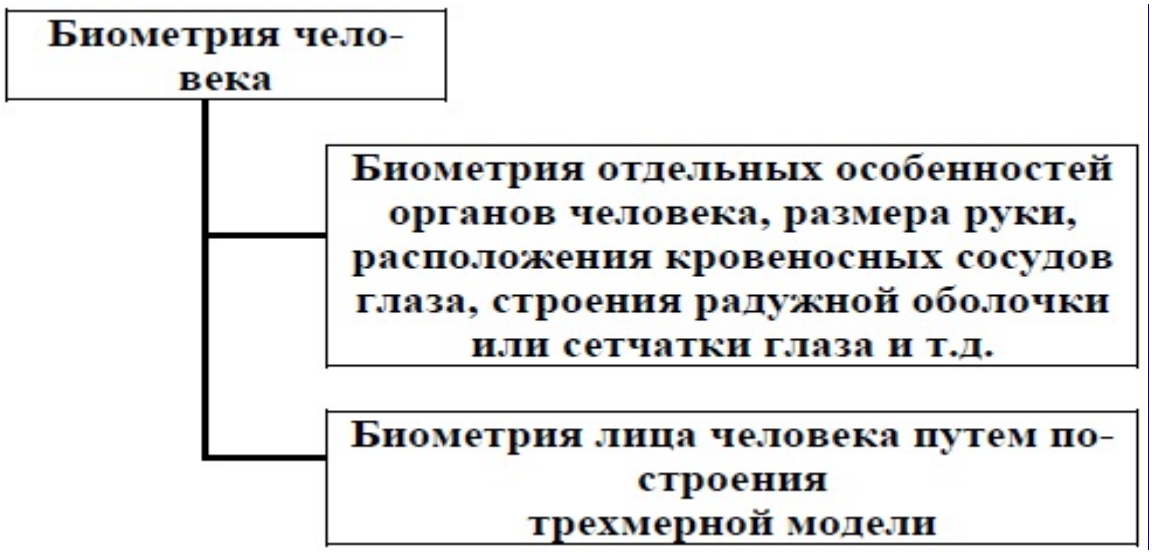


Рис. Биометрия человека (Расширенная классификация видеоаналитики)

Биометрия человека является перспективным направлением развития видеоаналитики, поскольку биометрия является наиболее надежным способом классификации человека

Биометрия отдельных особенностей органов человека, размера руки, расположения кровеносных сосудов глаза, строения радужной оболочки глаза и т.д. наиболее часто используется для обеспечения функции допуска в системах контроля и управления доступом (СКУД). Данная технология требует проведения определенных манипуляций от контролируемого человека, что требует, как минимум, согласия на эти действия от проверяемого лица.

Биометрия путем построения двухмерной или трехмерной модели лица человека позволяет осуществлять контроль дистанционно, что является большим преимуществом

данной технологии, однако и здесь есть определенные ограничения по применению, связанные в первую очередь с техническими возможностями данной технологии.

Все существующие методы распознавания лиц можно разбить на две группы: аналитические и холистические. Аналитические методы основаны на выделении геометрических признаков лица, описывающих его индивидуальные особенности.

В холистических методах рассматриваются общие свойства изображений человеческих лиц. Лицо распознается как нечто целое, а не состоящее из отдельных частей, таких как глаза, нос, рот, уши и т.п.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ВСЕ ЕЩЕ НАХОДИТСЯ НА РАННЕЙ СТАДИИ РАЗВИТИЯ

Необходимо провести сравнение между потенциалом системы на базе искусственного интеллекта и возможностями человека. Операторы систем видеонаблюдения способны сохранять бдительность и внимательность только в течение *короткого времени*, компьютер же может обрабатывать большие объемы данных неустанно и очень быстро.

Однако было бы глубочайшим заблуждением думать, что искусственный интеллект может заменить человека. Успех заключается в использовании преимуществ систем ИИ для увеличения потенциала и возможностей оператора. Машинное и глубокое обучение зачастую описывают как возможность системы автоматически учиться и совершенствоваться на основе полученного опыта. Но доступные на сегодняшний день системы ИИ не обучаются новым навыкам самостоятельно и не запоминают произошедшие события. Чтобы повысить эффективность системы, ее необходимо переобучить, используя более точные данные во время сеансов контролируемого обучения.

Неконтролируемое обучение обычно требует большого количества данных для создания кластеров и поэтому не используется в приложениях видеонаблюдения. Зато его применяют для анализа больших наборов данных при поиске аномалий, в частности в финансовых транзакциях.

Большинство подходов, в видеонаблюдении рекламируются как «самообучение», основаны на анализе статистических данных, а не на фактическом переобучении моделей глубокого обучения. Человеческий опыт по-прежнему превосходит большинство аналитических приложений на основе ИИ, используемых для целей видеонаблюдения.

Особенно когда такие приложения должны выполнять очень общие задачи и когда понимание контекста имеет решающее значение. Приложение на основе машинного обучения может успешно обнаружить бегущего человека (если оно было специально обучено этому), но в отличие от человека, который способен поместить данные в контекст, приложение не понимает, почему человек бежит: чтобы успеть на автобус или чтобы его не догнал полицейский?

Что бы ни обещали компании, применяющие ИИ в своих приложениях видеоаналитики, эти приложения не способны понимать, что происходит в кадре, с такой же проницательностью, как человек. По этой же причине аналитические приложения на базе искусственного интеллекта могут выдавать *ложную тревогу или, в случае реального происшествия, не подавать сигналы*. Обычно такое происходит в сложной среде с интенсивным движением или когда человек несет крупный предмет, из-за которого приложение не может правильно классифицировать объект.

Видеоаналитика на базе ИИ на современном этапе должна использоваться как вспомогательный инструмент, например чтобы определить, насколько важен инцидент, прежде чем оповестить оператора, чтобы тот решил, как реагировать. Таким образом, искусственный интеллект используется для обеспечения масштабируемости, а задача человека — оценивать потенциальные инциденты.

ФАКТОРЫ, ОПРЕДЕЛЯЮЩИЕ ЭФФЕКТИВНОСТЬ АНАЛИТИКИ

Чтобы знать, какое качество можно ожидать от аналитического приложения на базе ИИ, рекомендуется внимательно изучить и понять известные предварительные условия и ограничения, которые обычно указываются в документации к приложению.

Все системы видеонаблюдения уникальны, и эффективность приложения должна оцениваться на каждом конкретном объекте. Если качество не соответствует ожидаемому или прогнозируемому уровню, настоятельно рекомендуется искать причину не только в самом приложении.

Необходимо выяснить причину в комплексе, поскольку эффективность аналитического приложения зависит от множества факторов, большинство из которых можно оптимизировать, если знать о том, как они влияют на качество.

К таким факторам относятся оснащение камеры, качество и динамические характеристики видеоизображения, уровень освещения, а также конфигурация, положение и направление камеры.

Пригодность изображения

Качество изображения зависит от высокого разрешения и высокой светочувствительности камеры. Несмотря на то, что важность этих параметров не подлежит сомнению, существуют и другие факторы, не менее важные при определении пригодности фото или видеозаписи.

Видеопоток с высоким качеством камеры видеонаблюдения может оказаться абсолютно бесполезным из-за недостаточной подсветки в ночное время, перенаправления камеры в ненужную сторону или сбоя связи с системой.

Перед развертыванием аналитического приложения необходимо тщательно изучить место размещения камеры. Чтобы видеоаналитика работала надлежащим образом, камера должна быть расположена таким образом, чтобы зона наблюдения просматривалась полностью и беспрепятственно.

Пригодность изображения также может зависеть от сценария его использования. Качество видео, приемлемое для человеческого глаза, может быть недостаточно для приложения видеоаналитики. Более того, многие методы обработки изображений, обычно используемые для улучшения восприятия видео человеком, не рекомендуются при использовании видеоаналитики. К ним, в частности, относятся методы шумоподавления, технология широкого динамического диапазона и алгоритмы автоматического управления экспозицией.

Современные видеокамеры часто оснащены ИК-подсветкой, благодаря которой они могут работать в полной темноте. В этом есть положительный момент, ведь такая функция позволяет размещать камеры в труднодоступных местах и устраняет необходимость установки дополнительного освещения. Однако, если на объекте возможны сильные дожди или снегопад, рекомендуется не полагаться на свет, исходящий от камеры или из источника, расположенного в непосредственной близости.

Капли дождя и снежинки могут отражать в камеру слишком много света и существенно затруднить аналитику.

При рассеянном свете больше шансов, что аналитика будет работать результативно даже в плохую погоду.

Расстояние обнаружения объектов

Определить максимальное расстояние обнаружения объектов аналитическим приложением на базе ИИ сложно: указанное в спецификации значение в метрах или футах не всегда соответствует истине. Нужно помнить, что на расстояние обнаружения существенно влияют:

- качество изображения,
- характеристики места наблюдения,
- погодные условия и свойства объекта, в частности цвет и яркость.
- от скорости перемещения объектов.

Например, что яркий объект на темном фоне в солнечный день может быть обнаружен с гораздо большего расстояния, чем темный объект в дождливую погоду.

Для получения точных результатов приложению видеоаналитики необходимо «видеть» объект достаточно долго. Это время зависит от эффективности обработки (частоты кадров) платформы: чем она ниже, тем дольше объект должен находиться в кадре, чтобы его можно было обнаружить.

Если выдержка камеры не соответствует скорости движения объекта, точность обнаружения может пострадать из-за размытости изображения. Быстрые объекты могут оказаться необнаруженными, если они перемещаются вблизи камеры. Например, легко обнаружить человека, бегущего достаточно далеко от камеры, в то время как человек, бегущий с такой же скоростью очень близко к камере, может войти в сектор обзора и выйти из него так быстро, что сигнал тревоги не успеет сработать.

Для аналитических приложений, основанных на обнаружении движения, еще одну проблему представляют объекты, движущиеся непосредственно к камере или от нее. Особенно трудно обнаруживать медленно движущиеся объекты, которые вызывают лишь очень небольшие изменения в изображении по сравнению с движением через весь кадр.

Как правило, более высокое разрешение камеры не означает большее расстояние обнаружения. Возможности обработки, необходимые для выполнения алгоритма машинного обучения, пропорциональны размеру входных данных. Это означает, что для анализа полного разрешения камеры 4K требуется как минимум в четыре раза больше вычислительной мощности, чем для камеры с разрешением 1080p. Очень часто из-за ограничений в возможностях обработки камерой в приложениях на основе ИИ используют более низкое разрешение, чем может предложить камера или видеопоток.

Настройка сигналов тревоги и записи

Из-за различных уровней применяемых фильтров аналитические приложения для обнаружения и классификации объектов генерируют очень мало ложных срабатываний. Однако такие приложения работают должным образом только при соблюдении всех указанных предварительных условий. В противном случае они могут пропустить важные события. Если нет полной уверенности в том, что все условия будут выполняться во всех без исключения случаях, рекомендуется использовать консервативный подход и настроить систему таким образом, чтобы конкретная классификация объектов не являлась единственной причиной срабатывания сигнала тревоги. Такая настройка вызовет больше ложных срабатываний, но уменьшит риск пропустить важное событие.

Когда сигналы тревоги или инициирующие их срабатывание данные поступают непосредственно в ЦОУ или другие подразделения ОВД, каждая ложная тревога оборачивается большими расходами.

Совершенно очевидно, что необходима надежная классификация объектов, позволяющая отфильтровывать нежелательные сигналы тревоги. Однако механизм записи может и должен быть настроен так, чтобы полагаться не только на классификацию объектов.

В случае пропущенного *реального сигнала тревоги* эта настройка позволяет оценить по записи причину пропуска, а затем внести изменения в монтаж и конфигурацию всей системы. Если классификация объектов выполняется на сервере во время поиска инцидента, рекомендуется настроить систему на непрерывную запись и вообще не фильтровать исходную запись. Непрерывная запись занимает много места, но

это в некоторой степени компенсируется современными алгоритмами сжатия, такими как Zipstream.

Алгоритмы глубокого обучения позволяют быстро решать сложные задачи с высокой, хотя и не 100%-ной точностью. Однако чем больше система учится, тем лучше результат. Во многих случаях результаты анализа дополняются уровнем достоверности, который в процентах показывает, насколько алгоритм уверен в том, что обнаруженный объект или событие соответствует описанию. Чаще всего такой подход применяется в системах распознавания лиц или номерных знаков.

С точки зрения правильности обнаружения возможны четыре ситуации:

- True positive – объект обнаружен, тревога активирована;
- True negative – объект не обнаружен, тревога не активирована;
- False positive – объект отсутствует, но обнаружен, активирована ложная тревога;
- False negative – объект присутствует, но не обнаружен, тревога не активирована.

Видеоанализ должен давать в основном результаты True positive. При слишком большом количестве ложных срабатываний сигналы тревоги в конце концов игнорируются. Важно также, насколько быстро событие или появление объекта обнаруживаются, особенно при анализе видео в реальном времени. Если учесть, что видеоаналитика работает с 25 или 30 кадрами в секунду, то теоретически самое малое время отклика составляет 40 мс (1/25 с). Среднее время реакции человека («глаз – мозг») – 200 мс. Максимальная задержка обнаружения события или объекта в системе видеонаблюдения с оператором не должна превышать 1–2 с.

Независимо от того, какой объект наблюдается, общее эмпирическое правило состоит в следующем: чтобы можно было распознать детали объекта(ов), размер картинки должен быть не менее 30–50 пикселей. Например, для распознавания номера автомобиля высота изображения номерного знака должна быть не менее 30 пикселей, для идентификации лица требуемая высота изображения головы – 80–90 пикселей.

Обслуживание Системы видеонаблюдения необходимо регулярно обслуживать. Рекомендуется не только просматривать картинку через интерфейс ПО для управления видео, но и проводить физический осмотр оборудования, чтобы своевременно обнаруживать и удалять все, что может мешать наблюдению или блокировать поле обзора. Это важно в отношении стандартных (только ведущих запись) систем, но еще более важно при использовании средств аналитики. Если говорить о базовом видеообнаружении движения, то такая типичная помеха, как паутина, качающаяся на ветру, может увеличить количество сигналов тревоги, что приведет к более высокому потреблению дискового пространства.

При использовании приложения для обнаружения и классификации объектов паутина создаст зону исключения в области обнаружения. Ее нити будут скрывать объекты и значительно снизят вероятность их обнаружения и классификации. Паутина может мешать обзору камеры видеонаблюдения.

Грязь на объективе или защитном колпаке камеры вряд ли создаст проблемы днем. Но в условиях низкой освещенности свет, падающий на грязный колпак сбоку (например, от фар автомобиля), может вызвать непредвиденное отражение, что снизит точность обнаружения.

Не менее важно проводить регулярное обслуживание зоны видеонаблюдения, ведь в течение срока службы камеры в секторе ее наблюдения может произойти многое. Выявить потенциальные проблемы позволит простое сравнение изображений местности «до и после». Как выглядела зона видеонаблюдения в момент установки камеры, и как она выглядит сегодня? Также необходимо корректировать зоны обнаружения.

КРИМИНАЛИСТИЧЕСКИЕ ИССЛЕДОВАНИЯ ПРОВОДИМЫЕ ДЛЯ ИДЕНТИФИКАЦИИ ЧЕЛОВЕКА

На базе имеющихся данных, разработанных такими науками, как анатомия, антропология, судебная медицина, психология, а также на основе практики раскрытия и расследования преступлений в криминалистике сформировалась самостоятельная отрасль, именуемая «габитоскопией», которая изучает закономерности запечатления внешнего облика человека в различных отображениях и разрабатывает технико-криминалистические методы и средства собирания, исследования и использования данных о внешнем облике человека в целях раскрытия и предупреждения преступлений. К установлению личности по признакам внешнего облика чаще всего прибегают органы досудебного расследования при проведении:

- оперативно-разыскных мероприятий (наблюдение, отождествление личности, проверка по учету субъективных портретов);
- следственных действий (допрос, предъявление лица для опознания и назначение портретной экспертизы);
- производстве судебно-портретных исследований (экспертиз).

Сегодня в условиях научно-технического прогресса, когда темпы разработки и совершенствования новых технологий значительно ускорились криминалистика и судебная экспертиза по-прежнему нуждаются в обновлении и расширении спектра технологий, методов и методик позволяющих автоматизировать и значительно объективизировать процесс идентификации человека.

В то же время, как отмечается в одной из работ по теоретическим проблемам криминалистики: «в следственную и судебную практику можно внедрять лишь те из новинок современной техники, которые способны обеспечить надежные результаты при строгом соблюдении законности».

Современные достижения научно-технического прогресса, внедряемые в область борьбы с преступностью, должны отвечать целому ряду особых требований, вытекающих из специфики решаемых задач в данной сфере деятельности.

Следует отметить, что биометрические технологии, уже существующие к настоящему времени, не могут быть непосредственно (без изменений) внедрены в правоохранительную сферу. Для этого потребуется адаптация таких технологий, методов и методик как минимум в трех направлениях: техническом, правовом и организационном.

Биометрическая идентификация личности, являясь одним из методов распознавания или аутентификации человека, имеет некоторые отличия от криминалистической идентификации личности.

Биометрические системы создаются с целью ограничения доступа к информации, предотвращения проникновения злоумышленников на охраняемые территории и в помещения, для защиты от подделки электронных идентификационных документов и т.д. Современные возможности биометрических технологий обеспечивают необходимые требования по надежности идентификации, простоте использования и низкой стоимости оборудования.

Биометрия по существу является одним из методов аутентификации. Как известно аутентификация подразумевает проверку подлинности субъекта, которым в принципе может быть не только человек, но и программный процесс.

Существует три традиционных способа аутентификации: по собственности - физическим предметам, таким, как ключи, паспорт и смарт-карты; по знаниям информации, которая должна храниться в секрете и которую может знать только определенный человек, например пароль; по биометрическим параметрам - физиологическим или поведенческим характеристикам индивида. Это части

человеческого тела или действия, по которым можно отличить людей друг от друга. Главная цель биометрических технологий заключается в создании такой системы регистрации, которая крайне редко отказывала в доступе легитимным пользователям и в то же время полностью исключала несанкционированный вход в компьютерные хранилища информации.

Существующие биометрические технологии можно разделить на две ветви.

К первой следует отнести группу технологий, построенных на анализе статических (неизменяемых) образов личности, данных ей от рождения и хорошо наблюдаемых окружающими (особенности геометрии лица, руки, отпечатка пальца, структура глаза).

Ко второй, следует отнести биометрические программы, построенные на анализе динамических образов личности, которые отражают особенности характерных для неё быстрых подсознательных движений (динамические параметры письма, голос человека, его походка).

К наиболее разработанным биометрическим технологиям, основанным на анализе статистических образов личности (физиологических), относятся:

1) Идентификация на основе папиллярных рисунков пальцев рук. На долю использования этого параметра приходит большинство существующих биометрических систем. Данный метод идентификации наиболее широко распространён в криминалистике.

1) Идентификация по индивидуальным особенностям геометрии лица основывается на применении методов габитоскопии.

3) Идентификация по рисунку радужной оболочки глаза производится путем измерения и анализа цветного кольца вокруг зрачка глаза.

4) Идентификация по силуэту кисти руки. Данные биометрические технологии основаны на измерении длины и ширины пальцев руки, появились одними из первых более 25 лет назад. Сейчас ведется разработка более сложных систем, дополнительно измеряющих профиль руки (объём пальцев, объём кисти, неровности ладони, расположение складок кожи).

5) Идентификация по рисунку кровеносных сосудов глазного дна. Вены и артерии, снабжающие глаз кровью, хорошо видны при подсветке глазного дна внешним источником света. Является одним из наиболее новых и достаточно надёжных методов идентификации.

6) Идентификация по термограмме лица (схеме артерий, снабжающих кожу лица тёплой кровью) - осуществляется с использованием специализированной видеокамеры дальнего инфракрасного диапазона, которая может работать в полной темноте.

7) Идентификация по венам руки производится по рисунку вен тыльной стороны кисти руки, сжатой в кулак.

Вторую группу биометрических технологий, основанных на анализе динамических образов личности (поведенческих), составляют:

1) Идентификация по голосу - метод, который основывается на распознавании таких уникальных свойств голоса, как частота, модуляция, интонация и т.д.

2) Идентификация по рукописному почерку осуществляется на основе анализа характерных для личности быстрых подсознательных движений в процессе воспроизведения контрольного слова.

3) В настоящее время ведётся разработка новых биометрических систем, работа которых основана на идентификации человека по таким динамическим проявлениям его внешнего облика, как походка, мимика, артикуляция, жестикуляция. При этом значимая для идентификации информация может быть адекватно зафиксирована, сохранена и воспроизведена только с помощью современных технических средств видеозаписи.

Отличием криминалистической идентификации человека от биоидентификации является то, что субъектом криминалистического идентификационного исследования является человек, обладающий специальными знаниями - эксперт. Биометрические технологии же основаны полностью на автоматизированных системах, осуществляющих следующие функции:

- получение и хранение в базе данных оцифрованного образца биометрической характеристики индивида;
- введение в систему проверяемой характеристики человека;
- извлечение индивидуализирующих признаков;
- сравнение признаков введенной характеристики с признаками образца из базы данных;
- заключение о тождестве или различии сравниваемых биометрических характеристик (является ли человек тем, за кого себя выдает).

В правоохранительной сфере биометрические технологии могут использоваться для борьбы общеуголовной преступностью, терроризмом, незаконной миграцией, для обеспечения общественной и личной безопасности граждан и т.д.

К основным сферам практического внедрения биометрических технологий идентификации личности для решения правоохранительных задач следует отнести: осуществление пограничного и паспортного контроля, использование в работе иммиграционных служб, при проведении оперативно-разыскной деятельности, в системе криминалистической регистрации и при проведении криминалистических исследований (экспертиз) и т.п.

Здесь будет рассмотрено использование биометрических систем при проведении оперативно-разыскной деятельности, в системе криминалистической регистрации и при проведении криминалистических исследований (экспертиз).

Оперативно-розыскная деятельность, оперативное распознавание (идентификация) при осуществлении оперативно-разыскных мероприятий. Биометрические технологии, позволяющие осуществлять дистанционно и незаметно для объекта идентификацию его личности. Такие технологии, например, могут быть интегрированы в уже широко распространенные сегодня системы видеонаблюдения. Системы видеонаблюдения стали уже привычным атрибутом публичных мест - метро, вокзалов, аэропортов, крупных торговых центров. С их помощью органы общественной безопасности и оперативно-розыскные структуры ведут мониторинг ***«лицевых потоков»*** целью обнаружения известных преступников. Сотрудники безопасности игровых заведений ведут постоянное видеонаблюдение за игровыми столами, входами и ресторанами казино, выявляя мошенников (шулеров и их помощников). Автоматизация процесса идентификации на основе биометрических технологий позволяет увеличить эффективность работы систем видеонаблюдения в несколько раз.

Криминалистическая регистрация. Различные биометрические данные, индивидуализирующие человека, которые ранее не использовались в системе криминалистической регистрации, могут также фиксироваться в базах данных для получения информации о лицах попавших в сферу уголовного судопроизводства.

Криминалистические исследования (экспертизы) по идентификации личности. Развитие биометрических технологий оказывает влияние на развитие таких традиционных криминалистических экспертиз, как дактилоскопическая, почерковедческая, фоноскопическая, портретная и др. При этом внедрение новейших биометрических технологий в правоохранительную деятельность, несомненно, потребует становления новых видов экспертных исследований - экспертизы соответствующих биометрических параметров. Для этого, на законном основании, могут применяться лишь

те биометрические технологии, которые предусматривают участие экспертов-людей в установлении и подтверждении тождества.

В настоящий момент очень мало существующих биометрических технологий применяется в целях криминалистической идентификации личности человека (проверка криминального прошлого, поиск по картотекам, быстрая идентификация).

Теория и практика криминалистической идентификации личности, по нашему мнению, нуждается в пополнении своего арсенала новыми биометрическими технологиями.

Внедрение таких технологий в криминалистическую деятельность возможно только на базе современных информационно-коммуникационных технологий, позволяющих автоматизировать процесс фиксации и анализа биометрической информации. Наиболее перспективными для использования в правоохранительной деятельности будут являться те биометрические параметры, которые позволяют идентифицировать человека на расстоянии.

Активное развитие цифровых технологий позволяют лучше и четче фиксировать объекты расположенные как на расстоянии, так и в их движении, что обусловило их широкое и эффективное применение в деле предупреждения, раскрытия и расследования преступлений.

Растущая популяризация в использовании средств видео позволило органам правопорядка своевременно и качественно реагировать на противоправные действия, совершаемые как случайными правонарушителями, так и криминальными элементами.

Развитие науки и техники позволяют констатировать о расширении современных возможностей изучения биометрических, и в частности динамических признаков человека, а интерес в их исследовании только возрастает по причине практической необходимости, в том числе и при раскрытии и расследовании преступлений.

В настоящее время формируется новое поисковое междисциплинарное направление – криминалистическое исследование динамических признаков человека», которое, может являться интегрирующим звеном различных отраслей научного знания и прикладных наук: криминалистики (габитоскопия, трасология).

Целью является изучение теоретических основ по идентификации динамических проявлений человека (правонарушителя) зафиксированных средствами и приборами видео наблюдения с последующим установлением личности (правонарушителя).

В Казахстане и в России криминалистические исследования динамических признаков человека отнесены к портретным исследованиям. Поскольку как вытекает из терминологического смысла определений «портретное исследование» и «динамические признаки человека» эти понятия нетождественны.

Под термином портрет понимается изображение или описание какого-либо человека либо группы людей, существующих или существовавших в реальной действительности, где (изображенные или описываемые) объекты и их признаки находятся в неподвижном состоянии.

В то время как динамические признаки человека проявляются в движении. Динамика – состояние движения, ход развития, изменение какого-либо объекта под действием приложенных сил или какого-либо явления под влиянием действующих на него факторов.

При исследовании динамических признаков человека или группы людей, в отличие от портретного, элементам и признакам изучаемого объекта присуще свойство динамичности, то есть они проявляются в движении.

Использование криминалистически значимой информации о динамических признаках человека в раскрытии и расследовании преступлений» указывает, что по форме проявления динамические элементы походки и их признаки делятся на две группы.

К первой отнесены проявления, «которые могут отображаться в виде материально фиксированных следов (в статике); ко второй относятся отличительные признаки, воспринимаемые только в динамике и соответственно зафиксировать их можно только с помощью средств видеозаписи».

Под динамическими признаками человека принято понимать, проявления внешних особенностей человека в виде двигательной активности совокупности или отдельных анатомических элементов облика воспринимаемые визуально или фиксируемые техническими средствами и приборами.

Общая классификация построения системы динамических признаков человека с позиции экспертно-криминалистической идентификации включает в себя: динамические двигательные признаки, связанные с перемещением тела в пространстве и его ориентацией; динамические коммуникативные признаки (динамика изменения мимики лица, артикуляции речевого аппарата, жестикуляции и т.д.); динамические признаки человека, проявляются в реализации его навыков (трудовых, спортивных, преступных) и привычек.

В зарубежных странах (Великобритания, Израиль, Испания, Китай, США и т.д.) уже существуют методики установления личности по биометрическим признакам, которые достаточно успешно применяются в практической деятельности полицейских органов этих стран.

В настоящее время, криминалистами уже разработана теоретическая основа по идентификации таких признаков личности. а также уже существуют методики их фиксации и исследования».

Наиболее распространенными видами динамических признаков, используемых в габитоскопических исследованиях, являются: походка, мимика, жестикуляция, артикуляция, а так же двигательные проявления навыков и привычек человека.

Так, важным динамическим элементом человека является его способность передвигаться на ногах путем ходьбы и беге, различия в которых преимущественно заключается в скорости передвижения.

Походка для каждого человека является сугубо индивидуальной и формируется в течение всей жизни при помощи создания нервно-мышечного автоматизма под постоянным контролем нервной системы путем образования устойчивых условно-рефлекторных связей.

Уникальность ***«динамических образов»*** движений является не только следствием антропоморфологических различий людей, но и тем, что они закладываются в раннем детстве в ходе обучения и формирования динамического вариотипа этого навыка. Особенности (отличительные признаки) походки зависят от возраста, пола, патологий опорно-двигательного аппарата (в силу различных заболеваний, травм), состояния, одежды, обуви, наличия спортивных, профессиональных или иных навыков, переносимого груза, условий и целей ходьбы и других факторов.

К первой группе динамических элементов и их признаков относятся:

- длина шага,
- ширина шага,
- положение и постановка стоп при ходьбе, которые могут быть исследованы,

Ко второй группе относятся следующие динамические элементы и их признаки:

- темп (скорость),
- равномерность,
- симметричность ходьбы,
- степень поднимания стоп при ходьбе,
- степень сгибания коленей,
- особенности положения и движения головы, туловища, рук и т.д.

Динамические элементы походки и их отличительные признаки, относящиеся ко второй группе, ранее не исследовались по причине отсутствия технических средств, методик для проведения измерений и таким образом получения количественной информации о них.

В связи с наличием у человека биологических и функциональных асимметрий, они также оказывают значительное влияние на походку в виде различий в амплитудах движений симметричных частей тела, например, разная амплитуда правой и левой руки (ноги), отличающееся отклонение корпуса вправо и влево при движении, и др.

При описании внешности человека выделяются от 6 до 29 различных видов походки и движений сопряженных частей тела, а также их разновидностей. При описании ходьбы рассматриваются ее скорость, равномерность, симметричность, отмечаются размер шага, расстановка ног в стороны, положение и постановка стоп при ходьбе, степень их отрывания от земли, степень сгибания коленей.

Для характеристики походки используется совокупность этих признаков, а также положение и движение головы, плеч, туловища, таза, рук». Классификация походки:

—по темпу движения: быстрая, «поспешная», торопливая, деловая, расслабленная, неторопливая, суетливая;

—по степени поднимания стоп и сгибания коленей: «подпрыгивающую», «пружинистую», «танцующую», «на цыпочках», «журавлиную», семенящую;

—по положению и постановке стоп: спотыкающуюся, «лисью» и «косолапую»;

—по положению и особенностям движении туловища, головы, плеч, рук: «вихляющую», вразвалку и ее вариации (враскачку, «качающуюся», «морскую», «утиную» и т.п.), «кланяющуюся», «скользящую», смешную, «пробирающуюся».

Относительно признаков бега, они, описываются так же, как и признаки ходьбы.

Отождествление личности по следам ходьбы должно базироваться на:

– установлении и сопоставлении устойчивых индивидуально выраженных закономерных соотношений между отдельными элементами дорожек следов ходьбы;

– на установлении того, что эти закономерности характеризуют анатомо-физиологические особенности отождествляемого лица.

Исходя из вышеуказанного можно отметить, теоретические подходы направленные на идентификацию динамических элементов и их признаков по походке, могут быть реализована только на основе целого комплекса полученной из разных источников информации, характеризующих те или иные свойства и проявления личности (биологические, социально-демографические, функциональные, медицинские, психолого-психиатрические и др.).

В этой связи, представляется целесообразным обобщить динамические признаки походки человека в единый комплекс информации с последующей их дифференциацией по следующим категориям:

– медицинские особенности (проявляющиеся в виду имеющихся или пережитых заболеваний);

– профессиональные особенности и навыки (приобретенные в процессе трудовой деятельности);

– физиологические (биологические) особенности (врожденные).

Подобная «комплексная информация при создании розыскного портрета неизвестного преступника может быть осуществлена только при использовании информационно-аналитической поисковой системы, без которой ее практическая реализация не возможна. Кроме того, более широкие возможности получения большого объема информации об искомом лице и достоверного прогнозирования его свойств

предоставляют генотипоскопия, дерматоглифика, изучение биологических следов человека (включающие его динамические проявления) и т.п.».

Одним из наиболее передовых средств фиксации динамических признаков человека являются современные системы видеонаблюдения в виду присущих им следующих свойств:

– объективности информации (передаваемых в виде материально-фиксированных отображений внешности человека);

– высокого разрешения качества изображения;

– резкостью кадра, делающих их пригодными для дальнейшего экспертного исследования с использованием инструментальных методов (аналитической фотограмметрии с математической обработки результатов измерений);

— совместимостью (с различными компьютерными программами и технологиями, открывающими новые возможности для изучения и анализа изображений путем масштабирования, нанесения антропометрических точек на отдельных кадрах, покадрового анализа изображений).

Анализа информации запечатленной на видеоносителе о динамических проявлениях человека разработали соответствующую последовательность, включающую следующие этапы:

– перенос видеоизображения в память компьютера;

– разбивка видеоизображения на отдельные кадры;

– нанесение на каждое из статических изображений видеоряда пространственных координат;

– разметка на каждом из статических изображений антропометрических точек, соответствующих частям тела или элементам внешности человека;

– измерение значений отличительных динамических признаков человека;

– статистическая и математическая обработка результатов измерения динамических признаков человека.

Особенности криминалистической идентификация человека по видеоизображениям:

1. Криминалистическая идентификация человека по признакам анатомических элементов внешнего облика, запечатленным на видеоизображениях, – это процесс установления наличия или отсутствия тождества человека по признакам анатомических элементов внешнего облика по материально-фиксированным отображениям (видеоизображениям), осуществляемый путем производства судебно-портретной экспертизы, а также по чувственно-конкретным отображениям – представлению о внешнем облике человека, сохранившемуся в памяти очевидца, в ходе проведения оперативно-разыскных мероприятий, следственных действий и осуществления криминалистической регистрации с помощью методов, средств и приемов идентификации, разрабатываемых габитоскопией и портретной экспертизой, в целях раскрытия и расследования преступлений.

2. Классификация факторов, влияющих на отображение признаков анатомических элементов внешнего облика человека, запечатленных на видеоизображениях, к числу которых относятся: факторы материальной части средств видеозаписи, факторы процесса записи видеоизображения на носителях, факторы условий видеозаписи, факторы состояния внешности объекта запечатления, факторы условий хранения видеозаписи.

3. Обоснование необходимости формирования видеоучетов отображений признаков анатомических элементов для использования при проведении оперативно-разыскных мероприятий и выполнения индивидуально-профилактических функций в отношении

подучетных лиц. С учетом потребностей практики предлагается сформировать такой вид учетов в экспертно-криминалистических подразделениях.

4. Классификация видеоизображений анатомических элементов внешнего облика, получаемых в качестве образцов для сравнительного исследования:

а) по виду видеозаписывающего устройства, с помощью которого может быть получено видеоизображение;

б) по формату видеозаписи;

в) по формату сжатия видеозаписи;

г) по субъекту получения;

д) по процессуальному положению лица, изображение которого используется в качестве отображения внешнего облика человека;

е) по связи с уголовным делом;

ж) по содержанию;

з) по значимости для идентификации человека по признакам элементов внешнего облика.

В особую группу следует выделить образцы, получаемые экспертом путем проведения эксперимента в рамках портретной экспертизы.

5. Методика судебно-портретной экспертизы с использованием видеоизображений, учитывающая особенности содержания каждой стадии портретной экспертизы, должна включать в себя: специфику определения пригодности видеоизображения для идентификации человека по признакам внешности; при проведении раздельного исследования необходимо решать вопрос о суммировании видеокадров, на которых получили отображение признаки анатомических элементов внешности человека с целью получения пригодного для идентификации комплекса этих признаков; при оценке результатов сравнительного исследования предложены критерии формулирования того или иного вывода при производстве портретной экспертизы по видеоизображениям.

6. Классификация совокупностей признаков элементов внешнего облика человека при оценке результатов сравнительного исследования:

1) по объективному отображению: а) достоверные, б) мнимые);

2) по полноте отображения: а) полные, б) частичные;

3) по степени значимости: а) существенные, б) несущественные;

4) по характеру устойчивости: а) устойчивые, б) неустойчивые;

5) по степени встречаемости в группе людей: а) групповые, б) индивидуальные;

6) по объективной сущности: а) качественные, б) количественные;

7) по объему: а) достаточные, б) недостаточные.

Факторы, влияющие на полноту и достоверность отображения элементов и признаков внешности, связанные с видеозаписью.

Отождествление человека по видеоизображениям и фотоснимкам является одним из наиболее сложных видов криминалистической идентификации. Это обусловлено, прежде всего, относительной ограниченной информативностью сравниваемых объектов.

В первую очередь это относится к видеопортретам, которые в последнее время в связи с развитием видеотехники и внедрением ее в практику ОВД все чаще встречаются в качестве объектов криминалистической портретной экспертизы.

Видеофиксация активно используется при проведении оперативно-розыскных мероприятий, следственных действий (осмотр места происшествия, следственный эксперимент, обыск, выемка, предъявление для опознания), а также при создании видеотек лиц, причастных к совершению преступлений. Кроме того, видеозапись используется при проведении различных экспертных исследований и других действий,

связанных с идентификацией или распознаванием отдельных личностных характеристик человека.

Полнота и достоверность отображения признаков внешности при видеосъемке зависит от следующих факторов:

- технических характеристик видеокамеры;
- условий съемки;
- масштаба изображения головы человека, расположение ее по площади кадра;
- положения запечатлеваемого объекта относительно видеокамеры;
- способ выполнения видеосъемки.

При воспроизведении видеозаписи на полноту отображения признаков внешности влияют технические характеристики видеоаппаратуры и монитора, а также способы получения твердой копии с кадра (с помощью принтера, фотографирования с экрана монитора).

При определении технических характеристик видеокамеры учитывается ее формат, параметры размещения видео и звукового сигнала.

Освещенность объекта при видеосъемке влияет на полноту отображения признаков внешности также как и при фотосъемке.

Расстояние до объекта съемки как и при фотографировании определяет уровень воспроизведения мелких деталей строения лица. Так при размере головы менее 1/6 кадра элементы внешности при последующем их увеличении будут размываться, будет видна строчная развертка монитора. Поэтому для удовлетворительного воспроизведения размер головы должен быть 1/3 площади кадра.

Как и при фотографировании на качество отображения влияют ракурс видеосъемки и положение камеры относительно объекта съемки.

На качество изображения на видеоносителе влияют:

- помехи видеосигналов в виде сетки, муара, полос;
- искажение временного масштаба видеосигнала (искажаются размерные характеристики изображения);
- цветопередача (понижение насыщенности и потеря цвета приводят к искажению цвета элементов внешности)

Перевод портретной информации на твердый носитель возможно с помощью, принтеров и фотографированием с экрана монитора. В последнем случае качество изображения значительно снижается.

Особенности исследования видеоизображений, полученных с видеоконтрольных устройств

Одной из наиболее сложных задач при производстве портретной экспертизы является изучение и сопоставление видеоизображений, полученных с видео – контрольных устройств. Это связано с тем, что элементы и признаки внешнего облика человека, отобразившиеся на такого рода объектах имеют геометрические искажения пропорций, часть мелких признаков не отображается.

Кроме этого существенной причиной затрудняющий производство экспертиз по видеоизображением является невысокое качество представленных на исследования видеокадров и отсутствие при сравнении фотоснимков и видеоизображений (при наличии подозреваемого) сопоставимого материала.

-влияния условий видеосъемки на полноту и достоверность отобразившихся признаков;

-наиболее эффективные методы, используемые на стадии сравнительного исследования.

Освещение лица в момент видеосъемки оказывает существенное влияние на отображение его особенностей. Образуемые светом светотени позволяют судить о форме,

контурах и рельефе отдельных частей лица. Элементы лица по-разному отражают падающий на них свет. Эта особенность на видеоснимках передается определенной тональностью. Игра света и тени, с одной стороны, подчеркивает общий рельеф лица и его элементов, с другой делает незаметными мелкие детали частей лица. В свете эти детали оказываются высвеченными, в тени затемненными. Это может значительно ограничить возможность использования особенностей элементов в качестве идентификационных признаков.

Далее рассматривается такой фактор, как влияние дистанции видеосъемки на достоверность и полноту отображения признаков внешности на видеоизображениях.

Также не менее важным фактором, влияющим на достоверность и полноту отображения признаков внешности на видеоснимках, является их качество, которое зависит от разрешающей способности видеокамеры. При этом необходимо учесть, что чем больше разрешение, тем качественнее отображаются анатомические признаки внешности.

При исследовании видеоизображений необходимо особое внимание уделить подготовке сравнительного материала. Алгоритм действий по подготовке сравнительного материала при выполнении экспертиз по видеоизображениям, который включает в себя:

1. внимательно просмотреть представленную на исследование видеозапись например, с помощью программы
2. выбрать на представленной видеозаписи видеокадры на которых наиболее полно и достоверно отобразились анатомические элементы и признаки;
3. привести видеоизображения к одному масштабу и распечатать их на твердом носителе например, фотобумаге;
4. разработать сценарий действий подозреваемого с учетом отобранных видеокадров;
5. произвести фотосъемку подозреваемого по разработанному сценарию с максимальным разрешением;
6. обработать фотоснимки с помощью программы AdobePhotoshop, и привести представленные изображения к одному масштабу.

Таким образом, рассмотрение теоретических предпосылок связанной с изучением анатомических (статических) и функциональных (динамических) элементов и их признаков внешности направленных на идентификацию личности (правонарушителя), позволяет констатировать, что способы их фиксации возможны только на основе использования самых новейших информационно-коммуникационных технологий.

ПРАВОВЫЕ И ЭТИЧЕСКИЕ НОРМЫ В СФЕРЕ ВИДЕОАНАЛИТИКИ С ПРИМИНЕНИЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Правовое регулирование видеоаналитики с использованием искусственного интеллекта (ИИ) в Республике Казахстан основывается на ряде законодательных актов и нормативных документов, направленных на защиту персональных данных, обеспечение безопасности и регулирование использования ИИ.

Правовые основы работы с видеоаналитикой

1. Закон Республики Казахстан "О персональных данных и их защите" от 21 мая 2013 года N 94-V.

– Регулирует порядок сбора, обработки и хранения персональных данных, включая данные, получаемые с использованием видеоаналитики.

– Требует от организаций получения согласия субъектов данных на обработку их персональных данных.

– Определяет меры по защите персональных данных от несанкционированного доступа, утраты, изменения и других угроз.

2. Закон Республики Казахстан "О доступе к информации" 16 ноября 2015 года № 401-V:

– Устанавливает требования к информационной безопасности при использовании систем видеоаналитики.

– Включает положения о защите информации в системах видеонаблюдения и видеоаналитики, а также о предотвращении утечек данных.

3. Закон Республики Казахстан "О связи" Закон Республики Казахстан от 5 июля 2004 года N 567.:

– Регулирует вопросы, связанные с передачей данных, включая видеоинформацию, через сети связи.

– Определяет ответственность операторов связи за защиту передаваемых данных.

4. ***ИНСТРУКЦИЯ по организации надзора за законностью деятельности государственных, местных представительных и исполнительных органов, органов местного самоуправления и их должностных лиц, иных организаций независимо от формы собственности, а также принимаемых ими актов и решений, судебных актов, вступивших в законную силу, исполнительного производства, представительства интересов государства в суде по гражданским и административным делам*** *от 2 мая 2018 года № 60*

– Включает положения о надзоре за соблюдением законодательства в сфере обработки и защиты персональных данных.

– Определяет полномочия государственных органов в области контроля за использованием систем видеоаналитики.

5. Приказ Председателя Комитета национальной безопасности Республики Казахстан от 27 октября 2020 года № 69-қе. Зарегистрирован в Министерстве юстиции Республики Казахстан 30 ноября 2020 года № 21693 - Правила функционирования Национальной системы видеомониторинга

Дополнительные документы и стандарты:

- Стандарты и нормы в области защиты информации: включают технические и организационные меры по защите данных, используемых в системах видеоаналитики.

- Инструкции и методические рекомендации государственных органов: Определяют конкретные процедуры и требования к использованию систем видеоаналитики, включая использование ИИ.

Особенности правового регулирования:

1. Получение согласия субъектов данных:

– Обязательное получение согласия на сбор и обработку данных при использовании систем видеоаналитики.

– Информирование субъектов данных о целях и способах обработки их данных.

2. Защита данных:

– Обеспечение конфиденциальности, целостности и доступности данных.

– Применение мер по защите данных от несанкционированного доступа и утечек.

3. Прозрачность и ответственность:

– Предоставление субъектам данных информации о том, как их данные обрабатываются.

– Установление ответственности за нарушение законодательства в области защиты персональных данных.

4. Государственный контроль и надзор:

Осуществление контроля за соблюдением законодательства в области видеоаналитики и защиты персональных данных.

Проведение проверок и аудитов систем видеоаналитики на соответствие требованиям законодательства.

В целом, правовое регулирование видеоаналитики с использованием ИИ в Казахстане направлено на обеспечение защиты персональных данных, информационной безопасности и соблюдения прав граждан при использовании современных технологий.

Как и во многих государствах, новости о том, что камеры наружного наблюдения будут объединены в общую систему, вызвали негативные ассоциации.

Как жить в городе, который за тобой следит?» В этой связи представляется крайне важным определить направления правового регулирования систем общественной безопасности таким образом, чтобы обеспечить соблюдение права на неприкосновенность частной жизни, не допустить произвольное вмешательство в жизнь человека.

Наряду с большим положительным эффектом от внедрения систем ИИ для общественной безопасности, существуют и отрицательные стороны. В сознании людей существует определенная связь между постоянным наблюдением за ними и тоталитаризмом, как следствие, любое обсуждение видеонаблюдения неизбежно приходит к дискуссии об использование таких метафор как «Большой брат»

Этический вопрос «вторжения» систем видеонаблюдения и видеоаналитики в частную жизнь каждого отдельного добропорядочного гражданина, на которое он не давал своего предварительного согласия, заслуживает отдельного обсуждения.

Но главный правовой вопрос можно сформулировать довольно быстро: насколько это в принципе согласуется с нормами основного закона страны – Конституции.

К настоящему времени в стране функционирует достаточно большое количество баз данных, содержащих как персональные, так и иные данные в отношении каждого человека. Так, создана и функционирует государственная централизованная автоматизированная информационная система «Правительство для граждан», основу которой составляет база персональных данных граждан, иностранных граждан и лиц без

гражданства, постоянно проживающих в Республике Казахстан. В связи с этим применение систем ИИ позволяет не только распознать лицо человека, но и получить всю информацию о нем путем выборки, которая содержится во всех базах данных страны. Таким образом, следует определить четкий правовой механизм сбора и защиты персональных данных и частной жизни в части получения данной информации:

– обозначить цели, для которых возможно использование информации с камер видеонаблюдения;

– определить круг лиц, имеющих доступ к базам с обязанностью сохранности данной информации в тайне и ответственности за ее разглашение;

– строго регламентировать порядок доступа иных лиц;

– обеспечить эффективную техническую защиту (в том числе идентификация пользователей системы);

– получать согласие лица на сбор и обработку данных и др.

Кроме того, в современных условиях недостаточно проработанным и понятным для простого гражданина является механизм защиты его прав в случае их нарушения.

В свою очередь, органы общественной безопасности не должны рассматривать ИИ просто как еще одну программу или инструмент. Поскольку системы ИИ совершают выбор, затрагивающий людей, организации должны учить их действовать ответственно и прозрачно. Наличие хорошего управления становится все более важным для создания доверия к ИИ. Необходимо информировать граждан, почему и как государственные органы применяют ИИ. Почти треть граждан заявляют, что не до конца понимают преимущества ИИ и как правительство его использует. Поэтому прозрачность и обмен информацией играют важнейшую роль.

КОДЕКС ЭТИКИ В СФЕРЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА

Кодекс этики в сфере искусственного интеллекта (далее – Кодекс) устанавливает общие этические принципы и стандарты поведения, которыми следует руководствоваться участникам отношений в сфере искусственного интеллекта (далее – Акторы ИИ) в своей деятельности, а также механизмы реализации положений настоящего

Кодекса. Кодекс распространяется на отношения, связанные с этическими аспектами создания (проектирования, конструирования, пилотирования), внедрения и использования технологий ИИ на всех этапах жизненного цикла, которые в настоящее время не урегулированы законодательством и/или актами технического регулирования.

Рекомендации Кодекса рассчитаны на ***системы искусственного интеллекта (далее – СИИ),*** применяемые исключительно в гражданских (не военных) целях.

Кодекс был принят на I Международном форуме «Этика искусственного интеллекта: начало доверия» в 2021 году

Главный приоритет развития технологий ИИ в защите интересов и прав людей и отдельного человека

1.1. Человеко-ориентированный и гуманистический подход.
1.2. Уважение автономии и свободы воли человека.
1.3. Соответствие закону.
1.4. Недискриминация.
1.5. Оценка рисков и гуманитарного воздействия

Необходимо осознавать ответственность при создании и использовании ИИ

1.6. Риск-ориентированный подход
1.7. Ответственное отношение.
1.8. Предосторожность.
1.9. Непричинение вреда.
1.10. Идентификация ИИ в общении с человеком
1.11. Безопасность работы с данными.
1.12. Информационная безопасность.
1.13. Добровольная сертификация и соответствие положениям Кодекса.
1.14. Контроль рекурсивного самосовершенствования СИИ.

Ответственность за последствия применения СИИ всегда несет человек.

1. Поднадзорность - Авторам ИИ следует обеспечивать комплексный надзор человека за любыми СИИ в объеме и порядке, зависящих от назначения СИИ, в том числе, например, фиксировать существенные решения человека на всех этапах жизненного цикла СИИ, или предусматривать регистрационные записи работы СИИ; обеспечивать прозрачность применения СИИ и возможность отмены человеком и (или) предотвращения принятия социально и юридически значимых решений и действий СИИ на любом этапе жизненного цикла СИИ там, где это разумно применимо.

2.Ответственность -Авторы ИИ не должны допускать передачи полномочий ответственного нравственного выбора СИИ, делегировать ответственность за последствия принятия решений СИИ – за все последствия работы СИИ всегда должен отвечать человек (физическое или юридическое лицо, признаваемое субъектом ответственности в соответствии с действующим законодательством Российской Федерации). Акторам ИИ рекомендуется принимать все меры для определения ответственности конкретных участников жизненного цикла СИИ с учетом их роли и специфики каждого этапа

Ключевые задачи регулирования в сфере ИИ:

– создание основ правового регулирования новых общественных отношений, формирующихся в связи с применением систем искусственного интеллекта и робототехники, имеющих преимущественно стимулирующий характер;

– определение правовых барьеров, затрудняющих разработку и применение систем искусственного интеллекта и робототехники в различных отраслях экономики и социальной сферы;

– формирование национальной системы стандартизации и оценки соответствия в области технологий искусственного интеллекта и робототехники.

Стандартизация

Стандартизация в сфере ИИ необходима для того, чтобы:

– упорядочить процесс интеграции ИИ
– обеспечить стабильно высокое качество ИИ-продуктов
– повысить конкурентоспособность отечественных продуктов и услуг

Для этого в России вводятся стандарты по разработке и внедрению ИИ. Политика стандартизации.

Она включает в себя разработку не менее 111 стандартов, которые призваны преодолеть нормативно-технические барьеры в реализации проекта «Искусственный интеллект».

Этика

В таких условиях цена ошибки ИИ как никогда высока — в отсутствие нужной регулятории и его использование может привести к распространению дезинформации, дискриминации, пагубному влиянию на демократические процессы.

Чтобы этого избежать, эксперты из Альянса в сфере искусственного интеллекта разработали Кодекс этики в сфере ИИ. Кодекс устанавливает общие этические принципы и стандарты поведения, которыми следует руководствоваться участникам отношений в сфере ИИ, и предназначен для создания среды доверенного развития технологий искусственного интеллекта.

Главные положения Кодекса:

1. Главный приоритет развития технологий ИИ в защите интересов и прав людей и отдельного человека
2. Необходимо осознавать ответственность при создании и использовании ИИ
3. Ответственность за последствия применения СИИ всегда несет человек
4. Технологии ИИ нужно применять по назначению и внедрять там, где это принесёт пользу людям
5. Интересы развития технологий ИИ выше интересов конкуренции
6. Важна максимальная прозрачность и правдивость в информировании об уровне развития технологий ИИ, их возможностях и рисках

ГЛОССАРИЙ

Область применения

Настоящий перечень терминов и определения понятий рекомендуются к применению в области ситуационной видеоаналитики.

Термины и определения рекомендуются для применения во всех видах документации и литературы, входящих в сферу действия работ по стандартизации интеллектуальных систем ситуационной видеоаналитики и (или) использующих результаты этих работ.

В рекомендациях введены базовые понятия, на которых могут быть основаны последующие уточнения и дополнения, относящиеся к разным техническим областям и отраслям применения.

Понятия рекомендуются к использованию при разработке технических заданий, нормативных документов, производстве продукции предметной области, а также они могут быть уточнены и (или) дополнены с учетом специфики отраслей применения интеллектуальных систем ситуационной видеоаналитики.

Учитывая стремительное развитие и производство продуктов видеоаналитики с применением технологии искусственного интеллекта, возникает потребность в разработке стандарта, устанавливающего единое терминологическое обеспечение для осуществления взаимопонимания между всеми участниками процесса: разработчиками, поставщиками, пользователями, прочими заинтересованными сторонами. Он позволит упорядочить документообразование в области ситуационной видеоаналитики и устранить технические барьеры при применении подобных «умных» информационных систем,

Термины и определения

Аутентификация - процесс проверки учетные данные человека, компьютерного процесса или устройства. Аутентификация требует, чтобы человек, процесс или устройство, выполняющее запрос, предоставляет учетные данные, которые доказывает, что это то, что или кто он говорит.

учетные данные - это цифровые сертификаты, цифровые подписи, смарт-карты, биометрические данные и сочетание имена пользователей и пароли. См. Биометрия.

Регистрация: процесс хранения и поддержания информация. В частности, в распознавании лиц контекст, биометрическая регистрация — это фиксация лица изображение, создание биометрического шаблона из изображения, и ввод шаблона в распознавание лиц репозиторий

Выражение лица: аспекты лица, обусловленные мышцами. движение или положение.

Сравнение лиц: ручное исследование различия и сходства между двумя изображениями лиц или живой объект и изображение лица (один в один) для целью определения, представляют ли они одно и то же или разные люди.

Распознавание лиц: автоматическое определение расположение и размеры человеческих лиц на цифровых

Распознавание лиц: автоматический поиск эталонное изображение в репозитории изображений путем сравнения черт лица зондовое изображение с характеристиками изображений, содержащихся в репозиторий изображений (поиск «один ко многим»).

Программа распознавания лиц: лицо объекта. инициатива признания, которая включает в себя управление человеческий компонент (менеджмент, аналитики, эксперты, авторизованные пользователи), право собственности и управление системой распознавания лиц (техническое компоненты), а также создание и обеспечение соблюдения процессов, политик и процедур в масштабе всей организации. См. Система распознавания лиц.

Программное обеспечение/технология распознавания лиц: стороннее программное обеспечение, в котором используются специальные алгоритмы для сравнения черт лица одного конкретная картина — пробное изображение — для многих других (один-ко-многим), которые хранятся в репозитории изображений, чтобы определить наиболее вероятных кандидатов. для дальнейшего расследования. См. изображения кандидатов.

Система распознавания лиц: техническая информация компоненты программы распознавания лиц, такие как аппаратное обеспечение, программное обеспечение, интерфейсы, репозитории изображений, биометрические шаблоны, автоматически создаваемые списки кандидатов, и т. д. Хотя некоторые организации владеют такой системой, другие может иметь только авторизованный доступ к данным другого объекта система распознавания лиц. См. Распознавание лиц Программа.

система видеоаналитики: Совокупность программных и (или) технических средств, использующих методы компьютерного зрения для автоматизированного получения данных на основании анализа изображений или последовательностей изображений (видеопотоков).

видеоаналитический детектор (детектор видеоаналитики): Функциональный модуль системы видеоаналитики, осуществляющий анализ изображений по заданному алгоритму анализа видео изображений или набору алгоритмов.

Сцена видеонаблюдения; СцВ: Пространство в поле зрения видеокамеры

автоматизированная система: Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций

вычислительные средства (средства вычислительной техники): Технические средства, непосредственно осуществляющие обработку данных.

доверие к системе искусственного интеллекта: Уверенность потребителя, и при необходимости, организаций, ответственных за регулирование вопросов создания и применения систем искусственного интеллекта, и иных заинтересованных сторон в том, что система способна выполнять возложенные на нее задачи с требуемым качеством.

доверенная система искусственного интеллекта: Система искусственного интеллекта, в отношении которой потребитель и, при необходимости, организации, ответственные за регулирование вопросов создания и применения систем искусственного интеллекта, проявляют доверие.

информационная технология, ИТ: Методы, способы, приемы и процессы обработки (сбора, накопления, ввода-вывода, приема-передачи, хранения, поиска, регистрации, преобразования, предоставления, отображения, распространения и уничтожения) информации с применением программного обеспечения и аппаратных средств.

искусственный интеллект, ИИ: Способность технической системы имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных практически значимых задач обработки данных результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека.

надежность: Свойство объекта сохранять во времени способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования.

Объяснимость (explainability): Свойство системы искусственного интеллекта, заключающееся в возможности представления причин, приводящих к тому или иному решению системы, в виде, понятном человеку.

показатель качества системы искусственного интеллекта: Степень соответствия представительного набора существенных (значимых) характеристик системы искусственного интеллекта требованиям, то есть потребностям или ожиданиям, которые установлены, обычно предполагаются или являются обязательными для этой системы.

Понятность (transparency): Свойство системы искусственного интеллекта, заключающееся в возможности открытого, исчерпывающего, доступного, четкого и понятного представления информации.

предвзятость, необъективность(bias): Свойство системы искусственного интеллекта, заключающееся в принятии ошибочных решений, связанных со статистической смещенностью обучающей выборки исходных данных.

Предсказуемость (predictability): Свойство системы искусственного интеллекта, заключающееся в способности принимать решения ожидаемым (естественным, приемлемым) для человека способом.

представительный набор существенных характеристик: Минимально необходимая и достаточная совокупность характеристик системы искусственного интеллекта, позволяющая потребителю, организациям, ответственным за регулирование вопросов создания и применения систем искусственного интеллекта, или любой другой заинтересованной стороне достоверно оценивать качество системы при решении конкретной прикладной задачи.

программное обеспечение: Упорядоченная последовательность инструкций (кодов) для вычислительного средства, находящаяся в памяти этого средства и представляющая собой описание алгоритма управления вычислительными средствами и действий с данными.

сильный (общий) искусственный интеллект: Способность технической системы, подобно человеку, мыслить, взаимодействовать, адаптироваться к изменяющимся условиям и решать другие задачи в области обработки информации, ассоциирующиеся с естественным интеллектом человека.

система искусственного интеллекта: Техническая система, в которой используются технологии искусственного интеллекта и обладающая искусственным интеллектом.

существенные (значимые) характеристики системы искусственного интеллекта: Характеристики системы искусственного интеллекта, определяющие его качество при решении конкретной прикладной задачи, подтверждение соответствия которых установленным требованиям может быть выполнено потребителем системы, организациями, ответственными за регулирование вопросов создания и применения систем искусственного интеллекта, или любой другой заинтересованной стороной

Примечание - Характеристики систем искусственного интеллекта, подтверждение соответствия которых установленным требованиям может быть выполнено исключительно разработчиком системы, не относятся к существенным.

техническая система: Целостная совокупность конечного числа взаимосвязанных материальных объектов, имеющая последовательно взаимодействующие сенсорную и исполнительную функциональные части, модель их предопределенного поведения в пространстве равновесных устойчивых состояний и способная при нахождении хотя бы в одном из них (целевом состоянии) самостоятельно в штатных условиях выполнять предусмотренные ее конструкцией потребительские функции.

технические средства: Аппаратные и программные средства, используемые для сбора, обработки, хранения, манипуляции и выдачи данных.

технологии искусственного интеллекта: Комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и

поиск решений без заранее заданного алгоритма) и получать результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека при решении задач компьютерного зрения, обработки естественного языка, распознавания и синтеза речи, поддержки принятия решений и других практически значимых задач обработки данных.

оцифровка: Процесс представления в цифровой форме данных, не являющихся дискретными.

оцифрованная сцена видеонаблюдения; ОСцВ: Сцена видеонаблюдения, представленная в цифровой форме после преобразования СцВ устройством формирования видеоизображений и оцифровки полученных видеоданных.

цифровое устройство формирования видеоизображений; ЦУФВ: Техническое средство, осуществляющее преобразование оптических данных различных диапазонов, в том числе с применением нанотехнологических решений, в цифровой формат.

объект сцены видеонаблюдения: Объект в сцене видеонаблюдения, анализ свойств и действий которого осуществляется посредством системы видеоаналитики.

свойства объекта: Совокупность характерных признаков объекта сцены видеонаблюдения на изображении или видеозаписи.

ситуация: Соответствие наблюдаемой на сцене видеонаблюдения совокупности (количественных и качественных) изменений или их отсутствия заданному описанию, подлежащее обнаружению системой видеоаналитики.

сценарий ситуации: Заданная совокупность или последовательность взаимосвязанных событий в сцене видеонаблюдения, характеризующая ситуацию.

класс ситуаций [сценариев]: Характеристика ситуаций [сценариев], классифицирующая принадлежность тех или иных ситуаций [сценариев] по области применения систем ситуационной видеоаналитики по основанию принадлежности к определенной отрасли (например, промышленное производство, здравоохранение, обеспечение безопасности) или сфере человеческой деятельности.

ситуационная видеоаналитика: Видеоаналитика, предназначенная для анализа ситуаций и (или) сценариев в сцене видеонаблюдения.

предиктивная видеоаналитика: Видеоаналитика, предназначенная для прогнозирования развития ситуаций и (или) сценариев в сцене видеонаблюдения.

метаданные: В отрасли видеоаналитики — это данные, получаемые в результате анализа видеоизображений системой видеоаналитики, описывающие сцену видеонаблюдения, ситуации, сценарии, происходящие на сцене видеонаблюдения, а также технические данные о видеоизображении: частота кадров, разрешение видеоизображения, формат компрессии и др.

зарегистрированное событие: Ситуация или сценарий в сцене видеонаблюдения, зарегистрированные в результате анализа видеоизображения системой видеоаналитики.

задержка обнаружения: Интервал времени между возникновением обнаруживаемой ситуации на сцене видеонаблюдения и временем формирования системой информационного сигнала об обнаружении ситуации.

условия применимости детектора: совокупность условий, относящихся к сцене видеонаблюдения, при которых детектор видеоаналитики обеспечивает характеристики обнаружения ситуаций не ниже требуемых.

Термины и определения, относящиеся к видам анализа

детекция [детектирование] объекта: Функция системы видеоаналитики, заключающаяся в автоматизированном определении положения и границ объекта на изображении в сцене видеонаблюдения.

классификация объекта: Функция системы видеоаналитики, заключающаяся в распознавании в сцене видеонаблюдения принадлежности объекта к определенному классу.

Примечание — Например: человек, животное, автомобиль, сумка, скамейка.

идентификация [распознавание] объекта: Функция системы видеоаналитики, заключающаяся в установлении соответствия экземпляра объекта в сцене видеонаблюдения по характерным при знакам объекту из предварительно сформированного перечня.

распознавание действий: Функция системы видеоаналитики, заключающаяся в распознавании и классификации заданных действий, совершаемых объектами сцены видеонаблюдения.

тепловая карта: Визуализированная статистическая информация о частоте возникновения (обнаружения) ситуаций и (или) сценариев в сцене видеонаблюдения.

Примечание — Наиболее распространенным вариантом визуализации является цветовая карта, наложенная поверх видеоизображения, в которой посредством цвета и насыщенности представлены частоты возникновения ситуаций и/или сценариев в разных участках видеосцены.

сегментация фона: Технология или процесс разделения видеосцены на подвижные объекты и стационарный фон.

реидентификация объекта: Функция системы видеоаналитики обнаруживать и идентифицировать объект на последовательности видеокадров как один и тот же, с учетом нахождения нового положения объекта в кадре при перемещении объекта или при смене области зрения видеокамеры.

трекинг: Обнаружение перемещения объекта из одной области видеосцены в другую за счет реидентификации движущегося в наблюдаемой сцене объекта.

межкамерный трекинг: Реидентификация движущегося в наблюдаемой сцене объекта при перемещении объекта между зонами наблюдения разных видеокамер.

подсчет объектов: Функция системы видеоаналитики, осуществляющая подсчет объектов определенного класса или классов в контролируемой зоне или подсчет объектов определенного класса или классов, пересекающих сцену видеонаблюдения или контролируемую зону в сцене видеонаблюдения

Термины и определения, относящиеся к сцене видеонаблюдения

условия освещенности: Описание освещенности, соответствующее определенному диапазону освещенности, а также равномерности (неравномерности) освещенности сцены или объектов в сцене и стабильности освещенности сцены или объектов в сцене.

контрастность изображения: Отношение яркостей наиболее светлого и темного участков видеоизображения, сформированного видеокамерой.

фон: Совокупность стационарных (неподвижных) объектов и частей сцены видеонаблюдения.

плотность потока объектов: Количество объектов, пересекших сцену видеонаблюдения или зону в сцене видеонаблюдения за единицу времени.

плотность расположения объектов: Количество объектов в сцене видеонаблюдения или в выделенной зоне видеосцены на единицу площади.

помехообразующие факторы: Совокупность факторов в сцене видеонаблюдения, препятствующих обнаружению заданных объекта, ситуации или сценария.

(**сигнальная) линия:** Виртуальная линия произвольной формы (прямая, ломаная, кривая) в сцене видеонаблюдения, представляющая собой виртуальную границу в данной сцене.

Примечание — Факт пересечения объектами сцены видеонаблюдения сигнальной линии используется для регистрации ситуаций и сценариев системами видеоаналитики.

(контролируемая) зона: Зона в сцене видеонаблюдения, внутри границ которой осуществляется обнаружение объектов, ситуаций или сценариев.

(охраняемый) периметр: Совокупность контролируемых зон на одной или нескольких видео камерах, объединенных по признаку принадлежности к единой физической области, на которой осуществляется видеонаблюдение.

непрерывный периметр: Свойство периметра, при котором обеспечивается фактическая непрерывность контролируемых границ физической области, на которой осуществляется видеонаблюдение.

Термины и определения, относящиеся к ситуациям и сценариям

оставленный предмет: Предмет (объект), внесенный в сцену видеонаблюдения человеком, другим объектом или иным способом, находящийся в сцене видеонаблюдения без движения более за данного периода времени.

принадлежность предмета человеку или объекту: Свойство предмета (объекта) в сцене видеонаблюдения, характеризующее его взаимосвязь с тем или иным человеком или объектом, при которой по видеоизображению возможно определение человека или объекта, внесшего предмет (объект) в сцену видеонаблюдения.

бесхозный предмет: Предмет (объект), оставленный в сцене видеонаблюдения, принадлежность которого определить невозможно.

унесенный предмет: Предмет (объект), изъятый из сцены видеонаблюдения человеком, другим объектом или иным способом.

исчезнувший предмет: Предмет (объект), изъятый из сцены видеонаблюдения без возможности определения человека или иного объекта, осуществившего изъятие.

оставление предмета: совокупность действий по оставлению предмета (объекта) в сцене видеонаблюдения человеком, другим объектом или иным способом.

скрытое [ая] оставление [закладка] предмета: Оставление предмета (объекта) в области сцены видеонаблюдения, в которой существенная часть предмета (объекта) заслонена от поля зрения видеокамеры иными объектами сцены видеонаблюдения (конструкциями, элементами интерьера, иными препятствиями), при этом идентификация и (или) классификация оставленного предмета (объекта) по видеоизображению в месте оставления затруднена или невозможна.

передача предмета другому лицу: Сценарий в сцене видеонаблюдения, при котором происходит передача какого-либо предмета или объекта от одного человека к другому.

Примечание — Различается как непосредственная передача предмета (так называемый сценарий «из рук в руки»), так и передача посредством оставления предмета одним лицом с последующим подбором предмета другим лицом.

переброс предмета: Сценарий, при котором в сцене видеонаблюдения осуществляется переброс предмета или объекта через другой объект, предмет или конструкцию.

движение в запрещенной зоне: Сценарий, при котором тревожным считается факт движения объекта в определенной зоне.

сценарий «Движение в запрещенном направлении»: Сценарий ситуации в регистрируемой сцене, по которому тревожным считается факт движения объекта (человека, транспортного средства, животного) в запрещенном направлении относительно условно заданных границ.

сценарий «Стерильная зона»: Сценарий ситуации в регистрируемой сцене, по которому тревожным считается факт появления объекта (человека, транспортного

средства, животного) в поле зрения камеры, пересечения им условно заданной запрещенной линии либо нахождения в запрещенной зоне.

сценарий «Нетипичные изменения в сцене»: Сценарий ситуации в регистрируемой сцене, по которому тревожным считается снижение качества видеосигнала (затемнение, засветка, расфокусировка).

перемещение объекта из одной зоны в другую: Перемещение человека или иного объекта из одной области сцены видеонаблюдения в другую.

пересечение линии: Сценарий в сцене видеонаблюдения, при котором осуществляется пере сечение сигнальной линии движущимся объектом.

возгорание [открытое пламя]: Сценарий, при котором в сцене видеонаблюдения присутствует открытый огонь.

дым: Сценарий, при котором в сцене видеонаблюдения присутствует дым либо источник дыма.

задымление [туман]: Снижение прозрачности воздуха или газовой среды в сцене видео наблюдения, связанное с повышением концентрации дыма, водяного или иного пара.

скопление людей: Сценарий в регистрируемой сцене, при котором в контролируемой зоне находится более одного человека.

очередь: Скопление людей или других объектов, организованное в порядке последовательно го доступа к тому или иному участку сцены видеонаблюдения.

толпа [образование толпы]: Сценарий в регистрируемой сцене, при котором в контролируемой зоне находится множество людей, превышающее заданное пороговое количество.

Примечание — Точного порогового количества человек, при котором скопление людей можно характеризовать как толпу, не существует. В системах видеоаналитики применяются различные способы оценки критерия толпы: по количеству людей в контролируемой зоне, по плотности заполнения зоны людьми и другие. В общем случае фактические критерии сценариев «скопление людей» и «образование толпы» устанавливаются пользователями систем видеоаналитики в зависимости от регламентов объекта видеонаблюдения.

праздношатание: Сценарий в наблюдаемой сцене, при котором человек или группа людей находятся или перемещаются в пределах контролируемой зоны дольше порогового заданного времени и цель нахождения данного человека или группы людей в контролируемой зоне не установлена.

нетипичное поведение: Поведение объектов в сцене видеонаблюдения, статистически значимо отличающееся от поведения, наиболее характерного для наблюдаемой сцены.

Примечание — Например, в зависимости от сцены видеонаблюдения, к нетипичному поведению могут быть отнесены: бег, праздношатание, проявление агрессивности, активная жестикуляция, остановившиеся на ма гистрали транспортные средства и другие ситуации и действия.

СОКРАЩЕНИЯ

АС - автоматизированная система;
ЖЦ - жизненный цикл;
ИНС - искусственная нейронная сеть;
ИТ - информационная технология;
ПО - программное обеспечение;
ПС - программное средство;
ТС - транспортное средство.

ЗАКЛЮЧЕНИЕ

В настоящее время применение систем видеонаблюдения является неотъемлемым признаком развитых стран, движущихся по пути построения «умных» городов. В эпоху развития искусственного интеллекта возможности данных систем не ограничиваются просто съемкой или обезличенным видеонаблюдением, а предоставляют возможности распознавания и полной идентификации человека. В связи с тем, что процесс информатизации привел к созданию многочисленных баз данных, включая автоматизированные информационные системы персональных данных, интеграция баз данных с системами видеонаблюдения в том числе видеоаналитики является вопросом времени.

Впоследствии полная идентификация человека станет возможной в автоматическом режиме. Следует отметить положительный аспект применения систем видеоаналитики: сократилось количество противоправных действий, повысилась раскрываемость преступлений, появилась возможность предотвращения крупных аварий и т. д. С другой стороны, вопросы неприкосновенности частной жизни и обеспечения информационной безопасности личности выходят на первый план. Потому необходимо на правовом уровне обеспечивать баланс интересов государства и личности. Со стороны использования систем видеонаблюдения государством, следует обеспечивать защиту на техническом, организационном (строгая регламентация доступа, ответственность лиц, имеющих доступ к системам, и др.) и правовом (с точки зрения защиты права на неприкосновенность частной жизни) уровнях. В связи с тем, что видеокамеры широко применяются частными лицами (видеорегистраторы, съемки блогеров, самовольно установленные камеры видеонаблюдения и др.), угроза для человека в части сохранения приватности возрастает.

С учетом имеющихся технических возможностей и с использованием общедоступных персональных данных, распространенных самим человеком (социальные сети и др.), идентификация человека также возможна. Полагаем своевременным дальнейшее совершенствование законодательства в сфере защиты персональных данных путем выделения отдельного подвида – визуальных персональных данных – и разработки правового регулирования в данной сфере. В том числе: рассмотрение случаев, когда можно применять собранную с помощью использования систем видеоаналитики биометрическую информацию (например, в расследовании преступлений и т. п.); кто (круг лиц) и каким образом может использовать данную информацию; каким образом граждане могут оспаривать и исключать информацию о себе из таких баз

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Зинин А.М., Подволодский И.Н. Габитоскопия: Учебное пособие. М.: Юрлитинформ. 2006. С. 101.
2. Снетков В.А. Габитоскопия: Учебник. Волгоград: ВСШ МВД СССР. 1979. С. 76.
3. Словарь основных терминов судебно-портретной экспертизы. М.: 1977. С. 22.
4. Зинин А.М., Подволодский И.Н. Габитоскопия: Учебное пособие. М.: Юрлитинформ. 2006. С 102.
5. Орлов П.Г. Идентификация личности по фотокарточкам: Пособие. М.: ВКШ КГБ СССР. 1974. С. 59; Зинин А.М., Подволодский И.Н. Габитоскопия: Учебное пособие. М.: Юрлитинформ, 2006. С. 34 и др.Селиванов Н.А., Танасевич В.Г., Эйсман А.А. и др. Советская криминалистика. Теоретические проблемы, - М.: Изд-во «Юридическая литература», 1978. - С. 125.
6. Закон О персональных данных и их защите ЗРК от 21 мая 2013 года N 94-V. (с изменениями и дополнениями по состоянию на *20.06.2024*г.) https://adilet.zan.kz/rus/docs/Z1300000094
7. Приказ Председателя Комитета национальной безопасности Республики Казахстан от 27 октября 2020 года № 69-қе. Зарегистрирован в Министерстве юстиции Республики Казахстан 30 ноября 2020 года № 21693 - Об утверждении Правил функционирования Национальной системы видеомониторинга[Электронный ресурс] https://adilet.zan.kz/rus/docs/V2000021693
8. Инструкция по использованию информации о внешности человека в раскрытии и расследовании преступлений, утвержденная Приказом ГУВД по Иркутской области №1020 от 3 марта 2000 года.
9. Приказ МВД России от 29 июня 2005 г. № 511 «Вопросы организации производства судебных экспертиз в экспертно криминалистических подразделениях органов внутренних дел Российской Федерации» [Электронный ресурс] : офиц. текст: по состоянию на 15 окт.2012 г. : зарегистр. в Минюсте России 23 авг. 2005 г. № 6931. - Доступ из справ.- правовой системы «КонсультантПлюс».
10. Моисеева Т. Ф. Биометрические технологии в аспекте экспертных исследований // Сборник статей: Актуальные проблемы теории и практики уголовного судопроизводства и криминалистики. Часть III: Вопросы теории и практики судебной экспертизы. - М.: Академия управления МВД России, 2004. - С. 56-59
11. Морзеев Ю. Современные биометрические решения в системах безопасности // Компьютер-Пресс. - 2003. - № 3. - С. 76-81.
12. Иванов А.И. Биометрическая идентификация личности по динамике подсознательных движений: Монография. - Пенза: Изд-во Пенз. гос ун-та, 2000. - С. 16- 17.
13. Барсуков В. С. Биоключ - путь к безопасности // Специальная техника. - № 3. - 2003.-С. 26-35.
14. Барсуков В.С., Зайцев А.В., Пономарев А.А. Идентификация личности - ключевая проблема безопасности // Специальная техника. - 2005. - № 3. - С. 32-40.
15. Сафонов А. А., Булгаков В. Г., Варченко И. А. Криминалистическое исследование динамических признаков человека: история и современное состояние // Общество и право. 2010 № 3 (30) С. 250-257.

16. Сафонов А. А., Булгаков В. Г., Варченко И. А. Криминалистическое исследование динамических признаков человека: история и современное состояние // Общество и право. 2010 № 3 (30) С. 250-257.
17. Судебная портретная экспертиза на современном этапе. Проблемы и пути решения: Материалы Всероссийской конференции (28 февраля 2017 года). – М.: Научно-практический журнал «Энциклопедия Судебной Экспертизы». № 2 (13) 2017 – 221 с.; Судебная портретная экспертиза на современном этапе. Проблемы и пути решения: Материалы Всероссийской конференции (29 ноября 2018 года). – М.: Энциклопедия Судебной Экспертизы: Научно-практический журнал. № 4 (19) 2018. – 214 с.
18. Использование криминалистически значимой информации о динамических признаках человека в раскрытии и расследовании преступлений: монография / под ред. докт. юрид. наук, проф. А.М. Зинина. — М.: Юрлитин- форм, 2013. — 160 с.
19. Основы судебной экспертизы / отв. ред. Ю.Г. Корухов. 4.1. Курс общей теории: методическое пособие для экспертов, следователей и судей. М.: РФЦСЭ, 1997. С. 124,128; Каганов А. Ш. Криминалистическая идентификация личности по голосу и звучащей речи. М.: Юрлит-информ, 2009. С. 87-95.
20. Дильбарханова Ж. Р. Криминалистическое исследование внешнего облика человека: учебно-практическое пособие. – Алматы: Юрист, 2008. – 100 с.
21. Распознавание походки с помощью изображения энтропии походки Халид Башир, Тао Сян, Шаоган Гун. Школа электронной инженерии и информатики, Лондонский университет королевы Марии, Великобритания; Пирамидальное движение Фишера для распознавания многоракурсной походки //
22. Булгаков В. Г., Булгакова Е. В. Роль информации о динамических признаках человека в розыскном портрете неизвестного преступника // Вестник Волгоградского государственного университета. Серия 5, Юриспруденция, 2011 № 2 (15), С. 149-152.
23. Бернштейн Н.А. Биомеханика и физиология движений / под ред. В.П. Зинчеко. М.-Воронеж: Изд-во «Институт практической психологии»; НПО «МОДЕК», 1997. 608 с.
24. Использование криминалистически значимой информации о динамических признаках человека в раскрытии и расследовании преступлений: монография / под ред. докт. юрид. наук, проф. А.М. Зинина. — М.: Юрлитин- форм, 2013. — 160 с.
25. Виниченко И.Ф., *Житников В.С., Зинин* А.М. и др. Криминалистическое описание внешности *человека.* М.: МЮИ МВД России; Щит-М, 1999. С. 128-142.
26. Кацитадзе З. И. Особенности следов ходьбы при некоторых патологиях нижних конечностей (к вопросу судебно-медицинского отождествления личности по следам ходьбы): Автореф. дисс. … канд. мед. наук. М., НИИ судебной медицины МЗ СССР, 1954. С. 10-11.
27. Булгаков В. Г., Булгакова Е. В. Роль информации о динамических признаках человека в розыскном портрете неизвестного преступника // Вестник Волгоградского государственного университета. Серия 5, Юриспруденция, 2011 № 2 (15), С. 149-152.
28. Сафонов А. А., Булгаков В. Г., Варченко И. А. Криминалистическое исследование динамических признаков человека: история и современное состояние // Общество и право. 2010 № 3 (30) С. 250-257
29. Buchanan B.G., Headrick T.E. Some Speculation About Artificial Intelligence and Legal Reasoning // Stanford Law Review. 1970. Vol. 23. No. 1. P. 40-62. [Электронный ресурс] (дата обращения:06.06.2024)
30. McCarty L.T. Reflections on «Taxman»: An Experiment in Artificial Intelligence and Legal Reasoning // Harvard Law Review 1977. Vol. 90. P. 837-893. 16 Susskind R.E.

Expert systems in law: a jurisprudential approach to artificial intelligence and legal reasoning // Modern Law Review. 1986. Vol. 49. Iss. 2. P. 168-194. [Электронный ресурс] (дата обращения:06.07.2024)
31. Computer Science and Law. An Advanced Course. Edited by Bryan Niblett. Cambridge: Cambridge University Press. 1980. 232 p. [Электронный ресурс] (дата обращения:06.06.2024)
32. Ciampi C. Artificial Intelligence and Legal Information Systems. Vol. I: Edited Versions of Selected Papers from the International Conference on «Logic, Informatics, Law». Florence, Italy, April 1981, North-Holland, Amsterdam. 1982. 476 p. [Электронный ресурс] (дата обращения:06.06.2024)
33. Rissland E.L. Artificial Intelligence and Law: Stepping Stones to a Model of Legal Reasoning // Yale Law Journal. 1990. Vol. 99. No 8. P. 1957-1981. [Электронный ресурс] (дата обращения:06.06.2024)
34. Ashley K.D. Modeling Legal Argument: Reasoning with Cases and Hypotheticals. Cambridge, Massachusetts: MIT Press. 1990. 329 p. [Электронный ресурс] (дата обращения:06.06.2024)
35. Ashley K.D. Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age. Cambridge University Press. 2017. 450 p. [Электронный ресурс] (дата обращения:09.07.2024)
36. Stone P. et al. Artificial Intelligence and Life in 2030. One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016. Stanford. Stanford University. 2016. 52 p.
37. Шрейнер, И.Ю. Внедрение системы «умный город» для повышения безопасности городской среды / И.Ю. Шрейнер, И.С. Пашкова // Безопасность городской среды : материалы IV Междунар. научно-практ. конф., Омск, 16– 18 нояб. 2016 г. – Омск : Омский гос. техн. ун-т, 2017. – С. 314–316. [Электронный ресурс] (дата обращения:06.06.2024)
38. Тургель, И.Д. Управление в области защиты окружающей среды городов как элемент Smartcity: опыт России и Казахстана / И.Д. Тургель, Л.Л. Божк, Е.А. Ульянова // Весенние дни науки ВШЭМ : сб. докл. Междунар. конф. студентов и молодых ученых, Екатеринбург, 17–19 апр. 2019 г.. – Екатеринбург : ООО «Изд-во УМЦ УПИ», 2019. – С. 656–658.
39. Климович, А.П. Влияние цифровых технологий на современное общество. Пример системы рейтинга социального кредита в Китае / А.П. Климович // Цифровая социология. – 2020. – Т. 3. – № 3. – С. 35–44.
40. Руф, Ю.Н. Возможности внедрения системы социального рейтинга в России в условиях цифровизации / Ю.Н. Руф, Д.В. Каримова // Вопросы инновационной экономики. – 2010. – Т. 10. – № 2. – С. 881 – 890. doi: 10.18334/vinec.10.2.100772. 2021 ВЕСТНИК ПОЛОЦКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА. Серия D 92
41. Богуш, Р.П. Алгоритм сопровождения людей на видеопоследовательностях с использованием сверточных нейронных сетей для видеонаблюдения внутри помещений / Р.П. Богуш, И.Ю. Захарова // Компьютерная оптика. – 2020. – Т.44. – № 1 – С. 109–116. doi: 10.18287/2412-6179-CO-565.
42. Богуш, Р.П. Обнаружение объектов на изображениях с большим разрешением на основе их пирамидально-блочной обработки / Р.П. Богуш, И.Ю. Захарова, С.В. Абламейко // Информатика. – 2020. – № 2 – С. 7–16. doi:10.37661/1816- 0301-2020-17-2-7-16.
43. Goold, B.J. CCTV and Policing / B.J. Goold. – Oxford University Press, 2004. – P. 2

44. Facing the Camera -The Protection of Freedoms Act 2012 & The Surveillance Camera Code of Practice. [Электронный ресурс] (дата обращения : 04.07.2024).
45. Exposing.ai. Duke MTMC. Available from: https://exposing.ai/duke_mtmc. [Электронный ресурс] (дата обращения : 04.07.2024).
46. Dataset and Code. Available from: https://www.pkuvmc.com/dataset.html. [Электронный ресурс] (дата обращения 04.07.2024).
47. Li W., Zhao R., Xiao T., Wang X. Deep Filter Pairing Neural Network for Person Re-identification. DeepReID: IEEE Conference on Computer Vision and Pattern Recognition. 2014. P. 152-159. Available from: https://doi.org/10.1109/ CVPR.2014.27. [Электронный ресурс] (а дата обращения: 10.08.2024).
48. Vil’tovskij D. Personal’nye dannye uslozhnjat zhizn’ rabotodateljam [Personal data will make life difficult for employers]. Available from: https://neg.by/novosti/otkrytj/personalnye-dannye-uslozhnyat-zhizn-rabotodatelyam. [Электронный ресурс] (дата обращения: 10.11.2021). (Russian).
49. Абламейко, М. С. Защита визуальных персональных данных: правовые аспекты / М. С. Абламейко // Веб-программирование и интернет-технологии WebConf2021: материалы 5-й Международной научно-практической конференции, Минск, 18-21 мая 2021 г. / БГУ, Механико-математический фак.; редкол.: И. М. Галкин (отв. ред.) [и др.]. - Минск: БГУ, 2021. - 400 с. - Деп. в БГУ 07.05.2021, № 005207052021. [Электронный ресурс] (а дата обращения: 05.09.2024).