ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 70268.1— 2023 (ИСО/МЭК 30137-1: 2019)

Информационные технологии

БИОМЕТРИЯ

Применение биометрии в системах видеонаблюдения

Часть 1

Проектирование систем и спецификация

(ISO/IEC 30137-1:2019, Information technology — Use of biometrics in video surveillance systems — Part 1: System design and specification, MOD)

Издание официальное

Москва
Российский институт стандартизации
2023

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Некоммерческим партнерством «Русское общество содействия развитию биометрических технологий, систем и коммуникаций» (Некоммерческое партнерство «Русское биометрическое общество») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4, при консультативной поддержке Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)» (МГТУ им. Н.Э. Баумана)

2 ВНЕСЕН Техническими комитетами по стандартизации ТК 098 «Биометрия и биомониторинг» и ТК 441 «Нанотехнологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 17 апреля 2023 г. № 240-ст

4 Настоящий стандарт является модифицированным по отношению к международному стандарту ИСО/МЭК 30137-1:2019 «Информационные технологии. Применение биометрии в системах видеонаблюдения. Часть 1. Проектирование систем и спецификация» (ISO/IEC 30137-1:2019 «Information technology — Use of biometrics in video surveillance systems — Part 1: System design and specification», MOD) путем изменения отдельных фраз (слов, значений показателей, ссылок), которые выделены в тексте курсивом, а также путем изменения его структуры для приведения в соответствие с правилами, установленными в ГОСТ 1.5—2001 (подразделы 4.2 и 4.3).

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте, приведены в дополнительном приложении ДА.

Сопоставление структуры настоящего стандарта со структурой указанного международного стандарта приведено в дополнительном приложении ДБ

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые элементы настоящего стандарта могут быть объектами патентных прав. Федеральное агентство по техническому регулированию и метрологии не несет ответственности за установление подлинности каких-либо или всех таких патентных прав

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© ISO, 2019
© IEC, 2019
© Оформление. ФГБУ «Институт стандартизации», 2023

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 2
3 Термины, определения и сокращения 2
3.1 Термины, связанные с целевым субъектом 2
3.2 Термины, связанные с СВН 3
3.3 Термины, связанные с биометрической системой 3
3.4 Термины, связанные с условиями окружающей среды/сценария 4
3.5 Сокращения 4
4 Архитектура 4
5 Сценарии использования 6
5.1 Общие положения 6
5.2 Сценарии постсобытийного использования 6
5.3 Сценарии использования в режиме реального времени 7
5.4 Сценарии регистрации 7
6 Спецификация аппаратного и программного обеспечения 7
6.1 Общие положения 7
6.2 Физические условия 7
6.3 Условия освещения 8
6.4 Обеспечение фронтального положения 8
6.5 Камеры и инфраструктура 8
6.6 Биометрическая система 14
6.7 Вычислительные требования 16
6.8 Спецификация базы биометрических контрольных шаблонов 17
7 Работа с несколькими камерами 19
8 Интерфейсы для сопутствующего программного обеспечения 19
9 Руководство по поддержке оператора 19
10 Требования и рекомендации по проектированию системы 20
10.1 Общие положения 20
10.2 Формирование бизнес-требований 20
10.3 Обследование объекта 21
10.4 Размер и содержание списка наблюдения 22
10.5 Требования к производительности 22
10.6 Данные и метаданные изображений 23
Приложение А (рекомендуемое) Методы и приложения видеоаналитики, связанные с биометрическим распознаванием 24
Приложение В (рекомендуемое) Социальные аспекты и процессы управления 27
Приложение С (рекомендуемое) Измерения при получении последовательности изображений 29
Приложение ДА (справочное) Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте 29
Приложение ДБ (справочное) Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта 30
Библиография 31

Введение

Значительные улучшения в производительности технологий автоматического распознавания лиц (АРЛ) привели к появлению таких приложений, как автоматический пограничный контроль с использованием изображений лиц, хранимых в электронных паспортах и формируемых в системе. Формирование изображений лиц для верификации проводится в специально разработанных условиях сбора изображений с равномерной освещенностью и оптимальным положением головы. Успех систем АРЛ первого поколения привел к появлению приложений, в которых условия сбора изображений могут значительно отличаться от оптимальных. Низкая производительность таких приложений может потребовать большего участия обученного персонала.

Серия стандартов *«Информационные технологии. Биометрия. Применение биометрии в системах видеонаблюдения»* определяет использование биометрических технологий в системах интеллектуального видеонаблюдения (СВН), схему испытаний производительности таких систем и формирования отчетности, а также процедуры для определения достоверных данных и аннотирования видеоданных для целей испытаний.

Настоящий стандарт определяет архитектуру, сценарии использования и требования по проектированию систем. Сценарии использования включают оповещение в реальном времени о присутствии интересующих лиц, использование правоохранительными органами, например просмотр видеозаписи после события с одной или нескольких камер по предварительно заполненным спискам наблюдения, а также коммерческое использование, например идентификация лиц с обслуживанием по приоритету и лиц, добавленных в список наблюдения после анализа поведения по видеоизображению.

Другие сценарии использования включают измерение плотности толпы и определение количества людей, пересекающих заданную точку. Информация о данных сценариях включена в приложение А.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

БИОМЕТРИЯ

Применение биометрии в системах видеонаблюдения

Часть 1

Проектирование систем и спецификация

Information technology. Biometrics. Use of biometrics in video surveillance systems.
Part 1. System design and specification

Дата введения — 2023—04—30

1 Область применения

Серия стандартов *«Информационные технологии. Биометрия. Применение биометрии в системах видеонаблюдения»* определяет использование биометрических данных в СВН, также известных как системы телевидения замкнутого контура (CCTV), для ряда сценариев, включая работу в режиме реального времени со списками наблюдения и постсобытийным анализом видеоданных. Настоящий стандарт содержит требования и рекомендации по распознаванию лица, но включает требования и рекомендации по другим биометрическим модальностям, например походки.

Настоящий стандарт:

- определяет термины для использования в спецификации биометрических технологий в СВН, в т. ч. метрики эксплуатационных характеристик;
- предоставляет руководство по выбору типов камер, размещению камер, характеристик изображения и т. д. для обеспечения производительности биометрического распознавания в СВН;
- предоставляет руководство по формированию списка наблюдения, по которому проводится сравнение изображений лиц из СВН, включая выбор изображений приемлемого качества и размер списка наблюдения в соответствии с требованиями к производительности;
- предоставляет рекомендации по форматам данных изображений лиц и другой соответствующей информации (включая метаданные), полученной из видеозаписей списков наблюдения или из наблюдений операторов;
- определяет общие принципы поддержки оператора СВН, включая пользовательские интерфейсы и процессы, обеспечивающие эффективную и результативную работу, и определяет необходимость проведения обучения персонала.

Настоящий стандарт предоставляет информацию о задачах в СВН, связанных с распознаванием и детектированием, таких как:

- оценка плотности толпы;
- определение закономерностей передвижения индивидов;
- идентификация индивидов, наблюдаемых более чем на одной камере;
- использование других биометрических модальностей, таких как походка или радужная оболочка глаза;
- определение характеристик людей, например оценка пола и возраста;
- видеоаналитика для измерения длины очереди или оповещения о брошенном багаже.

Издание официальное

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ ISO/IEC 2382-37 Информационные технологии. Словарь. Часть 37. Биометрия

ГОСТ Р 58292 (ИСО/МЭК 19795-2:2007) Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний

ГОСТ Р 58624.1 (ИСО/МЭК 30107-1:2016) Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура

ГОСТ Р 58624.2 (ИСО/МЭК 30107-2:2017) Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 2. Форматы данных

ГОСТ Р 58624.3 (ИСО/МЭК 30107-3:2017) Информационные технологии. Биометрия. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний

ГОСТ Р ИСО/МЭК 19794-5 Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

В настоящем стандарте применены термины по *ГОСТ ISO/IEC 2382-37, ГОСТ Р 58624.1*, а также следующие термины с соответствующими определениями:

3.1 Термины, связанные с целевым субъектом

3.1.1 **оператор** (operator): Индивид, ответственный за постоянную работу системы.

Примечание — Это может включать настройку камер видеонаблюдения, выбор данных для биометрического приложения и действия в соответствии с результатом биометрического сравнения.

3.1.2 **целевой субъект** (target subject): Индивид, представляющий интерес.

Примечание — Как правило, целевой субъект внесен в список наблюдения (*3.1.3*). При этом в некоторых сценариях субъекты являются целевыми, потому что должны быть внесены в список наблюдения.

3.1.3 **список наблюдений** (watchlist): Список целевых субъектов (*3.1.2*) и связанных с ними биометрических шаблонов для детектирования приложением СВН.

Примечания

1 Список наблюдения может быть списком индивидов с обслуживанием по приоритету (например, VIP-клиенты или премиум-клиенты). Такой список могут называть «белым списком».

2 Список наблюдения может быть списком «разыскиваемых» индивидов, которым следует отказать в доступе к помещениям или услугам. Такой список могут называть «черным списком».

3 Система может иметь несколько списков наблюдения для разных групп целевых субъектов с разными метриками эксплуатационных характеристик.

4 В случае обратного отслеживания (3.3.1) целевого субъекта список наблюдения обычно включает один целевой субъект (*3.1.2*), а в случае группы целевых субъектов — несколько целевых субъектов.

3.2 Термины, связанные с СВН

3.2.1 **кодек** (codec): Компьютерная программа для кодирования или декодирования потока цифровых данных или сигнала.

3.2.2 **коэффициент сжатия** (compression ratio): Отношение размера сжатого файла к размеру несжатого файла.

3.2.3 **отбракованные кадры** (dropped frames): Кадры видеоизображения, которые не обрабатываются или являются недоступными для детектирования лиц и создания биометрических контрольных шаблонов.

Примечание — Как правило, измеряется в числе отбракованных кадров в секунду или процентах отбракованных кадров в секунду.

3.2.4 **кадр** (frame): Отдельное изображение, показанное как часть последовательности изображений в видеопотоке.

3.2.5 **частота кадров** (frame rate): Периодичность, с которой устройство формирования изображений создает уникальные последовательные изображения, называемые кадрами (3.2.4).

Примечание — Как правило, единицей измерения частоты кадров является кадр/с (fps).

3.2.6 **размер кадра** (frame size): Габариты кадра в виде числа пикселей по горизонтали и вертикали или в виде общего числа пикселей.

3.2.7 **постобработка** (post-processing): Этапы, проводимые после процесса биометрического сравнения.

Пример — Решения по сортировке на основе объединения показателей качества и результатов биометрического сравнения.

3.2.8 **предварительная обработка** (pre-processing): Этапы, проводимые до процесса биометрического сравнения.

Пример — Улучшение качества изображения, детектирование субъекта и извлечение биометрических признаков.

3.2.9 **разрешение** (resolution): Мера размера деталей, которые могут быть сохранены на изображении.

Примечание — Как правило, единицей измерения разрешения является пиксель/мм.

3.2.10 **отслеживание субъекта** (subject tracking): Процесс объединения нескольких биометрических образцов одного человека, в том числе с нескольких камер, для предотвращения отдельных оповещений об детектировании одного и того же целевого субъекта (3.1.2).

3.2.11 **система управления видеонаблюдением;** СУВ (video management system; VMS): Компонент системы видеонаблюдения (3.2.12), в котором проводится сбор видеопотоков с камер и других источников, запись видеопотоков на запоминающее устройство и предоставление интерфейса для просмотра видеопотока в реальном времени и для произвольного доступа к записанному видеоизображению по времени.

3.2.12 **система видеонаблюдения;** СВН (video surveillance system; VSS): Система для наблюдения за охраняемой зоной, включающая камеры, оборудование для наблюдения и оборудование для передачи данных и управления.

3.3 Термины, связанные с биометрической системой

3.3.1 **обратное отслеживание** (back-tracking): Поиск заданного изображения (изображений) лица/индивида по всем видеопотокам, где оно может присутствовать.

Примечание — Обратное отслеживание может использовать или не использовать биометрию лица.

3.3.2 **детектирование лица** (face detection): Определение наличия лица на кадре (3.2.4) и местоположения каждого лица на кадре.

Примечание — Детектирование лица — это первый этап процесса распознавания лиц.

3.3.3 **постсобытийный анализ** (post event analysis): Анализ данных, снятых камерами видеонаблюдения до проведения анализа, не в режиме реального времени.

Примечание — Проводится после инцидента или события для выявления потенциальных подозреваемых.

3.3.4 **анализ в реальном времени** (real time analysis): Оперативная обработка данных видеонаблюдения по мере их сбора.

Примечание — Проводится для идентификации индивидов из списка наблюдения для принятия срочных мер.

3.3.5 **зона распознавания** (zone of recognition): Трехмерное пространство в поле зрения камеры, в котором выполняются условия формирования изображения для надежного биометрического распознавания.

Примечание — Как правило, зона распознавания меньше, чем поле зрения камеры, например не все лица в поле зрения камеры находятся в фокусе или отображаются с минимальным расстоянием между глазами (IED).

3.4 Термины, связанные с условиями окружающей среды/сценария

3.4.1 **точка притяжения** (atrractor): Визуальная или акустическая подсказка в окружающей среде, которая побуждает людей смотреть в определенном направлении (например, в сторону камеры для распознавания лица) и используется для повышения эксплуатационных характеристик системы распознавания.

3.4.2 **узкое место** (choke point): Точка скопления или препятствие, через которое проходят индивиды.

3.5 Сокращения

В настоящем стандарте применены следующие сокращения:

АРЛ — автоматическое распознавание лица (automatic face recognition, AFR);

ВОД — вероятность отказа детектирования;

ВОСД — вероятность отказа сбора данных;

ВИПИ — вероятность истинно положительной идентификации;

ВЛОИ — вероятность ложноотрицательной идентификации;

ВЛПИ — вероятность ложноположительной идентификации;

ВОКПА — вероятность ошибки классификации предъявления при атаке;

ВОКПБП — вероятность ошибки классификации подлинных биометрических предъявлений;

ВООПА — вероятность отсутствия ответа на предъявление артефакта;

ВООПБП — вероятность отсутствия ответа на подлинное биометрическое предъявление;

ДОПО — длительность обработки подсистемой обнаружения атаки на биометрическое предъявление;

ОАБП — обнаружение атаки на биометрическое предъявление;

IED — расстояние между глазами (inter-eye distance);

PTZ-камера — камера, которая поддерживает удаленное управление направлением и увеличением (pan-tilt-zoom-camera);

XMP — платформа расширяемых метаданных (extensible metadata platform).

4 Архитектура

На рисунке 1 показан поток процессов в типичной СВН с биометрическим распознаванием, имеющей следующие компоненты:

1) камеры видеонаблюдения, размещенные для сбора изображений, пригодных для сравнения с изображениями в списке наблюдения;

2) СУВ и инфраструктура для организации и передачи отснятого материала с нескольких камер на главный сервер и систему хранения;

3) программное обеспечение для детектирования и отслеживания лиц (и/или других биометрических признаков) в видеопотоке и для создания наборов биометрических признаков в формате, разработанном поставщиком системы биометрического распознавания. Набор биометрических признаков может создаваться путем объединения биометрических признаков, извлеченных из нескольких изображений лиц одного индивида по мере обработки новых кадров видеоизображения;

4) программное обеспечение для сравнения и принятия решений, как правило, разработанное поставщиком биометрической системы и устанавливающее распознавание индивида из списка наблюдения. Критерии сравнения и пороговые значения для принятия решения могут быть разными для групп индивидов в списке наблюдения. Например, если не будут распознаны индивиды из групп с низким уровнем риска, то последствия будут минимальные, а в случае групп с высоким уровнем риска необходимо максимально быстрое распознавание индивидов;

5) подсистема оповещений, генерируемых автоматизированной системой и передаваемых оператору для оценки;

6) подсистема поддержки принятия решений для оператора по реагированию на оповещения;

7) ссылки на системы аналитики для записи событий и принятых решений, а также для доступа к дополнительной информации, например предыдущие случаи аналогичного сравнения с индивидом в списке наблюдения и руководство по соответствующим действиям, которые необходимо предпринять;

8) «шина» управления системой, которая обеспечивает настройку и работу основных компонентов системы биометрического распознавания в соответствии с уровнем угрозы, рабочей нагрузкой операторов, временем суток и т. д., а также поддерживает объединение результатов распознаваний с разных камер в области наблюдения.

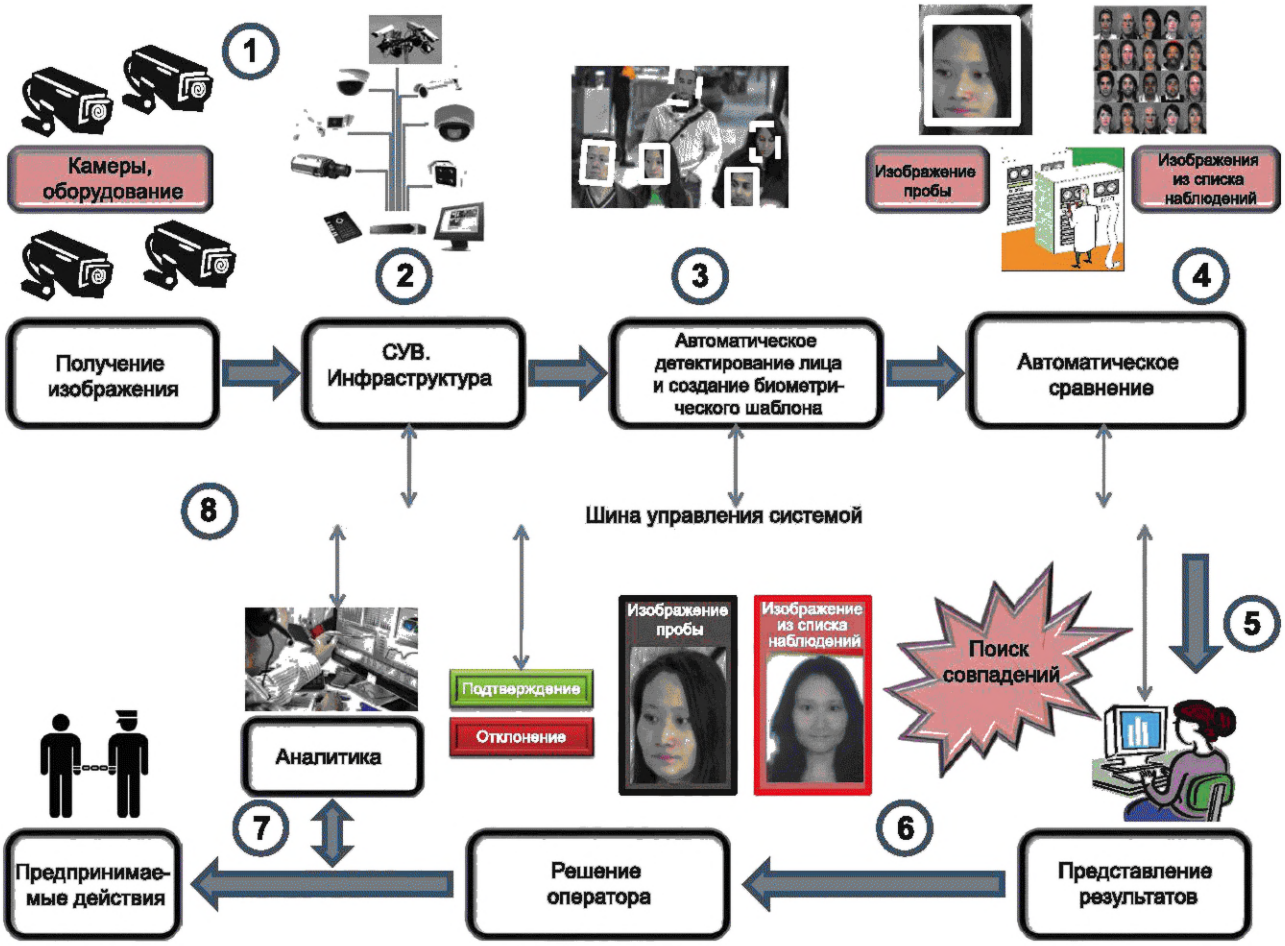


Рисунок 1 — Компоненты СВН с биометрическим распознаванием

На рисунке 1 показан пример сервер-ориентированной архитектуры. Могут быть использованы другие модели архитектуры, например распределенные архитектуры, использующие периферийные вычисления с проведением части обработки на видеокамере или предоставляющие доступ к камерам и вычислительным ресурсам в интеллектуальных устройствах, таких как смартфоны и ПК.

5 Сценарии использования

5.1 Общие положения

В настоящем разделе приведены примеры использования биометрии в СВН в различных сценариях, в том числе:

- оповещение о присутствии индивидов, представляющих интерес для полиции и правоохранительных органов, а также частных охранных предприятий;
- идентификация лиц на видеоизображениях, собранных после значимых событий или инцидентов, для полиции и правоохранительных органов;
- коммерческое использование для оповещения о присутствии лиц, представляющих интерес, для предоставления определенного уровня обслуживания *или получения услуги*;
- управление потоком людей или очередями в коммерческих или государственных учреждениях, в том числе в соответствии с определенным уровнем обслуживания;
- обеспечение качества и поддержка клиентов пограничными службами и службами работы с клиентами, например после жалобы или происшествия.

Сценарии использования включают три категории: постсобытийные, в режиме реального времени и регистрации (регистрация может проводиться в режиме реального времени или после события). В следующих подразделах приведены некоторые распространенные сценарии использования с точки зрения требований к производительности и ролей, выполняемых различными компонентами системы, включая обязанности оператора системы.

5.2 Сценарии постсобытийного использования

В сценариях постсобытийного использования целью является надежное детектирование, автоматическое извлечение биометрических признаков и поиск большого количества целевых субъектов по одному или нескольким спискам наблюдения или базам данных для идентификации возможных подозреваемых.

Данные сценарии использования являются сложными, так как в большинстве случаев качество и расположение видеокамер будет вне контроля оператора биометрической системы и видеокамеры не будут установлены с учетом использования биометрической системы.

Как правило, оператор выполняет роль эксперта и выбирает изображения, подходящие для использования в качестве биометрических проб, и проверяет кандидатов, возвращенных после поиска в базе данных. Операторы могут быть обучены методикам сравнения лиц, процесс принятия решений может поддерживаться специальными инструментами анализа изображений. В случае обратного отслеживания или кластеризации (связывания изображений одних и тех же субъектов) оператор может использовать другую визуальную информацию (например, одежду человека и относительное расположение камер) для подтверждения или отклонения совпадений.

Примеры сценариев постсобытийного использования включают:

- постсобытийный анализ записанных видеоизображений с одной или нескольких камер с использованием программного обеспечения биометрического распознавания для идентификации одного или нескольких лиц на кадрах или последовательностях кадров (с использованием одного или нескольких изображений в качестве биометрических контрольных шаблонов);
- постсобытийный анализ записанных видеоизображений с нескольких камер, на которых отслеживается идентифицированный или неидентифицированный индивид с учетом времени и перемещений между камерами. Помимо биометрического программного обеспечения при анализе может быть использовано программное обеспечение для видеоаналитики;
- ретроспективную кластеризацию — детектирование и извлечение лиц из нескольких видеоизображений с целью группирования изображений одних и тех же индивидов. Так как на нескольких видеоизображениях может появляться большое число субъектов, рекомендуется использовать автоматизированный процесс. В конце обработки оператор может просмотреть и скорректировать результаты.

5.3 Сценарии использования в режиме реального времени

В сценариях использования в режиме реального времени целью является высокая вероятность оповещения о присутствии целевых субъектов с использованием соответствующих шаблонов в списке наблюдения и низкая вероятность оповещения о присутствии субъектов, не включенных в список наблюдения. Как правило, список наблюдения представляет собой подмножество изображений из более крупной базы изображений, сформированное для решения конкретной задачи.

Данные сценарии использования являются сложными из-за большого объема обрабатываемых данных, особенно если система включает несколько камер с несколькими субъектами на каждом кадре. Сложной задачей является не только обеспечение высокой точности поиска, но и обеспечение минимального времени отклика для эффективных действий при оповещении.

Как правило, оператор проводит оценку любых оповещений от биометрической системы и принимает решение о том, является ли оповещение подлинным или ложным. Также оператор несет ответственность за инициирование дальнейших действий при необходимости, например направление специалистов на место события для задержания или беседы с целевым субъектом для подтверждения его личности.

Примеры сценариев использования в режиме реального времени включают:

- оповещение в реальном времени (или почти в реальном времени) о присутствии в поле зрения камеры видеонаблюдения человека, идентифицированного биометрической системой как человека, чьи биометрические данные (например, изображение лица) ранее были сохранены как биометрический контрольный шаблон в списке наблюдения. Примерами являются проверка индивидов, входящих в здание или выходящих из самолета или поезда, по списку наблюдения с целью предоставления или отказа в определенных привилегиях, а также мониторинг видеонаблюдения правоохранительными органами с целью предотвращения преступлений и обеспечения общественной безопасности. Данный сценарий использования называют «живым» распознаванием лиц;
- отслеживание в режиме реального времени конкретного индивида в поле зрения нескольких камер, поля зрения могут не перекрываться.

5.4 Сценарии регистрации

В сценариях регистрации целью является успешная регистрация целевых субъектов, представляющих интерес, в базе данных или списке наблюдения с обеспечением удовлетворительного качества созданных биометрических контрольных шаблонов. Перед регистрацией может быть проведен биометрический поиск для определения того, что целевой субъект уже зарегистрирован.

Оператор может осуществлять выбор изображений наилучшего качества для регистрации, но в большинстве случаев процесс будет полностью автоматизирован. Для выбора изображений наилучшего качества могут быть использованы машинное обучение и когнитивные вычисления.

Примеры сценариев регистрации включают:

- регистрацию в списке наблюдения индивидов, которые вошли в охраняемую зону или повторно посещают одну и ту же территорию;
- хронометраж индивидов для измерения времени, проводимого в определенной области, например для отслеживания времени обслуживания или длины очереди;
- регистрацию индивидов в поле зрения камеры видеонаблюдения в базе данных для будущего использования списка наблюдения в той же системе или с другими биометрическими приложениями и базами данных.

6 Спецификация аппаратного и программного обеспечения

6.1 Общие положения

В настоящем стандарте рассматриваются аспекты аппаратных и программных компонентов СВН, которые имеют прямое отношение к производительности биометрической подсистемы.

Настройки, оптимальные для обычной СВН, могут приводить к формированию изображений, не подходящих для использования в биометрических приложениях. Рекомендации, представленные в настоящем разделе, могут быть применены главным образом к системе АРЛ, но могут быть адаптированы для других биометрических модальностей.

6.2 Физические условия

В большинстве случаев физические условия, в которых будет работать СВН, будут вне контроля лиц, ответственных за развертывание или эксплуатацию камер. Рекомендуется обеспечить корректное расположение камер (см. *6.5.2*). При возможности влияния на физические условия работы системы рекомендуется:

- избегать неровных полов и ступеней, поскольку изменение угла/высоты вынуждает индивидов смотреть вниз, что затрудняет сбор изображений лица, пригодных для биометрического распознавания;
- вводить барьеры для изменения потока индивидов таким образом, чтобы все индивиды проходили в поле зрения камеры (камер) на необходимом расстоянии и двигались по направлению к камере (в случае системы АРЛ). Указанные методы и корректное размещение камер способствуют увеличению времени нахождения индивида в поле зрения камеры, что повышает производительность биометрической системы;
- вводить узкие места для уменьшения количества людей, проходящих через поле зрения камеры в отдельный момент времени, что уменьшит количество целевых субъектов, обрабатываемых биометрическим приложением одновременно. Узкие места способствуют повышению качества биометрических образцов, так как может быть ограничена скорость перемещения целевых субъектов через область получения изображения, улучшена освещенность в заданной области и обеспечено приемлемое положение целевого субъекта по отношению к камере.

Введение барьеров или узких мест может иметь негативные последствия для перемещающихся индивидов. Следует учитывать необходимость практичности, доступности и удобства использования для пользователя. Баланс между указанными факторами и необходимостью получения изображений высокого качества для повышения производительности биометрической системы следует определять в каждом конкретном случае. См. приложение В для получения дополнительной информации о социальных аспектах, которые следует учитывать при использовании представленных методов.

6.3 Условия освещения

Для обработки биометрических данных должно быть обеспечено достаточное освещение. При возможности влияния на условия освещения рекомендуется:

- избегать областей возле окон или с дневным освещением, поскольку в этом случае освещение невозможно контролировать и оно будет меняться в зависимости от времени дня/года и погодных условий. Рекомендуется использовать затененные или искусственно освещенные области;
- вводить дополнительное освещение для повышения общего уровня освещенности, а также для обеспечения сбалансированного освещения лиц без сильных теней или бликов. Дополнительное освещение позволяет использовать более короткие выдержки, что снижает размытость изображения при движении субъекта;
- использовать ближнее инфракрасное освещение (в сочетании с камерами, регистрирующими изображения в указанном диапазоне длин волн) для уменьшения теней и повышения качества биометрических образцов в условиях низкой освещенности.

6.4 Обеспечение фронтального положения

Алгоритмы распознавания лица являются высоко чувствительными к положению головы относительно оптической оси камеры. Рекомендуется устанавливать «точки притяжения» для побуждения людей смотреть в определенном направлении, например вверх или по направлению к камере.

Рекомендуется проверить отсутствие точек отвлечения внимания, например стороннего телевизионного экрана, которые могут снизить эффективность сбора биометрических данных в результате изменения направления от требуемого.

6.5 Камеры и инфраструктура

6.5.1 Выбор камер

Камеры и объективы к ним следует выбирать таким образом, чтобы разрешение изображения, частота кадров, поле зрения и производительность при низком уровне освещенности обеспечивали получение изображений качества, приемлемого для использования в биометрической системе.

Для оценки производительности камеры и системы, производящей видеопоток в СВН, используется несколько количественных показателей.

Пространственное разрешение — один из наиболее важных факторов качества изображения, сформированного в СВН. Пространственное разрешение может быть оценено с использованием функции передачи модуляции (ФПМ). Исходное изображение ФМП20 должно иметь не менее 0,4 пар линии/пиксель. Исходное изображение относится к некодированному сигналу.

В случае IP-камер измерение пространственного разрешения невозможно, поскольку генерируется только кодированный сигнал.

Примечания

1 В *[1]* определены методы измерения разрешения кадра видеоизображения, применимые как для монохромных, так и для цветных цифровых камер.

2 В *[2]* определены методы оценки СВН с целью управления цветом.

Требования к разрешению изображений лиц, полученных с помощью камеры, зависят от сценария использования и используемого алгоритма распознавания лица. Как правило, расстояние между глазами (IED) на изображении лица должно составлять не менее 50 пикселей, если биометрическая система возвращает результаты поиска по списку наблюдения.

Как правило, более высокое разрешение изображения приводит к более высокой производительности, однако производительность многих алгоритмов находится на плато при расстоянии между глазами, равном 95 пикселей. При значении IED, большем 95 пикселей, большее влияние на производительность оказывают другие факторы, такие как положение камеры, освещение и т. д.

В исследовании влияния разрешения изображения на производительность для ряда современных алгоритмов распознавания лица *[3]* установлено, что часть протестированных алгоритмов не детектирует лица при расстоянии между глазами, меньшем 20 пикселей, часть протестированных алгоритмов не работают при расстоянии между глазами, большем 80 пикселей. В связи с этим в настоящем стандарте не представлены более определенные требования к разрешению изображения.

Выдержка, частота кадров и алгоритмы сжатия изображения также влияют на качество изображения. Целью сбора изображения является получение наилучшего возможного изображения целевого субъекта, который может перемещаться в поле зрения и лишь недолго смотреть в направлении камеры. При низком уровне освещенности на кадрах может присутствовать размытость при движении, что уменьшает число деталей на изображении, доступных для анализа.

Выбор фокусного расстояния объектива камеры зависит от расстояния между целевым субъектом и камерой. Рекомендуется использовать фокусное расстояние, сопоставимое с фокусным расстоянием при получении изображений списка наблюдения. Существенное различие между фокусным расстоянием при получении изображений списка наблюдения и фокусным расстоянием камеры видеонаблюдения вызывает различия в перспективе, что может снизить производительность биометрической системы. Оптическое искажение, вызванное типом и качеством объектива, также может снизить производительность биометрической системы.

Многие камеры видеонаблюдения используют проприетарный формат или контейнер, что при произведении видеопотока требует использования специального программного обеспечения от производителя. В некоторых случаях производители не предоставляют возможность перекодировать проприетарный формат в более распространенные форматы, такие как H.264, что требует разработки или приобретения дополнительного программного обеспечения для данной цели. При выборе камер следует учитывать необходимость перекодирования формата записи в более распространенный формат.

Выбор камер играет важную роль в производительности биометрической системы, но является одним из многих факторов. При внедрении СВН с распознаванием лица рекомендуется обратиться за консультацией к специалисту для определения наиболее подходящего решения и проведения надлежащего тестирования производительности как на этапе закупок, так и перед эксплуатационным развертыванием.

6.5.2 Размещение камер

Во многих существующих системах видеонаблюдения камеры расположены так, чтобы контролировать широкое поле зрения и, следовательно, не подходят для биометрических приложений, таких как АРЛ. Если камеры видеонаблюдения должны обеспечивать качество изображения, приемлемое для систем АРЛ, необходимо учесть их размещение и положение.

Различают пять основных сценариев видеонаблюдения *[4]*:

1) «стационарный», например паспортный контроль или биометрический киоск/кабина;

2) «портал», например коридор с односторонним движением или портал с узкими местами;

3) «коридор», например коридор с двусторонним движением, в котором одновременно может находиться более одного человека;

4) «зал», например зал аэропорта, аэровокзала, автовокзала или железнодорожного вокзала, станция метрополитена, торговый центр и т. п.;

5) «на открытом воздухе» — все остальные сценарии.

Примеры изображений с установленных камер наблюдения в аэропорту, соответствующих сценариям 1, 3 и 4, показаны на рисунке 2. Представленные изображения демонстрируют, что поле зрения включает окружающую обстановку, но не является оптимальным полем зрения камеры для биометрического распознавания.



Рисунок 2 — Примеры сценариев 1, 3 и 4 *[4]*

В следующих пунктах представлены рекомендации по размещению камер для получения изображений для распознавания лица и для анализа походки.

6.5.2.1 Размещение камер

Рекомендуется использовать тип видеонаблюдения 1, когда индивид проводит некоторое время на одном и том же месте с предварительной фокусировкой камеры на этом месте. При невозможности использовать тип видеонаблюдения 1 рекомендуется два решения:

- использование массива видеокамер;
- использование комбинации камер point-and-shoot («наведи и снимай») и камер СВН с функцией видеоаналитики, отслеживающей лицо при измерении его разрешения.

Вне зависимости от типа видеонаблюдения рекомендуется:

- минимизировать углы наклона, поворота и отклонения с учетом того, что при низко установленных камерах лица целевых субъектов могут быть скрыты индивидами, находящимися перед ними.

Примечание — В *ГОСТ Р ИСО/МЭК 19794-5* для сбора изображения лица рекомендуется максимальное значение погрешности для углов наклона, поворота и отклонения, равное 5°, однако такие строгие ограничения, как правило, не поддерживаются в системе видеонаблюдения;

- камера должна быть направлена в направлении движения и ограничена узким местом, чтобы индивиды не пересекали основной поток движения;
- ограничить количество людей в поле зрения в произвольный момент времени во избежание чрезмерной нагрузки на программное обеспечение распознавания лица, обеспечивая при этом адекватное покрытие области;
- избегать изображения силуэтов субъектов, например при входе индивидов в здание с улицы; при невозможности избежать или при наличии сильных теней рекомендуется использование дополнительного (в том числе инфракрасного) освещения;
- обеспечивать равномерность освещенности лица при прохождении целевых субъектов через зону распознавания (см. рисунок 3);
- обеспечивать приемлемое освещение лиц во избежание размытости изображения из-за длинной выдержки или шума сенсора, влияющего на качество изображения.

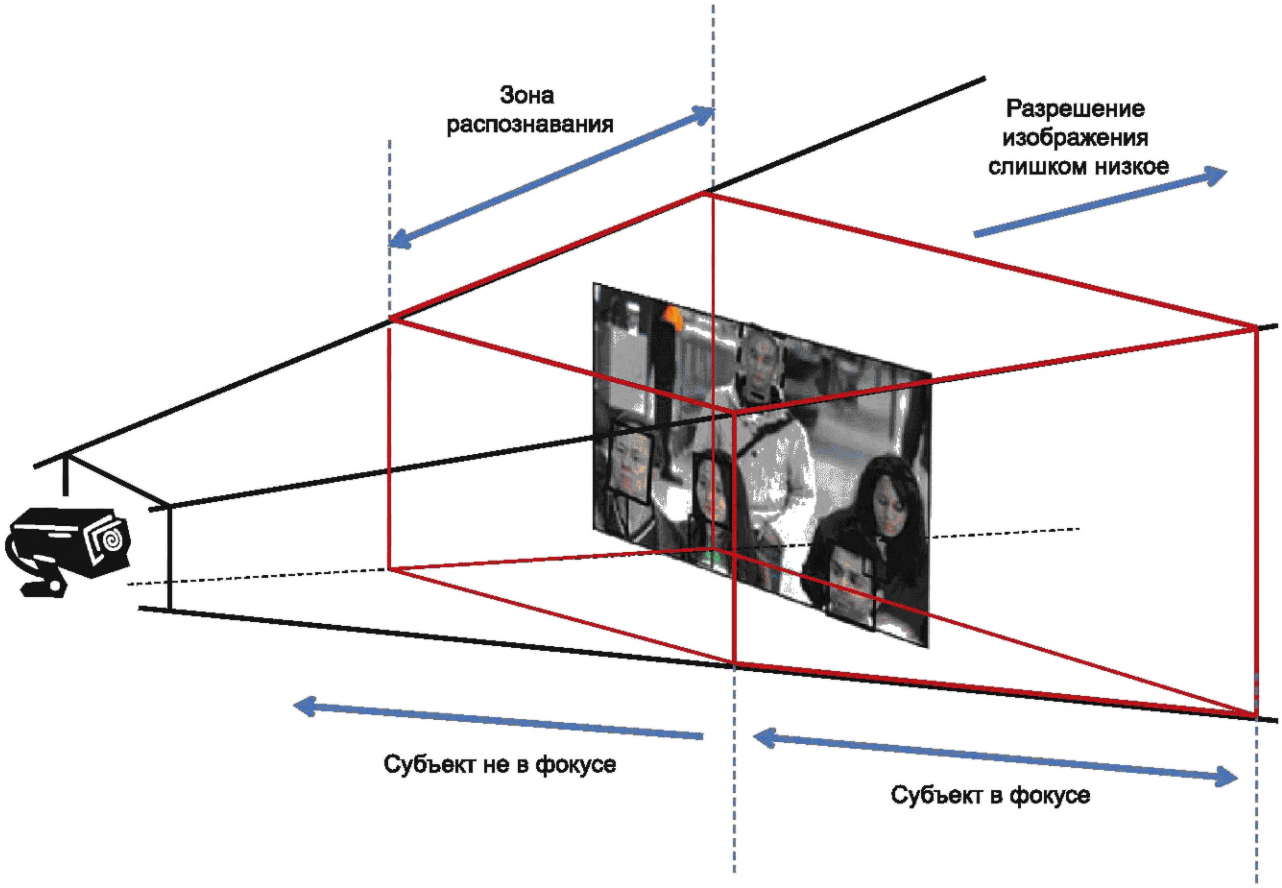


Рисунок 3 — Зона распознавания

В [*2*] приведена дополнительная информация о поле зрения камер в зависимости от размера объекта для различных сценариев, включая мониторинг толпы, детектирование присутствия индивида, распознавание известного индивида и идентификация неизвестного индивида.

Для приложений АРЛ горизонтальное поле зрения камеры в метрах должно быть сопоставлено с размером кадра по горизонтали в пикселях для получения эффективного разрешения [пикселей/м]. Данная оценка может быть рассмотрена как количество пикселей на миллиметр при оценке вероятной производительности биометрической системы на основе исследований, которые проверяют расстояние между зрачками или количество пикселей между центрами глаз. Для приложений АРЛ следует учитывать количество пикселей на метр на самом дальнем расстоянии, на котором предполагается получение изображения субъекта в фокусе. Например, система может быть оптимизирована для работы с изображениями лиц, имеющими приблизительно 95 пикселей между центрами глаз, что является плато производительности для многих современных систем распознавания лиц *[5]*, *[6]*. С учетом того, что типичное расстояние между глазами для взрослых составляет 63 мм, это потребует разрешения 1,5 пикселей/мм (95/63) или 1500 пикселей/м. При использовании камеры высокой четкости с размером кадра 1920 × 1080 пикселей горизонтальное количество пикселей в датчике камеры (1920) делится на требуемое разрешение в пикселях на метр (1500), в результате максимальная ширина области формирования изображения составляет 1,27 м. См. рисунок 4 и *таблицу 1*.

Примечание — На практике фактическое оптическое разрешение системы камер СВН всегда ниже значения, полученного с помощью данного метода.



Рисунок 4 — Расстояние между глазами для расчета максимальной ширины области формирования изображения

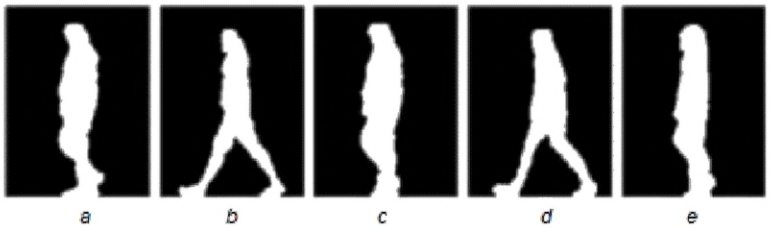
Таблица 1 — Соотношение между расстоянием между глазами в пикселях и максимальной шириной области формирования изображения

IED, пикселей	Максимальная ширина области формирования изображения	Ссылка на значение IED
20	6,04 м = 0,063 · 1920/20	Минимальное значение, установленное в *[1]*
50	2,41 м = 0,063 · 1920/50	Минимальное значение, рекомендуемое в *6.5.1*
80	1,51 м = 0,063 · 1920/80	Максимальное значение, установленное в *[1]*
95	1,27 м = 0,063 · 1920/95	Максимальное значение, рекомендуемое в *6.5.1*

6.5.2.2 Размещение камер для автоматического анализа походки

Силуэтом для распознавания походки является изображение индивида, представленное в виде сплошной фигуры одного цвета, обычно черного. Границы силуэта соответствуют контуру субъекта.

Анализ походки может быть использован для идентификации в сценариях видеонаблюдения с несколькими камерами. Для кадров видеоизображений нескольких камер используется поправка для вычисления координат вида сбоку. Видеозаписи с низкой частотой кадров (от 1 до 5 кадров в секунду), сделанные с помощью фотоаппаратов или систем видеонаблюдения, совместимы с нормализованными последовательностями силуэтов походки. Для фиксации всех деталей походки должен быть зафиксирован как минимум один полный цикл походки, т. е. два полных шага. На рисунке 5 показаны силуэты фаз одного полного цикла походки.



a, *c*, *e* — фаза опоры; *b*, *d* — фаза переноса

Рисунок 5 — Фазы полного цикла походки

Для биометрического распознавания походки разработаны различные автоматизированные методы. В качестве входных данных в методах могут быть использованы данные изображения или только

силуэты. Автоматизированные методы могут использовать как выровненные, так и невыровненные изображения. Рекомендуется фиксировать последовательность походки с помощью стационарной камеры.

Вид сбоку позволяет фиксировать последовательность походки наиболее информативно *[7]*. Необходимо проинструктировать субъекта, чтобы он шел по прямой линии, перпендикулярной к линии обзора камеры, как показано на рисунке 6. В дополнение к виду сбоку рекомендуется регистрировать видеоизображение с видом спереди и сзади.

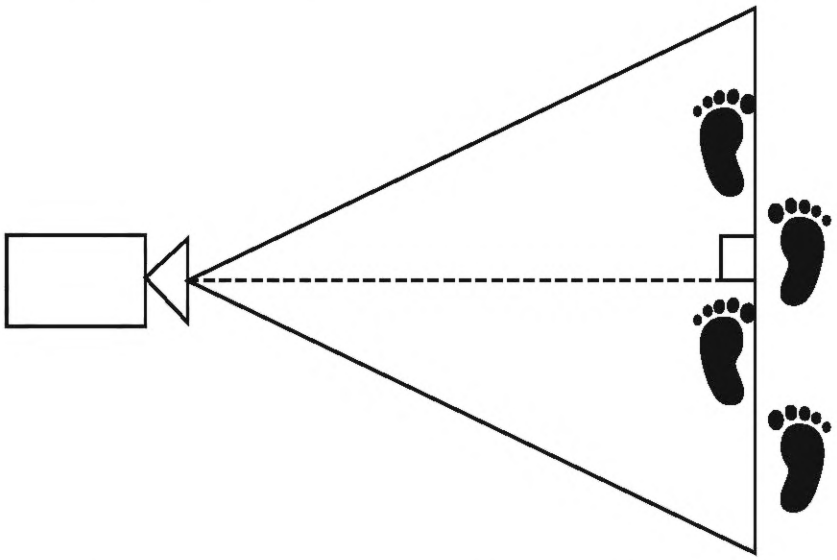


Рисунок 6 — Регистрация видеоизображения субъекта сбоку

Сочетание внешнего вида и пространственно-временного движения дает более эффективные результаты, чем использование одной модальности в наиболее сложных сценариях, где есть различия как во внешнем виде, так и в динамике.

Анализ видеоизображения ходьбы имеет меньшие временные затраты, если сведены к минимуму вариации освещения и фона. Существуют методы уменьшения влияния вариаций освещенности и динамического фона в видеоматериале *[7]*. Вычитание фона является сложной задачей, особенно в сложных динамических сценах, содержащих движущийся фон, растительность, рябь на воде и т. д.

С учетом ограничений по размещению камеры и условий, обусловленных автоматическим распознаванием походки, применимость данного метода для распознавания или отслеживания субъекта в реальных сценариях ограничена.

6.5.3 Требования и рекомендации для инфраструктуры

6.5.3.1 Мощность

Необходимо провести оценку энергопотребления:

- для камер;
- сетевых устройств;
- цифровых видеорегистраторов или общих сетевых устройств хранения данных;
- инфраструктуры для обработки.

Оценка может быть проведена на основе информации от производителей о потребляемой мощности устройств.

6.5.3.2 Сетевые требования и сжатие

Традиционные реализации СВН передают видеоизображения по сети для хранения и/или обработки. Как правило, передача проводится постоянно и без перерывов, и объем видеоданных является большим.

Пропускная способность сети должна быть достаточной для обеспечения непрерывной потоковой передачи видеоданных. Скорость потока данных по сети линейно увеличивается при увеличении:

- количества камер;
- ширины и высоты кадра камеры;

- частоты кадров;
- скорости передачи сжатого видео.

Как правило, видеоданные в СВН всегда сжимаются для сохранения полосы пропускания сети и места для хранения. Чаще всего сжатие проводится внутри камеры и с потерями. Это означает, что исходное видео с камеры не может быть восстановлено при декомпрессии. Потери минимизируются путем:

a) повышения скорости передачи в битах;

b) использования современных методов сжатия *[8]*.

Такие методы сжатия имеют высокую эффективность сжатия в том числе за счет включения компенсации движения. Скорость передачи данных пропорциональна скорости потока данных в сети. Скорость передачи данных также является мерой качества видео с низкой скоростью передачи данных, соответствующей высоким коэффициентам сжатия и большим потерям информации. Рекомендуется установить достаточную пропускную способность сети для обеспечения высокой скорости передачи данных, чтобы потери видеоданных являлись несущественными. Определение «несущественности» проводится на частоте ошибок автоматического распознавания или на выводах оператора о видимости деталей лица.

Примечание — В исследовании *[1]* с использованием потолочных камер высокой четкости с частотой 30 кадров в секунду и размерами пикселей 1920 × 1080, кодек AVC был настроен на передачу данных со скоростью 24 Мбита/с от каждой камеры.

6.5.3.3 Хранение

При непрерывной передаче видеоданных с одной или нескольких камер на специальный цифровой видеорегистратор или другое оборудование хранения, в конечном итоге данные заполняют все устройство. Следовательно, должно быть установлено окно хранения, размер которого соответствует целям оперативной проверки и экономическим соображениям, в дополнение к соблюдению соответствующих политик управления и законодательства о защите персональных данных.

6.6 Биометрическая система

6.6.1 Общие положения

Независимо от биометрической модальности, биометрическая система выполняет следующий ряд задач:

- детектирование присутствия индивидов в поле зрения камеры;
- извлечение информации для создания биометрического шаблона для каждого индивида с использованием одного или нескольких кадров видеопотока;
- создание биометрического(их) шаблона(ов);
- сравнение биометрического шаблона с биометрическими контрольными шаблонами в базе контрольных шаблонов и возвращение возможных совпадений для просмотра оператором.

В следующих пунктах представленные задачи рассмотрены более подробно с точки зрения АРЛ.

6.6.2 Программное обеспечение для детектирования лиц

Детектирование лиц является первым этапом процесса распознавания. Скорость и точность алгоритма детектирования лиц являются основными факторами при определении общей производительности системы. Детектирование лиц на видео требует больших вычислительных ресурсов. Задача усложняется, если должен быть обеспечен режим реального времени, и в поле зрения камеры находится несколько лиц, при этом каждый человек движется и может находиться в оптимальном положении (зоне распознавания) в пределах нескольких секунд.

Также задача усложняется, когда лица частично скрыты другими, или целевой субъект может не смотреть в камеру и в результате может быть не детектирован. Изображения и логотипы на одежде или даже статические объекты в поле зрения камеры могут быть неверно интерпретированы как лица, что приведет к созданию шаблонов, не представляющих никакой ценности. Разработчики программного обеспечения для детектирования лиц устанавливают пороговые значения для различных параметров. Если пороговые значения установлены на низком уровне («либеральная» политика детектирования), чтобы гарантировать детектирование всех «реальных» лиц в видеопотоке, это приводит к увеличению количества создаваемых ложных шаблонов. Если пороговые значения установлены на высоком уровне («консервативная» политика детектирования), сгенерированные шаблоны будут иметь более высокое качество, но повышается вероятность того, что многие целевые субъекты не будут детектированы и, следовательно, не будут найдены по списку наблюдения. В некоторых алгоритмах могут быть установ-

лены ограничения на общее число лиц, которое может быть детектировано одновременно на одном произвольном кадре, чтобы избежать ограничивающий фактор в нисходящем направлении.

Отдельной сложностью в приложениях СВН является частота кадров видеокамер. В большинстве приложений частота кадров составляет не менее 10 кадров/с, в том числе намного выше, что может привести к созданию десятков или сотен шаблонов каждого индивида в то время, когда он находится в поле зрения камеры. Поставщики программного обеспечения для детектирования лиц могут использовать различные методы (например, выборку только подмножества всех доступных кадров) для решения данной задачи, при этом теряется возможность выбора наилучшего шаблона целевого субъекта.

Оптимальные настройки программного обеспечения для детектирования лиц зависят от приложения. Во время ввода системы в эксплуатацию следует определить оптимальный баланс между скоростью, точностью и надежностью детектирования лиц в условиях эксплуатации.

Некоторые алгоритмы сравнения лиц используют наборы биометрических признаков, объединенных из нескольких изображений лица одного индивида, полученных из кадров разных видеоизображений. В таком случае получение нескольких изображений лица одного индивида проводится с использованием алгоритмов отслеживания лиц, часто отличных от алгоритмов детектирования лиц. Изображения лица выбираются на основе показателей качества изображения лица и сходства с предыдущими полученными данными (для минимизации риска ошибок отслеживания лиц), обрабатываются и объединяются в единый набор биометрических признаков.

***6.6.3* Программное обеспечение для сравнения лиц**

Программное обеспечение для сравнения лиц характеризуется скоростью и точностью сравнения. Поставщик может разрабатывать различные версии, которые имеют приоритет скорости или точности сравнения, и/или рекомендовать определенные процессоры и оборудование для достижения оптимальной производительности. Отдельный алгоритм может иметь высокую производительность для постсобытийного поиска в больших базах данных, когда биометрические пробы и биометрические контрольные шаблоны были собраны в оптимальных условиях, но иметь низкую производительность в режиме реального времени, когда биометрические пробы поступают с камер видеонаблюдения и имеют более низкое качество изображения. Для преодоления проблем с изображениями низкого качества разработчики программного обеспечения для сравнения лиц могут использовать различные методы, например «усреднение» лиц по нескольким видеокадрам или использование 3D-моделей для создания нескольких биометрических шаблонов из одного изображения. Настоящий стандарт не рассматривает детали разработки таких алгоритмов.

***6.6.4* Выбор и испытание алгоритма**

Как правило, поставщик биометрической системы заявляет о производительности своего алгоритма, но необходимо отметить, что указываемые результаты могли быть получены при оптимальных условиях, в значительной мере отличающихся от эксплуатационных условий. Рекомендуется использовать результаты независимых испытаний, однако такие результаты также могут не соответствовать тому, что будет получено в условиях эксплуатации. В процессе закупки и ввода в эксплуатацию необходимо проверить, что система обеспечивает ожидаемый уровень производительности, и что она была правильно настроена для конкретных условий и целей эксплуатации, *т. е. необходимо провести сценарные испытания.* Определение метрик эксплуатационных характеристик приведено в 10.5. Требования и рекомендации по проведению сценарных испытаний биометрических систем определены в *ГОСТ Р 58292*.

***6.6.5* Программное обеспечение, не связанное с биометрией**

Биометрическая система может включать дополнительное программное обеспечение, не связанное напрямую с функцией биометрического распознавания, но необходимое как часть более широких процессов, в том числе:

- программное обеспечение информации управления для мониторинга и управления эффективностью и результативностью системы;
- программное обеспечение аудита для регистрации использования системы и проведения расследований, например после запроса информации от представителя общественности или заявлений в ненадлежащем использовании системы;
- программное обеспечение для обеспечения постоянной доступности системы и/или данных в случае сбоев питания или системы.

6.7 Вычислительные требования

6.7.1 Общие положения

Требуемая вычислительная мощность зависит от сценария использования. В наиболее сложных случаях система может состоять из нескольких камер высокого разрешения с высокой частотой кадров и с несколькими целевыми субъектами в зоне распознавания каждой камеры, в сочетании с эксплуатационными требованиями поиска в режиме реального времени по большому списку наблюдения из тысяч или десятков тысяч биометрических контрольных шаблонов. Если время распознавания должно поддерживаться в допустимых пределах, может потребоваться значительная вычислительная мощность. В таком случае могут потребоваться специальные помещения для размещения оборудования с подходящими системами охлаждения. В менее требовательных сценариях оборудованием может являться ноутбук с высокими техническими характеристиками.

Отсутствие адекватной вычислительной мощности в ряде этапов процесса может привести к снижению производительности биометрической системы:

- в сети связи, необходимой для передачи изображений с камер в биометрическую систему;
- при работе программного обеспечения для детектирования и извлечения информации о местоположении каждого целевого субъекта в зоне распознавания каждой камеры;
- при работе программного обеспечения для создания биометрических шаблонов для поиска по списку наблюдения;
- при работе программного обеспечения поиска и сравнения биометрических шаблонов проб с изображениями в списке наблюдения;
- при поиске потенциально совпадающих изображений из базы данных с дополнительными данными, которые должны быть отображены для просмотра оператором.

6.7.2 Основные биометрические процессы

Биометрическое распознавание обычно выполняется в три этапа. Первым этапом является обработка изображений для детектирования и отслеживания, вторым — извлечение биометрических признаков, и третьим — поиск по списку наблюдения. Независимо от биометрической модальности стоимость обработки видеоизображений выше, чем у статических изображений, ввиду большего объема данных. Хотя некоторые алгоритмы могут работать только с отобранными подмножествами видеоданных, выделение кадров, представляющих интерес, требует затрат. Вычислительные затраты для задач обработки изображений увеличиваются с увеличением:

- размера изображений;
- продолжительности видеопоследовательности;
- количества индивидов, присутствующих на видеоизображении;
- продолжительности появления индивидов.

Время вычислений различных алгоритмов существенно отличается и увеличивается с увеличением:

- числа детектированных лиц (истинных и ложных);
- числа отслеживаемых дорожек (и потери целостности трека таким образом, что отдельный трек разбивается на несколько частей).

Затраты на поиск зависят от размера биометрического шаблона распознавания и увеличиваются с увеличением:

- количества извлеченных из видеоизображения биометрических шаблонов;
- количества зарегистрированных биометрических шаблонов.

Примечания

1 В исследовании *[1]* время, необходимое для обработки одной секунды видеоизображения размером 1920 × 1080, не содержащего лица, составляло от 0,4 до 4 с для наиболее точного алгоритма и до 20 с для других алгоритмов.

2 В исследовании *[1]* время, необходимое для обработки одной секунды видеоизображения размером 1920 × 1080, содержащего до семи человек, составляло от 3 до 11 с для наиболее точного алгоритма и до 80 с для других алгоритмов.

3 В исследовании [*1*] большинство алгоритмов производили биометрические шаблоны, размеры которых линейно увеличивались с увеличением продолжительности входного видеоизображения. Некоторые алгоритмы производили биометрические шаблоны, размеры которых не зависели от продолжительности входного видеоизображения, что может быть достигнуто путем выбора наилучшего кадра или путем интеграции информации с течением времени.

С учетом значительных различий во времени обработки различных алгоритмов, при выборе биометрической системы недостаточно указывать требование только к временным характеристикам, поскольку это может иметь неблагоприятные последствия для точности.

***6.7.3* Снижение вычислительных затрат**

Существует ряд методов снижения вычислительных затрат, в том числе:

- обработка изображений в камере позволяет существенно уменьшить объем передаваемых данных. Например, на камере может проводиться детектирование и извлечение данных изображения лица из кадров и передача наилучших изображений в биометрическую систему для поиска. Если в сценарии использования требуется просмотр или запись всех данных с камеры, то такой подход может быть неприемлемым, или может потребоваться отдельный видеопоток для просмотра или записи исходных данных;

- уменьшение частоты кадров, применение сжатия или уменьшение разрешения камеры позволяет существенно уменьшить объем передаваемых данных. При этом происходит потеря некоторых данных, что снижает точность распознавания;

- детектирование целевого субъекта, движущегося в поле зрения видеокамеры в реальном времени, требует значительных вычислительных ресурсов, особенно при высокой частоте кадров и/или при наличии нескольких целевых субъектов на кадре (см. приложение А). Методами снижения вычислительных затрат являются выбор подмножества кадров или повышение порога детектирования, но в результате может быть повышена вероятность ошибки детектирования;

- вычислительная мощность и время, необходимое для создания биометрического шаблона из изображения обнаруженного целевого субъекта, в значительной мере зависят от алгоритма. При выборе алгоритма, наиболее подходящего для конкретного сценария, необходимо учитывать такие факторы, как требуемая скорость получения результата, точность (с учетом типа и качества данных биометрических проб и биометрических шаблонов списка наблюдения), размер списка наблюдения и доступная вычислительная мощность;

- методы минимизации времени, затрачиваемого на отображение ответов оператору, включают уменьшение числа кандидатов путем повышения порогового значения принятия решения или ограничения длины списка, а также уменьшение размера и разрешения отображаемых изображений (например, изображение с более высоким разрешением предоставляется при запросе оператора).

6.8 Спецификация базы биометрических контрольных шаблонов

6.8.1 Общие положения

В других пунктах настоящего стандарта приведены требования и рекомендации по выбору и размещению камер СВН для получения изображений удовлетворительного качества. Помимо качества биометрической пробы/изображения на производительность биометрической системы значительно влияет количество и качество биометрических контрольных шаблонов/изображений в списке наблюдения или базе поиска.

6.8.2 Размер базы биометрических контрольных шаблонов

При отсутствии биометрических данных конкретного целевого субъекта в системе совпадение невозможно, вне зависимости от качества биометрических проб-изображений. Однако при увеличении размера базы увеличивается вероятность ложных совпадений, имеющих результаты сравнения выше порогового значения. При частом повторе таких ситуаций операторы могут перестать доверять результатам, что приведет к тому, что оператор не распознает или не отреагирует на истинное совпадение. При увеличении базы данных может возникнуть ситуация, когда в качестве результата возвращаются нескольких кандидатов, а кандидат с истинным совпадением находится в конце списка и не замечается оператором.

Для сценариев поиска по спискам наблюдения в режиме реального времени рекомендуется ограничить число целевых субъектов, шаблоны которых хранятся в базе, до нескольких тысяч для поддержания приемлемой производительности. Для сценариев, работающих не в режиме реального времени (например, расследование события после инцидента) допускается размер базы от нескольких субъектов (например, при поиске небольшого числа целевых субъектов, зафиксированных разными камерами или в нескольких местоположениях) до нескольких миллионов субъектов.

Примечание — В исследовании видеонаблюдения на транспортной станции [*1*] при увеличении численности выборки с 4800 до 48 000 и повышении порога принятия решений процент неидентифицированных целевых субъектов в списке наблюдения увеличился с 21 % до 35 %.

По мере увеличения размера базы данных рекомендуется использовать такие методы ограничения пространства поиска, как группирование или фильтрация. Необходимо учесть, что если методы используют метаданные изображения, то при отсутствии или некорректности метаданных использование методов может снизить, а не повысить точность поиска.

***6.8.3* Качество биометрических контрольных шаблонов/изображений**

Изображения в списке наблюдения должны иметь максимально возможное качество. Рекомендации по получению изображений лица удовлетворительного качества представлены в *ГОСТ Р ИСО МЭК 19794-5*. При сравнении изображений лица удовлетворительного качества современные алгоритмы распознавания лиц обеспечивают очень высокий уровень точности. Однако, как правило, в приложениях СВН изображения, получаемые с камер, не удовлетворяют требованиям к качеству изображений лица. В частности, освещенность может контролироваться, но камеры обычно размещаются таким образом, что лицо целевого субъекта снимается сверху или сбоку. Для повышения производительности как автоматизированного процесса сравнения, так и визуальной экспертизы рекомендуется хранить в базе данных несколько изображений каждого целевого субъекта. В таком случае допускается использовать изображения, не соответствующие требованиям и рекомендациям *ГОСТ Р ИСО МЭК 19794-5*. Изображения лиц, полученные в различных условиях освещения, с разным положением головы и с разными камерами/объективами, могут давать эффективные результаты сравнения, особенно если условия получения биометрического контрольного шаблона сопоставимы с условиями получения биометрической пробы.

Примечания

1 В исследовании видеоанализа на спортивной арене не в режиме реального времени *[1]* сравнивалась точность распознавания при использовании в качестве биометрического контрольного шаблона одного фронтального изображения и при использовании в качестве биометрических контрольных шаблонов фронтального изображения и нефронтальных изображений с поворотом три четверти вправо и влево. В зависимости от алгоритма уменьшение ошибок составило 15 % и 60 % при ранге 20. При ранге 1 также было уменьшение ошибок.

2 В исследовании *[1]* показано, что включение дополнительных нефронтальных биометрических контрольных изображений в базу данных имеет меньшую ценность при идентификации в реальном времени, когда, как правило, используется высокое пороговое значение. В этом случае при использовании двух дополнительных нефронтальных биометрических контрольных изображений число ошибок сократилось на 10 %.

Независимо от биометрической модальности, по которой установлено потенциальное совпадение, в большинстве случаев при принятии решения оператор использует изображения лиц. Это является сложной задачей, особенно в приложении реального времени, где требуется быстрое решение для принятия соответствующих мер. Для содействия принятию корректного решения рекомендуется предоставить оператору изображения, на которых изображен целевой субъект с различной внешностью (разная одежда, с растительностью на лице и без, наличие очков или шляпы и т.д.). Если изображения имеют удовлетворительное качество для создания биометрического контрольного шаблона, они могут быть добавлены в базу поиска. Если изображение не может быть использовано для создания биометрического контрольного шаблона, оно может быть связано через метаданные с изображениями того же целевого субъекта, из которых были созданы шаблоны. Предоставление таких изображений оператору наряду с биометрической пробой-изображением и изображениями, возвращаемыми с результатами сравнения выше порогового значения, может улучшить производительность биометрической системы.

***6.8.4* Управление базой биометрических контрольных шаблонов**

Размеры базы данных имеют тенденцию увеличиваться на протяжении времени по мере добавления большего числа изображений от большего числа людей, представляющих интерес. Как указано в *6.8.2*, это увеличивает полезность системы за счет расширения выборки, но приводит к большему числу ложных срабатываний. Скорость роста базы данных определяется как скорость добавления минус скорость удаления. Как правило, изображения не удаляются. Рекомендуется установить систематический процесс для курирования содержимого базы данных, путем:

- удаления шаблонов с изображений неприемлемого качества;
- замены на шаблоны новых изображений улучшенного качества;
- удаления шаблонов, полученных ранее заранее определенного количества лет;
- удаления шаблонов у лиц старше определенного возраста;
- удаления шаблонов субъектов согласно известным данным (например, в случае смерти, заключения);
- анализа критериев риска.

7 Работа с несколькими камерами

При использовании нескольких камер в СВН с биометрическим распознаванием существует два основных сценария:

- с перекрытием — когда одну и ту же зону охватывает более одной камеры (т. е. в зоне распознавания есть перекрытие);
- без перекрытия — когда камеры охватывают разные зоны (т.е. в зоне распознавания нет перекрытия).

При невозможности использования типа видеонаблюдения 1 (см. *6.5.2*) рекомендуется использовать массив камер, установленных вокруг «точки притяжения» (например, вокруг монитора, отображающего информацию для пассажиров в аэропорте) для получения фронтального изображения. Допускается распределенное размещение камер внутри окружающего пространства, при этом камеры должны быть направлены на определенную область для обеспечения того, что в любой момент времени целевой субъект в этой области обращен лицом минимум к одной из камер.

Работа с несколькими камерами является неотъемлемой частью нескольких зон распознавания и может включать в себя «слои» камер вдоль ожидаемого пути движения целевого субъекта для многократного детектирования субъекта (например, когда целевой субъект идет по коридору к камерам). Данный механизм рекомендуется использовать не только для решения проблем с частотой кадров и отбракованными кадрами, а также для отслеживания целевого субъекта при оповещении, особенно при значительной задержке детектирования.

Необходимо использовать несколько камер для одной зоны распознавания, если одна камера не позволяет обеспечить разрешение изображения лица, достаточное для требуемого уровня производительности, и не позволяет компенсировать положение головы целевых субъектов, не обращенных к камере при пересечении ее поля зрения или глубины резкости. Такие целевые субъекты могут намеренно избегать камеры или не знать об их наличии.

Камеры с широким полем зрения, охватывающим большую область, могут быть дополнены камерами с более узким полем зрения, охватывающими подмножество большой области и получающими биометрические образцы с более высоким разрешением.

При установке нескольких камер рекомендуется обеспечить управление отслеживанием целевого субъекта, что позволит избежать дублирующих ложных и положительных оповещений после принятия решения оператором. Отслеживание целевого субъекта может быть использовано для автоматического определения текущего местоположения целевого субъекта при запросах.

Использование нескольких камер в системах АРЛ не должно препятствовать операторам и персоналу, отвечающему за реагирование, проверять потенциальное совпадение и наблюдать текущее положение, одежду, багаж и т.д. целевого субъекта с использованием камер с ручным или автоматическим управлением (например, PTZ-камер).

8 Интерфейсы для сопутствующего программного обеспечения

СВН с биометрическим распознаванием может взаимодействовать с другими системами, такими как приложение управления доступом. В большинстве случаев коммуникация между СВН и приложением управления доступом в режиме реального времени основана на протоколе Wiegand или OSDP, коммуникация не в режиме реального времени (синхронизация баз данных, обновление активности и журналов аудита) — на IP-протоколах.

9 Руководство по поддержке оператора

Когда биометрической системой генерируется оповещение, в большинстве случаев оператор должен оценить оповещение с записью в списке наблюдения и принять решение о наиболее подходящих действиях. Независимо от биометрической модальности, вызвавшей оповещение, как правило, решение оператора основано на сравнении изображения лица целевого субъекта с одним или несколькими изображениями в списке наблюдения.

Однако точность визуального сравнения изображений лиц, незнакомых оператору, как правило, низка даже для операторов с многолетним опытом работы. Согласно исследованию (*[9]*, *[10]*), когнитивные способности для выполнения этой задачи распределяются неравномерно среди населения,

при этом некоторые люди (с лицевой агнозией) обладают исключительно низкой компетентностью, и небольшая часть людей демонстрирует высокий уровень компетентности.

Таким образом, для обеспечения высокой производительности биометрической системы должны быть проведены тщательный отбор операторов и их соответствующее обучение. В настоящий момент существуют обучающие курсы по сравнению лиц, однако это — область текущих исследований, и тренеры и экзаменаторы должны быть оценены с учетом существующей практики.

Конфигурация рабочего места оператора должна обеспечивать эффективную работу с использованием инструментов и процедур, разработанных для поддержки принятия решения, с учетом времени, доступного для принятия решения. Рекомендуется, чтобы просмотр изображений осуществлялся более чем одним специалистом для принятия решения путем консенсуса, или чтобы оператор выполнил начальный скрининг выходных данных биометрической системы и передал вероятные совпадения второму более высококвалифицированному специалисту для более детального анализа.

Изображения целевых субъектов, обнаруженные системой в режиме реального времени, для которых один или несколько кандидатов превышают порог сравнения, должны быть представлены на экране рядом с изображениями, полученными в процессе биометрического сравнения. Таким образом, оператор имеет возможность визуально проверить выходные данные биометрической системы и подтвердить или отклонить совпадение. При наличии, рекомендуется отобразить несколько изображений одного и того же целевого субъекта из списка наблюдения, полученных в разных условиях и в разное время. При наличии, рекомендуется предоставлять просмотр видеоизображений, а не только статических изображений.

Во многих приложениях число ложных оповещений значительно превышает число правильных совпадений, а время, доступное для принятия решения, очень короткое. Также может быть возвращено несколько потенциальных совпадений, и должны быть созданы процессы для обработки таких ситуаций. Рекомендуется предоставлять оператору дополнительную информацию из системы и из соответствующего программного обеспечения поддержки принятия решений для поддержки принятия правильного решения.

Помимо отбора компетентных операторов рекомендуется регулярно проводить оценку их работы, например путем проведения регулярных тренировок в оперативной среде и обобщения практического опыта. В сценариях, где ожидается очень мало истинных совпадений, рекомендуется использовать механизм внедрения «совпадений» в рабочий процесс для мониторинга и обеспечения бдительности операторов.

10 Требования и рекомендации по проектированию системы

10.1 Общие положения

В настоящем разделе представлены требования и рекомендации по разработке и внедрению биометрической системы для использования с камерами видеонаблюдения.

Примечания — Предполагается, что в большинстве случаев будет использоваться технология распознавания лиц, но могут быть использованы и другие биометрические модальности.

10.2 Формирование бизнес-требований

Перед проектированием системы должны быть сформированы бизнес-требования, для удовлетворения которых предназначена система, включая то, как биометрические компоненты вписываются в более широкие операционные процессы. Рекомендуется учесть следующие аспекты:

- является ли использование биометрии наиболее подходящим решением или существуют другие подходы, которые могут дать аналогичные результаты;
- наиболее подходящая биометрическая модальность для реализации биометрического решения и сценарий ее использования (например, идентификация в реальном времени или анализ событий);
- влияние внедрения новой системы на существующие бизнес-процессы (как внутренние, так и внешние);
- способ использования результатов биометрической системой, в том числе представление оператору для быстрого ознакомления или необходимость более детального изучения;
- требуемая подготовка оператора и перечень действий, предпринимаемых в результате решений оператора;

- правовые и социальные последствия внедрения биометрических данных в этой конкретной среде;

- вероятность представления и обоснования в суде результатов работы системы и решения оператора в суде.

10.3 Обследование объекта

За исключением работы с данными, предоставленными третьими сторонами и контроль над которыми практически отсутствует, первым этапом проектирования биометрической системы для использования с камерами видеонаблюдения является проведение подробного обследования объекта, где будет развернута система. Первоначально это может быть выполнено заказчиком, но для интеграции биометрического распознавания в установленную инфраструктуру объекта обследование должно проводиться поставщиком биометрического программного обеспечения и третьими сторонами, такими как системный интегратор. Должна быть проведена оценка числа людей, обычно присутствующих в разное время суток, их передвижения по территории, уровня, качества и изменчивости освещения, расположения существующих камер, возможностей для размещения дополнительных камер и т.д. При проведении обследования объекта заказчик может оценить уровень знаний и опыта потенциальных поставщиков, а поставщики могут улучшить свое понимание требований пользователей и, при необходимости, управлять ожиданиями пользователей относительно реально достижимого уровня технологии при текущих условиях с учетом ограничений (например, расположения камер, освещения, общей стоимости).

Должны быть учтены следующие аспекты:

- заинтересованные стороны:

- установление того, кто владеет, обслуживает, эксплуатирует или иным образом несет ответственность за все аспекты пространства или помещения, в котором будет развернута система;

- существуют ли зависимости от внешних систем или заинтересованных сторон, которые могут отправлять или получать данные, или на которые могут повлиять предлагаемые изменения существующих процессов;

- проведение консультаций с другими заинтересованными сторонами, такими как регулирующие органы, представители гражданского общества и организации, представляющие сотрудников;

- камеры:

- характеристики камер, используемых в настоящее время (аналоговые/цифровые, размер кадра, частота кадров, фокусное расстояние, фиксированные или подвижные, например, PTZ-камера);

- возможность использования установленных камер с рассматриваемыми биометрическими модальностями;

- необходимость модернизации, замены или дополнения установленных камер;

- окружающая среда:

- ожидаемое число индивидов в зоне действия камер в течение дня/недели/года (минимальное, среднее, максимальное);

- наиболее распространенные маршруты движения индивидов, включая направление движения;

- время нахождения индивидов в поле зрения каждой камеры;

- наличие узких мест, подходящих для организации сбора биометрических данных высокого качества;

- возможность организации узких мест или иного изменения потока индивидов;

- наличие точек притяжения или отвлекающих факторов, которые могут повлиять на поведение целевых субъектов в лучшую или в худшую сторону;

- возможность внедрения точек притяжения на стратегически важные положения в пространстве;

- освещение:

- является ли освещение искусственным (т.е. контролируемым) или естественным (т. е. неконтролируемым и меняющимся в течение дня и в зависимости от погоды);

- тип освещения и уровень его яркости;

- равномерность освещения и наличие ярких или темных областей, которые могут отбрасывать тени;

- возможность ввода дополнительного освещения;

- сетевая инфраструктура:
  - тип коммуникационной сети для установленных камер;
  - используемые стандарты и протоколы (например, видеокодеки, другие форматы данных, интерфейсы с внешними системами);
  - емкость/скорость сети и необходимость ее модернизации.

10.4 Размер и содержание списка наблюдения

Руководство по выбору изображений для списка наблюдения и влиянию размера списка наблюдений на производительность представлено в 6.8. При проектировании системы необходимо установить, что будет содержать список наблюдения и как данные списка наблюдений будут использоваться биометрической подсистемой. Должны быть учтены следующие аспекты:

- источник изображений в базе данных и их качество;
- в случае изображений лиц будут использованы фотографии паспортного образца в соответствии с *ГОСТ Р ИСО МЭК 19794-5*, изображения лиц, извлеченные из видеоматериалов с камер видеонаблюдения или аналогичных неконтролируемых пространств, или комбинации изображений;
- число изображений/биометрических контрольных шаблонов для одного целевого субъекта и их связь между собой;
- критерии качества при определении приемлемости качества изображения для регистрации; определение оптимального порога регистрации;
- доступность метаданных и способ их хранения и использования системой;
- необходимость использовать фильтрацию при поиске или логическое разделение данных по таким параметрам, как пол, возраст, этническая принадлежность и т.д.;
- требования и процессы для создания, чтения, обновления и удаления записей из базы данных;
- ожидаемое количество шаблонов в базе данных;
- физическое расположение базы данных.

10.5 Требования к производительности

10.5.1 Общие положения

На практике термин «производительность» в биометрических системах часто используется в значении «точность», но точность является только одним из многих факторов определения того, насколько эффективно работает биометрическая система. Каждый компонент архитектуры системы (см. рисунок 1) влияет на общую производительность системы, в том числе условия окружающей среды, качество видеокамер, пропускная способность сети, точность алгоритмов детектирования и сравнения, качество и количество изображений в списке наблюдения или способ взаимодействия оператора с системой и принятия правильного решения при потенциальном совпадении. Поэтому при установке требований к производительности необходимо учитывать сквозную производительность всей биометрической системы, а не какого-либо отдельного компонента.

Как правило, требования к производительности для приложений реального времени, где скорость ответа имеет решающее значение, значительно отличаются от требований к производительности для приложений постсобытийного поиска, где приоритетом является максимизация точности поиска и минимизация числа ложных несовпадений (даже за счет повышения числа ложных совпадений).

10.5.2 Основные метрики эксплуатационных характеристик

Требования к сквозной производительности должны быть определены в процессе сбора требований пользователя и преобразованы в измеримые показатели системы.

В большинстве приложений сквозной процесс включает в себя одного или нескольких операторов, роль которых заключается в проверке и подтверждении или отклонении потенциальных совпадений, возвращаемых биометрической системой. Человеческий фактор может иметь значительное влияние на общую производительность системы, но часто исключается из метрик эксплуатационных характеристик из-за сложности его измерения.

Основные метрики эксплуатационных характеристик:

- ВОД (доля индивидов, чьи лица появляются в поле зрения одной или нескольких камер, но которые не обнаруживаются или не принимаются для последующей обработки и сравнения);
- ВОСД (доля индивидов, чьи лица появляются в поле зрения одной или нескольких камер, но для которых не создается биометрическая проба или биометрический контрольный шаблон для последующего сравнения);

- ВИПИ (доля индивидов, которые находятся в списке наблюдения и чьи лица появляются в поле зрения одной или нескольких камер, и которые были обнаружены и сопоставлены правильно).

Примечание — В некоторых сценариях данный показатель может быть не определен в виду того, не определена корректность оповещения;

- ВЛОИ (доля индивидов, которые находятся в списке наблюдения, чьи лица обнаруживаются, но для которых установлено ложное совпадение с другим человеком из списка наблюдения).

Примечание — В некоторых сценариях количество ложных совпадений может быть значительно больше, чем количество правильных распознаваний, и это является ключевым фактором при определении нагрузки на оператора;

- ВЛПИ (доля индивидов, которые не находятся в списке наблюдения, чьи лица обнаруживаются, но для которых установлено ложное совпадение с другим человеком из списка наблюдения).

Примечание — В некоторых сценариях количество ложных совпадений может быть значительно больше, чем количество правильных распознаваний, и это является ключевым фактором при определении нагрузки на оператора;

- время распознавания: среднее время с момента появления лица в поле зрения камеры или камер до момента, когда система распознавания лиц выдает потенциальное совпадение. В большинстве приложений фактическое время распознавания больше, так как оно включает дополнительное время, необходимое оператору для проверки и подтверждения соответствия.

Примечание — В приведенных определениях используется понятие лиц индивидов, появляющихся в поле зрения камер. Также может быть использовано понятие лиц индивидов, появляющихся в зоне распознавания.

10.5.3 **Метрики эксплуатационных характеристик подсистем обнаружения атак на биометрическое предъявление (ОАБП)**

Биометрическая система может включать дополнительное программное обеспечение ОАБП для обнаружения атак на биометрическое предъявление или других попыток вмешательства в работу системы. Использование такого программного обеспечения может повлиять на общие показатели производительности (например, в результате неправильной классификации надлежащего биометрического предъявления как атаки и наоборот). Рекомендуется определять метрики эксплуатационных характеристик системы с включенным программным обеспечением ОАБП и без него, и/или указывать метрики эксплуатационных характеристик для подсистемы ОАБП.

Метрики эксплуатационных характеристик подсистем ОАБП:

- ВОКПА;
- ВОКПБП;
- ВООПА;
- ВООПБП;
- *ДОПО*.

Требования и рекомендации относительно подсистем ОАБП определены в *ГОСТ Р 58624.1 — ГОСТ Р 58624.3*.

10.6 **Данные и метаданные изображений**

Для записи видеоизображений допускается использовать видеокамеры и цифровые фотоаппараты. Определения форматов JPEG и MPEG-4 включают метаданные для параметров камеры и ориентации камеры. В качестве формата метаданных в JPEG используется формат EXIF, в MPEG-4 — платформа расширяемых метаданных XMP. Рекомендуется использовать указанные форматы для видеонаблюдения и наблюдения с использованием статических изображений.

Приложение А
(рекомендуемое)

Методы и приложения видеоаналитики, связанные с биометрическим распознаванием

А.1 Общие положения

В настоящем приложении представлен обзор методов и приложений, не являющихся непосредственно биометрическим распознаванием, но включающих биометрическое распознавание в процесс функционирования. Например, автоматическое отслеживание субъектов в зоне видимости одной/нескольких камер или оценка плотности толпы с помощью видеонаблюдения, когда система должна быть способна различать индивидов, возможно, путем детектирования и временного сохранения изображений/биометрических шаблонов лиц.

Видеоаналитика представляет собой компьютерное воспроизведение визуальной экспертизы, которую бы проводил оператор при просмотре видеозаписей с камер наблюдения. Программное обеспечение для аналитики обрабатывает видеоизображения для автоматического детектирования людей и событий, представляющих интерес, в целях безопасности. После их детектирования доступны идентификация, отслеживание и определение местонахождения индивидов.

Хотя многие методы видеоаналитики не применимы напрямую к биометрическим приложениям, способность распознавать индивидов в видеопотоке и в большинстве случаев определять местонахождение и извлекать изображения лиц является предпосылкой для последующего процесса сравнения. В настоящем приложении представлена справочная информация о методах, обычно используемых для детектирования, классификации и извлечения информации из видеоизображения.

А.2 Оповещения в режиме реального времени

Большинство условий оповещений определяет пользователь системы видеонаблюдения. Это могут быть общие оповещения, такие как детектирования объекта или элемента на сцене, движущихся с превышением установленного ограничения скорости. В данном случае система анализирует только характеристики движений объекта. Более конкретные оповещения могут включать классификацию объектов или их движений (например, распознавание движений человека или животного на территории). Предопределенные оповещения основаны на соответствии или несоответствии модели поведения, введенной в систему (например, попытка индивида открыть более одного автомобиля на парковке).

А.3 Поиск по видеоизображениям в целях расследования

Обработка аналитики позволяет индексировать видеоизображения на основе таких характеристик, как форма человека, его размер, внешний вид, траектория, тип, а также модель действий. Данная информация, сохраненная в виде метаданных, позволяет проводить пространственно-временные поиски, например «найти все кадры с человеком в красной одежде, проходящем перед определенным зданием между двумя заданными датами».

Поиск по видеоизображениям в целях расследования выполняется как на пиксельном уровне, так и на уровне объекта и включает следующие задачи:

- обнаружение изменений;
- сегментация движущихся индивидов;
- мониторинг индивидов;
- классификация и идентификация индивидов;
- классификация действий и поведения.

А.4 Обнаружение и сегментация

Обнаружение изменений на видеозаписи позволяет определить модуляцию изображения, что включает не только движения индивидов. Для сегментации движущихся индивидов необходимо разделить колебания значений пикселей, соответствующие последовательным движениям, и колебания, вызванные изменениями окружающей среды.

Пример — Система предназначена для обнаружения активности на наблюдаемом пространстве, в частности, движения объектов. Система может выявить появление или исчезновение объекта (например, брошенного или украденного объекта). Система также используется для автоматического оповещения о случайных или намеренных изменениях в камере: окклюзии (пыль, паутина, влага, краска и наклейки), изменении ориентации и появления размытости.

Методы сегментации движения включают:

- вычитание фона. Метод заключается в сравнении каждого кадра в последовательности с контрольным изображением-фоном, которое представляет собой визуализируемое пространство без помех. Области изменения формируются из пикселей, имеющих разницу в интенсивности, превышающей пороговое значение. Пиксельное

вычитание между двумя изображениями очень чувствительно к малейшим изменениям окружающей среды, таким как изменения освещения и движения, характерные для пространства (например, движения листвы дерева при ветре). Для решения указанной сложности проводится адаптация фоновой модели к внутренним изменениям в окружающей среде. Метод вычитания фона подходит для помещений с контролируемыми условиями освещения и небольшим уровнем активности (например, наблюдение в коридоре);

- временная разность. Метод основан на определении разности между несколькими последовательными кадрами. Метод адаптирован к временным изменениям окружающей среды, однако может быть сверхчувствительным к определенным движениям объектов, особенно медленным. На результирующем изображении могут существовать отверстия на обнаруженных объектах. Данный метод требует проведения сглаживания с морфологическими операторами и фильтрации отверстий и слишком малых форм. Для сохранения значимых движений и исключения случайных движений может быть составлена карта областей с высоким уровнем активности на основе модели движения;

- оптический поток. Метод позволяет обнаружить согласованные направления изменения пикселей, связанных с движением объектов в пространстве. Сложные вычисления метода усложняют обработку в реальном времени. Метод является чувствительным к шуму изображения.

А.5 Отслеживание

Как правило, методы отслеживания основаны на математических методах, прогнозирующих положение человека в кадре на основе его движения в предыдущих кадрах.

Одновременное отслеживание нескольких индивидов включает такую сложную задачу, как привязка каждого индивида, детектированного на кадре, к соответствующему индивиду на последующем кадре. Такое сопоставление выполняется на основе очертаний людей, их характеристик (например, углов, площади, соотношений и т. д.) или модели их внешнего вида.

Примечание — Основную сложность при отслеживании людей представляют окклюзии (области, скрытые объектами или другими индивидами). Отслеживаемый объект может быть потерян, если он полностью или частично загражден в течение определенного периода времени. Также является сложностью разделение двух индивидов при их близком расположении, или если один индивид загораживает другого.

А.6 Классификация и идентификация объектов

Как правило, объекты, обнаруживаемые СВН, классифицируются по категориям: люди, транспортные средства, животные и т.д. Классификация может быть выполнена до отслеживания для сохранения траекторий объектов, релевантных для целей наблюдения.

Пример — Отображение человека является фигурой, большей в высоту, чем в ширину, отображение автомобиля является большим в ширину, чем в высоту. Характерные особенности имеет походка человека (в частности, определенную периодичность). Следовательно, классификация обнаруженного объекта проводится на основе свойств его формы и свойств движения в целом.

Классификация объекта позволяет проводить дальнейшее распознавание. Объекту помимо класса, к которому принадлежит объект, также назначается идентификатор. При наблюдении, в частности для контроля доступа или при поиске подозреваемого, цель состоит в распознавании конкретного индивида или определении номерного знака конкретного транспортного средства.

На способность системы правильно анализировать изображение влияет множество факторов окружающей среды: погодные условия, яркость фар, наличие грязи или повреждения номерного знака. Например, номерной знак, снятый под углом, искажает символы на изображении и усложняет процесс распознавания. Для повышения эффективности системы распознавание номеров выполняется с использованием специализированных систем, которые учитывают положение камеры и качество освещения.

А.7 Классификация действий и поведения

Анализ и интерпретация поведения означают распознавание моделей движений и определение на более высоком уровне описания действий и взаимодействий. Данная задача решается путем моделирования типичного поведения посредством обучения или определения и подбора метода сравнения, допускающего небольшие вариации.

Пример — Скрытые марковские модели, нейронные сети и байесовские сети являются одними из наиболее часто используемых методов для моделирования типичного поведения и, следовательно, для обнаружения аномального поведения. Данные методы формируют оповещения на основе статистического несоответствия предполагаемой модели. Существуют предопределенные методы обнаружения событий на основе системы правил, например формирование оповещения, если объект, размер которого превышает пороговое значение, остается неподвижным в течение определенного периода времени в данной области.

А.8 Анализ толпы

Анализ движений в толпе проводится в целях безопасности.

Пример — Анализ траектории и потока толпы. Методы могут использовать модель толпы в целом и интерпретировать движения различных частей. Для моделирования движений используются такие методы, как оптический поток и скрытые марковские модели. Модели могут комбинировать микроскопический (индивидуальный) и макроскопический (массовый) анализ.

Приложение В
(рекомендуемое)

Социальные аспекты и процессы управления

В настоящем приложении приведены дополнительные рекомендации на основе пилотных проектов биометрических технологий.

При разворачивании СВН с биометрическим распознаванием рекомендуется применять систематический подход для своевременного решения всех соответствующих вопросов. Вопросы должны быть определены в начале планирования системы и должны охватывать юридические вопросы (например, защита персональных данных, здоровья и безопасности, использование доказательств в судах), соображения безопасности (включая предупреждения о попытках взлома), удобство использования, частоту и детали испытаний и т.д.

На ранней стадии процесса планирования рекомендуется создавать структуру управления, которая объединяет заинтересованные стороны.

Вопросы, вызывающие внимание общества, могут быть решены путем создания комитета по этике, независимого от органов управления проектом. Такой комитет может работать в заранее установленных рамках этики, смоделированных на принципах из других технологических областей или использующих идеи исследовательских проектов, таких как RISE *[11]*, HIDE *[12]*, Tabula Rasa *[13]* и PRESCIENT *[14]*. Комитет по этике рассматривает вопросы помимо защиты и конфиденциальности персональных данных и может проводить консультации непредставленных групп (например, маргинализованные, временные посетители зоны наблюдения и лица с ограниченными возможностями).

Этический принцип, который часто не принимается во внимание, — это равный доступ к опыту работы биометрических систем. Хотя взаимосвязь между компонентами, интерфейсами и методами оценки работы СВН с биометрическим распознаванием известна эксплуатационному органу, но глубоко понимается только теми, кто отвечает за интеграцию системы. И наоборот, специалисты, которые отвечают за введение системы наблюдения, могут не знать о возможных воздействиях на систему. Комитет по этике может обратиться к техническим отделам университетов, колледжей искусства и дизайна и т.д. для поиска способов представления спорных вопросов в доступной форме. Впоследствии разработанные ресурсы могут быть использованы в других проектах.

Например, развернутая система может являться автономным сервисом, например для выявления премиальных клиентов в торговом центре, для недопуска индивидов из черного списка в зоны наблюдения, в бары, казино и пункты приема ставок. Однако, если позже система будет подключена как часть сети систем по всему городу, тем самым снизив затраты на мониторинг и используя его для целей правоохранительных органов, необходима подготовка другого юридического обоснования.

Работа систем видеонаблюдения с биометрическим распознаванием может привести к неблагоприятным последствиям для человека или для эффективного функционирования системы. Например, неравномерное распределение ложных предупреждений среди населения может приводить к тому, что определенных лиц неоднократно ошибочно идентифицируют как лиц из списка наблюдения, а другие станут трудно идентифицируемыми. В неудовлетворительно спроектированных системах целевые субъекты могут избежать распознавания простыми способами (например, отвернувшись от камеры), что ставит под угрозу эффективность системы. Неоднократные сообщения в средствах массовой информации о подобных ошибочных идентификациях могут привести к потере доверия к технологии.

Во время проектирования, развертывания и испытания систем должны быть учтены вопросы сбора и использования метаданных, ведения списков наблюдения и возможного доказательного использования идентификации людей в судах.

Метаданные, связанные с датчиками и камерами, список возможных совпадений в результате работы программного обеспечения для биометрического сравнения, решения оператора об оповещениях и т.д. могут быть сохранены для последующего использования при мониторинге работоспособности системы, для исследования повышения производительности или для подтверждения доказательств в судах. Рекомендуется провести анализ использования метаданных для обеспечения отсутствия избыточности персональных данных, обеспечения удовлетворительного качества данных и оптимизации поиска.

Должна быть разработана однозначная политика оператора в отношении управления списками наблюдения. При использовании изображений низкого качества качество распознавания ухудшается. Если в список наблюдения будут добавлены изображения лиц, полученные с видеокамер, необходимо заранее провести испытания системы на эффективную работу системы и установить минимальный порог качества. В некоторых сценариях несколько операторов могут использовать видеокамеры с отдельными списками наблюдения, что требует политики, которая сводит к минимуму возможность конфликтующих действий после возможной идентификации.

В сценариях, когда изображения и данные систем видеонаблюдения с биометрическим распознаванием могут быть использованы в суде, требуют внимания вопросы извлечения и безопасного управления материалами, метаданными и выводами операторов. Следует проводить периодические испытания доступности данных и пригодности процессов для поставленной цели. Должны быть разработаны стандарты обучения операторов, контро-

лирующих оповещения автоматической системы. Для точной настройки работы системы необходимо использовать информацию о подтвержденных случаях ошибочной идентификации (или пропущенной идентификации).

СВН с функцией биометрического распознавания следует обозначать как использующую данную функцию. Вывески, предупреждающие о развертывании системы, должны быть размещены на местах, которые будут видны индивидам, входящим в зону наблюдения, вместе с указаниями о том, как получить дополнительную информацию.

Приложение С
(рекомендуемое)

Измерения при получении последовательности изображений

Для целей настоящего стандарта применяются методики измерений при настройке системы во время установки, калибровки и технического обслуживания с целью обеспечения высокого качества изображения, определенные в [15], приложение С.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных и межгосударственных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте

Таблица ДА.1

Обозначение ссылочного национального, межгосударственного стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ ISO/IEC 2382-37—2016	IDT	ISO/IEC 2382-37:2012 «Информационные технологии. Словарь. Часть 37. Биометрия»
ГОСТ Р 58292—2018 (ИСО/МЭК 19795-2:2007)	MOD	ISO/IEC 19795-2:2007 «Информационные технологии. Биометрия. Эксплуатационные испытания и протоколы испытаний в биометрии. Часть 2. Методы проведения технологического и сценарного испытаний»
ГОСТ Р 58624.1—2019 (ИСО/МЭК 30107-1:2016)	MOD	ISO/IEC 30107-1:2016 «Информационные технологии. Обнаружение атаки на биометрическое предъявление. Часть 1. Структура»
ГОСТ Р 58624.2—2019 (ИСО/МЭК 30107-2:2017)	MOD	ISO/IEC 30107-2:2017 «Информационные технологии. Обнаружение атаки на биометрическое предъявление. Часть 2. Форматы данных»
ГОСТ Р 58624.3—2019 (ИСО/МЭК 30107-3:2017)	MOD	ISO/IEC 30107-3:2017 «Информационные технологии. Обнаружение атаки на биометрическое предъявление. Часть 3. Испытания и протоколы испытаний»
ГОСТ Р ИСО/МЭК 19794-5—2013	IDT	ISO/IEC 19794-5:2011 «Информационные технологии. Биометрия. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица»
Примечание — В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов: - IDT — идентичные стандарты; - MOD — модифицированные стандарты.		

Приложение ДБ
(справочное)

Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта

Таблица ДБ.1

Структура настоящего стандарта	Структура проекта международного стандарта ИСО/МЭК 30137-1:2019
1 Область применения	1 Область применения
2 Нормативные ссылки	2 Нормативные ссылки
3 Термины, определения и сокращения	3 Термины, определения и сокращения
*	4 Сопоставление терминов, используемых в области биометрических систем и используемых в области видеонаблюдения
4 Архитектура	5 Архитектура
5 Сценарии использования	6 Сценарии использования
6 Спецификация аппаратного и программного обеспечения	7 Спецификация аппаратного и программного обеспечения
7 Работа с несколькими камерами	8 Работа с несколькими камерами
8 Интерфейсы для сопутствующего программного обеспечения	9 Интерфейсы для сопутствующего программного обеспечения
9 Руководство по поддержке оператора	10 Руководство по поддержке оператора
10 Требования и рекомендации по проектированию системы	11 Требования и рекомендации по проектированию системы
Приложение А Методы и приложения видеоаналитики, связанные с биометрическим распознаванием	Приложение А Методы и приложения видеоаналитики, связанные с биометрическим распознаванием
Приложение В Социальные аспекты и процессы управления	Приложение В Социальные аспекты и процессы управления
**	Приложение С Практический пример: использование VVS с распознаванием лица для сортировки пассажиров на границе
Приложение С Измерения при получении последовательности изображений	Приложение D Измерения при получении последовательности изображений
Приложение ДА Сведения о соответствии ссылочных национальных и межгосударственного стандартов международным стандартам, использованным в качестве ссылочных в примененном международном стандарте	
Приложение ДБ Сопоставление структуры настоящего стандарта со структурой примененного в нем международного стандарта	

* Данный раздел исключен.

** Данное приложение исключено.

Библиография

[1] ИСО 12233:2017 — Фотография. Электронные фотокамеры. Измерение разрешающей способности (Photography — Electronic still-picture cameras — Resolution measurements)

[2] МЭК 61966-8:2001 — Система и аппаратура мультимедиа. Измерение цвета и управление им. Часть 8. Цветные сканеры для мультимедиа (Multimedia systems and equipment — Colour measurement and management — Part 8: Multimedia colour scanners)

[3] Grother P., & Quinn G. Mei Ngan — Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects, NIST Interagency Report 8173, January 2017, gost.e-ecolog.ru

[4] Gorodnichy D., & Granger E. (2014) — 'PROVE-IT(FRiV): framework and results'. International Biometrics Performance Conference, Gaithersburg, MD, April 1-4, 2014

[5] ISO/IEC/TR 29794-5 — Информационная технология. Качество биометрических образцов. Часть 5. Данные изображения лица (Information technology — Biometric sample quality — Part 5: Face image data)

[6] Gross R., Shi J. (2001) — The CMU motion of body (MoBo) database. Technical Report CMU-RI-TR-01-18, Robotics Institute, Carnegie Mellon University

[7] Liao S., & Zhao G. Vili Kellokumpu, Matti Pietikainen, Stan Z Li (2010) — Modeling pixel process with scale invariant local patterns for background subtraction in complex scenes, Center for Biometrics and Security Research & National Laboratory of Pattern Recognition, Institute of Automation, Chinese Academy of Sciences, Machine Vision Group, University of Oulu, Finland

[8] *ИСО/МЭК 14496-10:*2020 — Информационные технологии. Кодирование аудиовизуальных объектов. Часть 10. Улучшенное видеокодирование (Information technology — Coding of audio-visual objects — Part 10: Advanced video coding)

[9] Burton A.M, White D., McNeill A. (2010) — The Glasgow Face Matching Test. Behaviour Research Methods, Volume 42

[10] Robertson D.J, Noyes E., Dowsett A.J, Jenkins R., Burton A.M (2016) — Face Recognition by Metropolitan Police Super-Recognisers. PLoS ONE 11(2): e0150036. gost.e-ecolog.ru

[11] RISE. Research and Innovation Science Policy Experts: gost.e-ecolog.ru

[12] HIDE project — Ethical Brief on Biometrics & Embedded Technology. gost.e-ecolog.ru gost.e-ecolog.ru

[13] Rasa T. Trusted Biometrics under Spoofing Attacks: gost.e-ecolog.ru

[14] Prescient: Privacy and Emerging Technologies and Sciences: gost.e-ecolog.ru

[15] *ПНСТ 656—2022 (ИСО/МЭК 39794-17)* — *Информационные технологии. Биометрия. Расширяемые форматы обмена биометрическими данными. Часть 17. Данные походки*

УДК 004.93'1:006.89:006.354 ОКС 35.240.15

Ключевые слова: информационные технологии, биометрия, система видеонаблюдения

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *М.И. Першина*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 30.03.2023. Подписано в печать 21.04.2023. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,76.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru