УДК 004

ВЛИЯНИЕ РАЗРЕШЕНИЯ КАМЕРЫ НА УЯЗВИМОСТЬ БИОМЕТРИЧЕСКОЙ СИСТЕМЫ К ПОДДЕЛКЕ БИОМЕТРИЧЕСКОЙ ИНФОРМАЦИИ

Кузнецова Е.М., студентка гр.ДИБСС-51, 5 курс
Научный руководитель: Космачева И.М., к.т.н., доцент
ФГБОУ ВО «Астраханский государственный технический университет»
г. Астрахань

Современные технологии идентификации личности, использующие распознавание лиц, отпечатков пальцев и радужной оболочки глаз, становятся все более популярными благодаря своим высоким показателям точности и удобству эксплуатации для пользователей, которым не нужно запоминать пароли и соблюдать парольные политики.

Такие системы позволяют очень быстро, а главное эффективно проверять подлинность пользователей, они становятся все более популярными благодаря своим высоким показателям точности и удобству эксплуатации. Биометрические данные являются уникальными для каждого человека, это и делает их идеальным инструментом для подтверждения подлинности. Однако такие системы также подвержены различным видам атак, включая подделку биометрической информации. С ростом популярности данных систем, увеличивается и риск возможных преступлений, направленных на биометрию. Одним из ключевых факторов, который влияет на эффективность и надежность биометрических систем, является разрешение используемых камер. Именно оно оказывает значительное воздействие на способность системы точно считать и определить данные пользователя. В статье проведем анализ насколько сильно оказывает влияние разрешение камеры на уязвимость биометрической системы к подделкам.

Для того, чтобы оценить влияние разрешения камеры на уязвимости биометрических систем, необходимо рассмотреть процесс сбора и обработки биометрических данных. Существует два вида биометрических данных: статистические и динамические. Статические сведения — это уникальные свойства, которые даны человеку при рождении и не изменяются со временем, к ним можно отнести: рисунок вен, папиллярные узоры пальцев, радужная оболочка, сетчатка глаза, черты лица. Второй вид – это динамические сведения. Они характеризуют поведение человека. К ним относится голос, походка и поведенческие паттерны (например, нажатие клавиш на клавиатуре или подпись). На рисунке 1 представлена схема обработки динамических данных, а на рисунке 2 – статических. [1]

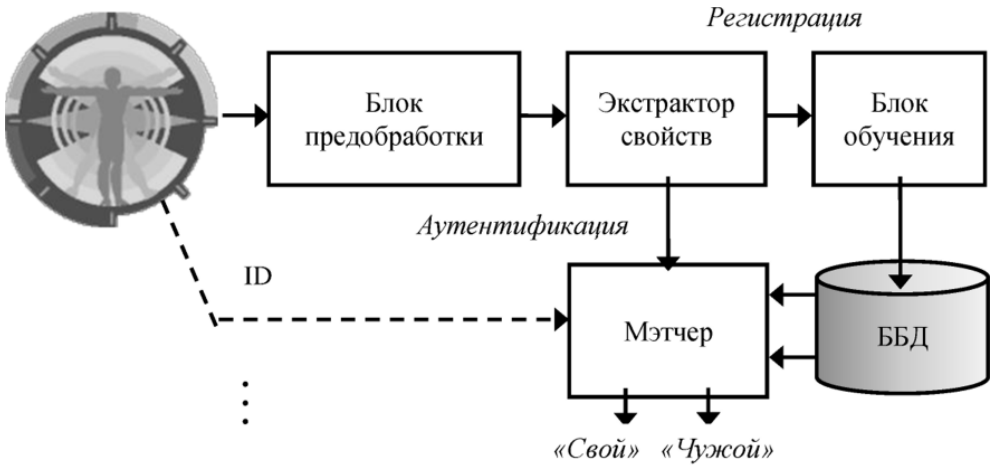

Рисунок 1 - Структурная схема динамических биометрических систем

В данной схеме блок предварительной обработки – блок, где данные преобразуются в электрические сигналы и, если это необходимо, оцифровываются и нормируются.

Экстрактор свойств – это функциональный блок, который занимается извлечением значимых биометрических параметров из поступающих данных и на их основе формирует машинную репрезентацию биометрического образа личности (биометрический эталон личности).

Блок обучения – это блок, в котором происходит усреднение данных.

ББД – это биометрическая база данных.

Мэтчер – это устройство сопоставления, осуществляющее сравнение двух шаблонов: машинной репрезентации предъявленного биометрического образа личности и биометрических эталонов, которые хранятся в базе данных. После подсчета степени сходства, он определяет, имеет объект допуск или нет.

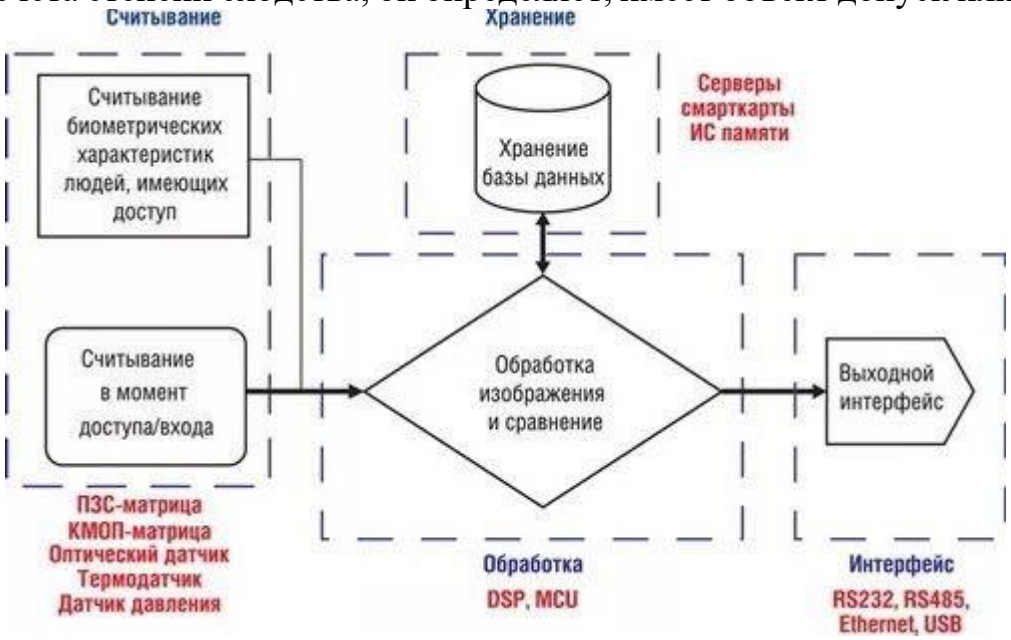

Рисунок 2 - Структурная схема статических биометрических систем

Для выбора способа идентификации в режиме реального времени задают пороги показателей качества распознавания, например, 98-99% точности распознавания, время распознавания 1 изображения – не более 5 секунд. Они определяются статистическими данными.

Для разных способов идентификации есть свои статистические значения FAR (коэффициент ложного пропуска) и FRR (коэффициент ложного отказа), например:[2]

- отпечаток пальца: FAR — 0,001%, FRR — 0,6%;
- изображение лица 2D: FAR — 0,1%, FRR — 2,5%;
- изображение лица 3D: FAR — 0,0005%, FRR — 0,1%;
- радужная оболочка глаза (РОГ): FAR — 0,00001%, FRR — 0,016%;
- сетчатка глаза: FAR — 0,0001%, FRR — 0,4%

Разрешение камеры и качество изображения

На качество распознавания изображения влияют такие характеристики камер как частота кадров, высота установки камеры, угол обзора, условия получения изображения (освещенность), фон, размер лица на фоне (фокус), др.

Разрешение камеры определяет количество пикселей, содержащихся в одном кадре изображения. Чем выше разрешение, тем больше деталей удается зафиксировать. Высокое разрешение позволяет системе лучше различать уникальные особенности каждого человека, такие как морщины, поры, текстура кожи, узоры на пальцах или структуру радужки. Все это помогает снизить вероятность ошибок в процессе верификации.

Сравним особо популярные модели камер видеонаблюдения и приведем анализ их характеристик в Таблице 1.

Таблица 1 – Сравнение камер видеонаблюдения

№	Модель	Разрешение	Фокусное расстояние	Угол обзора	Скорость кадров	Цена (руб.)	Особенности
1	Hikvision DS-2CD6365G0-IH	6 Мп	2.8–12 мм	90°–33°	25 fps	от 40 000	ИК-подсветка, WDR, поддерживает протоколы ONVIF, RTSP, интеграция с системами контроля доступа
2	Dahua IPC-HFW8232E-Z	4K (8 Мп)	2.7–13.5 мм	103°–29°	15 fps	от 45 000	Поддерживает H.265+,

							WDR, интеграция с системой управления доступом
3	Axis P3375-LVE	5 Мп	3–10.5 мм	92°–34°	30 fps	от 65 000	Светодиодная подсветка, аудиоканал, совместимость с ПО VMS
4	Uniview UNV IPC323SR3-DUGZ-VF	2 Мп	2.8–12 мм	106°–32°	25 fps	от 27 000	Совместима с системой контроля доступа, PoE, ИК-подсветка
5	Bosch FLEXIDOME IP panoramic 7000 MP	12 Мп	Панорамная камера	360°	30 fps	от 100 000	Поддержка видеостен, панорамное видеонаблюдение, интеграция с СКУД

Разновидности уязвимостей [2], [3]

Уровень уязвимости системы к атакам на биометрические системы во многом зависит от разрешения камеры. Можно выделить следующие виды:

1. Низкое разрешение – камеры, которые имеют низкое разрешение могут не захватывать достаточное количество деталей, необходимых для точного распознавания, что делает систему более уязвимой к подделкам.

2. Среднее разрешение – камеры со средним разрешением могут обеспечивать достаточное качество изображения, но они все еще могут быть подвержены различным атакам, если подделка выполнена с достаточной степенью детализации.

3. Высокое разрешение – камеры с высоким разрешением обеспечивают наиболее детализированное изображение. Это позволяет биометрическим системам различать оригиналы и подделки с максимальной эффективностью. Такое разрешение позволяет системе захватывать мельчайшие детали, такие как поры кожи или текстуру отпечатков пальцев, что делает подделку значительно сложнее.

При использовании камер с недостаточным разрешением существенно снижается безопасность биометрической системы. Низкое качество изображений ограничивает возможность точного определения индивидуальных особенностей. Это приводит к увеличению вероятности ошибочных срабатываний — как ложноположительных (ложное подтверждение личности), так и ложноотрицательных (непризнание подлинности). Это создаёт серьёзную брешь в системе безопасности, которой могут воспользоваться злоумышленники. Например, они могут попытаться обмануть систему, использую фотографии низкого качества или маски, имитирующие внешность настоящего владельца аккаунта.

Уязвимость к различным типам подделки:

1. Фотографии – системы с низким разрешением камеры можно обмануть при помощи фотографий лица. При высоком разрешении камеры есть возможность анализировать детали, которые сложно воспроизвести на фотографии. К ним можно отнести трехмерную структуру лица и естественные блики.

2. Видео – по аналогии с фотографиями, видео-подделки становятся менее эффективными против систем с высоким разрешением. Анализ мельчайших движений лица, таких как моргание или едва заметные подрагивания мышц, становится возможным благодаря большему количеству пикселей.

3. 3D-маски – при высоком разрешении камеры система может лучше анализировать трехмерную структуру лица и выявлять несоответствия между маской и реальным лицом. Однако, постоянное совершенствование технологий создания масок требует разработки более сложных алгоритмов распознавания, даже при очень высоком разрешении.

Влияние разрешения на алгоритмы Liveness Detection

Liveness Detection (детектирование живости) – это набор методов, которые используются для определения, является ли предъявляемый биометрический образец настоящим или нет. Для эффективной работы данных методов важную роль играет именно разрешение камеры. Так как только при высоком разрешении у системы есть возможность захватить наименее заметные детали.

Ограничения высокого разрешения

Несмотря на преимущества высокого разрешения, существуют и ограничения, которые играют немало важную роль в использовании биометрических систем. К таким ограничениям можно отнести:

1. Вычислительная сложность – обработка изображений высокого разрешения требует больших вычислительных ресурсов. Это может привести к замедлению процесса аутентификации.

2. Стоимость – камеры с высоким разрешением, как правило, стоят очень дорого, это может увеличить стоимость внедрения биометрической системы.

3. Объем данных – хранение и передача изображений высокой чёткости требуют большого объема памяти и пропускной способности сети.

Технологические решения для повышения безопасности

Для повышения устойчивости биометрических систем к подделкам можно использовать различные технологические решения. К ним можно отнести:

1. Использование инфракрасных камер – данные камеры могут захватывать детали, которые не видны в обычном свете, что приводит к затруднениям при попытке подделки данных.

2. Многофакторная аутентификация – это использование сразу нескольких способов аутентификации, таких как пароли или токены. Это может значительно повысить уровень безопасности системы.

3. Анализ живости – это технологии, которые способны определять, является ли объект живым (например, анализ пульса или теплового излучения).

Дополнительно можно применить алгоритмы машинного обучения, которые способны выявлять поддельные данные путем анализа текстуры кожи, глубины изображения и других параметров.

В заключении хотелось бы отметить, что разрешение камеры играет ключевую роль в обеспечении безопасности биометрических систем. Высококачественное оборудование помогает снизить уязвимость к подделке биометрической информации, улучшить точность распознавания и уменьшить риски мошенничества. Тем не менее, важно учитывать комплексный подход к защите, включающий дополнительные меры безопасности, такие как многофакторная аутентификация и регулярные обновления программного обеспечения.

Список литературы:

1. Есаков, П. DeepFake – реальная угроза для систем биометрии. Конкретизируем риски // Журнал ПЛАС №6 (302) : электрон. журн. 2023. : сайт. URL: https://plusworld.ru/journal/2023/plus-6-2023/deepfake-realnaya-ugroza-dlya-sistem-biometrii-konkretiziruem-riski/. Дата публикации: 21.06.2023.

2. Мальцев, А. Современные биометрические методы идентификации // Хабр : электрон.журн. : сайт. URL: https://habr.com/ru/articles/126144/. Дата публикации: 11.08.2011.

3. Кураков, В.И., Худадян, А.С., Баева, У.М. Анализ уязвимостей биометрических методов аутентификации // Вестник науки : электрон. журн. май 2022. № 5 (50) Т. 2. : сайт. URL: https://cyberleninka.ru/article/n/analiz-uyazvimostey-biometricheskih-metodov-autentifikatsii/viewer. Дата публикации: май 2022.