Биометрия

Маслова Анастасия Сергеевна

Содержание

1 Введение

Биометрия и криптография играют ключевую роль в обеспечении безопасности данных. Биометрия — это технология аутентификации, основанная на уникальных физических или поведенческих характеристиках человека, таких как отпечатки пальцев, радужная оболочка глаза, лицо или голос. В криптографии основное внимание уделяется шифрованию и защите данных. Интеграция биометрии с криптографией предлагает новые подходы к защите систем и данных, что делает эти методы все более популярными в современной информационной безопасности.

2 Основная часть

2.1 История биометрии

Хотя биометрия является современной технологией, ее корни уходят в далекое прошлое. Первые упоминания использования биометрических данных можно найти в древних культурах. Известно, что уже две с половиной тысячи лет назад вавилоняне подписывали документы на глиняных табличках отпечатком большого пальца. Отпечатки пальцев использовались и на Древнем Востоке. В IX веке до н. э. в Древнем Китае купцы уже подписывали так бумажные закладные. Есть доказательства, что в III веке до н. э. в империи Цинь отпечатки пальцев использовали для расследования экономических преступлений. Позже, в 19 веке, антропометрия — наука, измеряющая физические характеристики человека — стала основой для идентификации преступников. В 1882 году французский юрист и изобретатель Альфонс Бертильон представил собственную систему биометрии. Она была основана на 14 параметрах, включая длину верхней части туловища, окружность головы, длину головы, ступней, рук, пальцев, ушей. Использование отпечатков пальцев Бертильон не отрицал, но придавал им второстепенное значение. Появление анализа отпечатков пальцев в начале 20-го века ознаменовало значительный сдвиг, приведший к появлению более надежного метода идентификации личности, который используется до сих пор. В 1903 году система Бертильона уступила место дактилоскопии после громкого случая в штате Канзас, когда в одном исправительном учреждении оказались Уилл Вест и Уильям Вест — двое мужчин с совпадающими метриками. Разобраться тогда помогло только сравне-

ние отпечатков пальцев. В 1960-х годах появились первые автоматизированные системы распознавания отпечатков пальцев. В 1980-х начались исследования в области распознавания лиц и голосов. С появлением компьютерных систем и искусственного интеллекта, биометрия превратилась в высокотехнологичную отрасль, активно применяемую в цифровой безопасности.

2.2 Современные биометрические системы

По мере развития технологий усложнялись и биометрические методы. Современная биометрия включает в себя широкий спектр методов, таких как распознавание отпечатков пальцев, лиц, радужной оболочки глаза, голоса и даже поведенческие биометрические данные, такие как динамика нажатия клавиш и анализ походки. Эти методы используют передовые алгоритмы и методы машинного обучения для повышения точности и эффективности, что делает их пригодными для различных применений - от безопасного контроля доступа до проверки личности при проведении финансовых транзакций.

В контексте криптографии биометрия служит мощным инструментом аутентификации и контроля доступа, эффективно заменяя традиционные пароли и PIN-коды, которые часто уязвимы для кражи и атак методом “brute-force”. Интеграция биометрических данных в криптографические системы значительно снижает риск несанкционированного доступа. Такие методы, как биометрическое хэширование, при котором биометрические данные преобразуются в защищенный хэш, гарантируют, что конфиденциальная информация не будет храниться в необработанном виде, обеспечивая дополнительный уровень безопасности.

2.3 Биометрия в криптографии

В контексте криптографии биометрия находит применение в двух основных направлениях:

- Аутентификация. Биометрические данные могут служить фактором аутентификации для получения доступа к зашифрованной информации или устройствам. В отличие от традиционных методов аутентификации, таких как пароли или PIN-коды, биометрические данные нельзя забыть или потерять. Однако существуют риски компрометации биометрической информации, и в случае утечки она не может быть изменена, как пароль.

- Шифрование и управление ключами. Биометрические данные могут быть использованы для генерации криптографических ключей, что улучшает безопасность. Один из таких методов — это использование биометрии для защиты приватных ключей, применяемых в асимметричных криптосистемах. В таком случае биометрия может выступать в роли «ключа» к ключу.

Примером такой системы является технология Biometric Encryption (BE). Это технология, которая использует биометрические данные для шифрования и защиты информации, объединяя криптографию и биометрию. Она позволяет зашифровать и расшифровать данные с помощью уникальных характеристик человека, таких как отпечатки пальцев, голос, сетчатка или лицо. Основной целью BE является защита биометрических данных и использование их для создания криптографических ключей, что делает системы более безопасными [1].

Основные компоненты Biometric Encryption:

- Шаблоны биометрии: В традиционных биометрических системах биометрические данные хранятся как зашифрованные шаблоны (templates). Эти шаблоны используются для последующей аутентификации. В BE вместо хранения самих шаблонов биометрия используется для непосредственного шифрования данных.

- Генерация и восстановление ключей: Один из ключевых аспектов Biometric Encryption — это способность извлекать криптографические ключи на основе биометрических данных. Вместо того чтобы хранить ключи в явном виде, система использует биометрию для их создания и восстановления.

При этом исходный ключ никогда не хранится в открытом виде, что повышает безопасность.

- Связывание биометрии с секретом: В BE биометрические данные связываются с секретной информацией, например с криптографическим ключом. Это может быть реализовано через различные методы, такие как Fuzzy Commitment Scheme или Fuzzy Vault. Эти методы позволяют системе извлекать корректные ключи даже при наличии некоторой погрешности в биометрических данных, что важно, поскольку биометрия может варьироваться при каждом сканировании.
- Проверка идентичности: Во время аутентификации пользователь предоставляет свои биометрические данные. Система сравнивает их с хранимым шаблоном или пытается восстановить ключ с помощью биометрии пользователя. Если биометрические данные достаточно точно совпадают, система успешно расшифровывает данные или подтверждает личность.

3 Виды биометрических криптографических систем

В биометрических криптографических системах различают три основных типа: системы с освобождением ключа, со связыванием ключа и с генерацией ключа. Эти системы используют биометрические данные для работы с криптографическими ключами и повышают безопасность, добавляя биометрическую аутентификацию к стандартным методам шифрования.

1) Системы с освобождением ключа (Key Release Cryptosystems):

В таких системах биометрические данные пользователя используются для аутентификации, после чего система освобождает (или предоставляет доступ) криптографический ключ, хранящийся где-то отдельно (например, на сервере или в базе данных). Этот ключ, после успешной аутентификации, может использоваться для расшифровки данных или проведения других криптографических операций. Основной принцип заключается в том, что биометрия не генерирует сам ключ, а лишь служит средством для его освобождения и передачи пользователю. При этом ключ может быть защищён дополнительно, чтобы предотвратить его кражу.

Преимущества:

- Биометрия облегчает процесс доступа к ключу.
- Ключ может быть защищен сильными криптографическими методами, поскольку хранитс

Недостатки:

- Если биометрические данные скомпрометированы, злоумышленник может получить дост
- Хранение ключа в сторонних системах может подвергать его риску кибератак.

2) Системы со связыванием ключа (Key Binding Cryptosystems):

В этих системах криптографический ключ связывается с биометрическими данными пользователя. Ключ хранится в зашифрованном виде и его можно восстановить или верифицировать только при наличии корректных биометрических данных. Примером может служить схема Fuzzy Vault, где биометрические данные используются для зашифровки ключа, и только корректные биометрические данные могут расшифровать этот ключ.

Преимущества:

- Ключ не хранится в явном виде; для его восстановления необходимы уникальные б
- Биометрия добавляет дополнительный слой безопасности, делая восстановление кл

Недостатки:

- Изменчивость биометрических данных может усложнить процесс восстановления ключа
- Требует надёжных алгоритмов, которые могут работать с неточностями в биометриче

3) Системы с генерацией ключа (Key Generation Cryptosystems):

В таких системах биометрические данные используются для непосредственной генерации криптографического ключа. При каждом сканировании биометрических данных система генерирует ключ, используя стабильные характеристики биометрии (например, уникальные черты лица или отпечатки пальцев).

Схема Fuzzy Extractor — хороший пример, где биометрические данные обрабатываются для создания стабильного криптографического ключа, который затем может использоваться для шифрования данных.

Преимущества:

- Не требуется хранение ключей: ключ генерируется заново при каждом вводе биометр
- Повышенная безопасность, так как ключи не хранятся в явном виде и зависят тольк

Недостатки:

- Как и в случае с системами связывания ключа, изменчивость биометрических данных
- Требует высокой стабильности биометрических характеристик для надёжной генераци

Эти системы играют важную роль в современных системах безопасности, позволяя использовать биометрию для более надёжной защиты данных.

3.1 Преимущества использования биометрии

Одной из основных проблем в использовании биометрии в криптографии является защита биометрических данных. Если биометрические данные будут скомпрометированы, злоумышленник может получить доступ к ключевым элементам системы [2]. Для этого разрабатываются методы защиты биометрических шаблонов, такие как:

1. Генерация криптографических ключей на основе биометрии: вместо использования паролей или числовых ключей, биометрические данные могут использоваться для создания ключей. Например, отпечаток пальца может быть преобразован в криптографический ключ, который затем используется для шифрования данных.
2. Fuzzy Extractors (размытие экстракторов): это криптографический механизм, который преобразует биометрические данные в стабильные криптографические ключи, несмотря на их изменчивость. Так как биометрические данные могут немного варьироваться от измерения к измерению, fuzzy extractors помогают сгладить эти вариации.
3. Biometric Encryption (биометрическое шифрование): это процесс использования биометрических данных для шифрования сообщений. Такой подход обеспечивает двухфакторную аутентификацию, где для доступа к зашифрованным данным требуется как знание ключа, так и подтверждение личности с помощью биометрии.

4. Template Protection (защита шаблонов): биометрические шаблоны (например, хэшированные данные отпечатка пальца) можно шифровать, чтобы предотвратить их перехват и неправомерное использование.
5. Fuzzy Vault: заключается в том, что биометрические данные «прячутся» в большом наборе случайных данных, что делает их восстановление возможным только при знании корректной биометрии [3]. Fuzzy Vault можно описать следующим образом:

- Зашифровка ключа: Сначала секрет (например, криптографический ключ) кодируется как набор данных. Этот набор зашифровывается с использованием биометрических данных человека, которые являются особым набором признаков (например, особенные точки отпечатка пальца).
- Шумовые данные: Для повышения безопасности к зашифрованному набору данных добавляются дополнительные «шумовые» данные, которые не имеют отношения к биометрическим данным. Эти данные увеличивают сложность взлома, так как злоумышленник не знает, какие данные настоящие, а какие случайные.
- Разблокировка хранилища (vault): Для того чтобы получить доступ к ключу, необходимо предъявить биометрические данные, которые близко соответствуют исходным данным. Если входные данные достаточно точны, система сможет отделить настоящий набор данных от шумовых и восстановить исходный ключ.

6. Cancelable Biometrics: эта концепция решает одну из главных проблем биометрии — невозможность изменения биометрических данных в случае их компрометации. Биометрические данные уникальны и постоянны для каждого человека, и если злоумышленник получит доступ к исходным данным, невозможно «перезапустить» отпечаток пальца или радужную оболочку глаза, как можно сменить пароль. Cancelable Biometrics решает эту проблему с помощью математических преобразований биометрических данных, создавая обратимые шаблоны, которые можно изменять, не затрагивая

оригинальные данные [4]. Вместо того чтобы использовать биометрические данные в их исходной форме (например, простой отпечаток пальца), система применяет к ним определенное математическое преобразование. Это может быть геометрическое или математическое преобразование, которое превращает биометрические данные в зашифрованный шаблон (template).

3.2 Подделка биометрических данных

Биометрический спуфинг (от англ. biometric spoofing) — это попытка обмануть биометрическую систему аутентификации, используя поддельные или поддельные биометрические данные для получения несанкционированного доступа. Спуфинг может быть направлен на различные биометрические методы: отпечатки пальцев, распознавание лица, радужной оболочки, голоса и другие.

3.2.1 Примеры методов спуфинга

1. Спуфинг отпечатков пальцев. Злоумышленники могут создать поддельный отпечаток пальца с помощью материалов, таких как латекс, силикон или желатин. Эти подделки способны копировать отпечатки реального пользователя, используя различные техники, например, создание формы отпечатка с ранее снятых образцов или следов на поверхностях.
2. Спуфинг лица. Злоумышленники могут использовать фотографии, видео или 3D-модели лица, чтобы обмануть систему распознавания лица. Некоторые системы, особенно те, которые используют 2D-распознавание, могут быть уязвимы к таким атакам.
3. Спуфинг радужной оболочки. Радужная оболочка глаза содержит уникальные узоры, которые используют системы аутентификации. Однако можно создать поддельные контактные линзы с изображениями радужной оболочки или использовать высококачественные фотографии глаза для спуфинга.

4. Спуфинг голоса. Голосовые системы могут быть обмануты с помощью записей голоса пользователя или искусственно сгенерированных голосов с помощью синтеза речи.

3.2.2 Вызовы для биометрических систем

Биометрические системы должны быть устойчивыми к спуфингу, чтобы обеспечить высокую степень безопасности. Однако сопротивляемость спуфингу зависит от качества и сложности используемых алгоритмов и методов:

1. False Acceptance Rate (FAR): это показатель того, как часто биометрическая система принимает поддельные данные как подлинные. Высокий показатель FAR делает систему уязвимой к спуфингу.

2. Anti-spoofing технологии: для защиты от спуфинга используются различные методы:

3.2.3 Примеры реальных атак

Биометрический спуфинг не раз использовался в реальных атаках. Например, в 2019 году мошенники использовали технологию, имитирующую голос руководителя немецкой компании, и обманом заставили его британского подчиненного перевести 240 000 долларов на секретный счет[5]. Из других ярких примеров - в 2017 году группа Chaos Computer Club (CCC) взломала систему распознавания радужной оболочки глаза на смартфоне Samsung Galaxy S8. Они сделали это, используя высококачественную фотографию глаза владельца, напечатанную на обычном принтере, и наклеив на изображение контактную линзу, чтобы имитировать изгиб радужки [6].

3.2.4 Способы защиты от спуфинга

- Мультифакторная аутентификация (MFA): использование нескольких уровней аутентификации, таких как комбинация пароля и биометрических данных, делает атаки спуфинга менее эффективными.
- Liveness detection (определение жизненности): проверяет, является ли подаваемый биометрический образец “живым” и активным. Например, система может проверять пульс или другие физиологические реакции для определения подлинности отпечатка пальца или обнаруживать моргание глаз при распознавании лица.
- 3D-сканирование: некоторые системы распознавания лиц используют 3D-сканирование, которое сложнее обмануть с помощью фотографий или видео.
- Анализ поведения: при спуфинге голоса системы могут использовать анализ времени произнесения или других нюансов речи, чтобы выявить подделку.

4 Заключение

Биометрия в криптографии представляет собой важный шаг в обеспечении безопасности данных. Ее уникальные свойства делают биометрические системы отличным выбором для аутентификации и управления ключами в криптографических системах. Несмотря на существующие проблемы, развитие технологий защиты биометрических данных и усовершенствование криптографических алгоритмов продолжают расширять возможности интеграции биометрии в сферу информационной безопасности.

Список литературы

1. Jain A.K., Ross A., Prabhakar S. An introduction to biometric recognition // IEEE Transactions on Circuits and Systems for Video Technology. 2004. Т. 14, № 1. С. 4–20.
2. Uludag U. и др. Biometric cryptosystems: issues and challenges // Proceedings of the IEEE. 2004. Т. 92, № 6. С. 948–960.
3. Juels A., Sudan M. A Fuzzy Vault Scheme // Designs, Codes and Cryptography. 2002. Т. 38. С. 237–257.
4. Ratha N. и др. Cancelable Biometrics: A Case Study in Fingerprints // 18th International Conference on Pattern Recognition (ICPR’06). 2006. Т. 4. С. 370–373.
5. Daily Mail, 2019. URL: https://www.dailymail.co.uk/news/article-7435863/amp/Scammers-mimic-voice-German-company-executive-240-000-sent-secret-account.html?ico=amp_articleInlineText.
6. Chaos Computer Clubs breaks iris recognition system of the Samsung Galaxy S8 [Электронный ресурс]. Chaos Computer Club, 2017. URL: https://www.ccc.de/en/updates/2017/iriden.