Старанцова Е.В. Современные методы биометрической идентификации // Международный журнал информационных технологий и энергоэффективности. – 2024. – Т. 9 № 9(39) с. 44–48

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 681.5.015

СОВРЕМЕННЫЕ МЕТОДЫ БИОМЕТРИЧЕСКОЙ ИДЕНТИФИКАЦИИ

Старанцова Е.В.
ФГБОУ ВО "САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФ. М.А. БОНЧ-БРУЕВИЧА", Санкт-Петербург, Россия (193232, г. Санкт-Петербург, пр. Большевиков д.22, корп.1), e-mail: chipsociety23@mail.ru

В данной статье исследуются распространённые методы биометрической идентификации, а также новые, постепенно внедряющиеся в нашу жизнь. Рассматриваются существующие проблемы. Анализируются преимущества использования искусственного интеллекта и машинного обучения в системах биометрической идентификации.

Ключевые слова: Биометрическая идентификация, аутентификация, биометрия, машинное обучение, искусственный интеллект, взлом, информационная безопасность.

MODERN METHODS OF BIOMETRIC IDENTIFICATION

Starantsova E.V.
BONCH-BRUEVICH ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS, St. Petersburg, *Russia (193232, St. Petersburg, 22 Bolshevikov Ave., bldg. 1), e-mail:* chipsociety23@mail.ru

This article researches the common methods of biometric identification, as well as new ones, which are gradually introduced into our life. The existing problems are considered. The advantages of using artificial intelligence and machine learning in biometric identification systems are analyzed.

Keywords: Biometric identification, authentication, biometrics, machine learning, artificial intelligence, hacking, information security.

Традиционные методы аутентификации имеют определённые ограничения, влияющие на эффективность и безопасноть. Пользователи могут забывать пароли, использовать слабые комбинации или сталкиваться с угрозой фишинга, когда злоумышленники могут перехватывать необходимые данные для идентификации личности.

Биометрическая идентификация предлагает уникальный и неизменяемый способ аутентификации путём использования уникальных физических характеристик и поведения человека. Отпечатки пальцев, черты и форма лица, голос, акцент являются оригинальными для каждого и могут быть использованы для проверки личности. Другие биометрические методы включают сканирование сетчатки глаза, расположения вен, распознавание почерка и даже анализ ходьбы и мимики [1].

Использование биометрической идентификации предоставляет некоторые значительные преимущества, такие как повышение безопасности и удобства. Она может быть использована для защиты конфиденциальной информации, предотвращения мошенничества и обеспечения

быстрого доступа к ресурсам. Однако, существуют и этические аспекты, которые нужно всегда учитывать.

Прежде всего, проблемой является защита приватности. Биометрические данные являются особо чувствительными и уникальными для каждого человека. Если эти данные попадут в неправильные руки или будут использоваться без согласия субъекта, это может привести к серьезным нарушениям приватности и злоупотреблению информацией [2].

Второй аспект - это потенциальное нарушение права на свободу и автономию личности. Некоторые люди могут считать использование биометрических данных вторжением в их личную жизнь или ограничением свободы передвижения. Например, некоторые страны используют системы распознавания лиц для наблюдения за гражданами, что может вызывать беспокойство относительно возможного нарушения прав личности.

Третий вопрос - это потенциальная дискриминация и ошибки идентификации. Некоторые методы биометрической идентификации могут быть менее точными для определенных групп населения, таких как дети, пожилые люди или люди с физическими особенностями. Это может привести к некорректной идентификации или дискриминации при доступе к ресурсам или услугам.

Существует несколько способов взлома биометрических данных. Один из них - использование фальшивых отпечатков пальцев или личности. Например, злоумышленник может создать модель отпечатка пальца из силикона или другого материала и использовать её для обхода системы сканирования отпечатков пальцев.

Также возможен взлом с помощью фотографий лица или голосовых записей. Злоумышленник может использовать высококачественное фото лица или запись голоса для обмана системы распознавания лица или голоса.

Другой метод взлома биометрических данных - компрометация самой системы биометрической аутентификации. Например, злоумышленник может перехватить данные, хранящиеся на сервере, или внедрить вредоносное программное обеспечение для изменения или обхода процесса аутентификации.

Для защиты от взлома биометрических данных необходимо использовать надежные и безопасные методы сбора и хранения биометрических данных, а также усилить защиту системы от внешних атак и компрометаций. Нельзя забывать и про регулярное обновление системы для устранения уязвимостей [3].

Использование искусственного интеллекта (ИИ) и машинного обучения (МО) может значительно повысить безопасность систем биометрической идентификации, а также способствовать повышению точности таких систем. Данные технологии позволяют анализировать большие объемы данных и обучать модели на основе образцов, что приводит к более точному распознаванию идентификационных характеристик.

Преимущества использования ИИ и МО:

1. Улучшенная точность: ИИ и МО могут обучаться на большом количестве данных, что позволяет им определять более точные шаблоны для распознавания биометрических характеристик. Это помогает уменьшить вероятность ошибок идентификации (например, ложных срабатываний) и повысить надежность системы, а также.
2. Автоматизация: С использованием ИИ и МО, процесс идентификации становится автоматизирован, что ускоряет процесс и делает его более эффективным. Это особенно ценно в ситуациях, когда необходим быстрый доступ или высшая степень безопасности.

3. Адаптивность: ИИ и МО могут обучаться на основе новых данных и изменять свои модели, чтобы учитывать изменения в биометрических характеристиках людей. Например, система может обучиться распознавать лица с измененной прической или возрастом, что делает ее более гибкой и универсальной.

4. Защита от мошенничества: ИИ и МО могут помочь в обнаружении попыток мошенничества или подделки биометрических данных. Они могут анализировать характеристики, такие как текстура кожи, тепловое излучение или движения глаз, чтобы определить, являются ли представленные данные подлинными. Алгоритмы анти-маскировки и анти-склейлинга обнаруживают попытки обмануть систему с помощью маскировки лица или изменения размера изображения. Это помогает предотвратить атаки, связанные с использованием фотографий или видеозаписей вместо реального лица. Алгоритмы детекции аномалий обнаруживают аномальное поведение или необычные паттерны в биометрических данных. Например, система может автоматически определить, если поведение пользователя не соответствует его обычному образу жизни или если распознанные биометрические данные не совпадают с предыдущими записями [4]

5. Улучшение пользовательского опыта: Благодаря использованию ИИ и МО, системы биометрической идентификации могут стать более удобными для пользователей. Например, системы лицевого распознавания могут обучаться распознавать лица в различных условиях освещения или с различными выражениями лица, что делает процесс идентификации более естественным и безопасным.

Постоянно разрабатываются новейшие методы биометрической аутентификации с целью повышения точности и надежности систем идентификации, а также для более удобного и естественного взаимодействия с технологиями. Они имеют потенциал для применения в многих сферах, от безопасности и финансов до медицины и транспорта. Рассмотрим некоторые из них [5]:

1. Распознавание вены ладони: Этот метод основан на характеристиках сосудов и сети вен на ладони. Системы сканирования вены ладони благодаря инфракрасному излучению создают изображения сосудистой сети, которое затем сравнивается с заранее сохраненным шаблоном.

2. Распознавание головного мозга: Этот метод основан на электрофизиологических характеристиках головного мозга, таких как электроэнцефалограмма (ЭЭГ) и связанные с ней параметры.

3. Распознавание сердечного ритма: Этот метод основан на распознавании сердечного ритма человека с помощью электрокардиограмм (ЭКГ).

4. Распознавание шага и походки: Этот метод основан на неповторимых характеристиках шага и походки человека. Системы распознавания шага и походки используют данные с акселерометров и гироскопов для анализа движения.

5. Распознавание динамики печати пальца: Этот метод основан на характеристиках динамики печати пальца, таких как давление, скорость и стиль печати.

В целом, биометрическая идентификация имеет большой потенциал в различных областях, но ее использование должно быть осуществлено с учетом этических аспектов, чтобы защитить приватность, свободу и равенство всех людей.

Список литературы

1. Рассмотрение компонентов технологии доверительных отношений freeipa, а также вопрос о целесообразности перехода на данное решение / А. Д. Макарова, Д. Н. Смирнов, А. Ю. Цветков, И. В. Чумаков // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023) : Сборник научных статей. XII Международная научно-техническая и научно-методическая конференция. В 4 т., Санкт-Петербург, 28 февраля – 01 2023 года. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2023. – С. 775-778.
2. Модель человеко-машинного взаимодействия на основе сенсорных экранов для мониторинга безопасности компьютерных сетей / И. В. Котенко, М. В. Коломеец, В. И. Комашинский [и др.] // Региональная информатика "РИ-2018" : материалы конференции, Санкт-Петербург, 24–26 октября 2018 года. – Санкт-Петербург: Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления, 2018. – С. 149.
3. Цветков, А. Ю. Обеспечение безопасности в клиент-серверном Java приложении для учета и автоматической проверки лабораторных работ / А. Ю. Цветков, М. Е. Шалаева, М. А. Юрченко // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019) : сборник научных статей VIII Международной научно-технической и научно-методической конференцияи : в 4 т., Санкт-Петербург, 27–28 февраля 2019 года. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2019. – С. 756-761.
4. Оценка рисков и угроз безопасности в среде "умный дом" / А. М. Гельфанд, А. А. Казанцев, А. В. Красов, Г. А. Орлов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2020) : IX Международная научно-техническая и научно-методическая конференция : сборник научных статей, Санкт-Петербург, 26–27 февраля 2020 года. Том 1. – Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2020. – С. 316-321.
5. Применение физически неклонируемых функций для выполнения аутентификации в среде интернета вещей / В. Н. Волкогонов, А. А. Казанцев, Г. А. Орлов, Д. Н. Смирнов // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021) : сборник научных статей: в 4-х томах, Санкт-Петербург, 24–25 февраля 2021 года. Том 4.–Санкт-Петербург: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, 2021. – С. 409-414.

References

1. Consideration of the components of the freeipa technology of trust relations, as well as the question of the expediency of switching to this solution / A.D. Makarova, D. N. Smirnov, A. Yu. Tsvetkov, I. V. Chumakov//Actual problems of infotelecommunications in science and education (APINO 2023): Collection of scientific articles. XII International Scientific-technical and scientific-methodical Conference. At 4 t., St. Petersburg, February 28 – 01, 2023. Volume 1. – St. Petersburg: St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, 2023. – pp. 775-778.

2. A model of human-machine interaction based on touch screens for monitoring the security of computer networks / I. V. Kotenko, M. V. Kolomeets, V. I. Komashinsky [et al.] // Regional Informatics "RI-2018" : materials of the conference, St. Petersburg, October 24-26, 2018. – St. Petersburg: St. Petersburg Society of Informatics, Computer Technology, Communication and Control Systems, 2018. – p. 149.
3. Tsvetkov, A. Yu. Ensuring security in a client-server Java application for accounting and automatic verification of laboratory work / A. Yu. Tsvetkov, M. E. Shalaeva, M. A. Yurchenko // Actual problems of infotelecommunications in science and education (APINO 2019) : collection of scientific articles of the VIII International Scientific, Technical and Scientific-methodological Conference : in 4 volumes, St. Petersburg, February 27-28, 2019. Volume 1. – St. Petersburg: St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, 2019. – pp. 756-761.
4. Assessment of risks and security threats in the smart home environment / A.M. Gelfand, A. A. Kazantsev, A.V. Krasov, G. A. Orlov // Actual problems of infotelecommunications in science and education (APINO 2020) : IX International Scientific, Technical and scientific-methodological conference: collection of scientific articles, St. PetersburgSt. Petersburg, February 26-27, 2020. Volume 1.–St. Petersburg: St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, 2020. – pp. 316-321.
5. The use of physically non-cloned functions to perform authentication in the Internet of Things environment / V. N. Volkogonov, A. A. Kazantsev, G. A. Orlov, D. N. Smirnov // Actual problems of infotelecommunications in science and education (APINO 2021) : collection of scientific articles: in 4 volumes, St. Petersburg, 24-25 February 2021. Volume 4. – St. Petersburg: St. Petersburg State University of Telecommunications named after Prof. M.A. Bonch-Bruevich, 2021. – pp. 409-414.