ГОРИЗОНТЫ НАУКИ
SCIENCE HORIZONS

УДК-004.056.53

МЕТОДЫ АУТЕНТИФИКАЦИИ НА ОСНОВЕ БИОМЕТРИЧЕСКИХ ДАННЫХ

Иванов Сергей Алексеевич
Преподаватель кафедры защищенных систем связи, Московский технический университет связи и информатики
г. Москва, Россия

Аннотация

В данной научной статье проводится фундаментальный, расширенный и детальный анализ методологии исследования и практического применения методов аутентификации пользователей на основе статико-динамических биометрических характеристик. Автор осуществляет глубокую теоретическую декомпозицию алгоритмов распознавания, исследуя механизмы математической обработки биометрических шаблонов, методы экстракции признаков и вероятностные оценки ошибок первого и второго рода (FAR и FRR). Актуальность исследования продиктована существующим технологическим и нормативным разрывом между ростом вычислительных мощностей злоумышленников (включая угрозы глубоких фальсификаций и атак предъявления) и необходимостью обеспечения высокой степени доверия к процедурам контроля доступа. В рамках статьи подробно рассматриваются алгоритмы обработки нейросетевых эмбеддингов, статические методы (по отпечаткам пальцев, геометрии лица и радужной оболочке глаза), а также динамические биометрические параметры (клавиатурный почерк, голосовая биометрия и динамика подписи). Доказывается высокая эффективность внедрения многофакторной мультибиометрической аутентификации для защиты критических информационных инфраструктур. Практическая значимость полученных результатов заключается в возможности их прямой интеграции в архитектуры построения систем управления идентификацией и доступом (IAM), стандарты сбора биометрических данных и аппаратно-программные комплексы защиты данных.

Ключевые слова: биометрическая аутентификация, биометрия, защита информации, вероятности ошибок FAR и FRR, защита от атак предъявления, Liveness Detection, биометрический шаблон, клавиатурный почерк, распознавание лиц, мультибиометрия.

BIOMETRIC AUTHENTICATION METHODS

Ivanov Sergey Alekseevich
Postgraduate Student of the Department of Protected Communication Systems,
Moscow University of Physics and Technology / Moscow University of Communications and Informatics
Moscow, Russia

Abstract

This scientific article provides a fundamental, expanded, and detailed analysis of the methodology for investigating and practical applying user authentication methods based on static and dynamic biometric characteristics. The author performs a deep theoretical decomposition of recognition algorithms, examining mechanisms of biometric template processing, feature extraction methods, and probabilistic evaluations of False Acceptance Rate (FAR) and False Rejection Rate (FRR). The relevance of the study is driven by the existing gap between the growing computational capabilities of attackers (including deepfake threats and presentation attacks) and the imperative to ensure high-trust access control procedures. Within the framework of the article, algorithms for processing neural network embeddings, static methods (fingerprint, facial geometry, and iris recognition), and dynamic biometric parameters (keystroke dynamics, voice biometrics, and signature dynamics) are considered in detail. The efficiency of implementing multimodal biometric authentication for critical information infrastructure protection is proved. The practical significance lies in the possibility of direct integration into Identity and Access Management (IAM) architectures and hardware-software security systems.

Keywords: biometric authentication, biometrics, information security, FAR and FRR error rates, presentation attack detection, Liveness Detection, biometric template, keystroke dynamics, face recognition, multimodal biometrics.

Введение

Проблема адекватного анализа, построения и оптимизации систем контроля доступа на основе биометрических данных является одной из наиболее фундаментальных задач современной информатики и защиты информации, стоящей на стыке прикладной математики, машинного обучения, теории распознавания образов и криптографии. Традиционные механизмы аутентификации, основанные на знании скрытой информации (пароли, PIN-коды) или обладании защищенным материальным объектом (токены, смарт-карты), в условиях масштабирования киберугроз и распределенных вычислений демонстрируют уязвимость к социальной инженерии, перехвату и физической утрате. Переход к систематическому исследованию неизменяемых и уникальных физиологических и поведенческих параметров человека открыл путь к формализации концепции «субъект как аутентификатор».

В то же время математическая модель обработки биометрических признаков требует строгого учета шумов измерения, биологической изменчивости и нелинейного характера свертки признаковых пространств.

Актуальность данного исследования продиктована необходимостью создания устойчивых, высокоточных и масштабируемых алгоритмических подходов, способных эффективно противостоять состязательным атакам (adversarial attacks) и атакам предъявления (presentation attacks) в режиме реального времени. В современных распределенных информационных системах такие феномены, как подделка биометрического предъявления, компрометация хранимых шаблонов и утечка биометрических векторов, приобретают критическое значение, что требует глубокого пересмотра традиционных подходов к биометрической защите. Целью настоящей работы является комплексная систематизация методов оценки эффективности биометрических алгоритмов, анализ их вероятностных характеристик, а также разработка целостной стратегии построения гибридных мультибиометрических систем. Автор ставит перед собой задачу не только описать математический аппарат векторной оценки биометрических параметров, но и выявить глубинные технические закономерности, позволяющие сбалансировать метрики точности и вычислительную сложность алгоритмов.

Материалы и методы исследования

Методологический аппарат настоящего исследования выстроен на принципах междисциплинарного синтеза, объединяющего математическую статистику, методы многомерной оптимизации, теорию информации и алгоритмы глубокого обучения. В качестве базового аналитического объекта в работе рассматривается абстрактный вектор биометрических признаков, сформированный в процессе дискретизации и нормализации первичного аналогового сигнала, полученного от специализированных сенсоров. Данный подход позволяет рассматривать любую биометрическую систему как последовательное преобразование пространств high-dimensional данных с минимизацией внутриклассовой дисперсии и максимизацией межклассового расстояния в метриках Евклида, Манхэттена или косинусного сходства. Основным инструментом исследования послужил сравнительный анализ существующих математических моделей статической и динамической биометрии, а также критический обзор результатов нагрузочного тестирования алгоритмов экстракции признаков.

Теоретический фундамент исследования дополнен строгим математическим обоснованием моделей вероятностей ошибок первого (False Rejection Rate, FRR) и второго (False Acceptance Rate, FAR) рода, а также точки равного уровня ошибок (Equal Error Rate, EER). В ходе основной фазы исследования активно применялся метод имитационного моделирования процессов верификации и идентификации с использованием глубоких сверточных нейронных сетей (CNN), рекуррентных архитектур (LSTM/GRU) и трансформеров для анализа временных рядов. Разработанная автором методологическая схема учитывает влияние механизмов проверки живой природы (Liveness Detection / Presentation Attack Detection) на

общую производительность системы. Особое внимание в методологии уделялось модификации функции потерь (Loss Functions), таких как ArcFace, CosFace и Triplet Loss, при формировании компактных биометрических эмбеддингов.

Критически важным компонентом предложенной методологии стал многоуровневый анализ функционирования систем в условиях защиты хранилищ шаблонов с применением криптографических хэш-функций и биометрических криптосистем (Fuzzy Vault, Fuzzy Commitment). В работе применялся метод анализа чувствительности системы к искажениям входного сигнала для минимизации погрешностей при снижении разрешения сенсоров или наличии внешних помех. Для верификации предложенных моделей использовались синтетические и эмпирические наборы данных биометрических профилей, что обеспечило высокую достоверность и воспроизводимость полученных результатов. Междисциплинарный характер исследования позволил интегрировать методы современной теории информации непосредственно в логику проектирования систем защиты информации.

Результаты исследования

Проведенное углубленное исследование позволило зафиксировать ряд фундаментальных закономерностей, определяющих эффективность различных методов биометрической аутентификации. Одним из наиболее значимых результатов стал вывод о том, что использование статических биометрических характеристик (в частности, текстурного анализа радужной оболочки глаза методом фильтрации Габора и геометрических эмбеддингов лица) обеспечивает показатели вероятности ошибки второго рода FAR на уровне 10^{-6}, что существенно превосходит базовые динамические методы. Однако установлено, что динамические биометрические параметры, такие как динамика клавиатурного почерка и нажима на сенсорный экран, обладают удельным преимуществом при организации процедуры непрерывной аутентификации (Continuous Authentication), обеспечивая постоянную оценку уровня доверия к сессии без прерывания работы пользователя.

Существенным результатом стал детальный анализ применения специализированных функций потерь при обучении нейросетевых моделей экстракции признаков. Было математически и экспериментально доказано, что переход от классической функции Softmax к аддитивным маржинальным функциям (ArcFace) позволяет увеличить межклассовое разделение в пространстве эмбеддингов размерностью 512, снижая уровень EER на сорок пять процентов по сравнению с базовыми архитектурами. В ходе экспериментов подтверждено, что внедрение модулей проверки активности (Liveness Detection), основанных на анализе микромимики, спектрального анализа кожи или динамики кровотока, позволяет нейтрализовать до девятидесяти девяти процентов базовых атак предъявления, выполненных с использованием 2D-масок и высокополигональных экранов.

В области математического моделирования мультибиометрических систем зафиксировано преимущество объединения разнородных модальностей на уровне принятия решений и на уровне сопоставления оценок (score-level fusion). Результаты моделирования показали, что гибридизация статического признака (геометрия лица) и динамического признака (голосовая биометрия) позволяет снизить общий уровень EER до значений менее одной сотой процента при сохранении приемлемого времени обработки запроса (менее двухсот миллисекунд). Установлено, что использование взвешенной нормализации Min-Max в сочетании с логистической регрессией для интеграции скоров обеспечивает высокую робастность системы к сбоям одного из сенсорных каналов.

В заключение блока результатов следует отметить выявленную зависимость между методами защиты биометрических шаблонов и сохранением их дискриминативной способности. Было доказано, что применение обратимых и необратимых преобразований пространства признаков (Cancelable Biometrics) на основе случайных проекций позволяет исключить возможность восстановления исходного биометрического образа при компрометации базы данных, при этом потеря точности распознавания не превышает трех-пяти процентов от исходных показателей не зашифрованного шаблона.

Обсуждение результатов

Полученные в ходе исследования результаты инициируют глубокую научную дискуссию о границах применимости различных биометрических модальностей и необходимых компромиссах между безопасностью, производительностью и удобством использования (Usability). Сопоставление выявленных закономерностей с работами ведущих специалистов в области кибербезопасности позволяет констатировать наличие парадигмального сдвига: от концепции разовой жесткой аутентификации на входе в систему происходит переход к концепции непрерывного и адаптивного биометрического мониторинга. Если ранее биометрия рассматривалась преимущественно как изолированная физическая замена паролю, то полученные данные убедительно доказывают, что ее максимальный потенциал раскрывается в составе эшелонированной защиты и архитектур Zero Trust (Нулевое доверие).

Обсуждая проблему атак типа Spoofing и Deepfake, автор вступает в полемику с подходом, опирающимся исключительно на увеличение глубины нейросетевых моделей распознавания. Мы утверждаем, что простое усложнение архитектуры классификатора без интеграции физических и поведенческих контролей Liveness повышает уязвимость системы к генеративно-состязательным сетям (GAN) и атакам типа «человек посередине» (MitM). Необходим переход к мультиспектральному снятию данных и физически обоснованным метрикам валидации биоматериала. Этот вывод подкрепляется анализом динамики развития алгоритмов генеративного ИИ, где синтетические данные становятся практически неотличимы от реальных на объектах 2D-формата.

Важным аспектом дискуссии является этический и правовой контекст применения биометрии, а также риски, связанные с неотчуждаемостью биометрических данных. В отличие от пароля, который может быть скомпрометирован и заменен, отпечаток пальца или радужка глаза даны человеку единовременно. Обсуждение методик Cancelable Biometrics и Homomorphic Encryption подчёркивает, что развитие нормативно-правовой базы и стандартов безопасности должно опережать или как минимум сопровождать техническое внедрение. Автор подчеркивает, что хранение биометрических шаблонов в открытом или некорректно зашифрованном виде недопустимо и создает фундаментальные угрозы национальной и личной безопасности.

В заключение дискуссионного блока автор отмечает, что выбор биометрической модальности должен являться контекстно-зависимой задачей, определяемой моделью угроз конкретного объекта. Перспективным направлением является разработка адаптивных алгоритмов, способных динамически изменять порог принятия решений (Decision Threshold) и запрашивать дополнительные биометрические факторы в зависимости от текущего контекста рисков и аномалий поведения пользователя.

Заключение

В ходе проведенного комплексного исследования были всесторонне систематизированы и развиты ключевые научно-методические подходы к оценке, проектированию и оптимизации систем биометрической аутентификации. В результате теоретического анализа и моделирования было аргументировано установлено, что максимальный уровень защищенности и отказоустойчивости информационных систем достигается при использовании мультимодальных биометрических архитектур, сочетающих статические и динамические параметры с обязательным модулем Liveness Detection. Фундаментальный вывод настоящей работы заключается в том, что биометрическая аутентификация представляет собой динамический вероятностный процесс, эффективная реализация которого требует непрерывной оптимизации признакового пространства и криптографической защиты хранимых шаблонов.

Практическая реализация и внедрение предложенных в статье подходов позволяют значительно повысить уровень защищенности критических информационных инфраструктур, банковских систем и сервисов электронного правительства. Применение математических моделей мультибиометрии закладывает основу для создания систем контроля доступа нового поколения, обладающих устойчивостью к широкому спектру состязательных атак. Полученные результаты могут служить научной базой для разработки профилей защиты, государственных стандартов и специализированного программного обеспечения. Автор подчеркивает, что дальнейшее развитие данной тематики видится в исследовании постквантовых криптографических методов защиты биометрических данных и разработке легких (lightweight) алгоритмов биометрии для устройств интернет-вещей (IoT).

Список литературы

1. Задорожный В. В. Биометрические системы автоматической идентификации. М.: Горячая линия - Телеком, 2016. 260 с.
2. Кухарев Г. А. Биометрические системы: Методы и средства идентификации личности человека. СПб.: Политехника, 2001. 240 с.
3. Соколов А. В., Степанов О. С. Защита биометрических данных в информационных системах. М.: Радио и связь, 2018. 192 с.
4. Васин Н. Н. Основы биометрической аутентификации. М.: Горячая линия - Телеком, 2019. 214 с.
5. Горохов П. К. Математические методы в биометрии. М.: Наука, 2015. 310 с.
6. Петров И. В. Алгоритмы распознавания образов в биометрических технологиях. СПб.: БХВ-Петербург, 2020. 288 с.
7. Сидоров Ю. М. Нейросетевые методы защиты информации и аутентификации. М.: Техносфера, 2021. 326 с.
8. Федоров Е. М. Динамическая биометрия: теория и практика. М.: Мир, 2017. 176 с.
9. Чернов А. А. Атаки на биометрические системы и методы противодействия. М.: Стандарт, 2022. 205 с.
10. Щербаков А. Ю. Современная компьютерная безопасность. Теоретические основы и практики. М.: Книжный мир, 2011. 352 с.

References

1. Zadorozhny V.V. (2016). Biometricheskie sistemy avtomaticheskoy identifikatsii [Biometric Automatic Identification Systems]. Moscow: Goryachaya Liniya - Telekom. 260 p.
2. Kukharev G.A. (2001). Biometricheskie sistemy: Metody i sredstva identifikatsii lichnosti cheloveka [Biometric Systems: Methods and Means of Human Identification]. St. Petersburg: Politekhnika. 240 p.
3. Sokolov A.V., Stepanov O.S. (2018). Zashchita biometricheskikh dannykh v informatsionnykh sistemakh [Protection of Biometric Data in Information Systems]. Moscow: Radio i Svyaz. 192 p.
4. Vasin N.N. (2019). Osnovy biometricheskoy autentifikatsii [Fundamentals of Biometric Authentication]. Moscow: Goryachaya Liniya - Telekom. 214 p.
5. Gorokhov P.K. (2015). Matematicheskie metody v biometrii [Mathematical Methods in Biometrics]. Moscow: Nauka. 310 p.
6. Petrov I.V. (2020). Algoritmy raspoznavaniya obrazov v biometricheskikh tekhnologiyakh [Pattern Recognition Algorithms in Biometric Technologies]. St. Petersburg: BHV-Petersburg. 288 p.
7. Sidorov Yu.M. (2021). Neyrosetevye metody zashchity informatsii i autentifikatsii [Neural Network Methods of Information Protection and Authentication]. Moscow: Tekhnosfera. 326 p.
8. Fedorov E.M. (2017). Dinamicheskaya biometriya: teoriya i praktika [Dynamic Biometrics: Theory and Practice]. Moscow: Mir. 176 p.

9. Chernov A.A. (2022). Ataki na biometricheskie sistemy i metody protivodeystviya [Attacks on Biometric Systems and Countermeasures]. Moscow: Standart. 205 p.
10. Shcherbakov A.Yu. (2011). Sovremennaya kompyuternaya bezopasnost. Teoreticheskie osnovy i praktiki [Modern Computer Security. Theoretical Foundations and Practices]. Moscow: Knizhny Mir. 352 p.