Инженерный вестник Дона, №2(2025)
ivdon.ru/ru/magazine/archive/n2y2025/9860

Применение нейросетивых технологий для аутентификации пользователей в современных мобильных системах

В.Ю. Герасин

МИРЭА - Российский технологический университет, Колледж программирования и кибербезопасности, Москва

Аннотация: В условиях стремительного развития мобильных технологий и повышения рисков утечки данных, обеспечение надежной аутентификации пользователей становится одной из ключевых задач информационной безопасности. Настоящая статья посвящена исследованию применения нейросетевых технологий для биометрической аутентификации в современных мобильных системах. В рамках статьи проведен всесторонний анализ существующих методов биометрической аутентификации, таких, как распознавание лиц, анализ голоса и отпечатков пальцев. Особое внимание уделено особенностям работы методов, точности и устойчивости к атакам. Приведены основные достоинства и недостатки каждого из рассмотренных методов аутентификации.
В конце статьи представлено практическое применение разработанного алгоритма нейросетевой аутентификации, основанного на анализе отпечатков пальцев, интегрированного в модуль идентификации абонента (Subscriber Identification Module – SIM-карта). Этот инновационный подход не только повышает уровень безопасности мобильных устройств, но и обеспечивает удобство для пользователя. Реализация данного примера станет основой для дальнейшего исследования, представленным в диссертационной работе, что подчеркивает значимость интеграции нейросетевых технологий в процессы аутентификации. Результаты исследования будут полезны как для ученых, так и для разработчиков в области информационной безопасности, открывая новые горизонты для совершенствования биометрических систем в мобильной среде.
Ключевые слова: аутентификация, нейросети, биометрия, мобильные системы, информационная безопасность, глубинное обучение, гибридные технологии, модуль идентификации абонента.

Введение

Популярность и важность мобильных устройств растёт с каждым годом, как и риски, связанные с угрозами информационной безопасности. В связи с этим перед специалистами возникает необходимость внедрения современных и надежных методов аутентификации пользователей, способных противостоять актуальным угрозам. Традиционные подходы, такие, как пароли и пуш-уведомления, не обеспечивают должного уровня защиты, что, в свою очередь, создает стимул для применения современных нейросетевых технологий для анализа биометрических данных пользователей.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

Современные методы аутентификации

Традиционные методы аутентификации, такие как пароли, персональные идентификационные номера (Personal Identification Number – PIN) и графические ключи, являются одними из самых распространённых способов защиты данных пользователей. Однако с точки зрения информационной безопасности они обладают как достоинствами, так и значительными недостатками, которые делают их уязвимыми перед современными угрозами.

Парольная аутентификация – это метод идентификации и проверки подлинности пользователя или системы на основе ввода пароля.

Такой способ защиты данных имеет ряд преимуществ и недостатков.

Преимущества заключаются в лёгкости использования и реализации; универсальность способа, из-за чего парольную аутентификацию можно применять для любой системы, которая адаптирована для этого; не требует сложного оборудования для обслуживания [1].

Несмотря на преимущества, у данного способа есть ряд недостатков, такие, как: низкая стойкость к атакам, так как большинство пользователей пренебрегают базовыми правилами информационной безопасности, в связи с чем создают максимально простые пароли, что облегчает атаку полным перебором (brute force); простые пароли очень подтверждены фишинговой атаки; в случае утечки базы данных злоумышленники могут использовать слабые пароли для доступа к другим аккаунтам, если они используются повторно [2].

Следующим способом защиты является PIN – это последовательность чисел, которая обычно используется для доступа к устройствам или приложениям. Данный метод часто используется в мобильных устройствах и банковских приложениях.

Преимущества данного способа заключается в простате и удобстве, так как обычному пользователю легче запомнить короткий набор цифр, чем

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

сложный пароль; более быстрый ввод, особенно на устройствах с сенсорными экранами [3].

Недостатками являются: лёгкость угадывания пароля, так как большинство пользователей выбирают довольно предсказуемые последовательности символов; злоумышленник может подглядеть ввод PIN-код в общественном месте.

Последним традиционным способом защиты является графический ключ. Графический ключ – способ аутентификации, при котором пользователь проводит по сенсорному экрану, соединяя точки в определённой последовательности. Данный метод стал очень популярным на мобильных устройствах.

Преимуществами данного способа является интуитивность и удобство, так как обычному пользователю легче запомнить рисунок, а не текстовый пароль или цифры; быстрота ввода.

Недостатки графического ключа: предсказуемость узоров, например, прямые линии или формы, напоминающее буквы; злоумышленник может легко запомнить последовательность, если увидит, как пользователь её вводит; необходимо использовать устройство с сенсорным экраном [4].

Подводя итог вышесказанного, можно с уверенностью сказать, что традиционные методы, несмотря на их простоту и доступность, уже отстают от требований безопасности. Их недостатки делают пользователей уязвимыми перед фишинговыми атаками, утечками данных и атаками с использованием социальной инженерии. Для повышения надёжности таких методов необходима интеграция с современными технологиями, включая нейросети, биометрию и многофакторную аутентификацию, что может значительно увеличить их эффективность и устойчивость к угрозам [3].

Современные биометрические методы аутентификации

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

Биометрические методы аутентификации основываются на уникальных физических или поведенческих характеристиках пользователя, что делает их популярным выбором в современных информационных системах. Такие методы обеспечивают более высокий уровень защиты, по сравнению с традиционными подходами, однако имеют свои уязвимости и ограничения.

Аутентификация по отпечатку пальца

Один из популярных способов биометрии является аутентификации по отпечатку пальцев. У данного вида биометрической аутентификации есть тонкости в работе, которые заключаются в использовании минуций отпечатка пальца пользователей [5].

Минуции — это специфические точки на отпечатке пальца, где линии папилляра прерываются, разветвляются или сливаются. Эти точки являются ключевыми элементами для идентификации личности, поскольку они уникальны для каждого человека [6]. Минуции делятся на три основных типа:

– конец (termination) — точка, где линия заканчивается;
– разветвление (bifurcation) — точка, где одна линия делится на две;
– дуга (ridge) — точка, где линия меняет направление.

Алгоритмы поиска минуций определяют координаты этих точек и их ориентацию на изображении.

На основе информации о минуциях создается шаблон отпечатка пальца. Шаблон включает в себя координаты всех минуций, их типы и ориентации. Этот шаблон хранится в зашифрованном виде в памяти устройства или базе данных [7].

Метод аутентификации пользователей по отпечатку пальца обеспечивает высокий уровень безопасности благодаря уникальности каждого отпечатка, что исключает вероятность неверной идентификации. Кроме того, данный

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

метод обеспечивает удобство и скорость процесса аутентификации, позволяя пользователям быстро и легко получать доступ к системе. Также метод обеспечивает устойчивость к подделке и возможность интеграции в многофакторные системы аутентификации, что делает его привлекательным выбором для современных решений в области безопасности [2].

Несмотря на все удобства и преимущества у данного решения есть минусы, например, метод может подвергаться угрозам, связанным с несовершенством технических систем, что приводит к возможным ошибкам в идентификации и несанкционированному доступу при использовании поддельных отпечатков. Кроме того, биометрические данные являются статичными и, в отличие от других методов аутентификации, не могут быть изменены в случае компрометации, что создает дополнительные риски для конфиденциальности и безопасности пользователей [8].

Биометрическая аутентификация на основе распознания лица

Другим популярным методом является распознание лица. Особенностью данного способа аутентификации является выделение ключевых точек на лице, так называемых ландмарков. Эти точки включают в себя углы глаз, кончик носа, уголки рта и другие характерные особенности. Обычно выделяется от 30 до 100 таких точек, хотя современные системы могут использовать гораздо больше.

На основе выделенных ландмарков создается геометрическая модель лица. Эта модель представляет собой набор координат, описывающих положение каждой ключевой точки относительно других. Геометрические параметры могут включать расстояния между точками, углы между линиями, соединяющими эти точки, и другие характеристики [4].

Геометрическая модель преобразуется в вектор признаков – набор чисел, который описывает уникальные черты лица. Векторы признаков создаются

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

таким образом, чтобы минимизировать влияние внешних факторов, таких как освещение, выражение лица или поворот головы [9].

Метод аутентификации пользователя по средствам распознавания лица обеспечивает высокий уровень удобства и быстроты, позволяя пользователям без физического контакта осуществлять идентификацию в реальном времени при помощи камер, что делает процесс аутентификации интуитивно понятным. Кроме того, технологии глубокого обучения, применяемые в системах распознавания лиц, обеспечивают высокую точность и устойчивость к подделкам, что повышает уровень безопасности данных пользователей [6].

Несмотря на все преимущества и удобства у данного метода, есть свои минусы, такие как: условия освещения, из-за которого низкая освещенность или излишний свет могут снижать точность системы; методика синтеза изображения или голоса, основанная на искусственном интеллекте (Deepfake) и маски до сих пор составляют уязвимость для сканеров, особенно тех, которые основаны на 2D-сканировании, напечатанные на 3D принтере модели, созданные при помощи искусственного интеллекта [7, 10].

Биометрическая аутентификация на основе распознания голоса

Метод биометрической аутентификации, который использует уникальные характеристики голоса человека для подтверждения его личности. Голос каждого человека уникален благодаря комбинации физических характеристик речевого тракта гортань, глотка, носовые пазухи, а также индивидуальных манер речи и интонации.

Особенностью работы метода является выделение системой ключевых особенностей голоса, такие как: форманты – частоты, при которых голос усиливается за счет резонанса в речевом тракте; мел-частотные кепстры (MFCC) – коэффициенты, характеризующие спектр звука, особенно важные для распознавания речи; спектральные характеристики – распределение

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

энергии звука по различным частотам; динамические параметры – изменения громкости и тембра со временем [11].

Эти данные преобразуются в числовую модель, которая отражает уникальные характеристики голоса конкретного индивида. На основе собранной информации формируется эталонный шаблон голоса, который будет служить основой для сопоставления с последующими образцами. Данный шаблон включает все ранее выделенные параметры и сохраняется в базе данных системы [1].

У данной системы аутентификации есть свой ряд плюсов: удобство, которое проявляется в том, что пользователю достаточно произнести несколько фраз, чтобы подтвердить свою личность; универсальность в том, что голосом можно управлять дистанционно, без необходимости физического контакта с устройством; высокая точность современных систем способны различать даже небольшие различия в голосах людей [12].

Но также стоит учитывать недостатки и ограничения: изменчивость голоса - голос может изменяться под влиянием различных факторов, таких как болезнь, стресс или усталость; фоновый шум - шумы окружающей среды могут затруднить точное распознавание голоса; обман системы – генерация голоса при помощи искусственного интеллекта [2].

Исходя из рассмотренных методов аутентификации можно сделать вывод, что отпечаток пальца является наиболее безопасным видом, который при должном обеспечении надежности хранения шаблона сложнее всего фальсифицировать [13].

Реализация алгоритма нейросетевой аутентификации в sim-карту

В качестве практической реализации рассмотрен пример применения алгоритма нейросетевой аутентификации, основанного на анализе отпечатков пальцев, создание шаблона и интеграцию его в файловой системе модуля идентификации абонента (Subscriber Identification Module – SIM-карта).

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

Процесс представляет собой значительный шаг вперед в области мобильной безопасности. Такой алгоритм обеспечивает высокую степень защиты данных пользователя благодаря использованию уникальных биометрических характеристик, что позволяет минимизировать риски несанкционированного доступа [14].

В основе алгоритма лежит архитектура глубокого обучения, адаптированная для обработки изображений отпечатков пальцев. Сначала сканированный отпечаток проходит предварительную обработку, включая нормализацию и удаление шумов, что способствует повышению точности последующего анализа. Затем с использованием сверточных нейронных сетей (Convolutional Neural Networks – CNN) осуществляется экстракция признаков, что позволяет выделить ключевые особенности отпечатка. Полученные признаки подвергаются обучению на заранее собранном наборе данных, где алгоритм оптимизирует свои параметры для достижения максимальной точности распознавания. Отпечаток пальца сохраняется в файловой системе SIM-карты с добавлением шифрования [9].

Метод сохранения шаблона отпечатков пальцев в файловой системе SIM-карты с использованием шифрования данных представляет собой многоступенчатый процесс, который обеспечивает как эффективность, так и безопасность хранения биометрической информации. Данный процесс включает в себя несколько ключевых этапов:

1. Экстракция шаблона отпечатка пальца: На первом этапе оригинальное изображение отпечатка пальца обрабатывается специальным алгоритмом, который выполняет экстракцию признаков. Этот процесс включает в себя фильтрацию, сегментацию и сопоставление, в результате чего формируется компактный и уникальный шаблон отпечатка. Этот шаблон обычно состоит из набора ключевых характеристик, таких как характеристики линий, поры и других уникальных маркеров отпечатка [6].

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

2. Шифрование шаблона: Полученный шаблон подвергается криптографическому шифрованию для повышения уровня безопасности. В зависимости от потребностей и особенностей реализации может использоваться симметричное (например, симметричный алгоритм шифрования, AES) или асимметричное (например, криптографический алгоритм с открытым ключом, RSA) шифрование. Шифрование позволяет преобразовать шаблон в непонятный для чтения формат, что защищает его от несанкционированного доступа и анализа. Ключи шифрования должны храниться в защищенном месте, доступном только авторизованным пользователям или приложениям [10].

3. Сохранение шаблона в файловой системе SIM-карты: Зашифрованный шаблон отпечатка пальца сохраняется в элементарном файле (Earth First – EF) файловой системы SIM-карты. Эта файловая система организована в соответствии с стандартом ETSI (European Telecommunications Standards Institute) и может содержать различные типы данных, включая личные и служебные. Шаблон может быть помещен в специальный EF, назначенный для биометрической информации, что упрощает управление и обработку этих данных. При этом элементарный файл должен иметь назначенные параметры доступа, чтобы ограничить доступ к хранимым данным.

4. Управление правами доступа: Для защиты данных, находящихся в EF, осуществляется внедрение механизмов контроля доступа, позволяющих определить, какие приложения или пользователи могут получать доступ к файлу с биометрическими данными. Это может включать в себя использование PIN-кодов, паролей или аутентификации на основе других факторов, что обеспечивает дополнительный уровень защиты [12].

Таким образом, данный метод хранения шаблона отпечатков пальцев в файловой системе SIM-карты, дополненный шифрованием данных, обеспечивает надежное и безопасное хранение биометрической информации,

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

соответствуя современным требованиям к безопасности и конфиденциальности данных. Это открывает возможности для эффективной аутентификации пользователей в мобильных системах.

Заключение

Подводя итог можно прийти к выводу, что традиционные технологи информационной безопасности устаревают и на замену к ним приходят новые технологии для аутентификации пользователей в современных системах. Несмотря на более современное решение, оно не является идеальным, так как имеет свои недостатки, которые при достаточном финансировании можно буде ликвидировать, так как данное направление является перспективным.

Литература

1. Суомалайнен А. Биометрическая защита: обзор технологии. – Москва. – Изд-во ДМК-Пресс., 2019. – с. 106.

2. Малыгина Е.А. Биометрико-нейросетевая аутентификация: перспективы применения сетей квадратичных нейронов с многоуровневым квантованием биометрических данных. – Пенза. – Изд-во ПГУ., 2020. – с. 113.

3. Протасова А.А., Козлова О.А. Современные технологии идентификации лица: исследование алгоритма работы и использование. – Москва. – Изд-во Синергия., 2020. – с. 13.

4. Исмагилова А.С., Лушников Н.Д. Комплексная биометрическая аутентификация пользователей информационной системы с применением нейронных сетей // Инженерный вестник Дона. 2024, №1. URL: ivdon.ru/uploads/article/pdf/IVD_41__1y24_ismagilova_lushnikov.pdf_62b8d10bc1.pdf

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

5. Жумажанова С.С. Перспективы использования широких нейронных сетей в задачах идентификации состояния человека по термограммам лица и шеи. – Москва. – Изд-во Синергия., 2019. – с. 10.

6. Сулавко А.Е., Шалиной Е.В. Биометрическая аутентификация пользователей информационных систем по клавиатурному почерку на основе иммунных сетевых алгоритмов. – Москва. – Изд-во Синергия., 2019. – с. 16.

7. Абзалова А.Р., Самигуллиной Р.Р., Жиганова А.В. Аутентификация пользователей по динамике нажатий клавиш при использовании систем автоматического прокторинга. – Москва. – Изд-во Синергия., 2022.– с. 11.

8. Тумбинская М. Моделирование аутентификации пользователей по динамике нажатий клавиш в промышленных автоматизированных системах. – Тверь. – Изд-во Научно-исследовательский институт «Центрпрограммсистем»., 2020. – с. 10.

9. Баланов А.Н. Биометрия. Разработка и внедрение систем идентификации. – Санкт-Петербург. – Изд-во Лань., 2024. – с. 228.

10. Ворон А.В. Биометрическая идентификация личности. – Москва. – Изд-во Горячая линия – Телеком., 2023. – с. 228.

11. Катмаков А.С., Гавриленко В.П., Бушов А.В. Биометрия. – Москва. – Изд-во Юрайт., 2024. – с. 186.

12. Кочеров Ю.Н., Тихонов Э.Е., Самойленко Д.В. Метод надежного хранения биометрических данных на пространственно-распределенных хранилищах // Инженерный вестник Дона. 2020, № 9. URL: ivdon.ru/uploads/article/pdf/IVD_10__9_Kocherov_Tihonov_Samoylenko.pdf_39ab83d5ab.pdf

13. Melissa Stock Biometric Data and New Technologies – The Law and Practical Issues on Technologies Such as CCTV, Facial Recognition and Drones. London: Law Brief Publishing, 2022. - p. 142.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

14. Kindt E.J. Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis. London: Springer, 2013. - p. 996.

References

1. Suomalajnen A. Biometricheskaya zashhita: obzor texnologii [Biometric protection: technology review]. Moskva. Izd-vo DMK-Press, 2019. p. 106.

2. Maly`gina E.A. Biometriko-nejrosetevaya autentifikaciya: perspektivy` primeneniya setej kvadratichny`x nejronov s mnogourovnevy`m kvantovaniem biometricheskix danny`x [Biometric-neural network authentication: prospects of application of networks of quadratic neurons with multilevel quantization of biometric data]. Penza. Izd-vo PGU., 2020. p. 113.

3. Protasova A.A., Kozlova O.A. Sovremenny`e texnologii identifikacii licza: issledovanie algoritma raboty` i ispol`zovanie [Modern technologies of face identification: research of the algorithm of work and use]. Moskva. Izd-vo Sinergiya, 2020. p. 13.

4. Ismagilova A.S., Lushnikov N.D. Inzhenernyj vestnik Dona. 2024, №1. URL: ivdon.ru/uploads/article/pdf/IVD_41__1y24_ismagilova_lushnikov.pdf_62b8d10bc1.pdf

5. Zhumazhanova S.S. Perspektivy` ispol`zovaniya shirokix nejronny`x setej v zadachax identifikacii sostoyaniya cheloveka po termogrammam licza i shei [Prospects of using wide neural networks in tasks of human state identification by face and neck thermograms]. Moskva. Izd-vo Sinergiya, 2019. p. 10.

6. Sulavko A.E., Shalinoj E.V. Biometricheskaya autentifikaciya pol`zovatelej informacionny`x sistem po klaviaturnomu pocherku na osnove immunny`x setevy`x algoritmov [Biometric authentication of information systems users by keyboard handwriting on the basis of immune network algorithms]. Moskva. Izd-vo Sinergiya, 2019. p. 16.

7. Abzalova A.R., Samigullinoj R.R., Zhiganova A.V. Autentifikaciya pol`zovatelej po dinamike nazhatij klavish pri ispol`zovanii sistem

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025

avtomaticheskogo proktoringa [Authentication of users by the dynamics of keystrokes when using automatic proctoring systems]. Moskva. Izd-vo Sinergiya, 2022. p. 11.

8. Tumbinskaya M. Modelirovanie autentifikacii pol`zovatelej po dinamike nazhatij klavish v promy`shlenny`x avtomatizirovanny`x sistemax [Modeling of user authentication by keystroke dynamics in industrial automated systems]. Tver`. Izd-vo Nauchno-issledovatel`skij institut «Centrprogrammsistem», 2020. p. 10.

9. Balanov A.N. Biometriya. Razrabotka i vnedrenie sistem identifikacii [Biometrics. Development and Implementation of Identification Systems]. Sankt-Peterburg. Izd-vo Lan`, 2024. p. 228.

10. Voron A.V. Biometricheskaya identifikaciya lichnosti [Biometric identification of the person]. Moskva. Izd-vo Goryachaya liniya. Telekom, 2023. p. 228.

11. Katmakov A.S., Gavrilenko V.P., Bushov A.V. Biometriya [Biometrics]. Moskva. Izd-vo Yurajt, 2024. p. 186.

12. Kocherov Yu.N., Tixonov E`.E., Samojlenko D.V. Inzhenernyj vestnik Dona. 2020, № 9. URL: ivdon.ru/uploads/article/pdf/IVD_10__9_Kocherov_Tihonov_Samoylenko.pdf_39ab83d5ab.pdf

13. Melissa Stock Biometric Data and New Technologies – The Law and Practical Issues on Technologies Such as CCTV, Facial Recognition and Drones. London: Law Brief Publishing, 2022. p. 142.

14. Kindt E.J. Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis. London: Springer, 2013. p. 996.

Дата поступления: 14.12.2024

Дата публикации: 2.02.2025

© Электронный научный журнал «Инженерный вестник Дона», 2007–2025