ORES
Научно-практический электронный журнал
Оригинальные исследования (ОРИС), *ISSN 2222-0402*
www.ores.su
original-research.ru

УДК 004.056

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ВЕРИФИКАЦИИ ДИНАМИЧЕСКОЙ РУКОПИСНОЙ ПОДПИСИ В ОНЛАЙН И ОФФЛАЙН СИСТЕМАХ

Дзямко-Гамулец Роман Николаевич,
Аспирант
Московский технический университет связи и информатики
Факультет кибернетики и информационной безопасности, кафедра экологии, безопасности жизнедеятельности и электропитания
roman.dzyamko-gamulets@outlook.com

Иевлев Олег Павлович,
Кандидат технических наук
Московский технический университет связи и информатики
Факультет кибернетики и информационной безопасности
ievlev@mtuci.ru

Аннотация

Верификация динамической рукописной подписи приобретает всё большее значение как один из наиболее перспективных методов биометрической аутентификации. Данная технология позволяет анализировать и выявлять уникальные характеристики рукописной подписи и её динамические параметры: скорость создания, давление при написании, углы наклона и т.п. Такой подход обеспечивает повышенную безопасность, поскольку злоумышленникам необходимо воспроизвести не только форму подписи, но и индивидуальный стиль написания. Это делает метод особенно востребованным в условиях растущих требований к надежности и удобству аутентификации в информационных системах. В статье рассматриваются ключевые аспекты технологии, её преимущества и ограничения, примеры использования в различных сферах, таких как интернет-авторизация, судебная экспертиза, системы доступа и документооборот. Особое внимание уделено влиянию качества алгоритмов и оборудования на точность распознавания, а также вопросам защиты биометрических данных. Оценены перспективы её массового внедрения и место среди альтернативных биометрических методов.

Ключевые слова: динамическая рукописная подпись, биометрия, аутентификация, безопасность, онлайн-сервисы, судебная экспертиза, сенсорные устройства, ошибки первого и второго рода, электронные технологии.

PROSPECTS FOR USING DYNAMIC HANDWRITTEN SIGNATURE VERIFICATION IN ONLINE AND OFFLINE SYSTEMS

Dzyamko-Gamulets Roman Nikolaevich,
Master
Moscow Technical University of Communications and Informatics

Faculty of cybernetics and information security, department of ecology,
life safety and power supply

Ievlev Oleg Pavlovich,
Candidate of technical sciences
Moscow Technical University of Communications and Informatics
Faculty of cybernetics and information security

ABSTRACT

Dynamic handwritten signature verification is becoming increasingly significance as one of the most promising methods of biometric authentication. This technology allows to analyze and identify the unique characteristics of handwritten signature and its dynamic parameters – speed of creation, writing pressure, tilt angles and etc. This approach provides increased security, since attackers need to reproduce not only the signature shape, but also individual writing style. This makes the method especially in demand in the context of growing requirements for reliability and convenience of authentication in information systems. The article discusses the key aspects of the technology, its advantages and limitations, examples of use in various fields, such as internet authorization, forensic examination, access systems and document management. Special attention is paid to the impact of algorithms quality and equipment accuracy of recognition, as well as issues related to the protection of biometric data. The prospects of its mass implementation and its place among alternative biometric methods are assessed.

Keywords: dynamic handwritten signature, biometrics, authentication, security, online services, forensic analysis, sensor devices, type I and type II errors, electronic technologies.

Введение

С увеличением количества электронных сервисов растёт потребность в надёжных и удобных способах авторизации. Стандартные пароли и PIN-коды долгое время оставались основными инструментами, но с каждым годом их недостатки становятся всё более явными [1, 2]. Утечки данных, фишинговые атаки, подбор паролей – все эти угрозы требуют новых решений [3, 4].

Биометрические методы аутентификации, основанные на уникальных биологических характеристиках человека, всё чаще рассматриваются как альтернативное решение данных проблем [5, 6]. Одной из таких технологий является верификация динамической рукописной подписи, которая позволяет использовать привычный людям процесс создания собственной подписи, добавляя в него уровень защиты, основанный на анализе и выявлении уникальных признаков подписи.

Общая концепция технологии

Динамическая рукописная подпись – это не стандартное изображение пользовательского автографа, а набор данных о том, каким образом представленный автограф был создан. Специальные устройства, например сенсорные планшеты, фиксируют множество параметров: от скорости создания изображения до угла наклона пера. Эти данные обрабатываются алгоритмами, которые формируют уникальный профиль для каждого пользователя.Процесс работы технологии можно описать следующим образом – устройство снимает технические данные рисунка подписи (общую длину подписи, количество отрывов пера, углы наклона, скорость написания и т.п.). После

предобработки входных данных происходит процесс выделения уникальных признаков и зависимостей различных параметров образца подписи. Полученные уникальные признаки сравниваются с сохранённым эталоном, созданном на основании усредненных параметров первоначальных обучающих образцов [7, 8].

Ключевым показателем эффективности работы являются ошибки первого рода (пропуск ложного пользователя) и второго рода (отказ в доступе истинному пользователю). При максимально возможной минимизации данных показателей, технология может стать практически применимой [9].

Преимущества и ограничения

Динамическая рукописная подпись обладает рядом достоинств, которые делают её перспективной для применения в различных сферах. Она легко воспринимается пользователями, поскольку рукописная подпись давно ассоциируется с подтверждением различных действий. Ещё одно преимущество заключается в сложности её подделки. Злоумышленнику необходимо воспроизвести не только форму подписи, но и её динамические параметры, такие как ритм написания отдельных участков, а также давление и угол наклона пера. Кроме того, технология универсальна и может применяться как в онлайн-среде, например, при авторизации в интернет-сервисах, так и в оффлайн-пространствах, таких как системы контроля доступа или документооборот. Однако у метода есть и ограничения. Для его максимально качественной работы требуются устройства с высокой точностью фиксации параметров письма и комфортные для пользователя условия. Усталость, возраст или иные физиологические и психологические особенности также могут влиять на стиль создания письма, что может привести к ошибочным отказам в доступе.

Примеры применения

Примеры использования динамической рукописной подписи охватывают широкий спектр задач, от авторизации и подтверждения личности до автоматизации процессов и интеграции с электронными системами, что делает эту технологию востребованной в различных сферах [10].

В онлайн-среде технология может улучшить привычные способы аутентификации в качестве основного или дополнительного способа подтверждения пользователя. Кроме того, рукописная подпись может применяться вместо технологии капчи для подтверждения личности, делая процесс более удобным и менее раздражающим. В оффлайн-среде рукописная подпись активно используется при аутентификации в офисах, банках и других учреждениях, а в документообороте позволяет подписывать юридически значимые документы без бумажных носителей. При достаточной минимизации показателей ошибок I и II рода, технология может быть улучшена и преобразована в более сложный вид программного обеспечения для применения в судебной экспертизе, где сочетание анализа визуальных и динамических характеристик помогает определить подлинность человеческого почерка, что особенно полезно в криминалистике.

Сравнение с другими методами

Существующие методы аутентификации, основанные на криптостойких паролях, PIN-кодах, одноразовых кодах являются основными методами при авторизации в большинстве информационных системах. Однако не каждая информационная система может быть устойчива к большинству кибератак, в связи с этим всегда присутствуют вероятность компрометации как личных данных пользователя, так и аутентификационных данных. В системах, в которых недопустимы утечки информации, помимо стандартных средств защиты, применяют и биометрические методы аутентификации, основанные на отпечатках пальцев пользователей, изображения 3D-лица,

радужной оболочки глаза и т.п. Данные методы прекрасно показывают себя при использовании в оффлайн-системах, но, к сожалению, не могут быть полноценно применены в онлайн системах, так как при компрометации биометрических данных, пользователь не может более пользоваться данными методами повсеместно. Но данная проблема относится только к статическим характеристикам человека (биометрические характеристики, которые сохраняются и не меняются на протяжении всей жизни человека). Рукописная подпись, как и клавиатурный почерк и голос, относятся к динамическим характеристикам человека. Динамические характеристики напрямую зависят не только от физиологических особенностей человека, но и от психологического состояния и поведения пользователя, которое он в состоянии частично контролировать. В связи с этим, при компрометации профиля с характеристиками рукописной подписи злоумышленник получит лишь характеристики одного изображения подписи, но не получит достаточных данных, чтобы повторить любую другую подпись пользователя. Можно сказать, что рукописная подпись в информационной среде представляет из себя пароль в качестве изображения подписи, но с дополнительной защитой в виде биометрической характеристики, которую злоумышленник никак не сможет получить. Это позволяет применять данный метод как в онлайн, так и оффлайн системах в качестве замены стандартному паролю, либо как дополнительный способ подтверждения личности пользователя.

Заключение

Верификация динамической рукописной подписи является перспективным биометрическим методом, который сочетает привычный для человека процесс подписывания с высокой степенью защиты данных.
Её уникальность заключается в сложности подделки, универсальности применения и возможности интеграции в широкий спектр областей, от авторизации и документооборота до судебной экспертизы [11].

Однако ключевым условием успешного внедрения технологии остается минимизация ошибок первого и второго рода. Только при достижении низких значений данных показателей технология сможет удовлетворить строгие требования надежности и безопасности.

Важно подчеркнуть, что данная технология может оказать значительное влияние на общество, обеспечивая не только более удобные, но и безопасные способы авторизации и подтверждения личности. В условиях цифровизации и роста числа киберугроз верификация рукописной подписи способна не только повысить уровень защиты, но и упростить повседневные процессы, делая их доступными для всех слоев населения.

Список литературы:

1. Большая часть российских пользователей продолжает использовать слабые пароли – статистика RTM Group. [Электронный ресурс] // RTM Group. 2023. Режим доступа: https://rtmtech.ru/news/bolshaya-chast-rossijskih-polzovatelej-prodolzhaet-ispolzovat-slabye-paroli-statistika-rtm-group
2. Петрухин Г.В. Об ужесточении ответственности за неисполнение законных требований прокурора // Оригинальные исследования. 2024. Т. 14. №. 12. С. 18-22. [Электронный ресурс] // ОРИС. 2024. Режим доступа: https://ores.su/media/filer_public/aa/91/aa91d0e4-4f73-4098-976f-e1a3ad8b7f78/18-22.pdf

3. Анализ утекших учетных записей и паролей за 2023 год. [Электронный ресурс] // Data Leakage & Breach Intelligence. 2024. Режим доступа: https://dlbi.ru/five-and-five-billion-password-2023
4. В 2024 году количество утекших паролей в России выросло в шесть раз. [Электронный ресурс] // Kaspersky. 2024. Режим доступа: https://www.kaspersky.ru/about/press-releases/v-2024-godu-kolichestvo-utyokshih-parolej-v-rossii-vyroslo-v-shest-raz
Федеральный закон "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации" от 29.12.2022 N 572-ФЗ. [Электронный ресурс] // КонсультантПлюс. 2022. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_436110/?ysclid=lpfhpkejs6527014142
5. Жиронкин Я. Биометрические методы аутентификации // Jetinfo: Будущее банков… перезагрузка. 2017. № 5-6. С. 62-68. [Электронный ресурс] // Jetinfo. 2017. Режим доступа: https://www.jetinfo.ru/biometricheskie-metody-autentifikatsii
6. Дзямко-Гамулец Р.Н. Статические алгоритмы выделения уникальных признаков из рукописной подписи человека // Инженерный вестник Дона. 2024. № 3 (111). С. 149-162. [Электронный ресурс] // Инженерный вестник Дона. 2024. Режим доступа: http://www.ivdon.ru/uploads/article/pdf/IVD_59N2y24_Dziamko_Gomulec.pdf_1f76d1de3f.pdf
7. Дзямко-Гамулец Р.Н. Динамические алгоритмы выделения уникальных признаков из рукописной подписи человека // Инженерный вестник Дона. 2024. № 3 (111). С. 163-178. [Электронный ресурс] // Инженерный вестник Дона. 2024. Режим доступа: http://www.ivdon.ru/uploads/article/pdf/IVD_60N2y24_Dziamko_Gomulec.pdf_db49857f99.pdf
8. Анисимова Э.С. Идентификация личности человека на основе динамической подписи // Экономика и социум. 2015. № 3 (16). С. 31-33. [Электронный ресурс] // CyberLeninka. 2015. Режим доступа: https://cyberleninka.ru/article/n/identifikatsiya-lichnosti-cheloveka-na-osnove-dinamicheskoy-podpisi/viewer
9. Дзямко-Гамулец Р.Н. Области применения динамической рукописной подписи // Оригинальные исследования. 2024. Т. 14. № 1. С. 91-99. [Электронный ресурс] // Elibrary. 2024. Режим доступа: https://www.elibrary.ru/download/elibrary_65656279_81528909.pdf
10. Дзямко-Гамулец Р.Н. Совместное применение рукописной и электронной подписи при авторизации // Оригинальные исследования. 2024. Т. 14. № 2. С. 120-127. [Электронный ресурс] // Elibrary. 2024. Режим доступа: https://www.elibrary.ru/download/elibrary_67907733_31574075.pdf.

References:

1. Most Russian users continue to use weak passwords – RTM Group statistics. [Electronic resource] // RTM Group. 2023. Access mode: https://rtmtech.ru/news/bolshaya-chast-rossijskih-polzovatelej-prodolzhaet-ispolzovat-slabye-paroli-statistika-rtm-group
2. Petrukhin G.V. On tightening liability for failure to comply with the legal requirements of the prosecutor // Original research. 2024. Vol. 14. No. 12. Pp. 18-22. [Electronic resource] // ORIS. 2024. Access mode: https://ores.su/media/filer_public/aa/91/aa91d0e4-4f73-4098-976f-e1a3ad8b7f78/18-22.pdf
3. Analysis of leaked accounts and passwords for 2023. [Electronic resource] // Data Leakage & Breach Intelligence. 2024. Access mode: https://dlbi.ru/five-and-five-billion-password-2023
4. In 2024, the number of leaked passwords in Russia increased sixfold. [Electronic resource] // Kaspersky. 2024. Access mode: https://www.kaspersky.ru/about/press-releases/v-2024-godu-kolichestvo-utyokshih-parolej-v-rossii-vyroslo-v-shest-raz
5. Федеральный закон "Об осуществлении идентификации и (или) аутентификации физических лиц с использованием биометрических персональных данных, о внесении изменений в отдельные законодательные акты Российской Федерации и признании утратившими силу отдельных положений законодательных актов Российской Федерации" от 29.12.2022 N 572-ФЗ. [Электронный ресурс] // КонсультантПлюс. 2022. Режим доступа: https://www.consultant.ru/document/cons_doc_LAW_436110/?ysclid=lpfhpkejs6527014142
6. Zhironkin Ya. Biometric authentication methods // Jetinfo: The future of banks... reboot. 2017. No. 5-6. Pp. 62-68. [Electronic resource] // Jetinfo. 2017. Access mode: https://www.jetinfo.ru/biometricheskie-metody-autentifikatsii
7. Dzyamko-Gamulets R.N. Static algorithms for extracting unique features from a person's handwritten signature // Engineering Bulletin of the Don. 2024. No. 3 (111). Pp. 149-162. [Electronic resource] // Engineering Bulletin of the Don. 2024. Access mode: http://www.ivdon.ru/uploads/article/pdf/IVD_59N2y24_Dziamko_Gomulec.pdf_1f76d1de3f.pdf
8. Dzyamko-Gamulets R.N. Dynamic algorithms for extracting unique features from a person's handwritten signature // Engineering Bulletin of the Don. 2024. No. 3 (111). P. 163-178. [Electronic resource] // Engineering Bulletin of the Don. 2024. Access mode: http://www.ivdon.ru/uploads/article/pdf/IVD_60N2y24_Dziamko_Gomulec.pdf_db49857f99.pdf
9. Anisimova E.S. Identification of a person based on a dynamic signature // Economy and Society. 2015. No. 3 (16). P. 31-33. [Electronic resource] // CyberLeninka. 2015. Access mode: https://cyberleninka.ru/article/n/identifikatsiya-lichnosti-cheloveka-na-osnove-dinamicheskoy-podpisi/viewer
10. Dzyamko-Gamulets R.N. Areas of application of a dynamic handwritten signature // Original research. 2024. Vol. 14. No. 1. P. 91-99. [Electronic resource] // Elibrary. 2024. Access mode: https://www.elibrary.ru/download/elibrary_65656279_81528909.pdf

11. Dzyamko-Gamulets R.N. Combined use of handwritten and electronic signatures during authorization // Original research. 2024. Vol. 14. No. 2. P. 120-127. [Electronic resource] // Elibrary. 2024. Access mode: https://www.elibrary.ru/download/elibrary_67907733_31574075.pdf