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

УДК 004.056

ПРИМЕНЕНИЕ ДИНАМИЧЕСКИХ И ТЕРМОГРАФИЧЕСКИХ ПОДХОДОВ В БИОМЕТРИЧЕСКИХ СИСТЕМАХ АУТЕНТИФИКАЦИИ

Калининский Даниил Сергеевич
Студент магистратуры
2 курс, факультет «Информационные технологии»
Кафедра «Сетевые информационные технологии и сервисы»
Московский технический университет связи и информатики
e-mail: daniilblag28@gmail.com

Аннотация

В данной научной работе представлен подробный обзор применения динамических и термографических подходов в биометрической аутентификации, подчеркивающий их значимость в обеспечении безопасности информационных систем. Также детализировано проанализированы принципы работы подходов в биометрических системах аутентификации и глубоко проанализированы преимущества и недостатки каждого из обозреваемых подходов, включая аспекты точности идентификации, устойчивости к подделке и потенциальные ограничения, такие как изменение состояния здоровья пользователя или технические препятствия.

Ключевые слова: биометрическая аутентификация, термография лица, распознавание голоса, клавиатурный почерк, верификация подписи

APPLICATION OF DYNAMIC AND THERMOGRAPHIC APPROACHES IN BIOMETRIC AUTHENTICATION SYSTEMS

Daniil S. Kalininskiy
Master's degree student
2nd year, Faculty of Information Technology
Department of "Network Information Technologies and Services"
Moscow Technical University of Communications and Informatics

ABSTRACT

This scientific paper presents a detailed overview of the use of dynamic and thermographic approaches in biometric authentication, emphasizing their importance in ensuring the security of information systems. Also, the principles of operation of approaches in biometric authentication systems are analyzed in detail and the advantages and disadvantages of each of the surveyed approaches are analyzed in depth, including aspects of identification accuracy, resistance to forgery and potential limitations, such as changes in the user's health status or technical obstacles.

Keywords: biometric authentication, facial thermography, voice recognition, keyboard handwriting, signature verification

Введение

Биометрическая аутентификация проверяет личность пользователя, используя его уникальные физиологические и поведенческие характеристики, например, отпечаток пальца или голос [1]. Процесс включает 3 этапа (рис. 1):

Регистрация биометрических данных: пользователь предоставляет свои биометрические данные, которые сохраняются в базе данных.

Сравнение биометрических данных: предоставленные пользователем данные сверяются с зарегистрированными.

Решение об аутентификации: система аутентифицирует пользователя, если представленные данные совпадают с зарегистрированными.

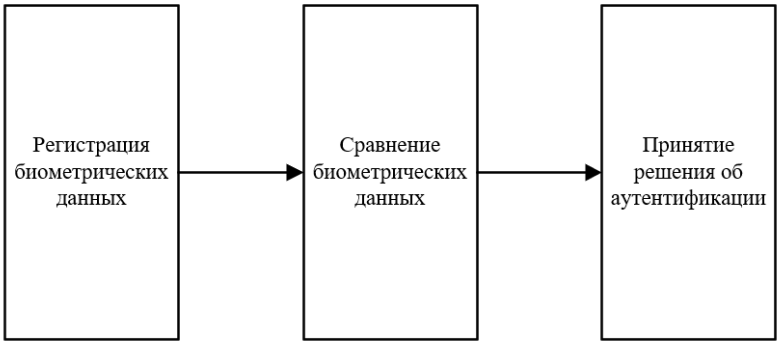

Рисунок 1. Принцип работы биометрической аутентификации

Биометрическая аутентификация использует уникальные биологические характеристики человека, что обеспечивает удобство и скорость аутентификации без необходимости запоминать пароли. Несмотря на удобство, эти системы требуют защиты от мошенничества и атак [2]. Основные методы биометрической аутентификации подразделяются на статический и динамический.

Статические методы аутентификации

Данные методы используют постоянные физические особенности, такие как отпечатки пальцев, лицо, сетчатку глаза или форму уха. В процессе статической аутентификации пользователь предоставляет свои уникальные данные для сравнения с уже зарегистрированными в системе. Если данные совпадают, пользователь получает доступ к системе [3].

Дактилоскопия – это пример статической биометрической аутентификации, основанной на уникальности отпечатков пальцев каждого человека [4] (рис. 2).

Рисунок 2. Дактилоскопия

Дактилоскопия начинается с получения изображения отпечатка пальца с помощью сканера. Это изображение затем преобразуется в математический код, который сравнивается с образцом в базе данных, используя различные алгоритмы, чтобы определить сходство между отпечатками. Дактилоскопия характеризуется высокой точностью и быстротой, но может быть ограничена при повреждении или загрязнении пальца, и в некоторых случаях возможна подделка отпечатков [5].

Аутентификация по сетчатке глаза – это биометрический метод, использующий уникальные особенности сетчатки, включая расположение капилляров и других элементов [6]. В процессе сканирования сетчатки измеряются различные характеристики, которые затем сравниваются с зарегистрированными в базе данных. Совпадение данных обеспечивает успешную аутентификацию [7] (рис3).

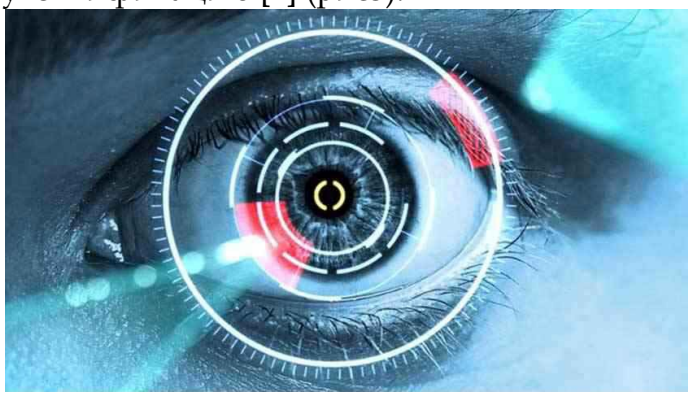

Рисунок 3. Аутентификация по сетчатке глаза

Этот метод предлагает высокую точность и надежность, так как сетчатка уникальна для каждого человека и сложна для подделки [8]. Недостатки включают высокую стоимость оборудования и потенциальный дискомфорт пользователя, поскольку глаз должен быть фиксирован в определенном положении во время сканирования.

Аутентификация по геометрии руки – биометрический метод, использующий уникальные геометрические характеристики руки, такие как длина и ширина пальцев, углы между суставами и прочее [9]. В ходе аутентификации система сравнивает введенные пользователем параметры руки с сохраненными в базе данных (рис. 4).

Рисунок 4. Аутентификация по геометрии руки

Процедура аутентификации включает сканирование руки или ввод геометрических параметров, их сохранение в базе данных, и последующее сравнение при попытках доступа. В случае совпадения пользователь получает доступ [10].

Этот метод отличается надежностью и уникальностью, но может быть неудобен из-за требования точного сканирования или ввода параметров. Болезни или травмы также могут изменить геометрию руки, что может затруднить аутентификацию.

Аутентификация по геометрии лица – это биометрический метод, основывающийся на уникальных характеристиках лица, таких как расстояние между глазами, размеры носа, форма лица и т.д. Используя камеру, система захватывает изображение лица, извлекает особенности и создает биометрический шаблон [11] (рис. 5).

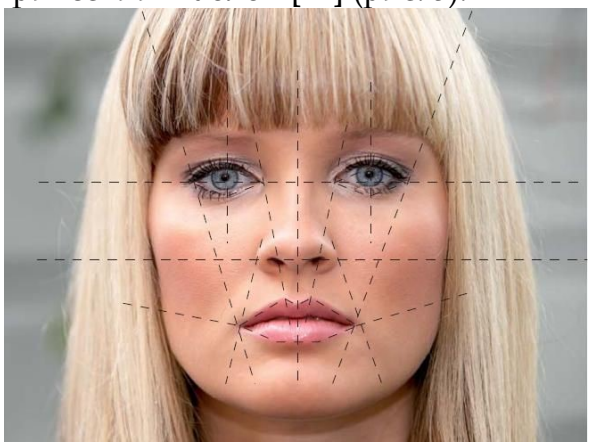

Рисунок 5. Аутентификация по геометрии лица

При аутентификации система сравнивает новый шаблон с ранее сохраненным. Если сходство высокое, аутентификация считается успешной. Этот метод быстрый и точный, но может столкнуться с проблемами при плохом освещении, изменении внешности пользователя или попытке обмана с помощью фотографии. Поэтому, для повышения безопасности, рекомендуется использовать системы, умеющие определить «живость» лица. [12]

Термография лица – биометрический метод аутентификации, основывающийся на измерении теплового излучения лица с помощью инфракрасной камеры [13] Это позволяет создать уникальную тепловую карту, служащую шаблоном для идентификации личности (рис. 6).

Рисунок 6. Термография лица

Каждый человек обладает индивидуальной термографической сигнатурой, связанной с физиологией и кровообращением. В процессе аутентификации сравнивается новый образец термографии лица с предварительно сохраненным шаблоном. Если данные совпадают, пользователь аутентифицирован [14].

Термография лица – точный и надежный метод, эффективный даже при низком освещении. Однако, он требует специализированного оборудования и имеет высокую стоимость.

Динамические методы биометрической аутентификации

Динамические методы биометрической аутентификации определяют личность по поведению и движениям человека, таким как почерк, подпись, речь, походка и манипуляции с устройствами ввода [15]. Они могут дополнять другие биометрические методы или использоваться самостоятельно, на сенсорных устройствах или обычных компьютерах.

Основная идея динамической аутентификации – сбор информации о действиях пользователя и сравнение ее с ранее сохраненными данными с помощью алгоритмов анализа и распознавания, чтобы определить степень соответствия [16].

Метод распознавания голоса – это динамический биометрический метод аутентификации, использующий уникальные акустические характеристики голоса. В процессе регистрации, система записывает и анализирует голос пользователя, сохраняя эти данные. При аутентификации, пользователь произносит определенные фразы, которые система сравнивает с сохраненными данными для проверки совпадения [17] (рис. 7).

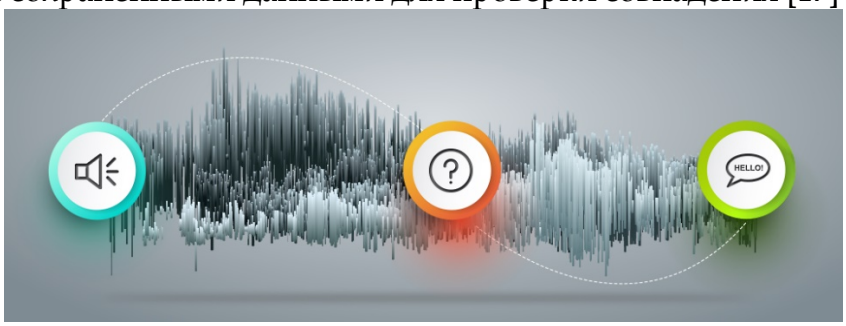

Рисунок 7. Метод распознавания голоса

Преимущества этого метода включают высокую точность и удобство использования, так как не требуется физического контакта с системой [17]. Однако, проблемы с голосом или использование разных устройств могут затруднить аутентификацию. К тому же, голос может быть записан и использован для обхода системы безопасности [18].

Метод распознавания клавиатурного почерка – это биометрическая техника, опирающаяся на уникальные характеристики способа набора текста пользователя. При регистрации, система анализирует параметры ввода текста, такие как скорость печати и задержка между нажатием клавиш, и сохраняет эту информацию. Во время попытки аутентификации пользовательский набор текста сравнивается с сохраненными данными, и на основе этого сравнения делается вывод о подлинности пользователя [19, 20] (рис. 8).

Рисунок 8. Метод распознавания клавиатурного почерка

Верификация подписи – это проверка цифровой подписи для аутентификации документов или сообщений. Она действует как электронный эквивалент ручной подписи, подтверждая авторство и целостность документа. В процессе верификации подпись из документа сравнивается с открытым ключом, связанным с ней при создании. При совпадении, подпись признается подлинной. Этот метод используется в электронном документообороте, банковских операциях и т. д., обеспечивая высокую защиту от мошенничества [19, 20] (рис. 9).

Рисунок 9. Верификация подписи

Заключение

Биометрические системы аутентификации становятся все более распространенными и важными в современном мире. Термография лица, распознавание голоса, клавиатурный почерк и верификация подписи представляют собой инновационные подходы к биометрической аутентификации, каждый из которых имеет свои уникальные преимущества и области применения. Однако, как и любые технологические решения, эти методы имеют свои недостатки, которые следует учитывать при разработке и внедрении систем биометрической аутентификации. Несмотря на это, важность и значимость этих методов продолжает расти, поскольку они предлагают надежные и эффективные решения для обеспечения безопасности информации.

Список литературы:

1. Иванова, О. С., Казакова, А. В. (2018). Применение анализа данных для обнаружения аномалий в офисных сетях. Информационные технологии и безопасность, 6(3), 39-47.
2. Гришин, С. В., Жуков, А. П. (2019). Методы и средства обеспечения безопасности беспроводных сетей офиса. Информационная безопасность и защита информации, 7(4), 14-21.
3. Федеральная служба безопасности (ФСБ). Отчет о состоянии информационной безопасности в Российской Федерации. Москва, 2020.
4. Беляев А.В. Информационная безопасность офисных систем: угрозы и защита. Москва: Финансы и статистика, 2018.
5. Лукьянов С.А. Организация и технологии защиты информации в офисных системах. Москва: Издательский центр "Академия", 2019.
6. Петрова Е.С. Методы и средства защиты информации в офисной среде. Санкт-Петербург: БХВ-Петербург, 2020.
7. Иванов Д.Н. Аудит информационной безопасности в офисных сетях. Москва: Издательство "Лань", 2017.
8. Смирнов П.А. Управление информационной безопасностью в офисных системах. Санкт-Петербург: Питер, 2021.
9. Николаев А.Г. Безопасность офисных сетей и серверов: анализ и практика. Москва: Издательство "Эксмо", 2018.
10. Козлов М.В. Защита периметра офисных сетей: технологии и методы. Санкт-Петербург: БХВ-Петербург, 2019.
11. Григорьев В.И. Обеспечение безопасности программного обеспечения в офисной среде. Москва: Финансы и статистика, 2020.
12. Жукова Н.С. Биометрическая аутентификация в офисных системах: технологии и применение. Санкт-Петербург: Питер, 2019.
13. Макаров И.Д. Программные решения для защиты данных в офисных приложениях. Москва: Издательство "Лань", 2021.
14. Государственный стандарт РФ ГОСТ Р ИСО/МЭК 27001-2013 "Информационная технология. Методы защиты. Системы менеджмента информационной безопасности. Требования". Москва, 2013.

15. Международный союз электросвязи (ITU). Рекомендация ITU-T X.805: Архитектура безопасности для систем, обеспечивающих коммуникации от источника к потребителю. Женева, 2010.
16. ISO/IEC 27001:2013 - Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования.
17. ISO/IEC 27002:2013 - Информационная технология. Методы обеспечения безопасности. Практические рекомендации по управлению информационной безопасностью.
18. ISO 31000:2018 - Управление рисками. Принципы и руководство.
19. ISO/IEC 27005:2018 - Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности.
20. NIST SP 800-53 - Стандарты по безопасности информации и системам управления рисками в федеральных информационных системах США.

References:

1. Ivanova, O. S., Kazakova, A. V. (2018). Application of data analysis for anomaly detection in office networks. Information Technology and Security, 6(3), 39-47.
2. Grishin, S. V., Zhukov, A. P. (2019). Methods and means of ensuring the security of office wireless networks. Information Security and Information Protection, 7(4), 14-21.
3. Federal Security Service (FSB). Report on the state of information security in the Russian Federation. Moscow, 2020.
4. Belyaev A.V. Information security of office systems: threats and protection. Moscow: Finance and statistics, 2018.
5. Lukyanov S.A. Organization and technology of information protection in office systems. Moscow: Publishing Center "Academy", 2019.
6. Petrova E.S. Methods and means of protecting information in the office environment. St. Petersburg: BHV-Petersburg, 2020.
7. Ivanov D.N. Information security audit in office networks. Moscow: Lan publishing house, 2017.
8. Smirnov P.A. Management of information security in office systems. St. Petersburg: Peter, 2021.
9. Nikolaev A.G. Security of office networks and servers: analysis and practice. Moscow: Eksmo Publishing House, 2018.
10. Kozlov M.V. Protecting the perimeter of office networks: technologies and methods. St. Petersburg: BHV-Petersburg, 2019.
11. Grigoriev V.I. Ensuring software security in the office environment. Moscow: Finance and statistics, 2020.
12. Zhukova N.S. Biometric authentication in office systems: technologies and applications. St. Petersburg: Peter, 2019.
13. Makarov I.D. Software solutions for data protection in office applications. Moscow: Lan publishing house, 2021.

14. State standard of the Russian Federation GOST R ISO / IEC 27001-2013 "Information technology. Protection methods. Information security management systems. Requirements". Moscow 2013.
15. International Telecommunication Union (ITU). ITU-T Recommendation X.805: Security architecture for systems providing source-to-consumer communications. Geneva, 2010.
16. ISO/IEC 27001:2013 - Information technology. Security methods. Information security management systems. Requirements.
17. ISO/IEC 27002:2013 - Information technology. Security methods. Practical recommendations for information security management.
18. ISO 31000:2018 - Risk management. Principles and leadership.
19. ISO/IEC 27005:2018 - Information technology. Security methods. Information security risk management.
20. NIST SP 800-53 - Standards for Information Security and Risk Management Systems in US Federal Information Systems.

References:

21. Research of the Russian market of online education // Portal of Media Netology. URL: https://netology.ru/blog/06-2022-edtech-research (date of access: 05/26/2023).
22. Dobrovinsky D. S., Lovetsky I. V., Popov M. A. Proctoring as a tool for the development of distance education // Scientific, technical and economic cooperation of the Asia-Pacific countries in the XXI century. 2018. V. 2. Pp. 27-32.
23. Cramp J., Medlin J. F., Lake P., Sharp C. (2019). Lessons learned from implementing remotely invigilated online exams. Journal of University Teaching & Learning Practice. 2019.16(1). URL: https://doi.org/10.53761/1.16.1.10 (Accessed: 05/26/2023).
24. Kalaavathi DR.B., Sangeetha M., Chowmiya S. B., Vaishnavi V., Pooja Shree K. Automating Online Proctoring System / Director and Professor, KSR Institute for Engineering and Technology, Tiruchengode. 2021.
25. Nigam A. et al. A systematic review on ai-based proctoring systems: Past, present and future // Education and Information Technologies. 2021. Vol. 26. No. 5. pp. 6421-6445.