

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ, ЧИСЛЕННЫЕ МЕТОДЫ И КОМПЛЕКСЫ ПРОГРАММ/MATHEMATICAL MODELING, NUMERICAL METHODS AND PROGRAM COMPLEXES

DOI: https://doi.org/10.60797/COMP.2026.10.1 EDN: FCQOFA

ПРИМЕНЕНИЕ ГЕНЕТИЧЕСКОГО АЛГОРИТМА ДЛЯ ПОВЫШЕНИЯ УСТОЙЧИВОСТИ МЕТОДИКИ ФОРМИРОВАНИЯ ПАРОЛЕЙ НА ОСНОВЕ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Научная статья

Беломойцев Д.Е.[1,] *, Волосатова Т.М.[2]
[1] ORCID : 0000-0001-8200-2963;
[2] ORCID : 0000-0002-2882-5464;
[1, 2] Московский государственный технический университет имени Н. Э. Баумана, Москва, Российская Федерация

* Корреспондирующий автор (belomoid[at]bmstu.ru)

Аннотация

Рассмотрен подход к многофакторной аутентификации с использованием биометрии и токена. Предложена методика формирования паролей для аутентификации из нескольких компонентов, один из которых размещается в защищенном хранилище токена и становится доступным в результате верификации биометрических шаблонов. Обозначена проблема применения биометрической верификации вследствие изменчивости и дрейфа шаблонов. Для решения проблемы дрейфа использован генетический алгоритм, для которого разработаны генетические операторы, учитывающие особенности шаблонов. Проведена успешная апробация реализованной методики, получены данные экспериментов о работе генетического алгоритма. На основании проведенного исследования определены эффективные параметры вычисления целевой функции.

Ключевые слова: аутентификация, биометрия, генетический алгоритм, токен, шаблон, генетические операторы.

THE APPLICATION OF A GENETIC ALGORITHM TO IMPROVE THE STABILITY OF A PASSWORD GENERATION METHOD BASED ON BIOMETRIC AUTHENTICATION

Research article

Belomoytsev D.E.[1,] *, Volosatova T.M.[2]
[1] ORCID : 0000-0001-8200-2963;
[2] ORCID : 0000-0002-2882-5464;
[1, 2] Bauman Moscow State Technical University, Moscow, Russian Federation

* Corresponding author (belomoid[at]bmstu.ru)

Abstract

An approach to multi-factor authentication using biometrics and a token is examined. A method is suggested for generating authentication passwords comprising several components, one of which is stored in a secure token repository and becomes accessible following the verification of biometric templates. The issue of applying biometric verification due to template variability and drift is highlighted. To address the drift problem, a genetic algorithm is applied, for which genetic operators have been developed that take into account the characteristics of the templates. The implemented method has been successfully tested, and experimental data on the performance of the genetic algorithm have been obtained. Based on the conducted research, effective parameters for calculating the objective function have been determined.

Keywords: authentication, biometrics, genetic algorithm, token, template, genetic operators.

Введение

В эпоху цифровой трансформации и повсеместного распространения распределенных информационных систем задача установления и подтверждения подлинности субъектов взаимодействия становится критически важной. При ее решении осуществляется аутентификация — процесс проверки подлинности предъявленных субъектом (пользователем, процессом, устройством) учетных данных с целью подтверждения его заявленной идентичности. Надежность аутентификации определяется используемыми факторами: знание (пароль, PIN), владение (токен, смарт-карта, мобильное устройство), свойство (биометрические данные) [1].

Повышение требований к безопасности и рост сложности атак (фишинг, брутфорс, перехват сессий) приводят к необходимости использования многофакторной аутентификации, которая комбинирует два и более фактора, что кратно повышает сложность компрометации [2]. При этом использование биометрических данных в качестве одного из факторов добавляет сопутствующие данной технологии уязвимости к спуфинг-атакам, подверженность ошибкам вследствие необходимости компромисса между величинами порогов ложных принятия и отклонения, а также необходимость решения проблемы изменчивости и «дрейфа» шаблона. Противодействие уязвимостям и достижение компромисса при определении порогов возможно путем применения организационных мер и работы со сценариями [3]. При этом проблемы с шаблоном обычно требуют его периодического обновления, что само по себе создает риски и операционные сложности.

В настоящей работе рассмотрен этап технологии аутентификации, в рамках которого происходит процесс формирования и предоставления пароля. Целью работы является автоматизация этого процесса с использованием биометрических данных, исследование и повышение устойчивости его реализации.

Методика формирования паролей на основе биометрической аутентификации

Идея использования уникальных биометрических характеристик человека для формирования паролей или криптографических ключей интуитивно привлекательна. Она обещает избавление от необходимости запоминания сложных паролей и их безопасное «хранение» непосредственно в сознании пользователя. Однако, существует фундаментальное противоречие между стабильностью, требуемой для криптографии, и вариативностью, присущей биометрическим сигналам [4].

Использовать биометрические данные (изображение лица, скан отпечатка) в качестве непосредственных данных для формирования пароля невозможно по ряду причин [5]. Во-первых, биометрические измерения зашумлены (каждый новый захват отпечатка, лица или радужки отличается от предыдущего из-за смещения, давления, освещения, возраста), а сформированный криптографический ключ или пароль должен быть абсолютно точным и воспроизводимым. Во-вторых, эффективная энтропия биометрического признака может быть ниже, чем у хорошего пароля. Кроме того, она распределена неравномерно и зависит от алгоритма извлечения признаков. В-третьих, прямое использование биометрии как пароля не решает проблемы ее компрометации. Если шаблон был однажды украден и используется как «пароль», его невозможно изменить после утечки.

В связи с этим данные для аутентификации (пароль) необходимо формировать так, чтобы проблема нестабильного, зашумленного и ограниченно энтропийного биометрического входа непосредственным образом не могла оказывать влияние на качество этих данных.

Существует обобщенная концепция, в соответствии с которой из биометрических данных и случайного ключа генерируются вспомогательные данные, которые не раскрывают ни биометрию, ни ключ, но позволяют воспроизвести ключ при предъявлении похожих биометрических данных. Такой подход обладает недостатками: ключ привязывается к биометрии, эффективность значительно зависит от качества биометрических данных и алгоритма их извлечения и др.

Поэтому в данной работе предлагается использовать биометрические данные для промежуточной верификации на токене, где хранится информация для восстановления аутентификационных данных (пароля). При этом непосредственно в восстановлении аутентификационных данных биометрические данные участие не принимают.

Токен в предлагаемой схеме функционирует как защищенный носитель шаблона и компонента пароля (Smart Card / USB-ключ), а также как средство промежуточной верификации по биометрическим данным. Такой токен не имеет встроенного биометрического датчика, но выступает в роли защищенного хранилища, а также вычислителя. Предлагается следующий алгоритм работы с токеном:

1. На этапе регистрации биометрический шаблон (или его защищенное преобразование) записывается в защищенную память токена. Одновременно на токене генерируется или загружается компонент для формирования пароля.
2. При аутентификации пользователь считывает свои биометрические данные через внешний считыватель (на ПК, терминале), а также опциональный компонент пароля.
3. Считанные данные по защищенному соединению передаются на токен.
4. Токен осуществляет верификацию — реализованный на нем алгоритм вычисляет шаблон по переданным данным биометрии и сравнивает его с эталонным шаблоном, хранящимся в хранилище токена.
5. Только в случае успешного проведения верификации токен разблокирует доступ к хранимому компоненту пароля и использует его восстановления совместно с опциональным компонентом.

К достоинствам данной методики формирования паролей возможно отнести реализацию принципа изоляции компонентов для их восстановления. Использовать эти компоненты возможно только в случае успеха локальной биометрической верификации. При этом компоненты не покидают защищенное хранилище токена.

Также существенным преимуществом методики является то, что восстановленный пароль после его выдачи с токена через защищенное соединение участвует в стандартном криптографическом протоколе с сервером аутентификации. При этом сервер никак не взаимодействует с биометрическими данными.

В то же время на результаты восстановления паролей по реализованной методике оказывает существенное влияние проблема изменчивости и «дрейфа» биометрических шаблонов [6]. Для ее решения без необходимости частой перекалибровки возможно применить подход с использованием генетического алгоритма [7] для создания адаптивного и устойчивого эталонного шаблона, который эволюционирует со временем, но защищён от резких и ошибочных изменений.

Предполагается, что при на начальном этапе на токене формируется первоначальный эталонный шаблон, а при каждой успешной верификации в дальнейшем генерируется новый актуальный шаблон. Простая замена первоначального шаблона на новый шаблон может быть рискованной (вследствие возможных ошибок верификации). Усреднение шаблонов может привести к потере важных черт.

При помощи генетического алгоритма необходимо формировать такой шаблон, который

• максимально похож на все успешные попытки верификации;

• сохраняет ключевые, неизменные черты из первоначального эталона;

• постепенно и контролируемо адаптируется к легитимным изменениям.

Хромосома проектного решения формируется из компонентов шаблона T.

Функция полезности $F_{\text{п}}(T)$ шаблона-кандидата T должна [8] учитывать:

– сходство с первоначальным эталоном TE для сохранения ядра идентичности: $F_{\text{СХ.Э}}(T, TE)$;

– среднее сходство с последними успешными шаблонами $\{TV\}$ для обеспечения адаптации: $F_{\text{СХ.СР}}(T, \{TV\})$;

– дисперсию сходства с последними успешными шаблонами $F_{\text{ДИСП}}(\{F_{\text{СХ.Э}}(T, TV_i)\})$, чтобы шаблон-кандидат T был стабильно похож на все успешные последние шаблоны.

$$F_{\text{п}}(T) = \alpha \cdot F_{\text{СХ.Э}}(T, TE) + \beta \cdot F_{\text{СХ.СР}}(T, \{TV\}) - \gamma \cdot F_{\text{ДИСП}}(\{F_{\text{СХ.Э}}(T, TV_i)\})$$

– здесь α, β и γ – весовые коэффициенты, определяющие баланс между доверием к истории, важностью адаптации и штрафом за нестабильность.

Алгоритм использует генетический оператор селекции для отбора шаблонов с наибольшим значением функции полезности [9]. Операторы кроссовера и мутации реализованы [10] таким образом, чтобы учитывать существование в шаблонах определенных зон признаков, имеющих максимальную вероятность изменения. Учет данных особенностей позволяет достигать большего эффекта в работе операторов кроссовера и мутации при формировании новых особей.

Результаты применения генетического алгоритма в рамках предложенной методики

Исследование показателей работы подсистемы биометрической верификации проведено с использованием изображений лиц, получаемых в различном разрешении (от 2МП до 12МП) с веб-камер или камер мобильных устройств. При помощи разработанного ПО на снимках выделялись области расположения лиц, наборы из 68 ключевых анатомических точек, а также дескриптор лица в составе 128 компонентов.

Всего в экспериментах участвовали изображения лиц 45 различных людей, снимаемые в течение 1 года.

В качестве показателей эффективности работы подсистемы биометрической верификации оценивались такие базовые метрики, как ошибки первого и второго рода — FRR и FAR.

Оценка этих метрик производилась на трёх группах шаблонов, изначально основанных на эталонных: шаблоны T_C не подвергались корректировке, шаблоны T_G адаптировались к дрейфу с применением генетического алгоритма, шаблоны T_U обновлялись методом селективного обновления (метод простого усреднения не применялся, т.к. его эффективность против дрейфа была расценена недостаточной).

На эталонных шаблонах после регистрации значения FRR и FAR составили, соответственно, 1,3% и 0,0012%.

На шаблонах T_C значения FRR и FAR через 1 год: 2,56% и 0,0016%.

На шаблонах T_G значения FRR и FAR через 1 год: 0,86% и 0,0011%.

На шаблонах T_U значения FRR и FAR через 1 год: 0,87% и 0,0010%.

Таким образом, на шаблонах без адаптации к дрейфу работа подсистемы ухудшилась — ошибочные отказы стали происходить чаще.

Верификация на шаблонах, которые подвергались обработке с использованием предложенного подхода с генетическим алгоритмом, стала проходить лучше — частота ошибочных отказов снизилась.

Практически аналогичная ситуация наблюдалась и на шаблонах, которые подвергались селективному обновлению.

Применение генетического алгоритма для обеспечения устойчивости к дрейфу биометрических шаблонов показывает результат не хуже, чем при работе с селективным обновлением. При этом в случае адаптации на основе генетического алгоритма нет зависимости от настройки алгоритмов обнаружения изменений, которая критически важна для качественного проведения селективного обновления.

Работа генетического алгоритма с отбором 20% особей при селекции на 50-100 поколениях после каждой успешной верификации и значениями весов α=0,3, β=0,6 и γ=0,1 функции полезности позволяет достигнуть поставленной цели — адаптации эталонного шаблона. При этом дрейф происходит не заменой, а эволюцией эталона. Функция полезности не даёт шаблону отклониться далеко от первоначального эталона и требует стабильного сходства со многими последними попытками. Если биометрические данные медленно меняются (растёт борода, происходит старение), то новые шаблоны будут постепенно вынуждать эталон меняться за собой.

Дополнительно необходимо отметить, что реализованная методика формирования паролей позволяет объединить предъявление биометрических признаков («свойство»), обработку на токене («владение») и опциональный ввод дополнительного компонента («знание»). Тем самым достигается эффект от использования многофакторности. Также существенным является децентрализованное хранение биометрических шаблонов, что потенциально исключает проведение атак на централизованных базы данных.

Заключение

Реализованная методика формирования паролей на основе биометрической аутентификации с использованием токена позволяет перенести критически важную операцию верификации в защищенную периферию. При этом в полной мере используются преимущества многофакторной аутентификации («знание-владение-свойство»). Предложенный в рамках данной методики подход к использованию генетического алгоритма позволяет улучшить показатели биометрической верификации в контексте проблемы «дрейфа» шаблонов.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. ISO/IEC 24745:2022. Information security, cybersecurity and privacy protection — Biometric information protection. — Introduced 2022-02-01. — Geneva : ISO/IEC, 2022. — 63 p. — URL: https://www.iso.org/standard/75302.html (accessed: 09.01.2026).

2. FIDO2: WebAuthn & CTAP Specifications // FIDO Alliance. — 2025. — URL: https://fidoalliance.org/specs/fido-v2.2-ps-20250714/fido-client-to-authenticator-protocol-v2.2-ps-20250714.pdf (accessed: 09.01.2026).

3. FIDO UAF Architectural Overview // FIDO Alliance. — 2020. — URL: https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-overview-v1.2-ps-20201020.html (accessed: 09.01.2026).

4. Cooper D. Interfaces for Personal Identity Verification / D. Cooper, H. Ferraiolo, J. Mohler [et al.] // NIST. — 2015. — URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=918402 (accessed: 09.01.2026).

5. Rattani A. Adaptive biometric systems: recent advances and challenges / A. Rattani, F. Roli, E. Granger. — Berlin : Springer, 2016. — 134 p.

6. Rattani A. Template update methods in adaptive biometric systems: a critical review / A. Rattani, B. Freni, G.L. Marcialis [et al.]. — Berlin : Springer, 2009. — P. 847–856.

7. Норенков И.П. Метагенетический алгоритм оптимизации и структурного синтеза проектных решений / И.П. Норенков, Н.М. Арутюнян // Информационные технологии. — 2007. — № 3. — С. 10–13.

8. Норенков И.П. Генетические алгоритмы поиска решений в онтологических базах знаний / И.П. Норенков // Информационные технологии. — 2010. — № 9. — С. 20–24.

9. Беломойцев Д.Е. Эволюционный подход к решению задачи автоматизации проектирования структуры образовательного контента / Д.Е. Беломойцев // Научно-технический вестник Брянского государственного университета. — 2016. — № 4. — С. 92–98.

10. Волосатова Т.М. Разработка генетического алгоритма составления учебных курсов индивидуального содержания / Т.М. Волосатова, Д.Е. Беломойцев // Ученые записки ИСГЗ. — 2017. — Т. 15. — № 1. — С. 136–142.

Список литературы на английском языке / References in English

1. ISO/IEC 24745:2022. Information security, cybersecurity and privacy protection — Biometric information protection. — Introduced 2022-02-01. — Geneva : ISO/IEC, 2022. — 63 p. — URL: https://www.iso.org/standard/75302.html (accessed: 09.01.2026).

2. FIDO2: WebAuthn & CTAP Specifications // FIDO Alliance. — 2025. — URL: https://fidoalliance.org/specs/fido-v2.2-ps-20250714/fido-client-to-authenticator-protocol-v2.2-ps-20250714.pdf (accessed: 09.01.2026).

3. FIDO UAF Architectural Overview // FIDO Alliance. — 2020. — URL: https://fidoalliance.org/specs/fido-uaf-v1.2-ps-20201020/fido-uaf-overview-v1.2-ps-20201020.html (accessed: 09.01.2026).

4. Cooper D. Interfaces for Personal Identity Verification / D. Cooper, H. Ferraiolo, J. Mohler [et al.] // NIST. — 2015. — URL: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=918402 (accessed: 09.01.2026).

5. Rattani A. Adaptive biometric systems: recent advances and challenges / A. Rattani, F. Roli, E. Granger. — Berlin : Springer, 2016. — 134 p.

6. Rattani A. Template update methods in adaptive biometric systems: a critical review / A. Rattani, B. Freni, G.L. Marcialis [et al.]. — Berlin : Springer, 2009. — P. 847–856.

7. Norenkov I.P. Metageneticheskii algoritm optimizatsii i strukturnogo sinteza proektnikh reshenii [A genetic approach lo structure synthesis using meta-genetic parameter optimization] / I.P. Norenkov, N.M. Harutyunyan // Informatsionnie tekhnologii [Information Technologies]. — 2007. — № 3. — P. 10–13. [in Russian]

8. Norenkov I.P. Geneticheskie algoritmi poiska reshenii v ontologicheskikh bazakh znanii [Genetic algorithms of decision search in ontological knowledge bases] / I.P. Norenkov // Informatsionnie tekhnologii [Information Technologies]. — 2010. — № 9. — P. 20–24. [in Russian]

9. Belomoitsev D.E. Evolyutsionnii podkhod k resheniyu zadachi avtomatizatsii proektirovaniya strukturi obrazovatelnogo kontenta [Evolutionary approach to the educational content structure design automation problem solution] / D.E. Belomoitsev // Nauchno-tekhnicheskii vestnik Bryanskogo gosudarstvennogo universiteta [Scientific and Technical Bulletin of Bryansk State University]. — 2016. — № 4. — P. 92–98. [in Russian]

10. Volosatova T.M. Razrabotka geneticheskogo algoritma sostavleniya uchebnikh kursov individualnogo soderzhaniya [Development of genetic algorithm for individual content training courses design] / T.M. Volosatova, D.E. Belomoitsev // Uchenie zapiski ISGZ [Scientific notes of ISGZ]. — 2017. — Vol. 15. — № 1. — P. 136–142. [in Russian]