УДК 004.624+004.032.26
DOI: 10.26102/2310-6018/2024.47.4.027

Разработка и исследование программной системы биометрической аутентификации пользователя по динамике рукописной подписи с использованием нечетких признаков

Э.С. Анисимова[1]✉, И.В. Аникин[2]

[1]Елабужский институт (филиал) Казанского (Приволжского) федерального университета, Елабуга, Российская Федерация
[2]Казанский национальный исследовательский технический университет им. А.Н. Туполева, Казань, Российская Федерация

Резюме. Сложность надежной биометрической аутентификации пользователя по динамике рукописных подписей обусловлена их высокой внутриклассовой вариативностью, связанной с изменениями физического и эмоционального состояния человека, а также условий написания. Существующие подходы не всегда обеспечивают достаточную точность и устойчивость к этим вариациям. Данная работа посвящена исследованию и разработке программной системы биометрической аутентификации, использующей аппарат теории нечетких множеств для повышения надежности распознавания. В работе предложена оригинальная признаковая модель динамической рукописной подписи, включающая набор статических и динамических признаков, в том числе нечеткие, учитывающие неопределенность и вариативность почерка. В качестве эталона подписи используется совокупность функций принадлежности, построенных на основе компонентов признаковой модели. Предложена архитектура системы распознавания, состоящая из подсистем обучения, создания модели тестовой подписи и принятия решения о подлинности. Разработана программная система, реализующая предложенный подход, с использованием математического пакета SciLab и языка программирования C++. Система предоставляет функционал регистрации пользователей и формирования обучающей выборки на основе подписей, введенных с помощью графического планшета, а также распознавание тестовых подписей. Экспериментальное исследование проведено на базе коллекции подписей MCYT Signature 100. В ходе исследования экспериментально определено оптимальное значение степени компактности кластера для построения функций принадлежности признаков, минимизирующее коэффициент равного уровня ошибок. Результаты экспериментов демонстрируют снижение коэффициента равного уровня ошибок по сравнению с известными методами, что свидетельствует об эффективности предложенного подхода. Применение нечетких признаков способствует повышению устойчивости системы к вариациям в подписях и, как следствие, повышению надежности биометрической аутентификации в различных приложениях, требующих подтверждения личности. Результаты исследования могут быть использованы для повышения безопасности систем аутентификации и защиты конфиденциальной информации.

Ключевые слова: биометрическая аутентификация, рукописная подпись, графический планшет, динамика ввода подписи, теория нечетких множеств, нечеткая логика, модель подписи, эталон подписи, характер нажима, ритм письма.

Для цитирования: Анисимова Э.С., Аникин И.В. Разработка и исследование программной системы биометрической аутентификации пользователя по динамике рукописной подписи с использованием нечетких признаков. *Моделирование, оптимизация и информационные технологии.* 2024;12(4). URL: https://moitvivt.ru/ru/journal/pdf?id=1750 DOI: 10.26102/2310-6018/2024.47.4.027

© Анисимова Э.С., Аникин И.В., 2024

Development and research of a software system for biometric authentication of a user based on the dynamics of a handwritten signature using fuzzy features

E.S. Anisimova[1]✉, I.V. Anikin[2]

[1]Elabuga Institute (branch) of Kazan (Volga Region) Federal University, Elabuga, the Russian Federation

[2]Kazan National Research Technical University named after A.N. Tupolev, Kazan, the Russian Federation

Abstract. The complexity of reliable biometric user authentication based on the dynamics of handwritten signatures is due to their high intra-class variability associated with changes in the physical and emotional state of a person, as well as writing conditions. Existing approaches do not always provide sufficient accuracy and resistance to these variations. This work is devoted to the study and development of a software system for biometric authentication using the apparatus of fuzzy set theory to improve the reliability of recognition. In this work, we proposed an original feature model of a dynamic handwritten signature, including a set of static and dynamic features, including fuzzy ones, taking into account the uncertainty and variability of handwriting. As a signature standard, we used a set of membership functions built on the basis of the components of the feature model. We proposed an architecture of the recognition system consisting of training subsystems, creating a test signature model, and making a decision on authenticity. We developed a software system that implements the proposed approach using the SciLab mathematical package and the C++ programming language. The system provides the functionality of user registration and formation of a training sample based on signatures entered using a graphic tablet, as well as recognition of test signatures. We conducted an experimental study based on the MCYT Signature 100 signature collection. During the study, we experimentally determined the optimal value of the cluster compactness degree for constructing feature membership functions that minimizes the equal error rate coefficient. The experimental results demonstrate a decrease in the equal error rate coefficient compared to known methods, which indicates the effectiveness of the proposed approach. The use of fuzzy features helps to increase the system's resistance to variations in signatures and, as a result, increase the reliability of biometric authentication in various applications that require identity verification. The results of the study can be used to improve the security of authentication systems and protect confidential information.

Keywords: biometric authentication, handwritten signature, graphic tablet, signature input dynamics, fuzzy set theory, fuzzy logic, signature model, signature standard, pressure pattern, writing rhythm.

For citation: Anisimova E.S., Anikin I.V. Development and research of a software system for biometric authentication of a user based on the dynamics of a handwritten signature using fuzzy features. *Modeling, Optimization and Information Technology*. 2024;12(4). (In Russ.). URL: https://moitvivt.ru/ru/journal/pdf?id=1750 DOI: 10.26102/2310-6018/2024.47.4.027

Введение

Биометрическая аутентификация человека, основанная на уникальных физиологических и поведенческих характеристиках, представляет собой одну из наиболее перспективных технологий обеспечения информационной безопасности. Актуальность данной темы обусловлена постоянным ростом числа киберугроз и необходимостью разработки надежных и удобных методов защиты информации и доступа к ресурсам. Среди различных биометрических методов динамическая рукописная подпись выделяется высокой степенью уникальности, сложностью подделки и относительной простотой сбора данных. Рукописная подпись не только отражает индивидуальный стиль написания, но и включает в себя множество динамических

параметров, таких как скорость, нажим, ритм и последовательность движений, что делает ее эффективным способом биометрической аутентификации.

В последние годы динамическая рукописная подпись стала предметом активных исследований [1–3]. Существующие подходы к биометрической аутентификации личности по динамической рукописной подписи включают нейросетевые методы [4] с применением архитектуры глубоких нейронных сетей, метод опорных векторов и скрытые марковские модели [5–6], моделирующие процесс подписания как последовательность скрытых состояний. Однако, несмотря на достигнутые успехи, традиционные методы часто сталкиваются с проблемой жестких границ классификации, что может привести к ошибкам при проведении процедуры аутентификации, особенно при изменении условий написания подписи (усталость, стресс и др.).

Настоящее исследование посвящено повышению точности работы систем биометрической аутентификации с динамической рукописной подписью, с учетом вариабельности индивидуальных характеристик подписи.

Цель исследования: разработать метод биометрической аутентификации по динамике рукописной подписи на основе нечеткой признаковой модели, обеспечивающий повышенную точность и устойчивость к вариациям почерка, а также реализовать программную систему распознавания подписей, демонстрирующую эффективность предложенного метода.

Для достижения поставленной цели необходимо решить следующие задачи:

1) разработка признаковой модели динамической рукописной подписи;

2) разработка метода формирования эталона подписи на основе нечеткой признаковой модели;

3) разработка и реализация программной системы распознавания динамических подписей;

4) экспериментальное исследование эффективности разработанного метода.

Применение теории нечетких множеств позволяет моделировать более гибкие системы, способные учитывать степень принадлежности объекта к определенным классам [7–8], что потенциально может улучшить точность распознавания и адаптивность системы к изменениям в образце подписи.

Материалы и методы

Графический планшет позволяет регистрировать не только графическое изображение подписи, но и динамику ее создания. Полученные данные представляют собой многомерный временной ряд, отражающий изменение различных параметров в процессе написания. Фиксируются координаты положения пера (X и Y), сила нажима (P), а также азимут (Az) и угол наклона пера (A) (Рисунки 1, 2).

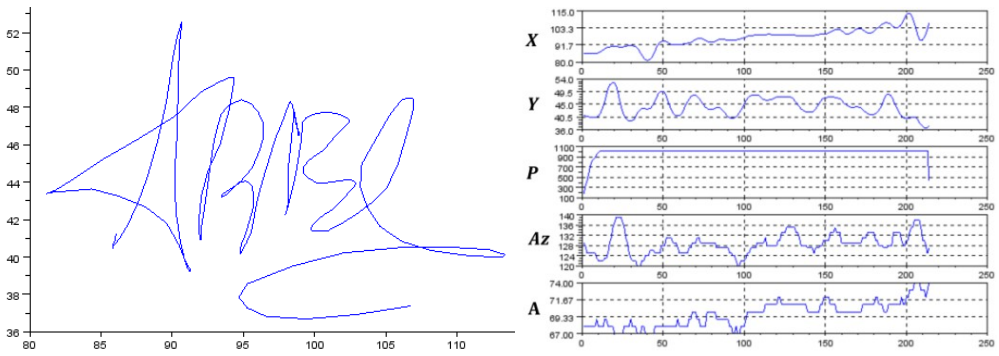

Рисунок 1 – Изображение динамической рукописной подписи и ее параметры
Figure 1 – Image of dynamic handwritten signature and its parameters

Эта информация о динамике письма является ключевой для биометрической аутентификации. Каждый из параметров, отражая динамику подписи по определенному каналу [9–10], может быть использован для построения модели рукописной подписи.

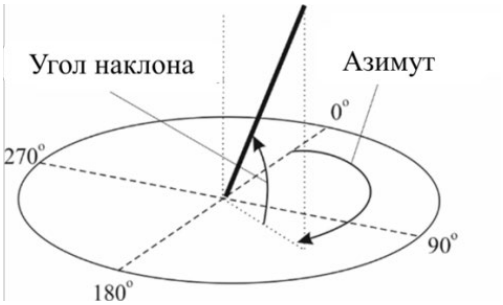

Рисунок 2 – Угол наклона и азимут пера
Figure 2 – Pen tilt angle and azimuth

Введем обозначения.

Пусть S_t – многомерный временной ряд, характеризующий динамическую рукописную подпись.

Представим S_t в виде:

$$S_t = (X_t, Y_t, Z_t, Az_t, A_t), \quad (1)$$

где X_t – одномерный временной ряд, характеризующий изменение положения конца пера относительно положительной полуоси OX на экране планшета, причем $X_t = x_1, x_2, x_3, \dots, x_n$ – значения временного ряда, полученные путем регистрации соответствующей характеристики X через определенные промежутки времени; Y_t – одномерный временной ряд, характеризующий изменение положения конца пера относительно положительной полуоси OY на экране планшета; Z_t – одномерный временной ряд, характеризующий изменение нажима пера на планшет; Az_t – одномерный временной ряд, характеризующий изменение азимута пера; A_t – одномерный временной ряд, характеризующий изменение угла наклона пера; t – момент времени, в который зафиксировано значение показателя.

Предварительно была проведена нормализация значений временных рядов X_t, Y_t, Z_t, Az_t, A_t, описывающих динамическую рукописную подпись, с учетом характеристик графического планшета.

Представим модель рукописной подписи S_t в следующем виде:

$$M(S_t) = (l, \lambda, \rho, \tau, \sigma, \omega, r, \{\xi_F\}_{F \in S_t}), \quad (2)$$

где l – длина подписи; λ – относительная пропорция подписи; ρ – средний нажим при вводе подписи; τ – относительная продолжительность подъема пера при вводе подписи; σ – неравномерность нажима; ω – характер нажима; r – ритм письма; ξ_F – площадь криволинейной области, ограниченной графиком временного ряда F (где $F \in S_t$).

Рассмотрим компоненты предложенной модели M.

1) Длина подписи, l, определяется длиной временных рядов X_t, Y_t, Z_t, Az_t, A_t.

2) Относительная пропорция подписи, λ, выражается соотношением ее высоты и ширины, т. е. $\lambda = \frac{\max(Y_t) - \min(Y_t)}{\max(X_t) - \min(X_t)}$.

3) Средний нажим, ρ, определяется средним значением давления пера на планшет во время ввода подписи $\rho = \overline{Z_t}$, т. е. $\rho = \frac{\sum_{i=1}^{l} z_i}{l}$. Следует отметить, что нажим подписи слабо поддается зрительному анализу, его воспроизведение недоступно для подражания.

4) Относительная продолжительность подъема пера при вводе подписи, τ, определяет отношение продолжительности подъема пера (отрыва его от планшета) к общей продолжительности ввода подписи $\tau = \frac{l_{z_t=0}}{l}$.

5) Неравномерность нажима, σ, характеризует разброс значений нажима пера при вводе подписи, $\sigma = \sqrt{\frac{\sum_{i=1}^{l}(z_i-\rho)^2}{l}}$.

6) Характер нажима ω как нечеткий признак определяется на основе лингвистических переменных «Нажим» и «Скорость письма». Определим множество термов лингвистической переменной «Характер нажима»: «Легкий и быстрый» (подпись с минимальным нажимом и высокой скоростью, на выходе остаются очень светлые, тонкие линии, письмо возможно небрежное), «Легкий и медленный» (подпись с минимальным нажимом и низкой скоростью, остаются светлые линии, но письмо более аккуратное), «Размашистый» (подпись со средним нажимом и высокой скоростью), «Тяжелый и медленный» (подпись с сильным нажимом и низкой скоростью, остаются четко видимые линии), «Акцентированный» (подпись с переменным нажимом, где в некоторых участках подписи (для выделения / выразительности) применяется более сильный нажим). Множество термов лингвистической переменной «Нажим»: «Легкий», «Средний», «Сильный». Множество термов лингвистической переменной «Скорость письма»: «Низкая», «Средняя», «Высокая». Опишем нечеткие правила:

Правило 1: ЕСЛИ Нажим «Легкий» И Скорость письма «Высокая», ТО Характер нажима «Легкий и быстрый»;

Правило 2: ЕСЛИ Нажим «Сильный» И Скорость письма «Низкая», ТО Характер нажима «Тяжелый и медленный»;

Правило 3: ЕСЛИ Нажим «Средний» И Скорость письма «Высокая», ТО Характер нажима «Размашистый»;

Правило 4: ЕСЛИ Нажим «Сильный» И Скорость письма «Средняя», ТО Характер нажима «Акцентированный»;

Правило 5: ЕСЛИ Нажим «Легкий» И Скорость письма «Низкая», ТО Характер нажима «Легкий и медленный».

7) Ритм письма r как нечеткий признак определяется на основе следующих параметров письма – лингвистических переменных «Скорость письма», «Нажим», «Ускорение», «Изменчивость скорости». Множество термов лингвистической переменной «Ритм письма»: «Прерывистый» (характеризуется частыми остановками и возобновлениями движения пера, создается впечатление неравномерности движения, возникает при неуверенности или сильном волнении), «Неустойчивый» (неравномерное письмо, с заметными колебаниями скорости, может свидетельствовать о недостаточной координации движений или эмоциональной неустойчивости), «Устойчивый» (равномерное письмо с относительно постоянной скоростью и нажимом), «Плавный» (письмо ровное, без резких перепадов скорости и нажима, характеризуется плавными движениями пера, свидетельствует о хорошей координации движений и автоматизме ввода подписи). Множество термов лингвистической переменной «Ускорение»: «Низкое», «Среднее», «Высокое». Множество термов лингвистической переменной «Изменчивость скорости»: «Низкая», «Средняя», «Высокая». Определим правила вывода лингвистической переменной «Ритм письма»:

Правило 1: ЕСЛИ Скорость «Низкая» И Нажим «Легкий» И Изменчивость скорости «Высокая», ТО Ритм письма «Прерывистый».

Правило 2: ЕСЛИ Ускорение «Высокое» ИЛИ (Скорость «Средняя» И Изменчивость скорости «Высокая»), ТО Ритм письма «Неустойчивый».

Правило 3: ЕСЛИ Скорость «Средняя» И Нажим «Средний» И Ускорение «Среднее» И Изменчивость скорости «Низкая», ТО Ритм письма «Устойчивый».

Правило 4: ЕСЛИ Скорость «Высокая» И Нажим «Сильный» И Ускорение «Низкое» И Изменчивость скорости «Низкая», ТО Ритм письма «Плавный».

Для определения значения признаков «Характер нажима», ω, и «Ритм письма», r, применяется нечёткий вывод по модели Мамдани. На основе значений входных лингвистических переменных и с помощью заданных правил определяется нечеткое значение выходной лингвистической переменной, которое затем дефаззифицируется для получения четкого значения.

8) Площадь ξ_F криволинейной области, ограниченной графиком временного ряда F вычисляется отдельно для каждого временного ряда $F \in (X_t, Y_t, Z_t, Az_t, A_t)$. Для вычисления используются численные методы интегрирования (методы трапеций, прямоугольников).

Для реализации биометрической аутентификации необходимо сформировать эталон подписи, который будет использоваться для сравнения с предъявляемыми подписями. Эталон подписи создается на основе образцов, предоставленных пользователем в процессе обучения. Эталон, обозначаемый T_{ID} для пользователя ID, представляет собой набор функций принадлежности:

$$T_{ID} = \left\{ f_l, f_\lambda, f_\rho, f_\tau, f_\sigma, f_\omega, f_r, \{f_{\xi_F}\}_{F \in S_t} \right\}. \quad (3)$$

Каждая функция f_γ отражает распределение значений соответствующего признака γ (где γ принадлежит множеству признаков $M(S_t) = (l, \lambda, \rho, \tau, \sigma, \omega, r, \{\xi_F\}_{F \in S_t})$) в обучающей выборке пользователя.

Для построения функций принадлежности используется метод потенциалов, эффективный при небольшом объеме обучающих данных. Этот метод, основанный на принципах кластерного анализа, позволяет выявить области концентрации значений признака. Степень компактности кластера α влияет на форму функции принадлежности (Рисунок 3): чем выше α, тем более «острыми» будут пики функции в областях скопления значений. Значение функции принадлежности $f_\gamma(\gamma_i)$ вычисляется как нормированное значение потенциала φ_i в точке γ_i: $f_\gamma(\gamma_i) = \frac{\varphi_i}{\max(\varphi_j)}$, где потенциал φ_i определяется суммой: $\varphi_i = \sum_{j=1}^{M} e^{-4\alpha^2(\gamma_i - \gamma_j)^2}$.

Пусть T_{ID} – эталон динамической рукописной подписи пользователя с идентификатором ID, построенный на основе подлинных подписей из обучающей выборки пользователя, $T_{ID} = \left\{ f_l, f_\lambda, f_\rho, f_\tau, f_\sigma, f_\omega, f_r, \{f_{\xi_F}\}_{F \in S_t} \right\}$.

Определим степени схожести подлинных и степени схожести поддельных подписей из обучающей выборки с эталоном T_{ID} динамической рукописной подписи пользователя. В качестве степени схожести подписи с эталоном примем произведение $\prod_{f_\gamma \in T_{ID}} f_\gamma(\gamma^{train})$, где S_t^{train} – подпись из обучающей выборки, $\gamma^{train} \epsilon M(S_t^{train})$.

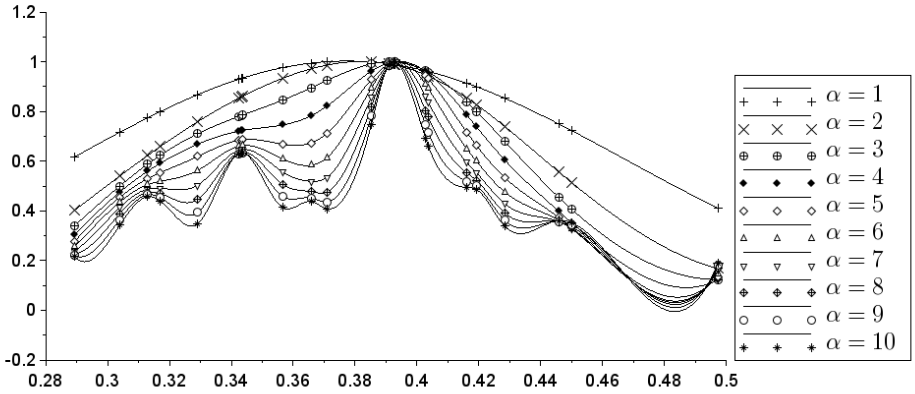

Рисунок 3 – Влияние степени компактности кластера α на функции принадлежности
Figure 3 – The influence of the degree of cluster compactness α on the membership functions

Упорядочим полученные степени схожести по возрастанию и обозначим $\{\delta_k\}$, где $k = 1, \dots, K$, K – объем обучающей выборки. Для каждого значения δ_k вычислим значение коэффициента равного уровня ошибок (EER), т. е. EER_k . В качестве индивидуального порога (порога схожести) δ^{ID} примем то значение δ_k, при котором наблюдается минимальное значение коэффициента равного уровня ошибок, т. е. $\delta^{ID} = \min(EER_k)$. Если степень схожести динамической рукописной подписи превышает значение индивидуального порога пользователя δ^{ID}, то проверяемая подпись считается подлинной, иначе – поддельной.

Результаты

Опишем структуру системы распознавания рукописной подписи (Рисунок 4).

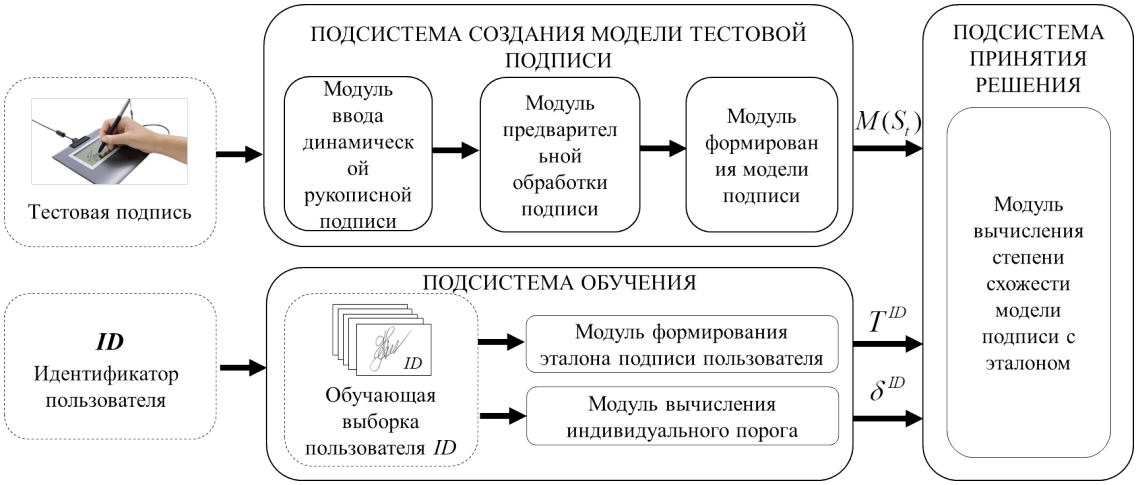

Рисунок 4 – Структура системы распознавания рукописной подписи
Figure 4 – Structure of dynamic handwritten signature recognition system

Система биометрической аутентификации по динамике рукописной подписи состоит из трех ключевых компонентов: подсистемы создания модели тестовой подписи, подсистемы обучения и подсистемы принятия решения. Подсистема создания модели, в свою очередь, включает модуль ввода, модуль предварительной обработки и модуль формирования самой модели. На вход этой подсистемы поступает подпись, введенная

для проверки. Модуль ввода регистрирует параметры подписи, представляя их в виде многомерного временного ряда $S_t = (X_t, Y_t, Z_t, Az_t, A_t)$. В модуле предварительной обработки осуществляется нормализация значений временных рядов, входящих в S_t. Выходом из подсистемы является модель тестовой подписи $M(S_t)$, построенная в модуле создания модели подписи.

Подсистема обучения включает в себя модуль формирования эталона подписи пользователя, модуль вычисления индивидуального порога, а также обучающую выборку пользователей. На вход подсистемы обучения поступает идентификатор пользователя *ID*. Выполняется обращение к подписям из обучающей выборки пользователя *ID*. На их основе в соответствующих модулях осуществляется формирование эталона подписи T_{ID} и вычисление индивидуального порога δ^{ID}.

На вход подсистемы принятия решения поступают модель тестовой подписи $M(S_t)$, эталон подписи T_{ID} и индивидуальный порог δ^{ID}. В модуле подсистемы вычисляется степень схожести модели тестовой подписи $M(S_t)$ с эталоном T_{ID}. Путем сравнения вычисленной степени схожести со значением индивидуального порога δ^{ID} принимается решение о подлинности / подделке тестовой подписи.

Система биометрической аутентификации по динамике рукописной подписи реализована программно с использованием математического пакета SciLab и среды разработки C++.

Программная система функционирует в двух режимах: «Регистрация» и «Распознавание» (Рисунок 5).

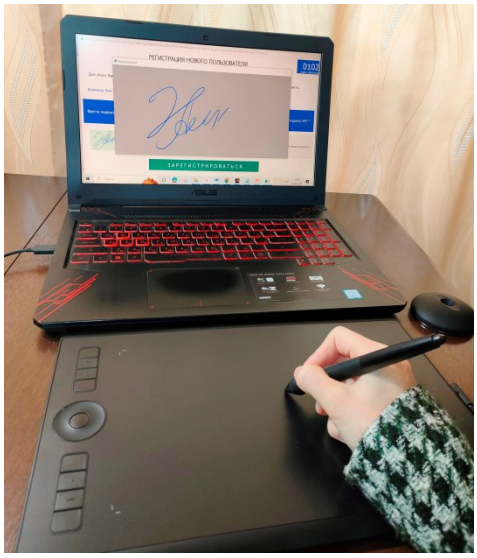

Рисунок 5 – Программный комплекс биометрической аутентификации
Figure 5 – Biometric authentication software package

Режим «Регистрация» (Рисунок 6) позволяет зарегистрировать в системе пользователя и сформировать его обучающую выборку. В этом режиме пользователю предлагается ввести имя и образцы рукописной подписи с помощью графического планшета. При вводе каждого образца подписи используется подключение к программному модулю ввода рукописной подписи, разработанному в среде разработки на C++. В исследовании использовался графический планшет Wacom Intuos Pro Medium PTH-660-R. В результате ввода рукописной подписи создается файл, содержащий значения координат, силу нажима пера на планшет, азимут, угол наклона пера в каждой точке подписи. Параметры рабочей области 224×148, время отклика – 200 точек в

секунду, чувствительность к нажиму – 8192 уровня. Таким образом, диапазоны значений временных рядов: X_t: [0; 22400]; Y_t: [0; 14800]; Z_t: [0; 8192]; Az_t: [0; 360]; A_t: [0; 90].

Процесс ввода подписи отображается на экране и далее, после закрытия окна ввода, подпись остается в виде миниатюры в соответствии с ее номером. Каждому пользователю при регистрации присваивается уникальный идентификатор. После ввода рукописных подписей происходит нормализация значений временных рядов, описывающих рукописную подпись, с учетом технических характеристик графического планшета. Кроме того, в связи с тем, что длины временных рядов рукописных подписей различны, осуществляется интерполяция их значений. Таким образом, в результате ввода подписей и предварительной обработки их значений формируется обучающая выборка пользователя с определенным идентификатором.

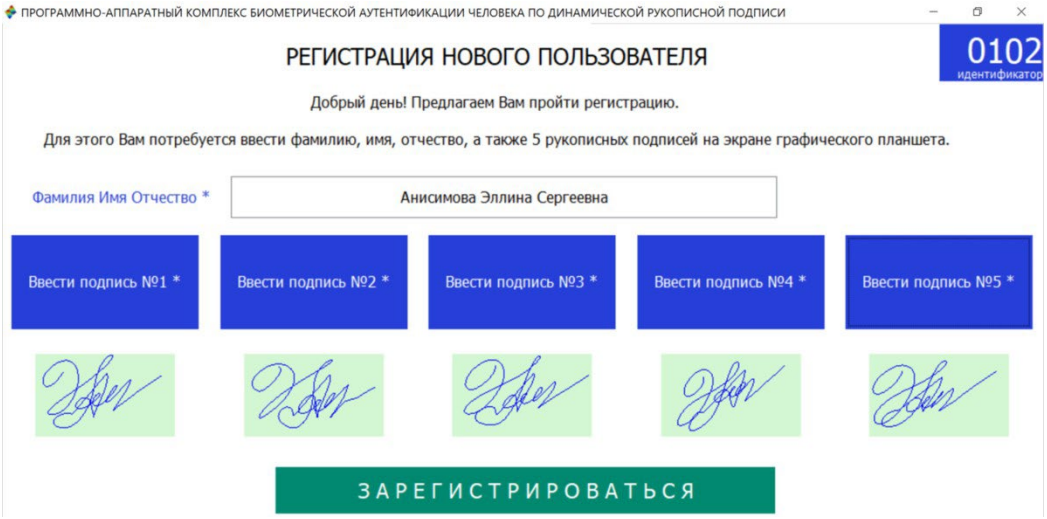

Рисунок 6 – Регистрация нового пользователя
Figure 6 – New User Registration

Режим «Распознавание» (Рисунок 7) предназначен для проведения процедуры аутентификации пользователя по динамической рукописной подписи.

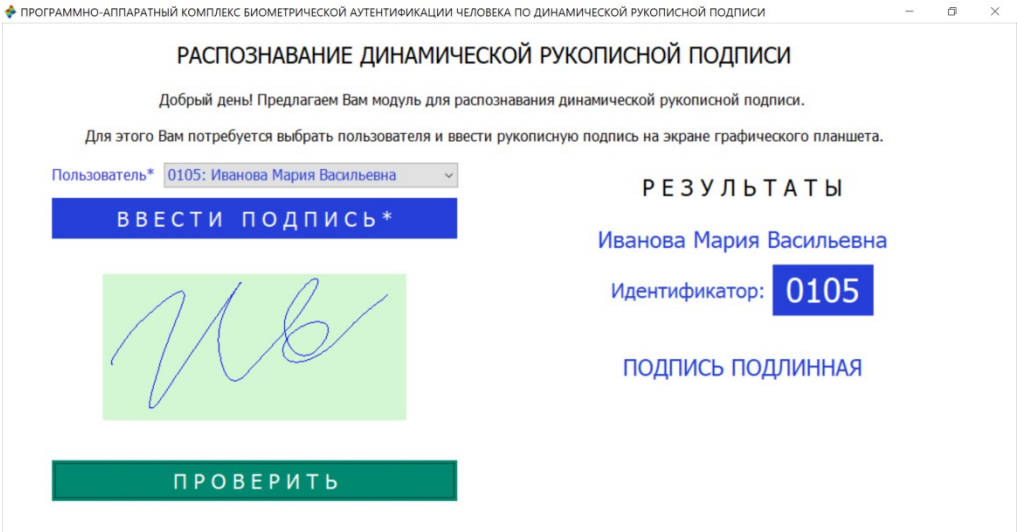

Рисунок 7 – Распознавание динамической рукописной подписи
Figure 7 – Dynamic handwritten signature recognition

В этом режиме пользователю предлагается указать идентификатор и ввести для проверки тестовую рукописную подпись.

Процесс аутентификации начинается с ввода подписи через специализированный модуль, написанный на C++. После ввода выполняется предварительная обработка полученной подписи и строится ее модель $M(S_t)$. Затем, используя идентификатор пользователя (ID), система обращается к обучающей выборке и формирует эталон T_{ID} и индивидуальный порог δ^{ID} для данного пользователя. Модель $M(S_t)$, эталон T_{ID} и порог δ^{ID} передаются в модуль принятия решения, который оценивает степень сходства введенной подписи с эталоном. Результат сравнения сопоставляется с индивидуальным порогом δ^{ID}, на основе чего принимается решение о подлинности или поддельности подписи.

Для тестирования системы использовалась база данных рукописных подписей MCYT Signature 100, содержащая по 25 оригинальных и 25 поддельных подписей для каждого из 100 человек. Подделки выполнялись разными людьми, имевшими доступ к образцам настоящих подписей.

При разных значениях степени компактности кластера, используя обучающую выборку из 5 подписей на одного пользователя, были определены значения коэффициента равного уровня ошибок (EER) в качестве интегрального показателя эффективности системы биометрической аутентификации (Таблица 1).

Таблица 1 – EER при различных значениях компактности кластера
Table 1 – EER for different values of cluster compactness

Степень компактности кластера, α	EER (%)
0,01	5,80
0,02	5,30
0,03	4,32
0,04	4,10
0,05	4,12
0,06	4,70
0,07	4,90
0,08	5,40
0,09	5,90
0,10	6,15

При значении $\alpha = 0{,}04$ при разных значениях размера обучающей выборки были определены значения коэффициента равного уровня ошибок EER (Таблица 2).

Таблица 2 – EER при различных размерах обучающей выборки
Table 2 – EER for different training sample sizes

Обучающая выборка (на 1 пользователя)	EER (%)
5	4,10
10	3,70
15	2,90
20	2,80

Обсуждение

Результаты исследования демонстрируют существенное влияние степени компактности кластера, определяемой при формировании функций принадлежности признаков эталона подписи, на эффективность биометрической аутентификации. Достигнутое минимальное значение EER, равное 4,10 %, при оптимальном значении

$\alpha = 0{,}04$ и использовании обучающей выборки из 5 подписей на пользователя, свидетельствует о высокой эффективности предложенного метода. Предполагается, что такая эффективность обусловлена более точным моделированием внутриклассовой вариабельности подписей благодаря оптимальному выбору α.

Сравнение с существующими методами, представленными в таблице (Таблица 3), подтверждает конкурентоспособность предложенного подхода. В частности, метод распознавания с использованием символьного представления [2] демонстрирует несколько меньший EER (3,80 %) при использовании значительно большей обучающей выборки (20 подписей). Однако при уменьшении размера обучающей выборки до 5 подписей, EER данного метода значительно возрастает (5,84 %), что указывает на его чувствительность к объему обучающих данных. В отличие от него, предложенный метод сохраняет высокую эффективность (EER 4,10 %) даже при малом объеме обучающих данных. Методы, основанные на скрытых марковских моделях [5–6] и импульсных нейронных сетях [4], также уступают предложенному методу по эффективности при сопоставимом или большем размере обучающей выборки.

Таким образом, предложенный метод демонстрирует перспективность для биометрической аутентификации по подписи, обеспечивая высокую эффективность при использовании ограниченного объема обучающих данных.

Таблица 3 – Эффективность методов аутентификации по динамике рукописной подписи (EER)
Table 3 – Efficiency of authentication methods based on handwritten signature dynamics (EER)

Метод аутентификации	Обучающая выборка (на 1 пользователя)	EER (%)
Метод распознавания с использованием символьного представления [2]	20 / 5	3,80 / 5,84
Метод распознавания с применением скрытых марковских моделей, обеспечивающих защиту шаблона подписи [5–6]	5	10,29
Метод распознавания с использованием импульсной нейронной сети [4]	15	3,90
Предложенный метод	5	4,10

Заключение

В заключение отметим, что применение нечетких признаков в сочетании с динамическими и статическими признаками позволяет повысить устойчивость системы биометрической аутентификации по динамике рукописной подписи к естественным вариациям почерка. Разработанная система, реализующая предложенный подход, демонстрирует снижение коэффициента равного уровня ошибок (EER) по сравнению с известными методами. Дальнейшие исследования могут быть направлены на совершенствование методов формирования нечетких признаков, адаптацию системы к различным типам графических планшетов и расширение экспериментальной базы для более полной оценки эффективности предложенного метода.

Перспективным также представляется исследование возможностей комбинирования данного подхода с другими биометрическими методами для повышения надежности аутентификации.

СПИСОК ИСТОЧНИКОВ / REFERENCES

1. Tolosana R., Vera-Rodriguez R., Gonzalez-Garcia C., et al. ICDAR 2021 Competition on On-Line Signature Verification. In: *Document Analysis and Recognition – ICDAR*

2021: 16th International Conference: Proceedings, Part IV, 5–10 September 2021, Lausanne, Switzerland. Cham: Springer; 2021. pp. 723–737. https://doi.org/10.1007/978-3-030-86337-1_48

2. Guru D.S., Prakash H.N. Online Signature Verification and Recognition: An Approach Based on Symbolic Representation. *IEEE Transactions on Pattern Analysis and Machine Intelligence*. 2009;31(6):1059–1073. https://doi.org/10.1109/TPAMI.2008.302
3. Jain A.K., Griess F.D., Connell S.D. On-line signature verification. *Pattern Recognition*. 2002;35(12):2963–2972. https://doi.org/10.1016/S0031-3203(01)00240-0
4. Kutsman V., Kolesnytskyj O. Dynamic handwritten signature identification using spiking neural network. *Informatyka, Automatyka, Pomiary W Gospodarce I Ochronie Środowiska*. 2021;11(3):34–39. https://doi.org/10.35784/iapgos.2718
5. Maiorana E., Campisi P., Fierrez J., Ortega-Garcia J., Neri A. Cancelable Templates for Sequence-Based Biometrics with Application to On-line Signature Recognition. *IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans.* 2010;40(3):525–538. https://doi.org/10.1109/TSMCA.2010.2041653
6. Maiorana E., Martinez-Diaz M., Campisi P., Ortega-Garcia J., Neri A. Template Protection for HMM-based On-Line Signature Authentication. In: *2008 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops*, *23–28 June 2008, Anchorage, AK, USA*. IEEE; 2008. pp. 1–6. https://doi.org/10.1109/CVPRW.2008.4563114
7. Zadeh L.A. Similarity relations and fuzzy orderings. *Information Sciences*. 1971;3(2):177–200. https://doi.org/10.1016/s0020-0255(71)80005-1
8. Zalasiński M., Cpałka K., Laskowski Ł., Wunsch D.C., Przybyszewski K. An Algorithm for the Evolutionary-Fuzzy Generation of on-Line Signature Hybrid Descriptors. *Journal of Artificial Intelligence and Soft Computing Research*. 2020;10(3):173–187. https://doi.org/10.2478/jaiscr-2020-0012
9. Anikin I., Anisimova E. Framework for Biometric User Authentication Based on a Dynamic Handwritten Signature. In: *Cyber-Physical Systems: Intelligent Models and Algorithms.* Cham: Springer; 2022. pp. 219–231. https://doi.org/10.1007/978-3-030-95116-0_18
10. Anisimova E.S., Anikin I.V. Fuzzy Sets Theory Approach for Recognition Handwritten Signatures. In: *Advances in Automation II: Proceedings of the International Russian Automation Conference, RusAutoConf2020, 6–12 September 2020, Sochi, Russia.* Cham: Springer; 2021. pp. 969–982. https://doi.org/10.1007/978-3-030-71119-1_93

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Анисимова Эллина Сергеевна, кандидат технических наук, доцент кафедры математики и прикладной информатики, Елабужский институт (филиал) Казанского (Приволжского) федерального университета, Елабуга, Российская Федерация.
e-mail: ellin_a@mail.ru
ORCID: 0000-0002-0036-5881

Ellina S. Anisimova, Candidate of Technical Sciences, Associate Professor of the Department of Mathematics and Applied Informatics, Elabuga Institute (branch) of Kazan (Volga Region) Federal University, Elabuga, the Russian Federation.

Аникин Игорь Вячеславович, доктор технических наук, профессор, проректор по цифровой трансформации, заведующий кафедрой систем информационной безопасности, Казанский национальный исследовательский технический университет

Igor V. Anikin, Doctor of Technical Sciences, Professor, Vice-Rector for Digital Transformation, Head of the Department of Information Security Systems, Kazan National Research Technical University named after A.N. Tupolev, Kazan, the Russian Federation.

им. А.Н. Туполева, Казань, Российская Федерация.
e-mail: anikinigor777@mail.ru
ORCID: 0000-0001-9478-4894

Статья поступила в редакцию 19.11.2024; одобрена после рецензирования 29.11.2024; принята к публикации 03.12.2024.

The article was submitted 19.11.2024; approved after reviewing 29.11.2024; accepted for publication 03.12.2024.