

РАСПОЗНАВАНИЕ ДИНАМИЧЕСКИХ РУКОПИСНЫХ ПОДПИСЕЙ С ИСПОЛЬЗОВАНИЕМ МЕТОДОВ ТЕОРИИ НЕЧЁТКИХ МНОЖЕСТВ

Э.С. Анисимова¹, И.В. Аникин²

¹ Елабужский институт (филиал) федерального государственного автономного
образовательного учреждения высшего образования
"Казанский (Приволжский) федеральный университет"
Российская Федерация, 423604, г. Елабуга, ул. Казанская, д. 89

² Казанский национальный исследовательский технический университет
им. А.Н. Туполева-КАИ
Российская Федерация, 420111, г. Казань, ул. К. Маркса, д. 10

Аннотация. Работа посвящена распознаванию рукописных подписей, введённых с помощью графического планшета. Предложена признаковая модель рукописной подписи, характеризующая особенности динамики написания подписи по различным каналам и использующая методы теории нечётких множеств. Предложен алгоритм создания эталонного шаблона рукописной подписи, использующий метод потенциалов для построения функций принадлежности признаков и работающий даже при небольшой обучающей выборке. Проведены исследования, в которых выявлены оптимальные значения степени компактности, используемой при построении функций принадлежности из эталонного шаблона, формы функций принадлежности термов лингвистических переменных, применяемых при построении признаковой модели, и, кроме того, получены рациональные составы признаков, минимизирующие ошибку распознавания. Предложена модульная структура программной системы распознавания рукописных подписей, введённых с помощью графического планшета. При найденных в результате исследований параметрах достигнуты значения показателя EER 0,36% и значение ошибки второго рода 0,2%.

Ключевые слова: динамическая рукописная подпись, динамическая характеристика, признаковая модель, эталонный шаблон.

Введение

Системы биометрической аутентификации пользователей всё чаще применяются в различных предметных областях [1]. Среди методов биометрической аутентификации выделяют физиологические (отпечаток пальца, сетчатка глаза, голос, термограмма лица [2]) и поведенческие (походка, динамика подписи [3], клавиатурный почерк [4]). Для проведения банковских операций, операций в сфере электронного документооборота [5, 6] особую актуальность приобретают системы биометрической аутентификации личности, основанные на применении рукописной подписи. При этом возможно использование как статической («off-line») [7, 8], учитывающей только изображение, так и динамической («on-line») рукописной подписи [9], учитывающей динамику её написания.

Динамическая рукописная подпись – это рукописная подпись человека, записываемая посредством графического планшета и хранящая, в отличие от статической, информацию о динамике её ввода. Эта информация записывается в виде последовательных значений динамических характеристик (рис. 1), поступающих по каналам:

- 1) X – «Положение пера по горизонтали»;
- 2) Y – «Положение пера по вертикали»;
- 3) P – «Величина нажатия пера»;
- 4) Г – «Азимут»;
- 5) Н – «Угол возвышения».

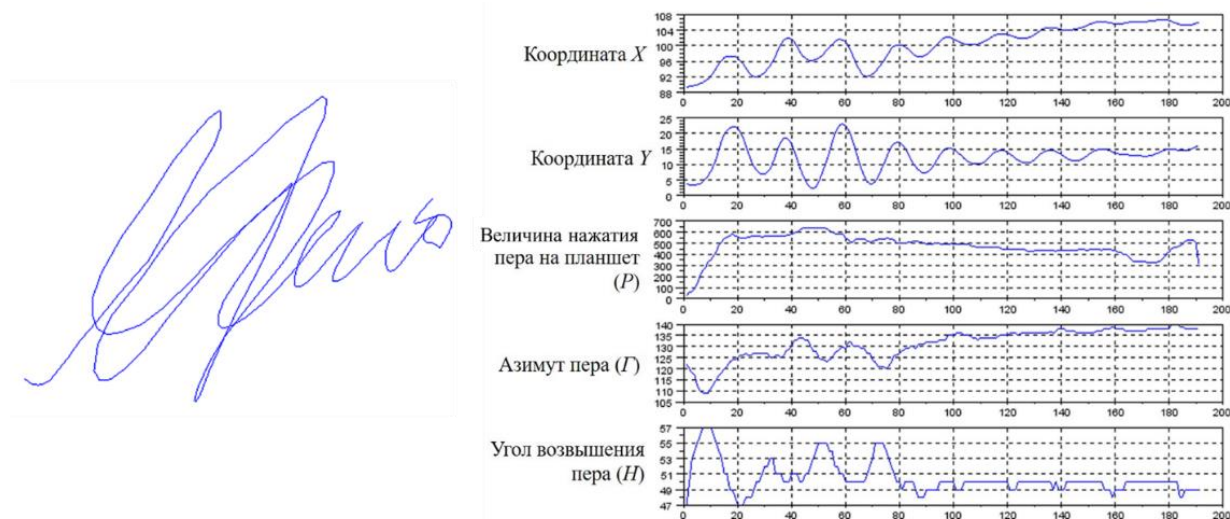


Рис.1. Рукописная подпись и её динамические характеристики

Применение рукописной подписи для биометрической аутентификации личности осложняется малым размером обучающей выборки, размытым характером подписи (подпись может меняться с течением времени, в результате эмоционального воздействия), возможным присутствием подделок.

Программное обеспечение распознавания динамических рукописных подписей

Авторами разработана программное обеспечение (ПО), позволяющее определять подлинность вводимой динамической рукописной подписи и на основе этого выполнять аутентификацию (проверку подлинности) пользователя. ПО было реализовано в математическом пакете SciLab с подключением среды разработки C++. Модульная структура ПО представлена на рис. 2, где ID – идентификатор пользователя, $\tilde{a}$ – сформированный образец динамической рукописной подписи, $\Omega(\tilde{a})$ – признаковая модель введенной динамической рукописной подписи, E_{ID} – эталонный шаблон (признаковая модель) динамической рукописной подписи пользователя с идентификатором ID , σ_{ID} – индивидуальный порог принятия решения о прохождении аутентификации для пользователя с идентификатором ID , τ – расстояние от динамической рукописной подписи пользователя до эталонного шаблона.

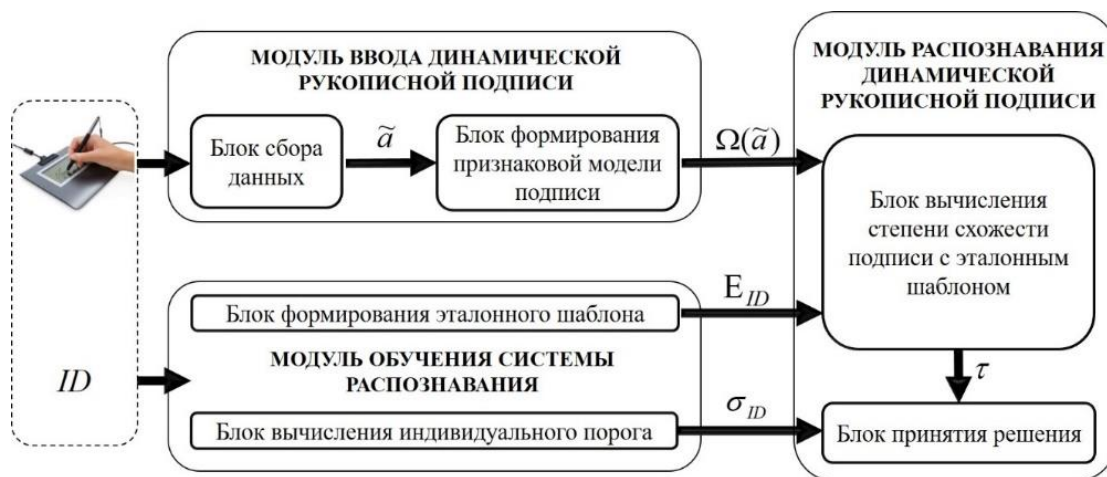


Рис. 2. Модульная структура программного обеспечения

Модуль ввода динамической рукописной подписи

В данном модуле организованы процессы сбора данных о подписи и формирования её признаковой модели. Для сбора исходных данных о динамической рукописной подписи пользователя использовался графический планшет WACOM Intuos A6 USB, частота дискретизации сигнала 100 Гц.

Обозначим через $f[n]$ – дискретную функцию (рис. 3), значениями которой выступают значения сигнала (динамической характеристики), поступающего по конкретному каналу F ($x[n]$, $y[n]$, $p[n]$, $\gamma[n]$, $\eta[n]$), определяемые значениями сигналов, поступающих по каналам X, Y, P, Γ, H .

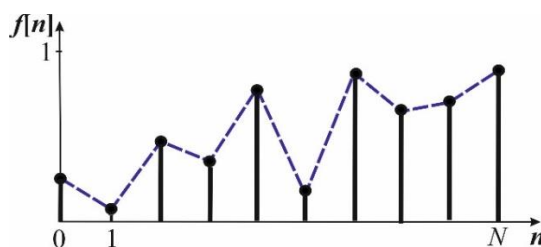


Рис. 3. Дискретная функция $f[n]$

На рис. 4 представлена блок-схема алгоритма сбора данных о подписи.

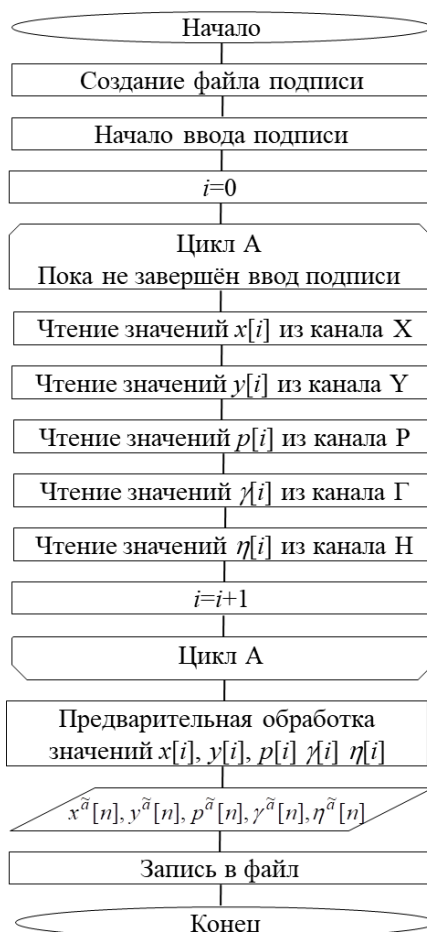


Рис. 4. Блок-схема алгоритма сбора данных

Здесь осуществляется запись в файл подписи значений дискретных функций $\tilde{x}[n]$, $\tilde{y}[n]$, $\tilde{p}[n]$, $\tilde{\gamma}[n]$, $\tilde{\eta}[n]$, прошедших предварительную обработку. В дальнейшем,

Пусть $\xi_f = (Sqr_f, FCLocMax_f, FuzInc_f, FuzDec_f, IncLeng_f, f[n], Sp_f[n])$ есть признаковое описание функции $f[n]$. Рассмотрим обозначения признаков, входящих в состав признакового описания.

Признаки $Sqr_f, FCLocMax_f, FuzInc_f, FuzDec_f$ – глобальные, они концентрируют особенности характеристик подписи за всё время её ввода [10, 11].

Sqr_f – площадь криволинейной области, ограниченной огибающей функции $f[n]$, прямыми $n = 0, n = N$ и осью n .

$FCLocMax_f$ – нечёткое количество локальных максимумов функции $f[n]$.

$FuzInc_f$ ($FuzDec_f$) – оценка нечёткого возрастания (убывания) функции $f[n]$.

$IncLeng_f$ – относительная длина участков возрастания функции $f[n]$.

Признаки $Sp_f[n], Angl[n]$ – локальные, они отражают особенности характеристик подписи в каждый момент времени.

$Sp_f[n]$ – последовательность скоростей функции $f[n]$.

$Angl[n]$ – последовательность углов между векторами, соединяющими каждые три последовательные точки рукописной подписи.

Признаковая модель Ω определяется совокупностью значений $\Omega = \{\xi_x, \xi_y, \xi_p, \xi_\gamma, \xi_\eta, Angl[n]\}$.

Результатом работы модуля ввода является файл со значениями признаковой модели подписи. Далее он будет использован для обучения системы распознавания.

Модуль обучения

В этом модуле происходит формирование эталонного шаблона и вычисляется значение индивидуального порога.

На основе ранее введённых каждым пользователем подписей формируется обучающая выборка. Она будет использована для построения эталонного шаблона подписи пользователя и вычисления индивидуального порога.

Обозначим через E – эталонный шаблон пользователя, который формируется на основе признаковых моделей, принадлежащих обучающей выборке пользователя.

На основе глобальных и локальных признаков, вычисленных по каждой функции $x[n], y[n], p[n], \gamma[n], \eta[n]$ и находящихся в признаковых моделях обучающей выборки пользователя, формируется составляющая эталонного шаблона

$$F_x, F_y, F_p, F_\gamma, F_\eta, \{f_n^{Angl}\}_{n=0}^{N_E-2}.$$

То есть $F_f = \left(f^{Sqr}, f^{FCLocMax}, f^{FuzInc}, f^{FuzDec}, f^{IncLeng}, \{f_n\}_{n=0}^{N_E}, \{f_n^{AcsI}\}_{n=0}^{N_E-1} \right)$ – составляющая эталонного шаблона по функции $f[n]$, построенная на основе глобальных и локальных признаков функции $f[n]$ из обучающей выборки пользователя.

$f^{Sqr}, f^{FCLocMax}, f^{FuzInc}, f^{FuzDec}, f^{IncLeng}$ – функции, построенные на основе всех возможных значений каждого из глобальных признаков функции $f[n]$ из обучающей выборки пользователя. Они представляют глобальную компоненту составляющей эталонного шаблона по функции $f[n]$.

$\{f_n\}_{n=0}^{N_E}, \{f_n^{AcsI}\}_{n=0}^{N_E-1}$ – последовательности функций, построенные на основе всех возможных значений каждого из локальных признаков функции $f[n]$ из обучающей выборки

пользователя. Они представляют локальную компоненту составляющей эталонного шаблона по функции $f[n]$.

Признак «Последовательность углов между векторами, соединяющими каждые три последовательные точки рукописной подписи» характеризует взаимосвязь между дискретными функциями $x[n]$ и $y[n]$, поэтому $\{f_n^{Angl}\}_{n=0}^{N_E-2}$ – последовательности функций, построенные на основе всех возможных значений локального признака $Angl[n]$ из обучающей выборки пользователя. Они представляют составляющую эталонного шаблона по признаку $Angl[n]$.

$$\text{Тогда эталонный шаблон } E = \left\{ F_x, F_y, F_p, F_\gamma, F_\eta, \{f_n^{Angl}\}_{n=0}^{N_E-2} \right\}.$$

Для построения каждой функции принадлежности из эталонного шаблона используется метод потенциалов. Благодаря ему наибольшие значения функций принадлежности будут наблюдаться при наиболее часто встречающихся значениях признака.

Блок-схема алгоритма формирования эталонного шаблона пользовательской подписи представлена на рис. 5.

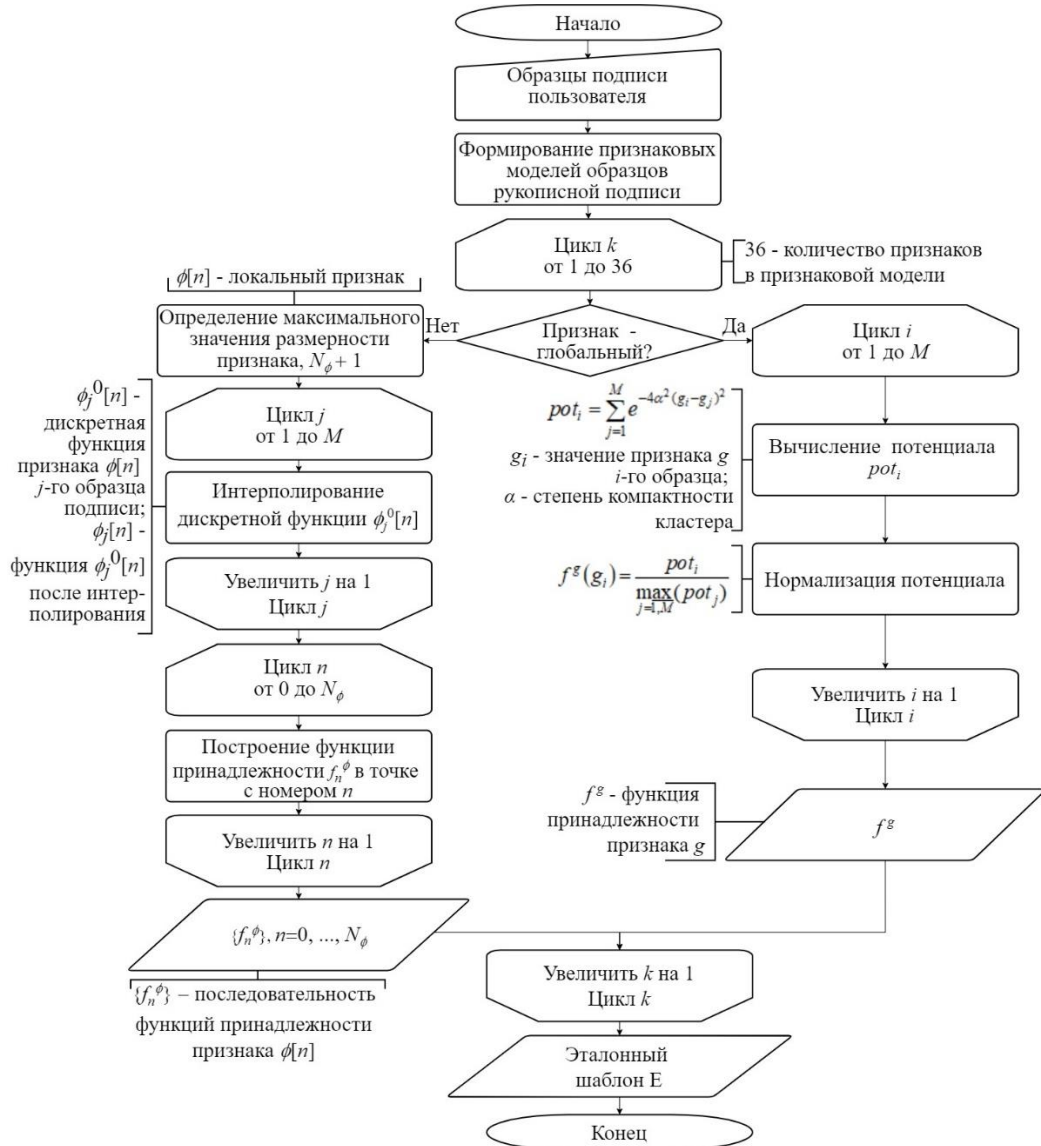


Рис. 5. Блок-схема алгоритма формирования эталонного шаблона пользовательской подписи

Эталонный шаблон подписи пользователя концентрирует в себе информацию о всех подписях из обучающей выборки. Поэтому он используется всякий раз при предъявлении очередной подписи и идентификатора для принятия решения о подлинности подписи. Однако для принятия решения о том, что подпись подлинна (или поддельна), необходимо также заранее вычислить значение индивидуального порога пользователя. Индивидуальный порог вычисляется на основе сходств и различий эталонного шаблон, подписей из обучающей выборки и поддельных подписей.

На рис. 6 представлена блок-схема алгоритма вычисления индивидуального порога σ_{ID} . Для формирования поддельных подписей пользователей на этапе разработки системы использовалась база данных MCYT_Signature_100 [12]. Для формирования поддельных подписей при эксплуатации системы их экземпляры могут формироваться легальными пользователями или автоматизированным путем с применением моделей GAN.



Рис. 6. Блок-схема алгоритма вычисления индивидуального порога

На вход алгоритма поступает идентификатор пользователя. По поступившему идентификатору идёт обращение к эталонному шаблону. Вычисляются степени схожести $\tau = (\tau_1, \dots, \tau_M, \hat{\tau}_1, \dots, \hat{\tau}_M)$ подписей из обучающей выборки и такого же (M) количества поддельных подписей. После сортировки полученных значений для каждого промежуточного значения (предполагаемого в качестве очередного значения порога) вычисляются значения ошибок. В качестве итогового значения σ_{ID} принимается значение, при котором ошибка второго рода принимает минимальное значение.

Индивидуальный порог позволяет на основе вычисленных оценок схожести принять решение о подлинности/поддельности подписи.

Модуль распознавания подписей

В данном модуле вычисляется оценка схожести подписи с эталонным шаблоном и принимается решение о легальности пользователя.

Оценка (или степень) схожести подписи с шаблоном вычисляется на основе определения соответствия значений признаковой модели подписи функциям из эталонного шаблона.

Рассмотрим алгоритм вычисления степени τ схожести подписи с эталонным шаблоном E_{ID} .

Шаг 1. Определение глобальной компоненты степени схожести P^G .

1) Вычисляется $f^g(g^{\tilde{a}})$,

где $f^g \subset E_{ID}$;

$g^{\tilde{a}}$ – конкретное значение признака g (т.е. $g \in G$, $G = \{G_x, G_y, G_p, G_\gamma, G_\eta\}$, $G_f = (Sqr_f, FCLocMax_f, FuzInc_f, FuzDec_f, IncLeng_f)$).

2) Вычисляется глобальная компонента $P^G = \prod_{g \in G} f^g(g^{\tilde{a}})$.

Шаг 2. Определение локальной компоненты степени схожести P^L .

1) Сначала выполняется интерполирование функции $\phi^{\tilde{a}}[n]$ со значениями $\phi[n] \in \Phi = \{x[n], Sp_x[n], y[n], Sp_y[n], p[n], Sp_p[n], \gamma[n], Sp_\gamma[n], \eta[n], Sp_\eta[n], Angl[n]\}$ с периодом дискретизации $T_\phi = T \cdot \frac{N^{\tilde{a}}}{N_\phi}$.

2) Для всех n вычисляется $f_n^\phi(\tilde{\phi}^{\tilde{a}}[n])$, где $\{f_n^\phi\}_{n=0}^{N_\phi} \subset E_{ID}$.

3) $\delta^\phi = \frac{\sum_{n=0}^{N_\phi} f_n^\phi(\tilde{\phi}^{\tilde{a}}[n])}{N_\phi + 1}$.

Пункты 1)-3) выполняются для всех $\phi[n] \in \Phi$.

4) $P^L = \prod_{\phi \in \Phi} \delta^\phi$.

Шаг 3. $\tau = P^G \cdot P^L$.

Степень схожести является важной оценкой, участвующей в вычислении индивидуального порога, и конечно, в принятии решения о подлинности подписи.

Блок-схема алгоритма распознавания представлена на рис. 7.



Рис.7. Блок-схема алгоритма распознавания

Таким образом, разработанное ПО имеет возможность организации записи новой подписи, построения признаковой модели, генерации эталонного шаблона, нахождения порогового значения и принятия решения о подлинности подписи.

Экспериментальные исследования модели

С использованием представленного ПО, на базе подписей [13] были проведены исследования, благодаря которым можно повысить точность распознавания.

Было установлено [14], что на точность распознавания подписей влияют:

- 1) значение степени компактности α (рис. 8);
- 2) состав признаков модели.

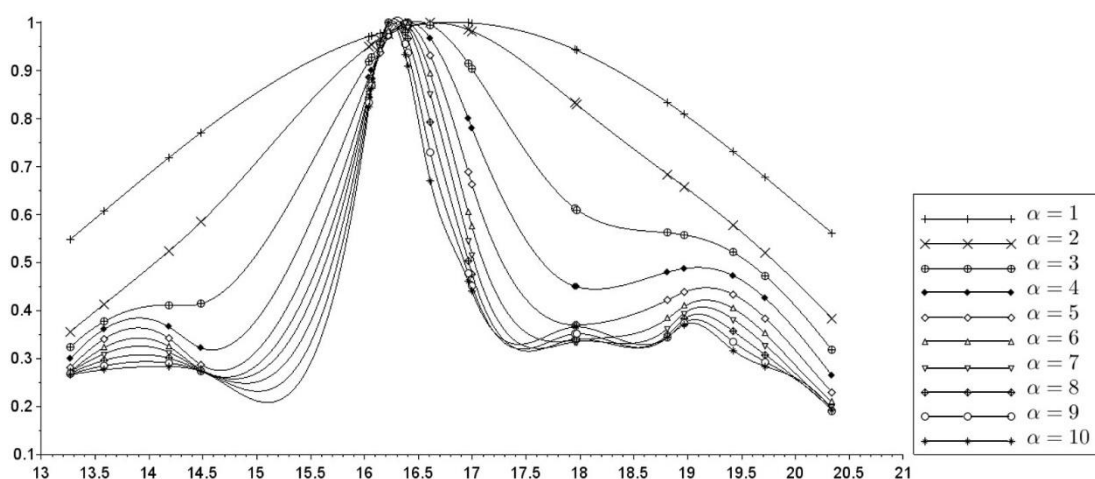


Рис. 8. Изменение функций принадлежности признака в зависимости от α

1) Было установлено, что при $\alpha=0,09$ можно достичь значения $EER=1\%$; при $\alpha=0,04$ значения $FAR=0,4\%$ (рис. 9).

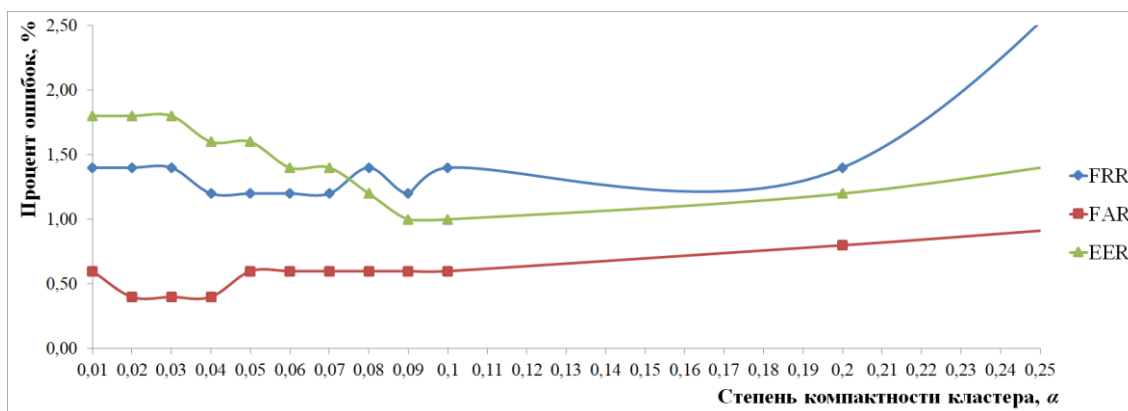


Рис. 9. Влияние степени компактности α кластера на точность распознавания

2) Получены рациональные составы признаков, при которых наблюдается низкий уровень ошибок распознавания.

Рациональный состав признаков, при котором значение ошибки второго рода $FAR=0,2\%$: $FCLocMax_x, FuzInc_x, Sp_x[n], Sqr_y, y[n], Sp_y[n], FCLocMax_p, p[n], Sp_p[n], Sqr_\gamma, FuzDec_\gamma, IncLeng_\gamma, Sp_\gamma[n], Sqr_\eta, FCLocMax_\eta, FuzDec_\eta, IncLeng_\eta, Angl[n]$.

Рациональный состав признаков, при котором значение $EER=0,36\%$: $Sqr_x, FuzDec_x, FCLocMax_x, FCLocMax_y, y[n], Sp_y[n], IncLeng_p, FCLocMax_p, Sqr_\gamma, FCLocMax_\gamma, FuzInc_\gamma, IncLeng_\gamma, \gamma[n], Sp_\gamma[n], FuzInc_\eta, Sp_\eta[n], Angl[n]$.

Экспериментальные результаты показали более высокую эффективность предложенного метода по сравнению с наиболее известными, существующими [15-17].

Обсуждение полученных результатов

Практическая ценность состоит в разработке ПО распознавания динамических рукописных подписей, основанной на предложенной признаковой модели и алгоритмах и осуществляющей распознавание подписей с точностью, превышающей многие известные методы по показателю EER.

Условия применимости предложенного метода

Предложенный алгоритм будет эффективен при распознавании динамических рукописных подписей, введенных с помощью графического планшета и представляющих собой набор динамических характеристик (положение пера по горизонтали и по вертикали, величина нажатия, азимут, угол возвышения пера).

Заключение

В данной работе предложена признаковая модель рукописной подписи. Она описывает подпись с помощью набора признаков, в том числе нечетких, позволяющих учитывать размытый характер рукописных подписей.

Предложенный эталонный шаблон подписи пользователя формируется на базе метода потенциалов, ключевой особенностью которого является возможность построения функции принадлежности признака при небольшом размере обучающих данных.

На базе разработанных алгоритмов создано ПО распознавания рукописных подписей.

Проведены исследования, позволившие определить оптимальные значения степени компактности кластера, формы функции принадлежности, рациональные наборы признаков, при которых достигаются минимальные значения ошибки распознавания (значение показателя EER=0,36%, ошибки второго рода 0,2%).

Список литературы

1. Ismail M. Development of a regional voice dataset and speaker classification based on machine learning / M. Ismail, S. Memon, L.D. Dhomeja, S.M. Shah, D. Hussain, S. Rahim, I. Ali // Big Data. – 2021. – 8.
2. Жумажанова С.С. Биометрическая аутентификация по тепловым изображениям лица на основе преобразователей "Биометрия-код" / С.С. Жумажанова, И.Е. Панфилова, А.Е. Сулавко, П.С. Ложников, А.Е. Серикова // Вопросы защиты информации. – 2023. – 1. – С.9-18.
3. Riesen K., Schmidt R. Online signature verification based on string edit distance / K. Riesen, R.Schmidt // International Journal on Document Analysis and Recognition. – 2019. – 1. – 41-54.
4. Сулавко А.Е. Биометрическая аутентификация пользователей информационных систем по клавиатурному почерку на основе иммунных сетевых алгоритмов / А.Е. Сулавко, Е.В. Шалина // Прикладная информатика. – 2019. – 3. – С. 39-54.
5. Ложников П.С. О возможности внедрения технологий распределенного реестра в системы смешанного документооборота / П.С. Ложников, А.Е. Сулавко, С.С. Жумажанова // Безопасность информационных технологий. – 2019. – 1. С. 15-24.
6. Самотуга А.Е. Распознавание субъектов и их психофизиологических состояний на основе параметров подписи для защиты документооборота. Системная инженерия и информационные технологии. – 2023. – 2. – С.56-65.
7. Mo L.-F. Off-line handwritten signature recognition based on discrete curvelet transform / L.-F. Mo, Y.-L. Zhu, H. Mamat, K. Ubul // Lecture Notes in Computer Science. – 2019. – P. 424-434.
8. Diaz M. Investigating the common authorship of signatures by off-line automatic signature verification without the use of reference signatures / M. Diaz, M.A. Ferrer, S. Ramalingam, R. Guest // IEEE Transactions on Information Forensics and Security. – 2020. – 1. – P. 487-499.
9. Tolosana R. ICDAR 2021 competition on on-line signature verification / R.Tolosana, R. Vera-Rodriguez, C. Gonzalez-Garcia // Lecture Notes in Computer Science. – 2021. – C. 723-737.
10. Anisimova E.S. Fuzzy Sets Theory Approach for Recognition Handwritten Signatures / E.S. Anisimova, I.V. Anikin // Lecture Notes in Electrical Engineering. – 2021. –P. 969-982.
11. Anisimova E.S. Finding a Rational Set of Features for Handwritten Signature Recognition / E.S. Anisimova, I.V. Anikin // 14th International IEEE Scientific and Technical Conference Dynamics of Systems, Mechanisms and Machines, Dynamics 2020 Proceedings 2020. – 9306154.
12. Ortega-Garcia J. MCYT Baseline Corpus: a Bimodal Biometric Database / J. Ortega-Garcia, J. Fierrez-Aguilar, D. Simon et al. // Vision, Image and Signal Processing, IEEE Proceedings 2003, 150 (6), 395-401.
13. Ortega-Garcia J. MCYT Baseline Corpus: a Bimodal Biometric Database / Ortega-Garcia, J. Fierrez-Aguilar, D. Simon // IEE Proceedings - Vision Image and Signal Processing 2003. – 15 0. – P.395-401.
14. Anikin I. Framework for Biometric User Authentication Based on a Dynamic Handwritten Signature / I. Anikin, E. Anisimova // Studies in Systems, Decision and Control. – 2022. – 417. – P.219-231.
15. Zalasinski M. An algorithm for the evolutionary-fuzzy generation of on-line signature hybrid descriptors / M. Zalasinski, K. Spalka, Ł. Laskowski, D.C.Wunsch, K. Przybyszewski // Journal of Artificial Intelligence and Soft Computing Research. – 2020. – 3. – P.173-187.

16. Maiorana E. Template Protection for HMM-based On-Line Signature Authentication / E. Maiorana, M. Martinez-Diaz, P. Campisi, J. Ortega-Garcia, A. Neri // CVPR Workshop. – 2008. – P.1-6.

17. Sae-Bae N. A Simple and Effective Method for Online Signature Verification / N. Sae-Bae, N. Memon Sae-Bae // BIOSIG 2013 – Proceedings of the 12th International Conference of the Biometrics Special Interest Group. – 2013. – P. 147-158.

RECOGNITION OF DYNAMIC HANDWRITTEN SIGNATURES USING METHODS OF FUZZY SET THEORY

E.S. Anisimova¹, I.V. Anikin²

¹ Elabuga Institute of Kazan Federal University
89, st. Kazanskaya, Elabuga, 423604, Russian Federation

² Kazan National Research Technical University named after A. N. Tupolev-KAI
10, st. Karl Marx, Kazan, 420111, Russian Federation

Annotation. We devoted this work to the recognition of handwritten signatures entered using a graphics tablet. We proposed a feature model of a handwritten signature that characterizes the dynamics of signature writing through various channels and uses methods of fuzzy set theory. We proposed an algorithm for creating a reference template for a handwritten signature that uses the potential method to construct feature membership functions and works even with a small training sample. We conducted studies in which we identified the optimal values of the degree of compactness used in constructing membership functions from a reference template, the form of membership functions of terms of linguistic variables used in constructing a feature model, and, in addition, obtained rational compositions of features that minimize recognition error. We proposed a modular structure of a software system for recognizing handwritten signatures entered using a graphics tablet. With the parameters found as a result of the research, we obtained an EER value of 0.36% and a type II error value of 0.2%.

Keywords: dynamic handwritten signature, dynamic characteristic, feature model, reference template.

Статья представлена в редакцию 12 декабря 2023 г.