Model of Handwritten Signature Based User Authentication

Ivan Horniichuk [1], Vitaliy Tsyganok [1,2,3], Viktor Evetskyi [1] and Artem Mykytiuk[1]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Verkhnoklyuchova str., 4, Kyiv, 03056, Ukraine*
[2] *Institute for Information Recording of National Academy of Sciences of Ukraine, Mykoly Shpaka str., 2, Kyiv, 03113, Ukraine*
[3] *Taras Shevchenko National University of Kyiv, Volodymyrs'ka str., 64/13, Kyiv, 01601, Ukraine*

Abstract

We propose and consider models and methods of user authentication based on their handwritten signature. Identification of users accessing confidential information is a critical and unresolved issue in information security. Traditional password protection methods have several drawbacks. Therefore, biometric identification of users is being considered as an alternative or addition to password systems. Biometric identifiers are closely associated with individual users, making it difficult to gain unauthorized access. The authentication decision in biometric authentication systems is determined by comparing the user's biometric etalon with the biometric data provided during the authentication attempt (login). The user's biometric etalon is created by studying specific individual characteristics of the user. These characteristics are reflecting the user's dynamic behavioral traits. A possible biometric characteristic that can be utilized for user authentication is the handwritten signature. Handwritten signatures are legally and socially recognized as a form of biometric authentication that is commonly used for human identification purposes. One major drawback of handwritten authentication systems is their high cost due to the need for specialized equipment installation. We propose a model for implementing a computer data protection system against unauthorized access based on handwritten signatures, utilizing mobile devices with the Android operating system as signature input devices. This approach aims to provide an affordable solution for biometric authentication, making it more accessible for a wider range of users. Functional structural and logic models of user authentication based on their handwritten signature are proposed. As part of the research, copyright registration certificates were obtained for the software applications that were developed to support the proposed model for user authentication based on handwritten signatures.

Keywords

Handwritten signature, signature recognition, biometric authentication system, person authentication, biometric indicator, biometric characteristics vector

1. Introduction

An important and still unsolved problem of information protection is the effective identification of the user who gets access to it. There are several drawbacks associated with relying on traditional password protection. [1, 2]. For example, in case of violation of the confidentiality of the password, which can often remain unnoticed by its owner, the protection of all information to which he has access is immediately violated. Biometric identification can be viewed as a viable replacement for or supplement to traditional password-based authentication [3, 4]. Biometric identification and

XXII International Scientific and Practical Conference "Information Technologies and Security (ITS-2022)", November 16, 2022, Kyiv, Ukraine
EMAIL: horniychuk.ivan@gmail.com (I. Horniichuk); viktorevetsky@gmail.com (V. Evetskyi); tsyganok@ipri.kiev.ua (V. Tsyganok); mukuta8888@gmail.com (A. Mykytiuk)
ORCID: 0000-0001-6754-4764 (I. Horniichuk); 0000-0002-5364-8076 (V. Evetskyi); 0000-0002-0821-4877 (V. Tsyganok); 0000-0002-8307-9978 (A. Mykytiuk)

authentication technologies have a number of advantages over traditional ones and are increasingly used in computer systems.

Biometric identification methods are broadly categorized into two groups: static methods, which rely on the physical characteristics of a person, and dynamic methods, which utilize behavioral patterns or subconscious movements during the performance of an action. Both static and dynamic biometric identification methods are complementary areas of research. However, dynamic methods, which are based on subconscious movements during action, offer stronger security than static methods. Nonetheless, these methods have certain drawbacks, including a higher likelihood of authentication errors and false positives, as well as a longer learning process compared to static methods [4]. Dynamic methods commonly involve the analysis of the user's voice or handwriting dynamics, both on paper and on a keyboard.

The handwritten signature is a biometric characteristic that is widely recognized for its legal and social significance in authenticating individuals. Therefore, it is relevant to consider its use in computer-based user authentication systems.

The complex and detailed structure of handwritten signatures poses a challenge for employing mathematical methods for authentication and identification, which often results in significant computational costs.

Handwritten signature recognition and verification systems can be classified into two types based on static and dynamic characteristics, respectively.

Static characteristics based systems analyze only a static image of a handwritten signature, without considering any additional attributes. That is, the graphic drawing obtained during the signature is evaluated. Most often, such systems are based on the use of neural networks, which are actually used as a decision-making algorithm [5]. Such recognition systems have one important advantage – they do not require access to additional input processing devices.

The main disadvantage of static signature recognition systems is the ease of compromising. For this, it is enough to have the author's signature and practice reproducing it, or simply encircle it [6, 7].

In dynamic characteristics based systems, during signing, additionally collected information about the dynamic features of the signing process. According to sources [6, 8], dynamic information can encompass the following characteristics:

- spatial coordinates of the pen tip;
- pressure exerted by the pen tip on the tablet;
- azimuthal angle of the pen;
- angle of the pen.

Dynamic features enable the creation of various biometric vectors and decision-making algorithms, such as statistical methods and neural networks, for improved user authentication based on handwritten signatures.

Dynamic signature recognition systems offer the advantage of incorporating dynamic characteristics, which renders it nearly impossible for an attacker to replicate the victim's signature [8]. However, the primary disadvantage of these systems is that they necessitate the installation of specialized equipment for signature implementation, making them a costly option for regular authentication purposes.

The presence today of mobile devices of almost all users, prompted the idea of using them in authentication systems. This may allow to replace specialized hardware by mobile devices.

A user authentication model based on handwritten signature recognition using mobile devices is proposed [12]. The peculiarity of this model is the presence in it of two components: stationary (server part) and mobile (client part).

2. Methods used across model

The proposed model involves several methods, including the method of establishing a secure connection, the method of forming the user's handwritten signature time characteristics vector, the method of forming the user's handwritten signature biometric characteristics vector, the method of forming the user's handwritten signature biometric etalon, and the user authenticity verification method based on the Hamming metric [12-14]. Let's briefly consider each of these methods.

2.1. Method of establishing a secure connection between a mobile and stationary component

Method of establishing a secure connection was considered in [12]. Its essence is the use of an SSL/TLS socket, which provides encryption of data transmitted between the client and the server [15].

To establish a secure connection, the stationary component compiles a list of necessary data, including the server's IP address, port, seed (random number), connection method label (LAN, WAN, server as access point), SSID, and wireless password (if applicable). The component then generates a QR code with the aforementioned data, which is displayed on the screen. The mobile component scans the QR code to initiate the SSL/TLS socket opening procedure (Fig. 1).

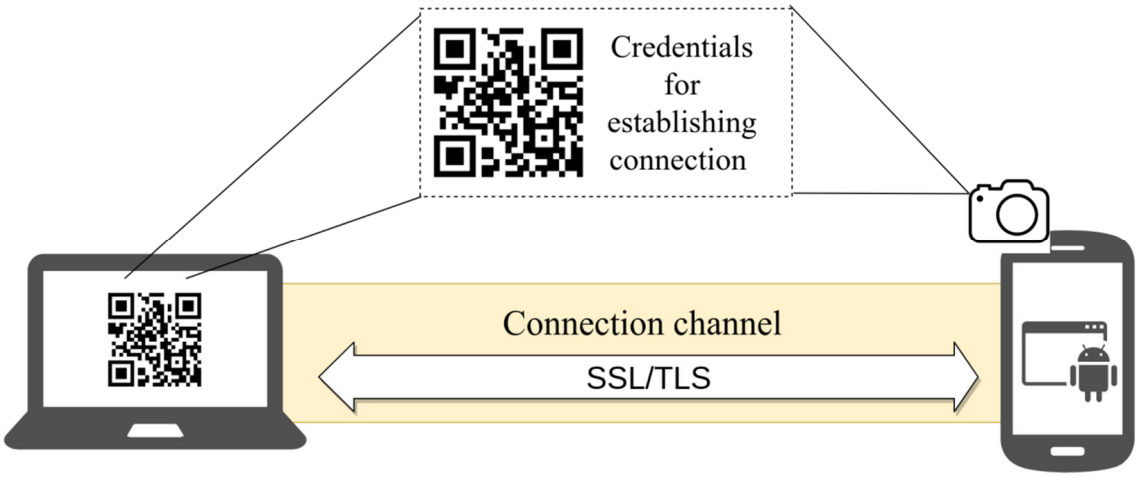

Figure 1: Secure connection establishing schema

2.2. Method of forming user's handwritten signature time characteristics vector

Method of forming user's handwritten signature time characteristics vector was considered in [12, 13]. The proposed model employs the *x* and *y* coordinates of the pen tip at a specific moment in time *t* as the parameters of the time characteristics vector. However, the period Δt after which the coordinates are collected must be both constant and sufficiently small to ensure the precision of calculations, in the system being developed $\Delta t = 17 * 10^{-3} s$. The following characteristics can be obtained through the touch screen of most all smartphone or tablet [16, 17]. Consequently, by inputting a signature, a vector of time characteristics v_τ can be obtained in the following format:

$$v_\tau = ((x_1; y_1), (x_2; y_2), ..., (x_N; y_N)), \quad N = T / \Delta t, \tag{1}$$

where *N* - the total number of points acquired during signature entry;

T - total time taken to input the signature.

2.3. Method of forming user's handwritten signature biometric characteristics vector

Method of forming user's handwritten signature biometric characteristics vector was considered in [12, 13]. When forming the biometric vector, the data of the time characteristics vector (1) are used. The entire signature is divided into a fixed number of intervals *n* of the same length $k = N / n$. For the proposed model $n = 40$ (determined experimentally [13]). It is proposed to determine the average speed of its entry s_i and the inclination angle of the vector between beginning and end of the studied interval d_i at each studied interval. It is proposed to calculate these values using the following formulas [18]:

$$s_i = \frac{\sum_{j=ik}^{(i+1)k} l_j}{k}, \quad i = \overline{0,\ n},$$

$$l_j = \sqrt{(x_{j+1} - x_j)^2 + (y_{j+1} - y_j)^2},$$

where s_i – is the average speed of entering the interval i;

l_j – Euclidean distance between adjacent points on the interval.

$$d_i = \begin{cases} \arccos(\cos\alpha_i), & \Delta y_i > 0, \\ 360^\circ - \arccos(\cos\alpha_i), & \Delta y_i < 0, \end{cases}$$

where d_i – the angle of inclination of the vector between beginning and end interval.

It is determined from the cosine of the angle obtained as the scalar product of the unit vector $\bar{e}(0;\ 1)$ and the interval vector $\overline{z_i}(x_{i+1} - x_i; y_{i+1} - y_i)$:

$$\cos\alpha_i = \frac{y_{i+1} - y_i}{\sqrt{(x_{i+1} - x_i)^2 + (y_{i+1} - y_i)^2}}$$

Thus, the biometric vector will have the following form:

$$v = (s_1, s_2, ...s_n, d_1, d_2, ...d_n) \tag{2}$$

Let's introduce the general form of the biometric vector based on (2):

$$v = (P_1, P_2, ..., P_n, P_{n+1}, P_{n+2}, ..., P_{2n}), \tag{3}$$

$$P_i = \begin{cases} s_i, & i = (\overline{1,n}) \\ d_{i/2}, & i = (\overline{n+1,2n}) \end{cases}, \tag{4}$$

where P_i – parameter of the biometric vector defined by (4).

2.4. Method of forming user's handwritten signature biometric etalon

The method of forming a user's biometric etalon is closely related to the method of making a decision on user authentication. It is proposed to use the Hamming measure as the basis of the user recognition algorithm. In general, the Hamming measure (distance) is used for row (vectors) of the same length and serves as a metric of difference (a function that allows you to determine the distance in metric space) of objects of the same size [11].

In training mode, the authorized user provides L of his signatures (enters the signature L times). This will correspond to L realizations of the biometric characteristics vectors $V = \{v_1, v_2, v_3, ..., v_L\}$. By analyzing the obtained matrix from L implementations of the user's time characteristics vector v, we can obtain the interval of change of each specific time parameter characteristic of a given user $[\min(P_i), \max(P_i)], i = \overline{1, N}$, which will later become the basis for forming user's biometric characteristics etalon.

In order to determine the Hamming distance, it is proposed to determine whether each parameter P_i of the biometric vector (3) falls within the limits of the confidence interval $[\min(P_i), \max(P_i)], i = \overline{1, N}$ for this parameter.

The confidence interval of the parameter is calculated as follows [19]:

$$\min(P_i) = m(P_i) - T[L, (1-p)] \cdot \sigma(P_i), \tag{5}$$

$$\max(P_i) = m(P_i) + T[L, (1-p)] \cdot \sigma(P_i), \tag{6}$$

where $m(P_i)$ – the mathematical expectation of the parameter P_i;

$\sigma(P_i)$ – mean square deviation of the parameter P_i;

L – the number of vectors used in training;

p – set value of errors of the first type (probability of refusing authentication to real user);

$T[L, (1-p)]$ – Student's coefficient.

The mean value and variance are calculated according to the following formulas [19]:

$$m(P_i) = \frac{1}{L}\sum_{j=1}^{L} P_{ij} ,$$

$$\sigma^2(P_i) = \frac{1}{L}\sum_{j=1}^{L}[m(P_i) - P_{ij}]^2 .$$

The threshold value E_p can be determined using the mathematical expectation and the variance of the Hamming measure values for a registered user:

$$E_p = m(E_v) + C[L,(1-p)] \cdot \sigma(E_v) ,$$

where $C[L,(1-p)]$ – Student's coefficient, given based on the number of used examples L and the values of the probability of the error of the first type p.

We form the final biometric etalon of the user. Its general form will have the following form:

$$v_e = (\min(P_1), \max(P_1), \min(P_2), \max(P_2), ..., \min(P_{2n}), \max(P_{2n}), E_p) \quad (7)$$

Having adapted (7) to the form of the biometric vector (2), we will obtain a biometric etalon of the following form:

$$\begin{aligned} v_e = (&\min(s_1), \max(s_1), ..., \min(s_n), \max(s_n), \\ &\min(d_1), \max(d_1), ..., \min(d_n), \max(d_n), E_p), \end{aligned} \quad (8)$$

where $\min(s_i), \max(s_i)$ – the minimum and maximum value of the confidence interval of the speed s_i on the interval i;

$\min(d_i), \max(d_i)$ – the minimum and maximum values of the confidence interval of the inclination angle d_i of the vector between beginning and end of the interval i;

E_p – the threshold value of the Hamming measure;

n – the number of intervals at which the signature is examined.

2.5. User authenticity verification method based on Hamming metric

During the authentication stage, the user submits their signature, which corresponds to a specific biometric characteristic vector v.

The provided biometric parameters vector is then analyzed to determine if it falls within the intervals defined by the user's biometric etalon v_e, which is used for logging into the system. During this analysis, the system generates a vector $E = (e_1, e_2, e_3, ..., e_N)$.The parameters of the vector E are formed as follows:

$$e_i = \begin{cases} 0, & P_i \in [\min(P_i), \ \max(P_i)] \\ 1, & P_i \notin [\min(P_i), \ \max(P_i)] \end{cases}$$

The resulting E represents the Hamming vector of the individual attempting to access the system. For a registered user, the E vector should contain mostly 0s, whereas an unregistered user with unreliable biometric data will have many 1s. The Hamming distance absolute value E_v from the presented biometric characteristics vector v to the biometric etalon v_e is calculated as the number of discrepancies with the biometric standard for the given parameters, which is the number of 1s in the Hamming vector. This distance E_v is always an integer and can range from *0* to N [11].

If $E_v \le E_p$, then the user is considered authenticated, and vice versa.

3. Handwritten signature user authentication model

3.1. Functional model

Since the system consists of two components, it is advisable to depict the functional model for each of the components. Thus, considering one component, the other will be an actor for it and vice versa.

The functional model of handwritten signature authentication for stationary and mobile components is shown in Fig. 2 and fig. 3 respectively.

So in Fig.2 mobile component act like an actor for stationary component, and in Fig. 3 stationary component act like actor for mobile component.

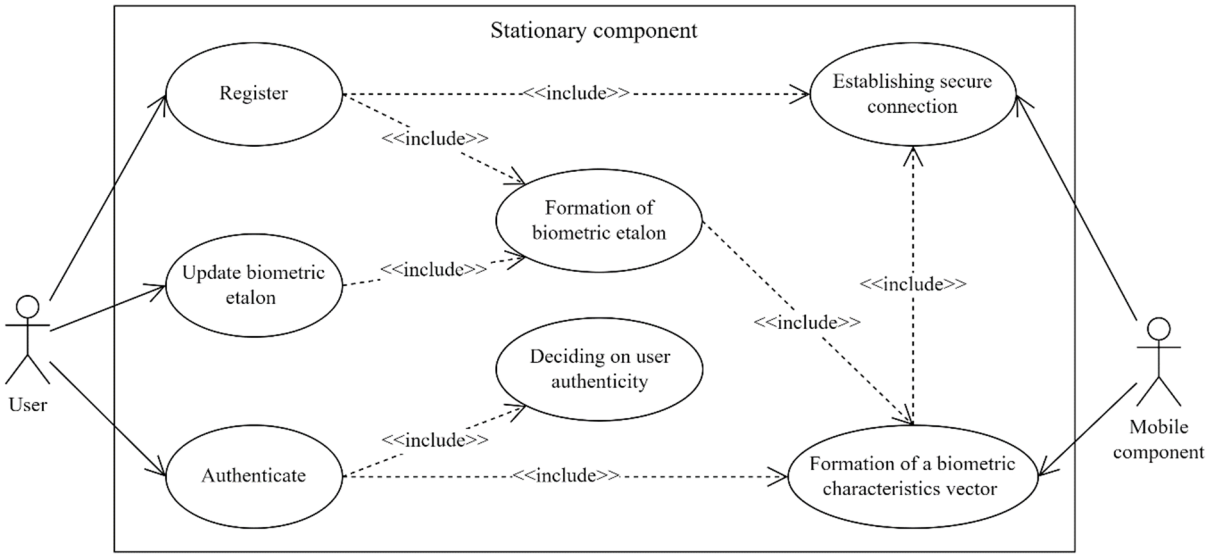

Figure 2: Functional model of authentication by handwritten signature (stationary component)

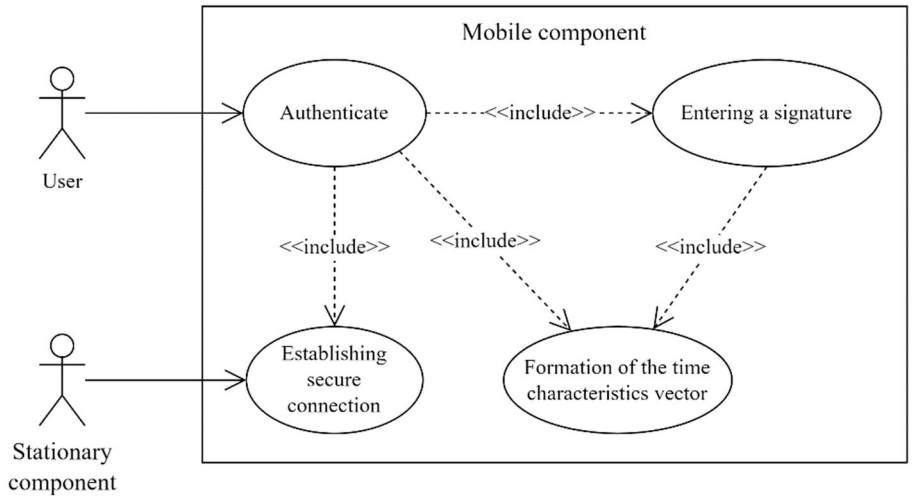

Figure 3: Functional model of authentication by handwritten signature (mobile component)

The user is given the opportunity to register, with subsequent formation of a biometric etalon, update the existing etalon, and pass authentication by entering a password. The function of establishing a secure connection appears in both components. The function of forming a time characteristics vector is performed by the mobile component, accordingly, the user performs all actions related to entering a handwritten signature with it.

3.2. Structural model

The basis of the structural model (Fig. 4) is a diagram of components showing the interaction and dependence between its modules [12-14]. Implementation of the model requires a system interface for interaction with the display in the mobile component. It, in turn, is an interface for input data. The output data is a user authentication decision used to authorize this user in the system (granting or denying access to it).

Communication between the components is carried out by the communication module, which is

present both in the stationary and in the mobile component. After that, all information exchange between components takes place via SSL/TLS socket in an encrypted form.

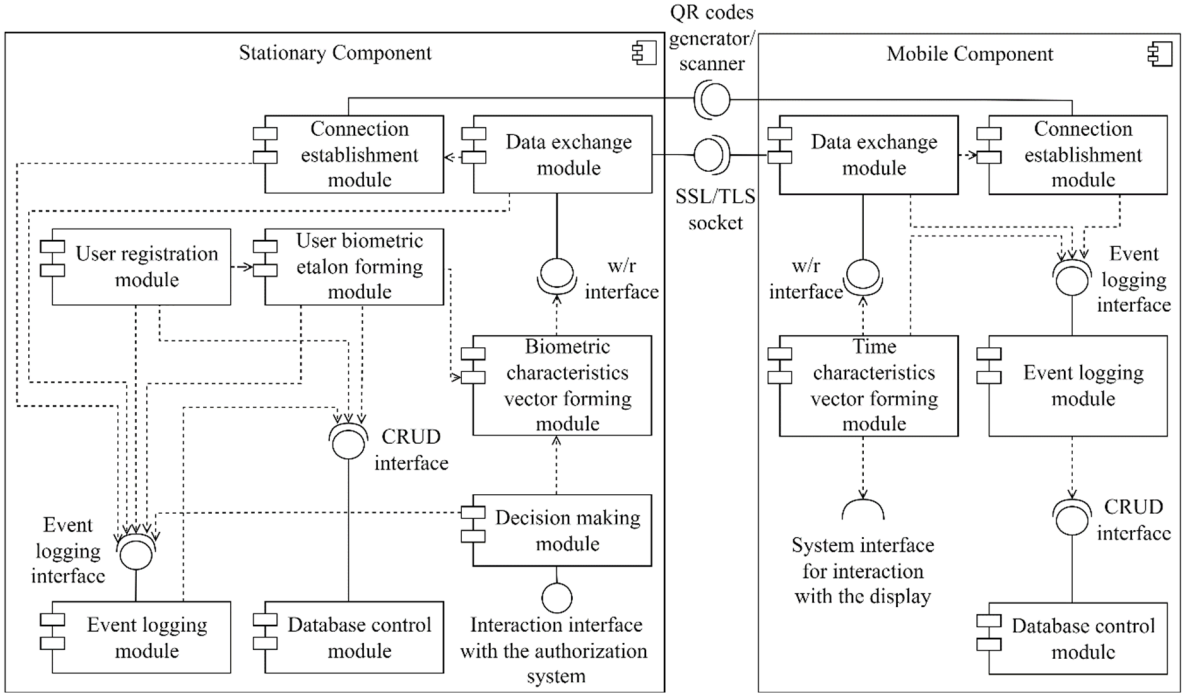

Figure 4: Structural model of user authentication by handwritten signature

3.3. Logic model

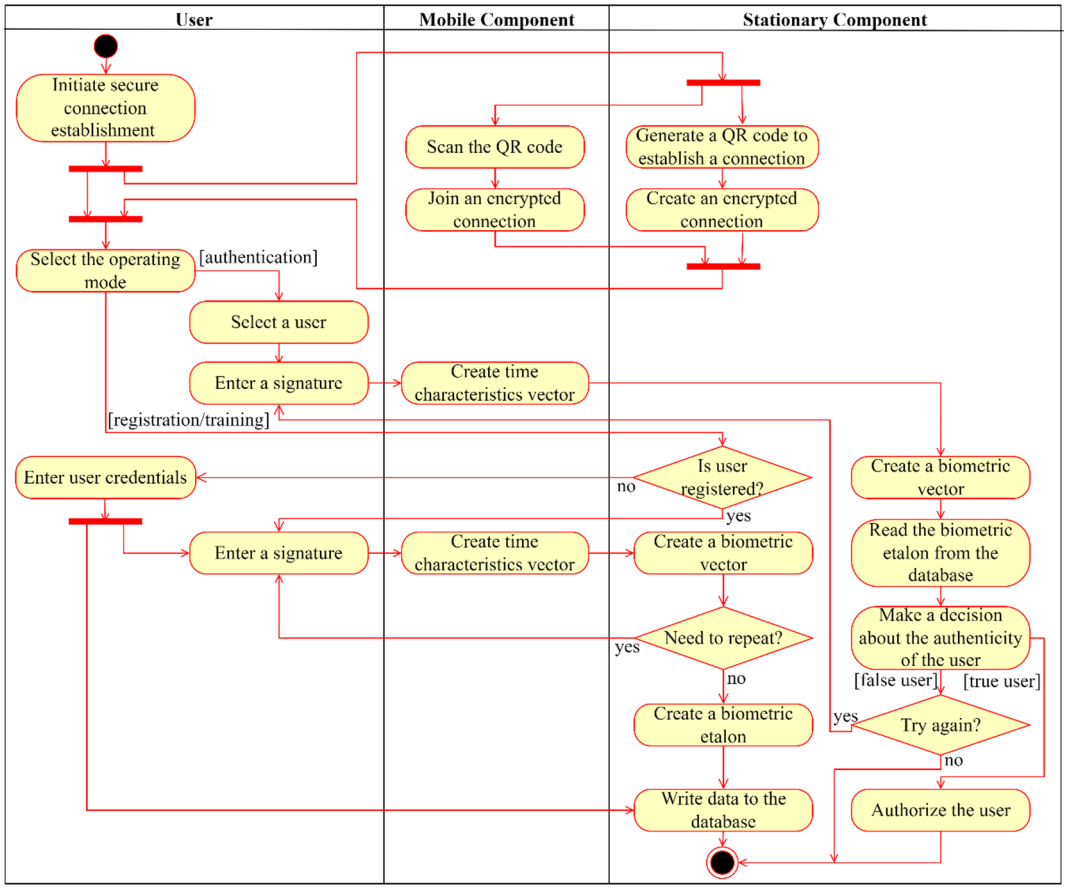

Figure 5: Logical model of user authentication by handwritten signature

In fig. 5 shows the logical model. It is nothing but a set of methods, actions and operations laid out in a logical sequence to authenticate the user by his handwritten signature. It reflects the implementation of the described system using the methods described above. Thus, it can be used as a methodology of user authentication by handwritten signature.

4. Evaluation of the proposed models' efficiency

To evaluate the efficiency of authentication systems, the concepts of errors of the first and second type are most often used. FRR (False Reject Rate) or error of the first type- the probability of false rejections to a registered user. FAR (False Accept Rate) or error of the second type - the probability of granting access to an unregistered user. They are calculated as follows [21, 22]:

$$FRR = \frac{FN}{FN + TP}, \tag{9}$$

$$FAR = \frac{FP}{FP + TN}, \tag{10}$$

where *FN (False Negative)* – the number of times a registered user has been denied access;
TP (True Positive) – the number of times a registered user has been granted access;
FP (False Positive) – the number of times an unregistered user was granted access;
TN (True Negative) – the number of times an unregistered user was denied access.

For this, a practical experiment was conducted, in which 5 users were involved. Its essence is to determine *TP, TN, FP, FN* for the proposed model. For this, a software application was created for collecting statistical material [20]. Each user tried to recreate the image of the given signature 150 times. As such image was the handwritten word "sign". In fig. 6 shows a screenshot of the application for collecting statistical material with the proposed image.

Figure 6: Screenshot of the application signature input screen for collecting statistical material

For each user, *TP* and *FN* were calculated using the biometric vector samples provided by them. To calculate *TN* and *FP* for each user, his biometric etalon was taken, and the biometric vectors of the other 4 participants of the experiment were presented for verification. Statistical data are given in Table 1.

Table 1
Results of the experiment

TP	*FN*	*FP*	*TN*
671	79	122	2878

In addition to error indicators of the first and second type, we will introduce the concepts of accuracy and balanced accuracy. *Accuracy* is the proportion of correctly determined results (granting and not granting access to registered and unregistered users, respectively) among the total number of examined cases [23]:

$$Accuracy = \frac{TP + TN}{TP + FN + TN + FP} \tag{11}$$

Balanced precision *BA* is an indicator that is calculated in case the sample is not proportional, that is, a different number of observations in the classes [23]:

$$BA = \frac{(1 - FRR) + (1 - FAR)}{2} \tag{12}$$

Using (9-12), we calculate errors of the 1st and 2nd type, as well as the accuracy of correctly determining the results. The results of the calculations are given in Table 2.

Table 2
Calculation results

FRR	*FAR*	*Accuracy*	*BA*
0,1053	0,0406	0,9464	0,9270

We should note that when users input their own signature into the system, the calculated estimates obtained are typically higher. This is justified by the fact that the user "trains" to enter his own signature during everyday use, which makes the movements more subconscious, brought to automaticity.

In addition, statistical material was accumulated with the help of the developed application. Based om it, the stability of the handwritten signature characteristics over a long period of time, in particular, about a year, was analyzed. According to this analysis, the probability of correct users' recognition at a 90% confidence interval [19] is in the range of 0.91-0.98 for a handwritten signature [13, 14].

In addition, the software applications developed during this work were granted copyright registration certificates [20].

5. Conclusions

To sum up the results obtained, it is pertinent to observe that utilizing users' dynamic biometric characteristics for authentication is an efficient method for safeguarding information. The decision to authenticate a user in such systems is based on comparing their biometric etalon with the data provided during the authentication process. The etalon is formed based on the study of its selected individual characteristics. It is appropriate to consider systems based on the handwritten signatures recognition.

We propose a model for user authentication based on dynamic biometric features extracted from handwritten signatures, along with a set of methods for its implementation. Within the framework of the proposed model, method of forming biometric characteristics vector have been developed. The speed of motion within specified intervals and the angle of inclination of the interval vector were selected as indicators for the handwritten signature. These indicators reflect the dynamic component of a handwritten signature and can be obtained without the use of specialized hardware. A method of establishing secure communication is proposed for safe interaction of devices within the model.

The user recognition algorithm based on the Hamming distance was chosen to implement the proposed model due to its speed and ease of implementation, making it a practical choice for real-world applications.

An efficiency analysis of the proposed model was conducted. Particularly, we calculated the probabilities of errors of the first and second type, along with the balanced accuracy. Balanced accuracy in this case is nothing more than the probability of making the right decision to grant or deny access to users. The values of errors of the first and second type were 0.1053 and 0.0406, respectively. Balanced accuracy for the proposed model was 0.92.

The stability of the characteristics of the handwritten signature over the year was analyzed. The range of the probability of correct user recognition values was calculated with a confidence interval of 90%, and was found to be between 0.91 and 0.98 for the proposed model.

The obtained estimates demonstrate the effectiveness of the proposed model for user authentication, and suggest that it has significant potential for improving the measures of technical information protection. The software implementation of the proposed model will enhance the provision of identification and authentication services, particularly when used in conjunction with existing authentication systems.

6. References

[1] R. Penerdji, G. Gavdan, Information security of state information systems, Bezopasnost informacionnyh tehnology Vol. 27 Iss. 3 (2020) 26–42. doi: 10.26583/bit.2020.3.03

[2] N. Sandhu, R. Kaur, Biometric Security Technique: A Review, Indian Journal of Science and Technology Vol. 9 Iss. 47 (2016). doi: 10.17485/ijst/2015/v8i1/106905
[3] V. Shvets, A. Fesenko, Basic biometric characteristics, modern systems & technologies of biometric authentication, Ukrainian Scientific Journal of Information Security Vol. 19 Iss. 2 (2013). doi: 10.18372/2225-5036.19.4882
[4] L. Irwin, GDPR: Things to consider when processing biometric data, 2017. URL: https://www.itgovernance.eu/blog/en/gdpr-things-to-consider-when-processing-biometric-data.
[5] S. Aqab, M. Tariq, Handwriting Recognition using Artificial Intelligence Neural Network and Image Processing, International Journal of Advanced Computer Science and Applications(IJACSA) Vol. 11 Iss. 7 (2020). doi:10.14569/IJACSA.2020.0110719
[6] K. Sarin, I. Hodashinsky, A. Slezkin, M. Svetlakov, E. Kostyuchenko, Identity authentication based on handwritten signature using fuzzy classifiers ensemble, International Journal of Advanced Research in Engineering and Technology (IJARET) Vol. 12 Iss. 1 (2021) 539–568. doi: 10.34218/IJARET.12.1.2021.0
[7] Panda Security, Signature recognition, a reliable replacement for passwords, 2016. URL: https://www.pandasecurity.com/mediacenter/news/signature-recognition-passwords.
[8] Y. Zhou, J. Zheng, H. Hu, Y. Wang, Handwritten Signature Verification Method Based on Improved Combined Features, Applied Sciences Vol. 11 Iss. 13 (2021). doi:10.3390/app11135867
[9] K. Kumari, S. Rana, A Robust Approach to Authentication of Handwritten Signature Using Voting classifier, Journal of Computational and Theoretical Nanoscience Vol. 17 Iss. 9 (2020) 4654–4659. doi: 10.1166/jctn.2020.9294.
[10] E. Hancer, M. Bardamova, I. Hodashinsky, K. Sarin, A. Slezkin, M. Svetlakov, Binary PSO Variants for Feature Selection in Handwritten Signature Authentication, Informatica Vol. 33 Iss. 3 (2022) 523–543. doi: 10.15388/21-infor472.
[11] D. Mackay, Information theory, inference and learning algorithms, 4th. ed., Cambridge University Press, Cambridge, 2005.
[12] I. Horniichuk, V. Yevetskyi, V. Kubrak, Applying mobile devices in biometric user authentication systems, Information Technology and Security Vol. 7 Iss. 1 (2019) 14-24. doi: 10.20535/2411-1031.2019.7.1.184213.
[13] I. Horniichuk, V. Yevetskyi, Selection of handwritten signature dynamic indicators for user authentication, Information Technology and Security Vol. 8 Iss. 1 (2020) 19-30. doi: 10.20535/2411-1031.2020.8.1.217994.
[14] I. Horniichuk, V. Yevetskyi, H. Nakonechna, Influence of destabilizing factors on the stability of user's handwritten signature indicators, Information Technology and Security Vol. 8 Iss. 2 (2020) 144-152. doi: 10.20535/2411-1031.2020.8.2.222592.
[15] Nick Naziridis, TLS 1.3 is here to stay, 2018. https://www.ssl.com/article/tls-1-3-is-here-to-stay/.
[16] S. Torres, What is the sample rate on phones and how does it affect my experience?, 2021. URL: https://impactotic.co/en/chipset-what-is-the-sample-rate-in-phones-and-how-does-it-affect-my-experience/.
[17] A. Jalan, Touch Sampling Rate vs. Refresh Rate: What's the Difference?, 2022. URL: https://www.makeuseof.com/touch-sampling-rate-vs-refresh-rate/.
[18] B. O'Neill, Elementary Differential Geometry, 2nd. ed., Elsevier Academic Press, San Diego, California, USA, 2006.
[19] E. Ventsel, Theory of probabilities, 4th. ed., Nauka, Moscow, USSR, 1969.
[20] I. Horniichuk, V. Yevetskiy, H. Nakonechna, Mobile application for the Android operating system designed to collect time characteristics of users' handwritten signature - Signature Statistic, 2021. Copyright registration certificate No. 102321, Filed Jan. 26th., 2021, Issued Feb. 4th., 2021.
[21] M. Sivaram, M. Ahamed, D. Yuvaraj, G. Megala, V. Porkodi, M. Kandasamy, Biometric Security and Performance Metrics: FAR, FER, CER, FRR, in: Proceedings of 2019 International Conference on Computational Intelligence and Knowledge Economy, ICCIKE, IEEE, Dubai, United Arab Emirates, 2019. doi: 10.1109/iccike47802.2019.9004275.
[22] D. Thakkar, False acceptance rate (FAR) and false recognition rate (FRR), 2020. URL: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/.
[23] I. Miroshnychenko, K. Ivlieva, Credit risk assessment using machine learning methods, Efficient economy, Vol. 12 (2019). doi: 10.32702/2307-2105-2019.12.87.