Stability of Users' Handwritten Signature Characteristics for Cybersecurity Purposes*

Ivan Horniichuk[1,†], Ihor Subach[1,2,*,†], Artem Mykytiuk[1,†], Vitalii Fesokha[2,†]
and Nadiia Fesokha[2,†]

[1] *National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute," 4 Verkhnoklyuchova str., 03056 Kyiv, Ukraine*

[2] *Kruty Heroes Military Institute of Telecommunications and Information Technologies, 45/1 Knyaziv Ostrozkyh str., 01011 Kyiv, Ukraine*

Abstract

The study examines the stability of handwritten signature characteristics over an extended period and their dependence on destabilizing factors. One of the key areas in ensuring cybersecurity remains protection against unauthorized access, which necessitates the implementation of effective methods for user identification and authentication in information and communication systems. The use of biometric characteristics for authentication is becoming increasingly popular, both as a primary authentication factor and as a supplementary factor in multi-factor authentication systems. From a cybersecurity standpoint, dynamic biometric characteristics are more resilient, as they reflect the inherent behavioral traits of users and are nearly impossible to forge. In this study, the handwritten signature was chosen as the dynamic biometric characteristic under investigation. The lack of research on the stability of handwritten signature characteristics and the impact of destabilizing factors prevents drawing definitive conclusions regarding their effective use in biometric authentication systems. The destabilizing factors considered in this study include the user's emotional state, physical condition, the time of day, and the passage of time in general. A specialized application was developed to collect time characteristics of handwritten signatures along with values of destabilizing factors. A substantial amount of statistical data was gathered over an extended period to facilitate further research. The stability of handwritten signature characteristics was assessed over time, along with an evaluation of the impact of destabilizing factors. Statistical variations in signature characteristics were identified. The most significant changes were observed under extreme forms of emotional and physical states, as well as depending on the time of day.

Keywords

cybersecurity, cyber defense, protection against unauthorized access, biometric authentication, handwritten signature, dynamic biometric characteristics, destabilizing factors

1. Introduction

In the modern digital era, protecting information from unauthorized access has become one of the primary measures of cyber defense. Unauthorized access to confidential data and systems poses significant risks, particularly in the context of cyber warfare. Therefore, ensuring data confidentiality is not merely a technical challenge but also a critical aspect of achieving cybersecurity for organizations, institutions, and the state as a whole [1–3].

Authentication plays a key role in protecting against unauthorized access [4]. Traditional authentication methods, such as passwords and PIN codes, have long been used to secure information and communication systems. However, these approaches are increasingly vulnerable to attacks, including phishing, brute-force password cracking, and credential theft. As cyber threats evolve, there is a pressing need to develop and implement more reliable and secure authentication mechanisms [2, 3, 5–8].

[*] CPITS 2025: Workshop on Cybersecurity Providing in Information and Telecommunication Systems, February 28, 2025, Kyiv, Ukraine

[*] Corresponding author.

[†] These authors contributed equally.

horniychuk.ivan@gmail.com (I. Horniichuk); igor_subach@ukr.net (I. Subach); mukuta8888@gmail.com (A. Mykytiuk); vitaliifesokha@gmail.com (V. Fesokha); nadya19020202@gmail.com (N. Fesokha)

0000-0001-6754-4764 (I. Horniichuk); 0000-0002-9344-713X (I. Subach); 0000-0002-8307-9978 (A. Mykytiuk); 0000-0001-6612-1970 (V. Fesokha); 0000-0002-9797-5589 (N. Fesokha)

Biometric authentication systems have emerged as a promising solution in this context. Unlike traditional methods, biometrics rely on unique physiological and behavioral characteristics—such as fingerprints, facial features, voice patterns, and handwritten signatures—to verify user identity [9]. These characteristics are difficult to replicate or steal, making biometric systems more secure and resilient against various types of cyberattacks [10–14].

There are two main types of biometric characteristics: static, which are based on the physical features of a user (e.g., fingerprints or facial structure), and dynamic, which take into account behavioral aspects such as handwriting, typing rhythm [3, 15, 16], or the dynamics of a handwritten signature [8, 17–20]. Dynamic biometric characteristics offer several advantages over static ones.

First, they incorporate not only physical attributes but also behavioral aspects, enhancing protection against forgery. Second, dynamic characteristics are more difficult to copy or reproduce, as they involve unique movement parameters, execution speed, and rhythm. These factors contribute to greater reliability in authentication systems. However, the use of dynamic biometric characteristics also has drawbacks, the most significant being the need for additional hardware and the influence of various destabilizing factors on these biometric features [8, 10–12, 21, 22].

The handwritten signature is one of the most natural and convenient methods of identity verification, as it is commonly used in everyday life. While a handwritten signature combines both static (shape, size, position) and dynamic (speed, pressure, rhythm) characteristics, the latter are particularly relevant for research and provide greater reliability in authentication. Various approaches to extracting dynamic biometric characteristics of a handwritten signature have been explored in the literature [6, 8, 23–25]. However, few studies focus on the stability of signature characteristics and the impact of destabilizing factors on them. Without such investigations, it is impossible to draw definitive conclusions regarding the applicability of these characteristics in biometric authentication systems.

This underscores the relevance of further scientific research on the stability of dynamic handwritten signature characteristics and their susceptibility to destabilizing factors.

2. Model of handwritten signature-based user authentication

A series of studies have proposed a model of handwritten signature-based user authentication [6–8]. The core idea of this approach involves utilizing mobile devices as input tools for capturing handwritten signatures. The touch-sensitive display of any modern smartphone enables the acquisition of x and y coordinate data at specific time intervals during the signing process, with an approximate sampling rate Δt of 17 ms [26]. This capability allows for the extraction of a vector of time characteristics v_τ in the following form [6, 8]:

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

where N is the total number of points recorded during the signing process; T is the total time taken to complete the signature.

As dynamic biometric features of the handwritten signature, it is proposed to use the speed of entering s_i and the inclination angle d_i of the vector connecting the start and end points of a given interval of the signature. The entire signature is divided into a predetermined number of intervals n, of equal length k, which is calculated as $k = N/n$. The optimal number of such intervals has been determined experimentally: for the most accurate signature recognition, it is 40 intervals [6–8].

The speed of entering s_i is defined as the sum of the Euclidean distances between points within a given interval, divided by the number of such points [6, 8]:

$$s_i = \frac{\sum_{j=ik}^{(i+1)k} l_j}{k}, \quad i = \overline{0,\ n}, \tag{2}$$

$$l_j = \sqrt{(x_{j+1} - x_j)^2 + (y_{j+1} - y_j)^2}, \tag{3}$$

where s_i is the average speed of entering the interval i; l_j is Euclidean distance between adjacent points on the interval.

The inclination angle d_i of the vector connecting the start and end points of the given interval is calculated as follows [6, 8]:

$$d_i = \begin{cases} \alpha_i, \text{ if } y_{i+1} - y_i \geq 0 \\ 360^\circ - \alpha_i, \text{ in other cases} \end{cases} \tag{4}$$

$$\alpha_i = \arctan\left(\frac{y_{i+1} - y_i}{x_{i+1} - x_i}\right) \tag{5}$$

Thus, using formulas (2-5) and based on the data from the time characteristics vector (1), a vector of biometric characteristics v is formed in the following form [6, 8]:

$$v = (s_1, s_2, \ldots s_n, d_1, d_2, \ldots d_n) \tag{6}$$

To determine the authenticity of the user, the Hamming distance measure [27, 28] is used, which indicates the number of biometric parameter mismatches within the confidence intervals defined by the biometric etalon. If this number is below a threshold, the user is considered authenticated; otherwise, they are not.

The biometric etalon v_e is formed during the training stage from L biometric characteristics vectors provided by the user (the required and sufficient number of such vectors is $L = 15$ [6–8]). Based on these vectors, the confidence interval [29, 30] for each biometric parameter of the specific signature is determined, along with the threshold value of the Hamming distance E_p for this user.

The final form of the biometric etalon is as follows [6, 8]:

$$\begin{gathered} v_e = (\min(s_1), \max(s_1), \ldots, \min(s_n), \max(s_n), \\ \min(d_1), \max(d_1), \ldots, \min(d_n), \max(d_n), E_p), \end{gathered} \tag{7}$$

where min() and max() are the minimum and maximum bounds of the confidence interval for the corresponding biometric parameter; E_p is the threshold value of the Hamming distance.

3. Analysis of the stability of handwritten signature characteristics

3.1. Destabilizing factors

The studies describe the dependence of dynamic biometric characteristics on the following destabilizing factors [19, 24]:

- Emotional state of the user
- Physical condition of the user
- Time of day
- The passage of time in general.

To obtain the values of the first two factors, the “Self-Assessment of Emotional States” methodology was used [7]. The basic scale dimension was simplified from 10 to 5 to avoid excessive detail and to facilitate self-assessment by users.

The emotional state of the user $EmSt = \{EmSt_1, EmSt_2, EmSt_3, EmSt_4, EmSt_5\}$ is represented by the “elation-depression” scale, where the following evaluative statements correspond to the states [7]:

- Very depressed. I feel the awful
- The mood is depressed and slightly sad
- I feel quite good, “okay”
- I feel very good. Cheerful
- Strong uplift, excitement, joy.

The physical condition of the user $PhSt = \{PhSt_1, PhSt_2, PhSt_3, PhSt_4, PhSt_5\}$ is represented by the “vitality-fatigue” scale, where the following evaluative statements correspond to the states [7]:

- Extremely tired. Nearly exhausted and practically incapable of action. There is almost no energy left.
- Quite tired. Not much energy left.
- I feel fairly refreshed and moderately energetic.
- I feel refreshed, with significant energy reserves.
- A surge of energy that knows no obstacles. Vitality is overflowing.

The time of day *ToD* is determined by the actual time *ts* of receiving the time feature vector and takes the following values:

$$ToD = \begin{cases} ToD_1, \text{ “Morning”}, \ 5^{00} \le ts \ < \ 12^{00}; \\ ToD_2, \text{ “}Day\text{”}, \ 12^{00} \le ts \ < \ 17^{00}; \\ ToD_3, \text{ “}Evening\text{”}, \ 17^{00} \le ts \ < \ 00^{00}; \\ ToD_4, \text{ “}Night\text{”}, \ 00^{00} \le ts \ < 5^{00}. \end{cases}$$

The passage of time expresses the stability of the feature of the biometric vector over a certain period.

3.2. Collection of statistical data

To assess the impact of destabilizing factors on the stability of handwritten signature features, statistical data accumulated over a long period by several users is required. To implement this, a mobile application for the Android operating system was developed [7].

The application was developed using Firebase. Firebase is a cloud platform that provides a range of services, SDKs (Software Development Kits), and APIs (Application Programming Interfaces) for developing mobile and web applications. In particular, the capabilities of Firebase Authentication and Firebase Realtime Database services were utilized (Fig. 1).

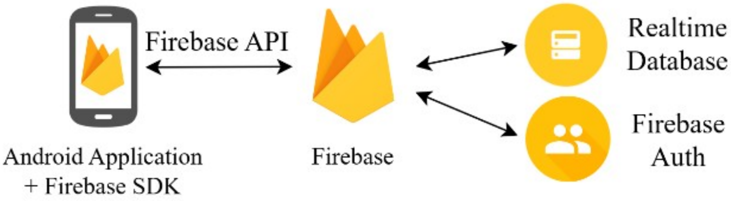

Figure 1: Scheme of the application operation for collecting time characteristics of the handwritten signature

Firebase Authentication provides server-side services, easy-to-use SDKs, and ready-made user interface libraries for authenticating users in applications. It supports authentication via passwords, phone numbers, and popular services such as Google, Facebook, and Twitter [34].

To register a user in the application, the user's authentication credentials are first obtained. These credentials include an email address and a password. After that, they are sent to the Firebase Authentication SDK.

After successful login, access to the user's profile main information is granted, and access to data stored in other Firebase products can be controlled.

Firebase Realtime Database is a NoSQL cloud-based database. The data is stored in JSON format and synchronized in real-time.

The database supports offline operation. The Realtime Database SDK keeps track of all operations and transactions locally on the disk, and once the connection is restored, it synchronizes the data with the current state of the server.

Access to the database can be made directly from the client application without the need to develop a server. At the same time, data security and validation are ensured by the security rules of the database itself. These rules allow for access control based on user identifiers provided by Firebase Authentication.

The database stores information about [7]:

- Device information is necessary for further normalization of the time feature vector (model name, screen height and width in pixels, screen density, and diagonal size in inches).
- User information (Firebase Auth identifier, first name, last name, email, date of birth, registration date, last activity date, number of days the user sent vectors, number of vectors recorded, access role).
- Time feature vectors (Firebase Auth identifier, vector creation date and time, the device from which it was sent, *EmSt*, *PhSt*, *ToD*, and the time characteristics vector in the form (1)).

The time characteristics vector (1) extended with the values of destabilizing factors will have the following form [7]:

$$\begin{aligned} V = (ts,\ EmSt,\ PhSt,\ ToD,\ (x_1;\, y_1;\, p_1), \\ (x_2;\, y_2;\, p_2),\ \ldots,\ (x_N;\, y_N;\, p_N)) \end{aligned} \tag{8}$$

The developed application allows for the accumulation of statistical data through users entering their signatures. Each time a user performs this procedure, they enter their signature three times; once they enter a template signature (the same for all users), and then they undergo self-assessment of their emotional and physical state.

A group of five individuals was selected for the study, all of whom possess smartphones at an adequate level. All participants entered their signatures an average of three times per week for about a year. As a result, time characteristics of the handwritten signature for the user group were obtained, totaling no less than 350 instances of signatures of both types for each user.

3.3. Stability of handwritten signature features over an extended period

Let's assess the stability of handwritten signature features over an extended period. Using the methodology described above, statistical data were obtained. For the users, 350 vectors of time parameters of their handwritten signatures were collected.

Based on the accumulated data, the mean values and standard deviations were calculated for the handwritten signature features—the speed of entering for the studied interval and the inclination angle between its start and end.

Fig. 2 shows the dynamics of the changes in the mean value and the standard deviation of the handwritten signature features over time [25–27].

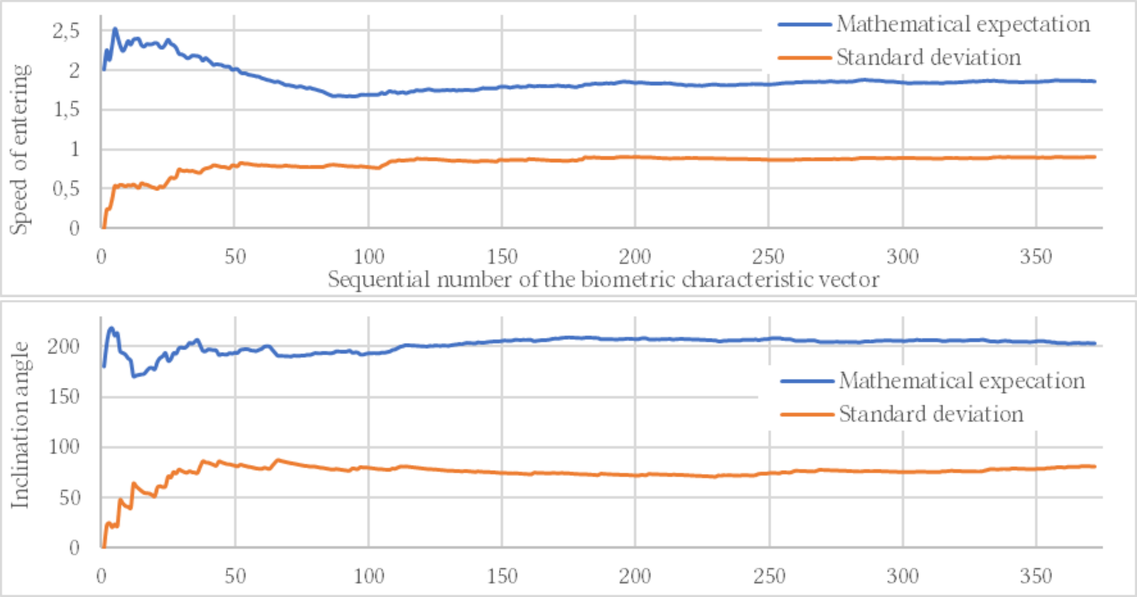

Figure 2: Dynamics of the change in the mean value and the standard deviation of the handwritten signature features

The calculated values allow us to conclude that the biometric features of the users' handwritten signatures exhibit a sufficiently high degree of stability over an extended period.

After analyzing the obtained data for each experiment participant, the number of rejections was counted, and the experimental frequency of correctly granting access to the system for the legitimate user was calculated. Typical values for the group of users are presented in Table 1.

Table 1

Data on the number of rejections in access to the legitimate user during user authentication by their handwritten signature

Parti-cipant no.	False rejection number	False rejection rate	Access granting frequency p_i^*
1	21	0.06	0.94
2	14	0.04	0.96
3	11	0.03	0.97
4	27	0.08	0.92
5	18	0.05	0.95

Let's estimate the probability of correctly recognizing the user based on their frequency in n independent trials, as described in [29]. Since the number of obtained handwriting signature samples in the experiment is 1750 units, the number of independent trials is $n = 1750$.

$$p^* = \frac{\sum_{i=1}^{n} p_i^*}{n} \tag{9}$$

According to equation (9), the frequency of the user correctly recognizing in a series of $n = 1750$ trials is $p^* \approx 0.948$.

For interval estimation of the probability of correct recognition, it is necessary to specify the confidence level β. Typically, large values are used for this, such as 0.9, 0.95, or even 0.99 [29–31].

However, there is a relationship between the confidence level β, the number of trials n, the event occurrence frequency p^*, and the estimation accuracy ε [29]:

$$\varepsilon = \frac{t_\beta \sqrt{p(1-p)}}{\sqrt{n}} \tag{10}$$

where t_β is root of the equation $2\Phi(t_\beta) = \beta$; $\Phi(t_\beta)$ is Laplace function.

As β increases, t_β increases as well. Therefore, with a constant frequency p^* and number of trials n, the value of ε will increase, which indicates a decrease in accuracy.

To determine t_β for the most typical values of reliability β and estimate accuracy ε, we will use the tables provided in [29]. The results are presented in Table 2.

Table 2

Accuracy assessment results

	$\beta = 0.90$	$\beta = 0.95$	$\beta = 0.99$
n	1750	1750	1750
p^*	0.948	0.948	0.948
t_β	1.643	1.960	2.576
ε	0.008	0.010	0.013

Under the given initial conditions for $\beta = 0.95$, the accuracy is quite high ($\varepsilon = 0.01$), which allows for an interval estimate of correct user recognition based on their handwritten signature for a year with a reliability of $\beta = 0.95$. For this, we will use the following formulas [29]:

$$p_1 = \frac{p^* + \frac{1}{2}\frac{t_\beta^2}{n} - t_\beta \sqrt{\frac{p^*(1-p^*)}{n} + \frac{1}{4}\frac{t_\beta^2}{n^2}}}{1 + \frac{t_\beta^2}{n}} \tag{11}$$

$$p_2 = \frac{p^* + \frac{1}{2}\frac{t_\beta^2}{n} + t_\beta \sqrt{\frac{p^*(1-p^*)}{n} + \frac{1}{4}\frac{t_\beta^2}{n^2}}}{1 + \frac{t_\beta^2}{n}} \tag{12}$$

where p_1 and p_2 are the lower and upper bounds of the reliable confidence interval of the probability, respectively. Using formulas (11, 12), we obtained the following results $p_1 \approx 0.92$ and $p_2 \approx 0.97$.

Thus, the reliable interval for the probability of correct user recognition based on their handwritten signature for a year is [0.92; 0.97].

3.4. The impact of destabilizing factors on correct user recognition

Let's evaluate the impact of destabilizing factors on correct user recognition. Using the previously formed biometric etalons and biometric characteristic vectors, we will assess the accuracy of user recognition by the system, taking into account the values of destabilizing factors.

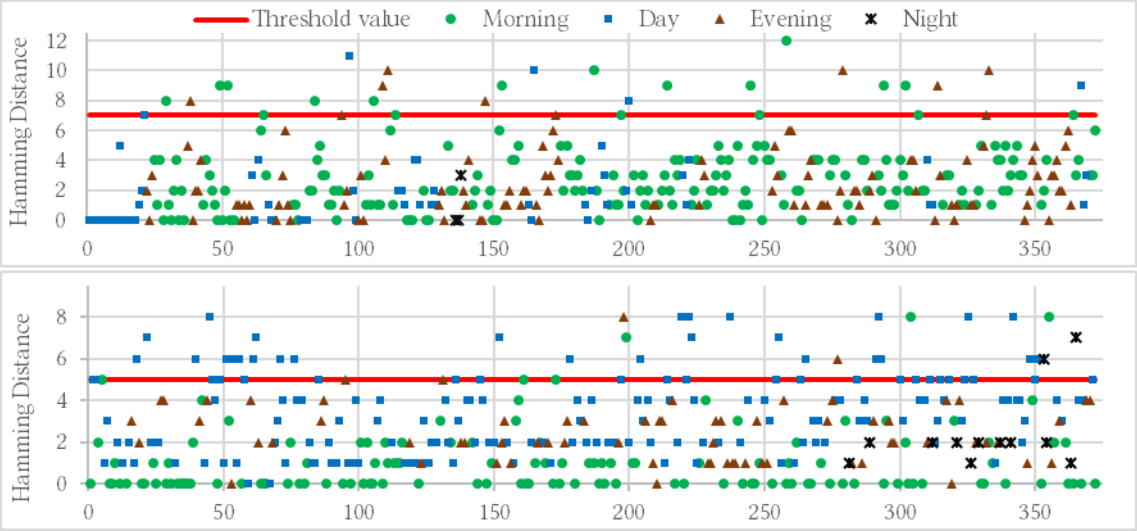

Figure 3: The dynamics of the change in Hamming distance to the biometric template for two research participants at different times of the day

To do this, each biometric characteristic vector will be analyzed to check if its parameters fall within the established biometric etalon intervals for the true user. As a result, we will note the Hamming distance from the provided vector to the biometric etalon, whether recognition occurred, and the values of the destabilizing factor parameters.

Fig. 3 illustrates the dynamics of the Hamming distance E_v to the biometric template v_e for two participants at different times of the day. The x-axis shows the sequential number of the biometric vector, and the y-axis shows the value of the Hamming measure, which represents the number of "misses" in the time parameter of the biometric vector falling outside the trusted interval of the etalon.

The threshold value of the Hamming distance E_p for the given user is marked in red. The dynamics of the Hamming distance at different times of the day are shown in different colors, as indicated in the legend.

Accordingly, all points above the threshold value can be counted as instances of denying access to the true user in the system.

More detailed data on the impact of destabilizing factors on user recognition accuracy are presented in Table 3. Analyzing the data, we can conclude that for the first participant, most of the access denials occurred in the morning, while for the second participant, they occurred throughout the day. Also, according to the data in Table 3, the emotional and physical states of the users, particularly their extreme forms, affect the probability of correct recognition. For instance, for the second participant, an extremely bad or excessively good mood leads to a decrease in correct recognition by at least 3%.

3.5. The impact of destabilizing factors on the features of handwritten signatures

Let's evaluate the impact of destabilizing factors on the features of handwritten signatures. Statistical changes in the features of handwritten signatures were detected depending on the values of destabilizing factors. For their analysis, a so-called "normal" state is introduced. This state is represented by vectors of time characteristics, excluding the influence of destabilizing factors, i.e., some average value.

Table 3
The results of evaluating the impact of destabilizing factors on the likelihood of correct user recognition

Destabilizing factor	The value of the destabilizing factor	Total		Recognized			Not recognized			
		part. 1	part. 2	part. 1		part. 2	part. 1		part. 2	
		pcs.	pcs.	pcs.	%	%	pcs.	%	pcs.	%
Time of day	Morning (05:00-12:00)	195	126	183	93.8	97.6	12	6.2	3	2.4
	Day (12:00-17:00)	63	165	59	93.7	83.6	4	6.3	27	16.4
	Evening (17:00-00:00)	111	69	104	93.7	97.1	7	6.3	2	2.9
	Night (00:00-05:00)	3	12	3	100	83.3	0	0	2	16.7
Emotional state	Very depressed	0	45	0	0	93.3	0	0	3	6.7
	A bit sad	24	94	23	95.8	88.3	1	4.2	11	11.7
	Quite good	141	84	133	94.3	91.7	8	5.7	7	8.3
	Very good	165	89	151	91.5	94.4	14	8.5	5	5.6
	Strong uplift	42	60	42	100	86.7	0	0	8	13.3
Physical condition	Extremely tired	6	57	6	100	89.5	0	0	6	10.5
	Quite tired	108	68	103	95.4	92.6	5	4.6	5	7.4
	Fairly refreshed	66	100	62	93.9	93.0	4	6.1	7	7.0
	Refreshed	135	84	123	91.1	88.1	12	8.9	10	11.9
	Surge of energy	57	63	55	96.5	90.5	2	3.5	6	9.5

Fig. 4 illustrates the statistical changes of the proposed features of handwritten signatures depending on the time of day when the biometric characteristic vector was introduced. Fig. 5 shows similar changes, but this time based on the user’s emotional state.

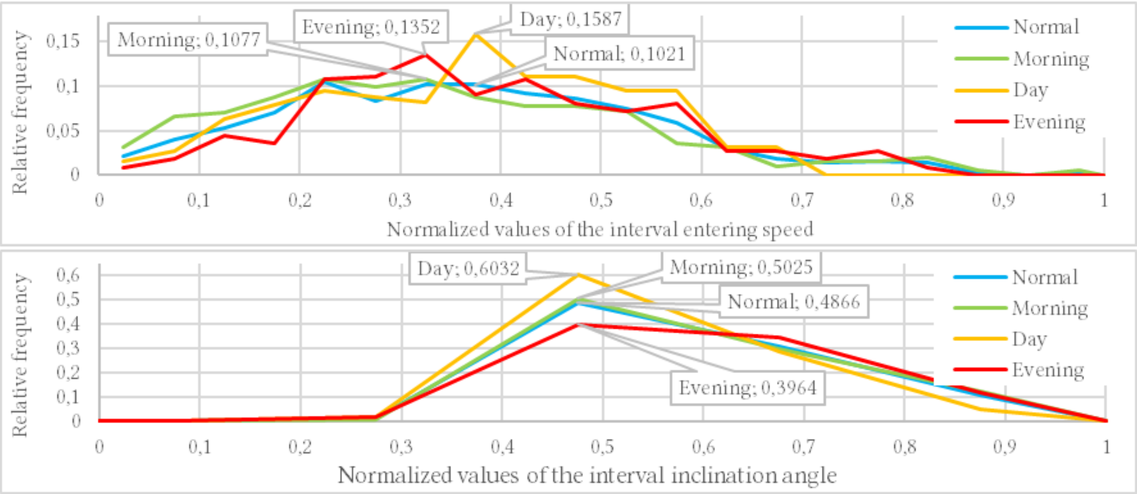

Figure 4: The relative frequency of the speed of input of the signature interval and the angle of inclination of its beginning and end during different times of the day

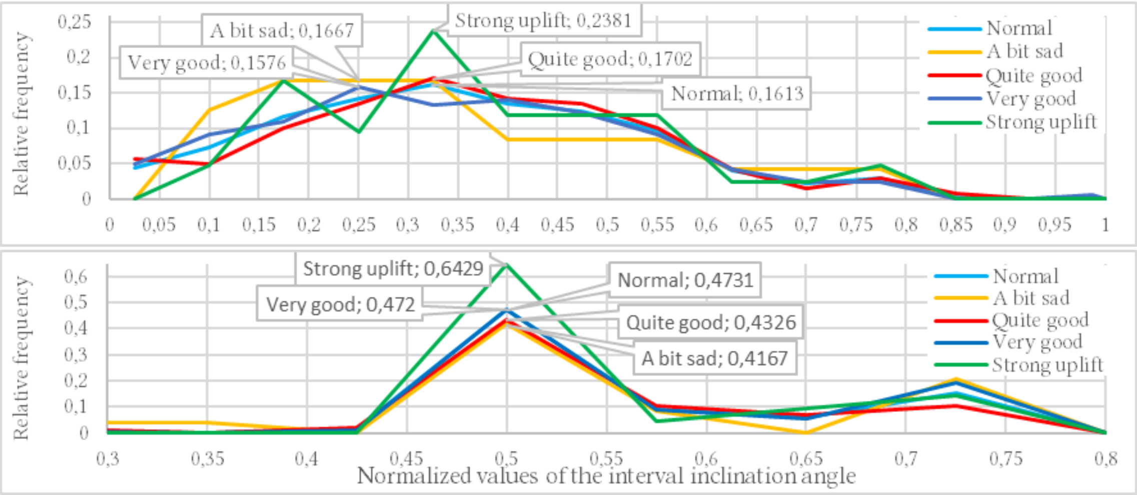

Figure 5: The relative frequency of the speed of input of the signature interval and the angle of inclination of its beginning and end at different emotional states

In these graphs, the normalized value of a particular feature of the handwritten signature is plotted on the x-axis. The y-axis represents the relative frequency with which values from the specified range appear in the matrix of the studied time characteristic vectors. On each graph, the “normal” state is marked in blue, which corresponds to the average value without considering the influence of destabilizing factors. Other colors represent the values for vectors selected based on the values of their destabilizing factors.

According to Fig. 4, it can be stated that the speed of signature input during the evening is higher than its value in the “normal” state. However, the overall duration of signature input increases during the day and night, while it decreases during the evening relative to the “normal” value.

In Fig. 5, the speed of signature entering shows minor changes depending on the user’s emotional state, with significant changes mainly occurring in the “strong uplift” state, i.e., in an overly excited condition. The tilt angle of the vector at the beginning and end of the signature interval is practically unaffected by the emotional state.

Table 4 presents detailed information regarding the change in the values of handwritten signature features under the influence of destabilizing factors. For each signature feature used, the expected value (M) and the standard deviation (σ) in the “normal” state, as well as considering destabilizing factors, have been calculated.

The increase in these parameters as percentages relative to the conditionally “normal value” (ΔM, $\Delta\sigma$) has also been calculated.

Analyzing the values from Table 4, the statistical changes under the influence of destabilizing factors become more evident. It can be observed that the greatest impact, depending on the time of day, is on the speed of signature entering.

A significant dependence of signature features on the physical condition has been detected. The most notable changes occur in a state of extreme tiredness, with slightly fewer changes in a state of surge of energy.

Conclusions

The necessity of using authentication systems based on the dynamic biometric characteristics of users has been considered. A biometric characteristic commonly found in average users—handwritten signature—has been chosen. A user authentication model based on their handwritten signature, utilizing mobile devices as input devices, has been proposed. New features of the handwritten signature have been explored—the speed of entering and the angle of inclination of the studied signature interval.

Table 4
Changes in the values of handwritten signature features under the influence of destabilizing factors

Destabilizing factor	The value of the destabilizing factor	Speed of interval entering (normalized value)				Inclination angle (normalized value)			
		M		M, %	, %	M		M, %	, %
“Normal state”		0.36	0.19	0	0	0.56	0.22	0	0
Time of day	Morning (05:00-12:00)	0.35	0.21	−4.7	12.6	0.58	0.23	2.3	1.6
	Day (12:00-17:00)	0.38	0.17	3.5	−10.4	0.54	0.17	−4.4	−22.8
	Evening (17:00-00:00)	0.39	0.18	6.2	−4.1	0.55	0.26	−2.2	15.2
	Night (00:00-05:00)	0.37	0.12	1	−36.6	0.71	0.25	25.5	11.6
Emotional state	Very depressed	0	0	0	0	0	0	0	0
	A bit sad	0.35	0.19	−3.4	−0.6	0.55	0.24	−2.0	5.9
	Quite good	0.37	0.19	1.1	0.6	0.58	0.24	2.1	8.0
	Very good	0.35	0.19	−2.3	1.9	0.55	0.22	−1.6	−0.5
	Strong uplift	0.39	0.17	7.4	−7.5	0.57	0.15	0.5	−31.8
Physical condition	Extremely tired	0.42	0.22	14.6	19.4	0.52	0.30	−8.3	34.9
	Quite tired	0.39	0.18	9.9	−4.5	0.55	0.24	−3.0	7.8
	Fairly refreshed	0.36	0.16	0.3	−13.8	0.58	0.24	3.7	8.6
	Refreshed	0.35	0.21	−4.5	10.8	0.57	0.22	1.9	−1.4
	Surge of energy	0.32	0.17	−9.9	−9.2	0.55	0.16	−2.3	−28.5

The necessity of investigating the stability of handwritten signature features for their subsequent use in biometric authentication systems has been substantiated, as well as the development of methodological recommendations for their use. Emotional state, physical condition of the user, time of day, and the passage of time, in general, have been chosen as destabilizing factors.

A software application has been developed for collecting time characteristics of the handwritten signature and values of destabilizing factors based on self-assessment of the emotional and physical state. With its use, a significant amount of statistical data has been gathered over an extended period to conduct further evaluation of the stability of biometric characteristics.

The stability of biometric features and the likelihood of correct user recognition over an extended period have been evaluated. The obtained data support the conclusion that there is no clear trend of increasing or decreasing biometric feature values. Additionally, a reliable probability interval for correct user recognition based on their handwritten signature over a year has been established, ranging from [0.92; 0.97]. This suggests that updating the biometric template, or retraining the system, can be performed only once a year.

The impact of destabilizing factors on the probability of correct user recognition and the values of the biometric features themselves has been assessed. Statistical changes in the features of handwritten signatures and, consequently, the probability of correct user recognition have been identified. It was found that the most significant impact, depending on the time of day, occurs on the speed of signature input. A significant dependence of signature features on the physical state of the user has also been revealed. The greatest changes occur in a state of extreme tiredness, with slightly fewer changes in a state of surge of energy.

Thus, it can be concluded that the use of the proposed handwritten signature features in authentication systems is only possible as an additional factor due to the influence of various destabilizing factors on them.

In future research, it is advisable to consider the possibility of developing correctional rules for forming the biometric vectors, as well as making decisions about the authenticity of a user considering the influence of destabilizing factors on the features of their handwritten signature.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] R. Penerdji, G. Gavdan, Information security of state information systems, Secur. Inf. Technol. 27(3) (2020) 26–42. doi:10.26583/bit.2020.3.03149

[2] O. M. Khrapkin, Protection of an Institution's Information and Communication Network from Unauthorized Access, Weapons Syst. Mil. Equip. 3(63) (2020) 45–53. doi:10.30748/soivt.2020.63.07

[3] V. Fesokha, et al., User authentication in critical infrastructure information systems using a keyboard handwriting biometric model, in: Information Technologies Security, vol. 3887, 2023, 73–82.

[4] D. Shevchuk, et al., Designing secured services for authentication, authorization, and accounting of users, in: Cybersecurity Providing in Information and Telecommunication Systems II Vol. 3550 (2023) 217–225.

[5] Panda Security, Signature recognition, a reliable replacement for passwords, 2016. URL: https://www.pandasecurity.com/mediacenter/news/signature-recognition-passwords

[6] I. Horniichuk, V. Yevetskyi, Selection of handwritten signature dynamic indicators for user authentication, Inf. Technol. Secur. 8(1) (2020) 19–30. doi:10.20535/2411-1031.2020.8.1.217994

[7] I. Horniichuk, V. Yevetskyi, H. Nakonechna, Influence of destabilizing factors on the stability of user's handwritten signature indicators, Inf. Technol. Secur. 8(2) (2020) 144–152. doi:10.20535/2411-1031.2020.8.2.222592

[8] I. Horniichuk, et al., Model of handwritten signature based user authentication, in: Information Technologies Security, vol. 3503, 2022, 141–150.

[9] B. Zhurakovskyi, et al., Modifications of the correlation method of face detection in biometric identification systems, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3288 (2022) 55–63.

[10] N. Sandhu, R. Kaur, Biometric security technique: A review, Indian J. Sci. Technol. 9(47) (2016). doi:10.17485/ijst/2015/v8i1/106905

[11] V. Shvets, A. Fesenko, Basic biometric characteristics, modern systems & technologies of biometric authentication, Ukrainian Sci. J. Inf. Secur. 19(2) (2013). doi:10.18372/2225-5036.19.4882

[12] 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

[13] Z. B. Hu, et al., Authentication system by human brainwaves using machine learning and artificial intelligence, in: Advances in Computer Science for Engineering and Education IV (2021) 374–388. doi:10.1007/978-3-03080472-5_31

[14] M. TajDini, et al., Brainwave-based authentication using features fusion, Comput. Secur. 129, no. 103198 (2023) 1–11. doi:10.1016/j.cose.2023.103198

[15] D. Kasiianenko, User authentication based on keystroke dynamics analysis, Sci. Notes Taurida National V. I. Vernadsky Univ. Ser. 3 (2022) 50–55. doi:10.32838/2663-5941/2022.3/08

[16] D. V. Pashchenko, E. A. Balzannikova, A method for identifying a user by keyboard handwriting using a trust model, XXI Century 10.55 (2021). doi:10.46548/21vek-2021-1055-0018

[17] Y. Zhou, et al., Handwritten signature verification method based on improved combined features, Appl. Sci. 11(13) (2021). doi:10.3390/app11135867

[18] K. Kumari, S. Rana, A Robust Approach to Authentication of Handwritten Signature Using Voting classifier, J. Comput. Theor. Nanosci. 17(9) (2020) 4654–4659. doi:10.1166/jctn.2020.9294

[19] V. V. Kutsman, O. K. Kolesnytskyj, Signature verification and recognition as a multiparametric process based on a spiking neural network, Inf. Technol. Comput. Eng. 50(1) (2021) 36–44. doi:10.31649/1999-9941-2021-50-1-36-44

[20] M. Kurowski, et al., An automated method for biometric handwritten signature authentication employing neural networks, Electronics 10(4) (2021) 456. doi:10.3390/electronics10040456

[21] Y. Skoryk, V. Bezruk, Selection of the preferred biometric authentication method, Int. Sci. J. Eng. Agric. 2(4) (2023) 28–34. doi:10.46299/j.isjea.20230204.04

[22] V. Fesyokha, N. Fesyokha, A model of fuzzy user authentication in information systems of military management bodies based on behavioral biometrics, Ukrainian Inf. Secur. Res. J. 23(2) (2021) 116–123. doi:10.18372/2410-7840.23.15728

[23] E. Hancer, et al., Binary PSO variants for feature selection in handwritten signature authentication, Inform. 33(3) (2022) 523–543. doi:10.15388/21-infor472

[24] O. Korchhenko, A. Davidenko, O. Vysotska, Authentication method of information systems users by their handwriting with multi-stage correction of primary data, Ukrainian Inf. Secur. Res. J. 21(1) (2019). doi:10.18372/2410-7840.21.13546

[25] K. Kumari, S. Rana, A robust approach to authentication of handwritten signature using voting classifier, J. Computat. Theor. Nanosci. 17(9) (2020) 4654–4659. doi:10.1166/jctn.2020.9294

[26] D. LeClair, From 60 Hz to 240 Hz: Refresh rates on phones explained, 2022. URL: https://www.pcmag.com/news/from-60hz-to-240hz-refresh-rates-on-phones-explained

[27] F. Horn, A practitioner's guide to machine learning, 2021. URL: https://franziskahorn.de/mlbook/_model_evaluation.html

[28] Performance metrics for binary classifier (in simple words), 2021. URL: https://towardsdatascience.com/performance-metrics-for-binary-classifier-in-simple-words-be958535db49

[29] V. M. Horbachuk, O. I. Kushlyk-Dyvulskaya, Theory of probabilities and mathematical statistics, Igor Sikorsky Kyiv Polytechnic Institute, Kyiv, 2023.

[30] S. R. Searle, G. Casella, C. E. McCulloch, Variance components, John Wiley & Sons, Inc., Hoboken, NJ, USA, 1992. doi:10.1002/9780470316856

[31] Y. Nakamura, Mean-variance utility, SSRN Electron. J. (2015). doi:10.2139/ssrn.2615290