## INFORMATION SECURITY

DOI 10.20535/2411-1031.2019.7.1.184213
UDC 004.056.53

IVAN HORNIICHUK,
VIKTOR YEVETSKYI,
VOLODYMYR KUBRAK

# APPLYING MOBILE DEVICES IN BIOMETRIC USER AUTHENTICATION SYSTEMS

The use of biometric characteristics to improve the efficiency of user authentication is considered. An identifier that uses biometric characteristics is inextricably linked to the user and is virtually impossible to use it unauthorized. According to this, it is proposed to use the dynamic biometric characteristics of users. Their advantage is that due to the dynamic component, the likelihood of their being forged by an attacker is very low. As a part of multifactor authentication system, biometrics can significantly reduce the chances of hacking user accounts by eliminating the disadvantages of classic password systems and card-based systems. The handwritten signature is used as the biometric characteristic of the user. The handwritten signature is a publicly and legally recognized biometric characteristic used for human authentication. It has a rather complex structure and high detail, all of which makes the solution of this problem mathematical methods rather complicated and requires a large computational cost. A major drawback is that handwritten signature authentication systems require the installation of additional specialized hardware. Therefore, using such systems as an ordinary authentication tool is very expensive. Nowadays the presence of mobile devices in almost all users has made it possible to form the idea of using them in authentication systems. Thanks to that a scheme for implementing a computer security system against unauthorized access based on handwritten signatures using Android-based mobile devices as signature input devices were proposed. In addition, a connection scheme between a computer and a mobile device was proposed. Its feature is that the connection between the mobile device and the computer is established by scanning the QR code displayed on the computer monitor by mobile device module. The practical value of the results obtained is confirmed by the copyright registration certificate of the software developed during the work.

**Keywords**: authentication; biometric user authentication; biometric characteristic; handwritten signature; biometric authentication system; mobile device.

**Problem Statement.** Traditional identification and authentication methods, which are based on the use of portable identifiers, as well as passwords and access codes, have a number of significant disadvantages due to the fact that attributive and knowledge-based characteristics are used to establish user authenticity. However, classic password systems, as well as card-based systems, have a number of vulnerabilities [1], [2]:

- access card theft;
- making a duplicate access card;
- password guessing;
- password definition by the method of “iteration” (brute force);
- password by phishing.

Thus, these vulnerabilities will compromise the system as a whole. They can be eliminated when using biometric identification methods [3], [4].

Biometric identification is a way of identifying a person by the individual biometric characteristics of a particular person. The biometric characteristics of a person are an integral part of

them – they cannot be forgotten or lost, compromised or used without a carrier. As a part of multifactor authentication system, biometrics can significantly reduce the chances of hacking user accounts [4]. There are two separate categories of information systems users authentication systems by type of human biometric characteristics [2]:

1) systems based on static features. Static, immutable characteristics of the person to which include fingerprints, face or hand shape, deoxyribonucleic acid (DNA) are used;

2) systems based on dynamic features. Dynamic, behavioral characteristics of the person which include the voice belong, the dynamics of writing text using the user's handwriting or keyboard handwriting are used.

Dynamic characteristics based authentication methods are more secure than static ones. The disadvantages of these methods are the high probability of false authentication and false security system events, as well as the need for a long learning process, compared with static methods [2].

Among the various biometric characteristics studied in the literature, the handwritten signature is one of the most attractive. It is a publicly and legally recognized biometric characteristic used for human authentication [1]. Because of this, its use in user authentication systems is relevant.

**Analysis of recent researches and publications.** Handwritten signatures have a fairly complex structure and high detail. According to this, solving user authentication problem by mathematical methods is very complex and requires a lot of computational costs [1], [4].

The following main groups of handwriting recognition methods can be identified [1], [4], [10]:

1. Methods based on local and global attributes. Global attributes are obtained from the entire signature and local attributes are from the restricted area of that signature. These methods analyze vertical and horizontal projections, along with the height and width of the signature. These approaches are also called parametric.

2. Functional methods. Dynamic signature attributes are logged as time sequences containing information about changes in signature attributes over time. This set includes dynamic features that describe the signature shape (coordinates $x$ and $y$), local pressure on the graphics tablet, speed, and acceleration. These methods are also called behavioral methods of signature analysis.

3. Methods based on area analysis. The signature is broken down into areas. A codebook is creating for each area. Signature tags along with the corresponding codebook can improve authentication results.

4. Combined (hybrid) methods. They are based on a combination of different methods from the above.

However, the pace of practical deployment of signature recognition is lower compared with other well-known technologies, such as fingerprints or iris. The low efficiency of handwriting recognition technology is explained by the following aspects characteristic of the dynamic class of biometric data [1], [5]:

– intraclass variability (difference of samples of the same user) is usually higher than in other biometric technologies;

– low degree of signature constancy over time, which reduces the accuracy of the recognition system;

– the ability to learn the signature contributes to the two different scenarios of counterfeiting:

Random forgery is a case where an attacker attempts to gain access to an authentication system using his or her own biometric characteristic while claiming the identity of another user. This is the most common case for determining system performance.

Professional fake – this is a unique case for the dynamic biometrics class. In this case, the attacker has a number of information about the signature of the author (his image, the pace of painting, the number breaks of a pen from the canvas) and tries to access the system by mimicking

the signature. Typically, such professional forgery can be explained by the intraclass variability of the author's signature, which impairs recognition efficiency.

Dynamic systems additionally collect information about the dynamic components of the signature process during the signing process (see fig. 1). Dynamic information may include the following characteristics [5], [6]:

- the spatial coordinates of the end of the pen $x(t)$ and $y(t)$;
- pen end pressure on the tablet $P(t)$;
- the azimuthal angle of the pen $A(t)$;
- the angle of the pen $I(t)$.

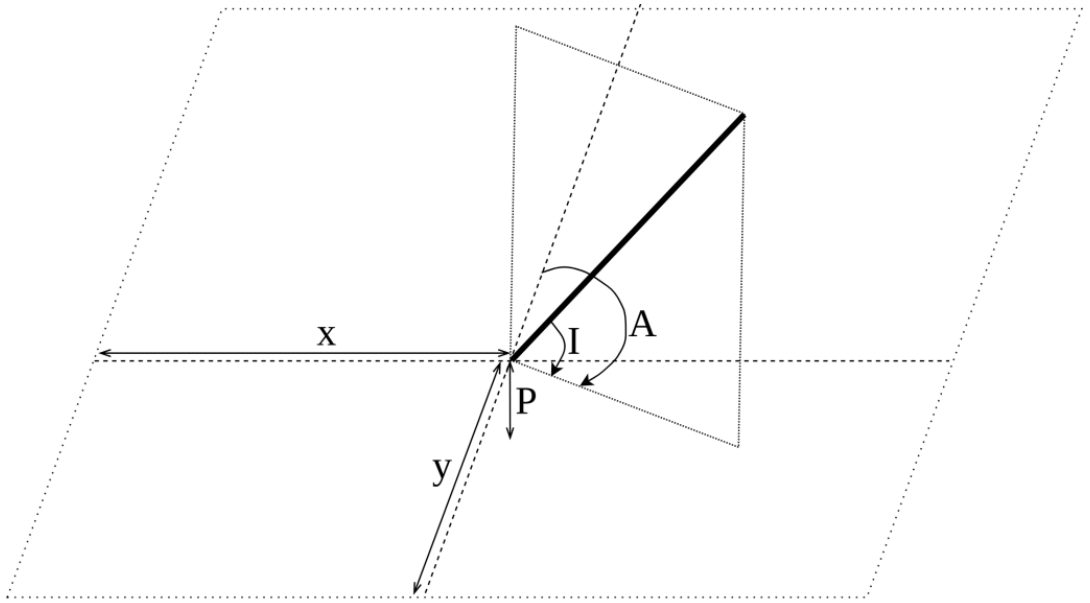


Figure 1 – Dynamic signature components

With a set of such dynamic features, it is possible to form and use various biometric vectors and algorithms for deciding of user's truth [7], [8].

The advantage of dynamic signature recognition systems is that thanks to the dynamic component of the attacker, it is virtually impossible to forge the victim's signature [6], [9], [10]. The major disadvantage of such systems is the need to install additional specialized signature-processing hardware, which makes them very expensive to use as a standard authentication tool.

Today, virtually all users of information systems own mobile devices, their use in authentication systems can allow the replacement of specialized hardware.

**The article goal is** to analyze the possibility of using mobile devices as an input device in users authentication systems by their handwritten signature. It is achieved by solving the following specific tasks:

1. Analyze existing approaches, recent research, and publications.
2. Develop a scheme for establishing a link between a mobile device and a computer.
3. Develop a scheme for implementing the system of authentication of users by their handwritten signature using mobile devices.

**The main material research.** Consider a biometric user authentication system based on handwritten signatures using mobile devices based on the Android operating system as input devices.

For the proposed system, it is decided to use only coordinate values $x$ and $y$ the end of the pen at the time $t$, because these characteristics are possible to get by the touch screen of any smartphone or tablet, without the use of specialized stylus. In this case, the length of time $\Delta t$ after

which the coordinates will be obtained must be constant and small enough, for the accuracy of the calculations, in the system being developed $\Delta t = 10^{-3} c$. Thus, after entering the signature we obtain the following temporal characteristics:

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

where $N$ – the total number of points received during the signature;

$T$ – total signature input time.

Knowledge of the coordinates of the signature at specific points in time allows calculating the various features of the signature when forming a biometric vector.

Using mobile devices as input devices in handwritten signature authentication systems allows to opt-out of specialized hardware. This greatly simplifies the use of such systems and reduces their cost. Most of the mobile devices on the market are Android operating systems (OS) devices, because of a reasonable price and convenience.

The system is implemented according to a client-server architecture. The system server is a desktop application for a personal computer. The system client is a mobile device with a touch screen running Android OS.

The feature is that the connection between the client and the server is established by scanning the QR code displayed on the server monitor by a module on the client (see fig. 2). The QR code itself contains credentials for establishing connection. Once the client and server are connected by a common communication channel, it is protected by the TLSv1.3 application layer cryptographic protocol. This protocol allows for sides authentication, channel integrity control, data encryption using asymmetric encryption, based on X.509 certificates. It has several advantages over its previous versions, in particular, it is more productive and safe [11]. This will protect the biometric vector from being intercepted by open communication channels at the time of transmission between devices.

Thus, the mobile acts as an input device. It creates a biometric vector that is sent to the server by secure connection after signing.

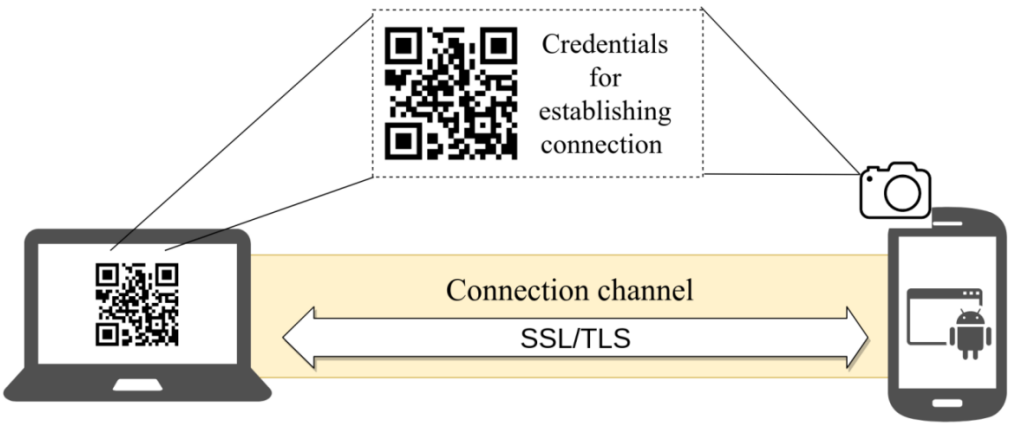


Figure 2 – Scheme for establishing a communication channel

The connection between the server and the client is realized using Wi-Fi technology, and the channel between the devices can be created in two ways (see fig. 3):

1) both devices are on the same Wi-Fi network;
2) personal computer acts as a hotspot for the mobile device.

The communication channel is implemented as a TCP socket.

The system consists of three modules:

– user registration software module;
– user authentication software module;
– user registration and authentication software module for Android devices.

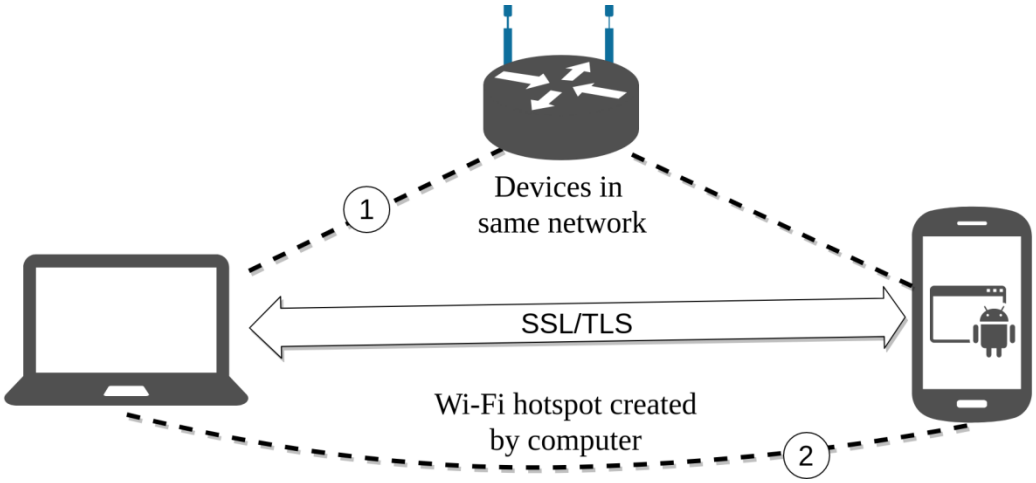


Figure 3 – Ways to implement a communication channel

Implementation system on Java language makes it versatile as this technology is actively supported by all operating systems. The developed system is easy to move to a corporate server, for implementation of a unified system of authentication. The way the channel is created can be easily modified from using Wi-Fi to access via the link, without much modification of the source code of the program, in accordance with the scheme of its operation.

A generic scheme of user registration on the system, using a mobile device as an input device (see fig. 4). At the user registration stage, two modules of the system interact: the user registration software module and the user registration and authentication software module for Android devices.

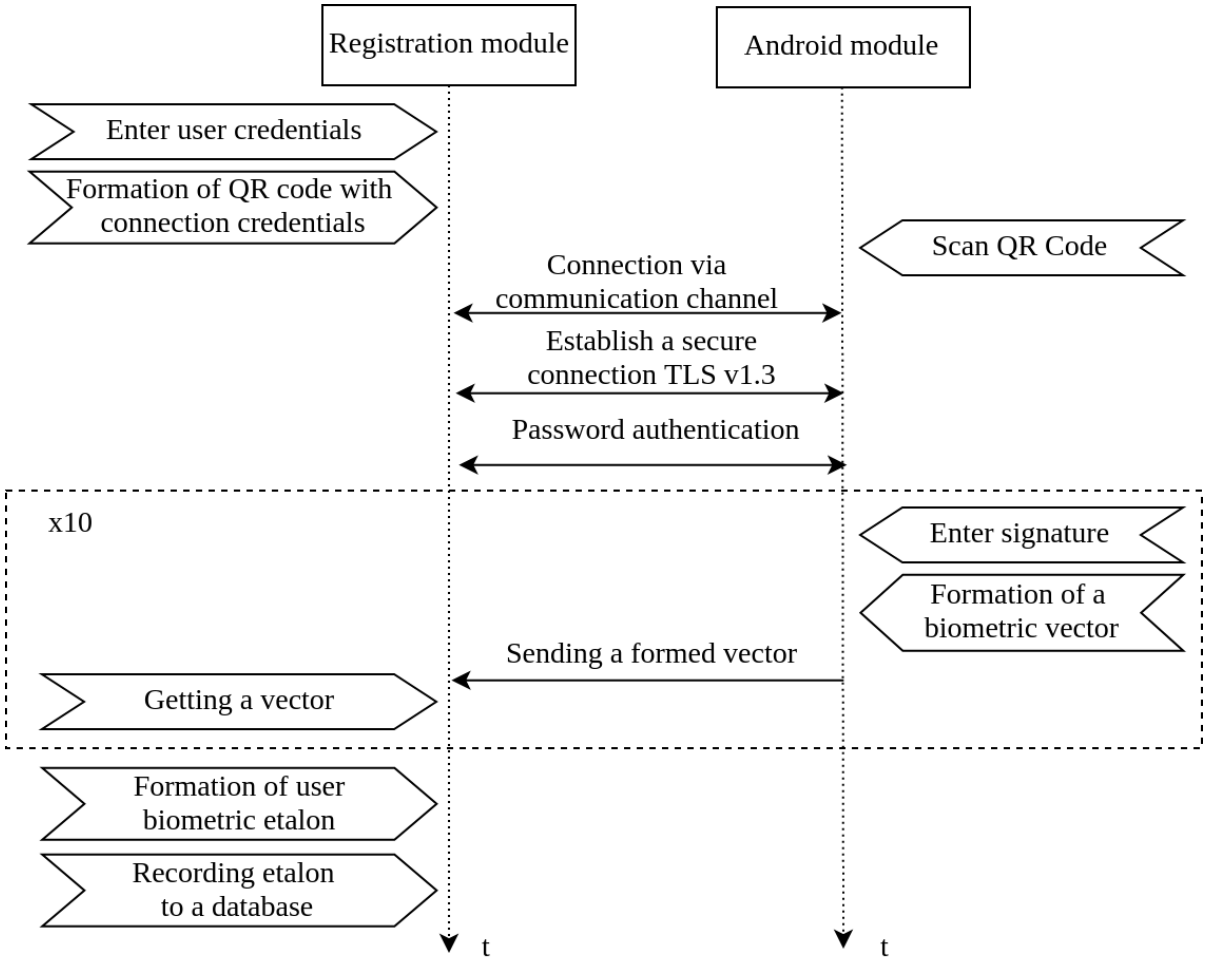


Figure 4 – Generalized scheme of user registration in the system

The proposed schemes are implemented as a series of software applications. The process of user registration is as follows.

The main window of the registration module (see fig. 5).

To register a new user, it is advisable to click “Add”, then in the registration window (see fig. 6) enter the user login in Latin letters, and a password of at least 8 characters.

After entering user data, you must select the client and server module communication scheme from the list:

– creating a Wi-Fi hotspot;
– connecting the client to the server’s Wi-Fi network.

For the second option, you must enter an administrator password to grant the permissions to share the active connection options.

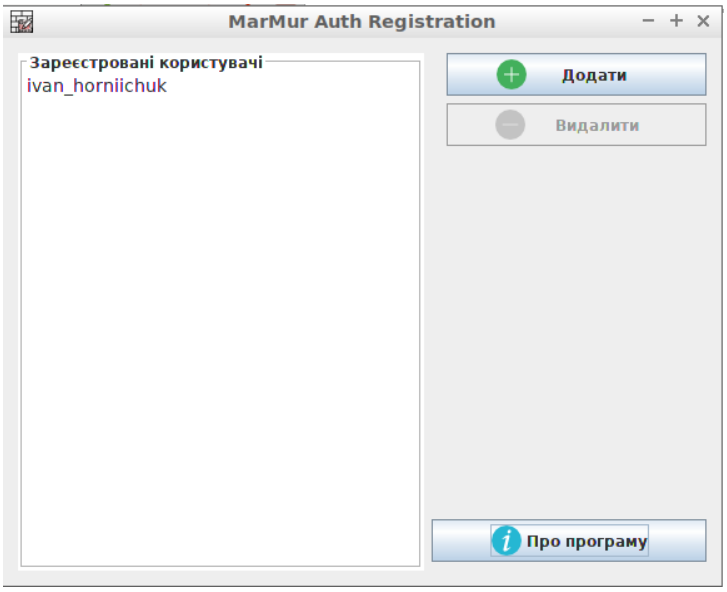


Figure 5 – Main window of the registration module

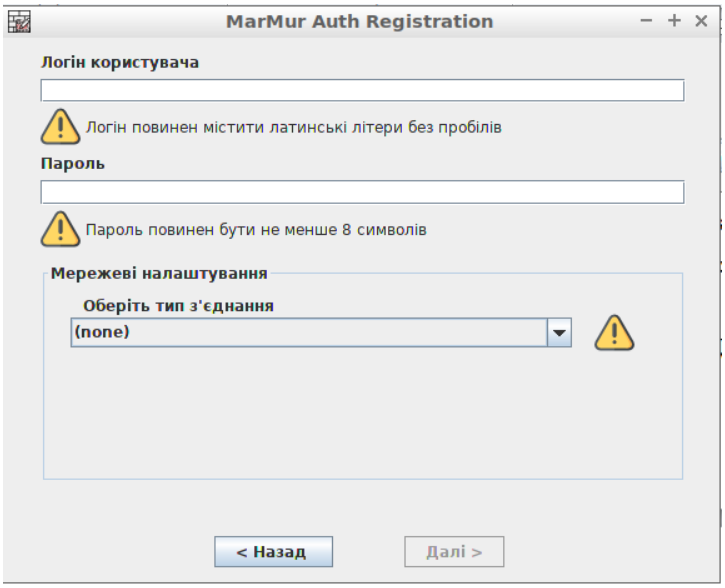


Figure 6 – User registration window

After clicking the “Next” button the user registration status window is displayed (see fig. 7).

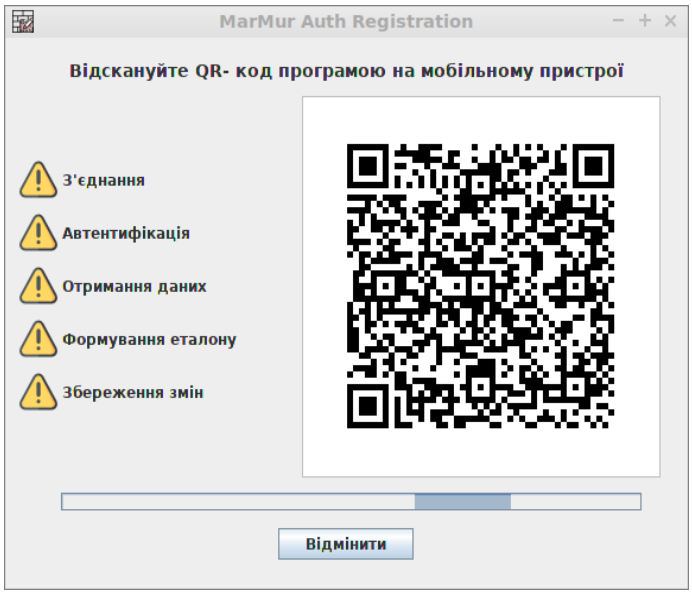


Figure 7 – User registration status window

The right side of this window displays a QR code that contains the data required by the client module to create the connection channel. It includes information on:

– network SSID;
– the password to connect to the network;
– IP address of the server;
– port to bind socket;
– client application mode.

If an access point creation option is selected, it will be given an SSID corresponding to (login) + “Reg”.

Next, you need to enable the Android OS module on your mobile device, it’s home screen (see fig. 8).

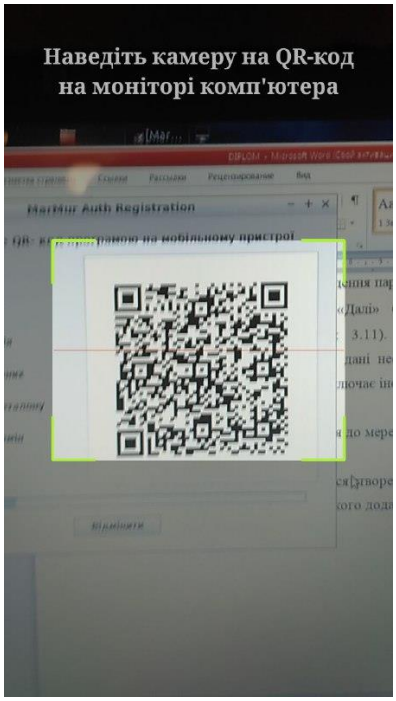


Figure 8 – Android module main screen

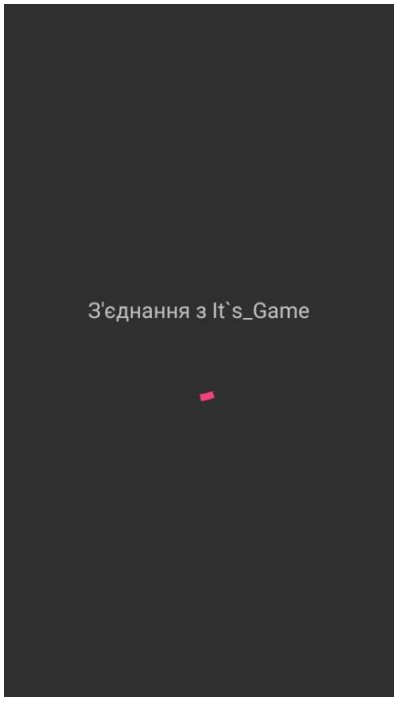


Figure 9 – Connection setup screen

The home screen has a QR code scanner. After scanning the QR code from the monitor screen, communication with the server part of the application will start automatically (see fig. 9).

Once the connection is established, the password authentication screen will appear (see fig. 10). You must enter the password you entered when registering on the server. The checkbox to the right of the password opens the entered characters (see fig. 11). If you click on the "Remember on this device" checkbox, with successful password authentication, all subsequent times it will automatically pass.

Clicking on the Next button opens the signature entry screen. On this screen, you need to sign your usual signature (see fig. 12). Clicking on the “OK” button creates a biometric vector and sends it to the registration module for processing. When you press the “Clear” button, the entered signature is deleted without saving. After entering the signature for 10 times, asuccess message will be displayed. You can then exit or continue using the application.

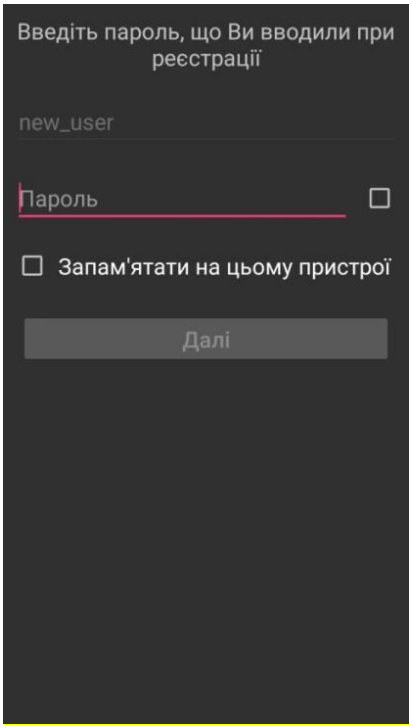


Figure 10 – Password authentication screen

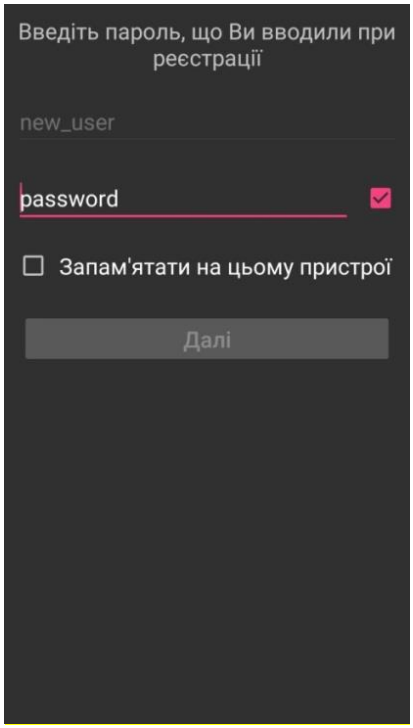


Figure 11 – Password authentication screen with open password


Figure 12 – Screen with entered signature

The registration status and every step of the mobile device interaction will be displayed in the registration status window. Upon registration, a message will also be displayed that the user has successfully registered. Thereafter, a biometric etalon is formed on the basis of several biometric vectors obtained, and it will be written to the database.

**Conclusions.** The work has analyzed the existing approaches, recent research, and publications developed a scheme for establishing a channel of communication between the mobile device and the computer, as well as a scheme for the implementation of the system of authentication of users by their handwritten signature using mobile devices.

The developed system should be used as an additional means of authentication, in systems with two-factor authentication. This allows for enhanced password authentication using biometrics.

The main advantages of the developed system are:

- cross-platforming;
- lack of additional hardware;
- ease of use;
- the same client program can be used for authentication on different systems;
- open source.

The practical value of the obtained results was confirmed by the copyright registration certificate for the software developed during the work [12].

## REFERENCE

[1] E. Anisimova, "About the verification problem using handwritten signatures", *Modern technology and technology*, no. 3, 2016. [Online]. Available: http://technology.snauka.ru/2016/03/9715. Accessed on: Sep. 24, 2018.

[2] A. Skorodumov, "Pros and cons of biometric identification", *Information Security,* no. 6, pp. 31-33, 2018. [Online]. Available: http://lib.itsec.ru/articles2. Accessed on: Jan. 20, 2019.

[3] I. Horniichuk, and V. Yevetskiy, "Use of keyboard handwriting in user authentication systems", *Information Technology and Security*, vol. 4, iss. 1, pp. 27-33, January-June 2016.

[4] L. Irwin, "GDPR: Things to consider when processing biometric data", *IT Governance European Blog,* 2017. [Online]. Available: https://www.itgovernance.eu/blog/en/gdpr-things-to-consider-when-processing-biometric-data. Accessed on: Dec. 12, 2018.

[5] Y. Zheludov, "Identification problems in handwritten recognition systems", *Scientific journal* "*Informatics*", no. 9 (32), 2018, [Online]. Available: https://cyberleninka.ru/article/n/problemy-identifikatsii-v-sistemah-raspoznavaniya-rukopisnyh-podpisey. Accessed on: Jan. 20, 2019.

[6] I. Anikin, and E. Anisimova, "Detection of dynamic handwritten signature based on fuzzy logic", *Bulletin of the Kazan State Energy University*, no. 3 (31), pp. 48-64, 2016.

[7] G. Kozlov, and S. Novikova, "Recognition of handwritten signatures using a wire-line neural network", in *Proc. XII International Scientific and Practical Conference. Scientific forum: technical and physical-mathematical sciences,* Moscow, 2018, pp. 17-20.

[8] V. Lipsky, "Identification of handwritten signatures using neural networks", in *Proc. 54-th scientific conference of post-graduate students, masters and students of BSUIR*, Minsk, 2018, pp. 84-85.

[9] Signature recognition, a reliable replacement for passwords. Panda Security., 2016. [Online]. Available: https://www.pandasecurity.com/mediacenter/news/signature-recognition-passwords. Accessed on: Aug 10, 2018.

[10] I. Smirnov, and S. Borisov, "Handwriting recognition when authenticating PC users", *Succeeding in modern natural science*, no. 6, pp. 99-100, 2012.

[11] TLS 1.3 is here to stay. 2018. [Online]. Available: https://www.ssl.com/article/tls-1-3-is-here-to-stay. Accessed on: Dec 20, 2018.

[12] I. Horniichuk, and V. Yevetskiy, "Certificate of registration of copyright for a work "Computer program for user registration for authentication by means of the system of authentication of users by their handwritten signature – MarMurAuth Registration Module", *Service of Intellectual Property of Ukraine No. 84551*, Jan. 2019.

The article was received 07.02.2019.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


[1] Э. Анисимова, "О проблеме верификации с использованием рукописных подписей", *Современная техника и технологи*, №3, 2016. [Электронний ресурс]. Доступно: http://technology.snauka.ru/2016/03/9715. Дата обращения: Сен. 24, 2018.

[2] А. Скородумов, "Плюсы и минусы биометрической идентификации", *Информационная безопасность,* № 6, с. 31-33, 2018. [Электронний ресурс]. Доступно: http://lib.itsec.ru/articles2. Дата обращения: Янв. 20, 2019.

[3] І. Горнійчук, В. Євецький, "Використання клавіатурного почерку в системах автентифікації користувача", *Information Technology and Security,* vol. 4, iss. 1 (6), pp. 27-33, January-June 2016.

[4] L. Irwin, "GDPR: Things to consider when processing biometric data", *IT Governance European Blog,* 2017. [Online]. Available: https://www.itgovernance.eu/blog/en/gdpr-things-to-consider-when-processing-biometric-data. Accessed on: Dec. 12, 2018.

[5] Ю. Желудов, "Проблемы идентификации в системах распознавания рукописных подписей", *Научный журнал* "*Информатика*", № 9 (32), 2018, [Электронный ресурс]. Доступно: https://cyberleninka.ru/article/n/problemy-identifikatsii-v-sistemah-raspoznavaniya-rukopisnyh-podpisey. Дата обращения: Янв. 20, 2019.

[6] И. Аникин, и Э. Анисимова, "Распознавание динамической рукописной подписи на основе нечёткой логики", *Вестник Казанского государственного энергетического университета,* № 3 (31), с. 48-64, 2016.

[7] Г. Козлов, и С. Новикова, "Распознавание рукописных подписей при помощи свёрточной нейронной сети", на *XII Международной научно-практической конференции. Научный форум: технические и физико-математические науки*, Москва, 2018, с. 17-20.

[8] В. Липский, "Идентификация рукописных подписей с использованием нейросетей", на *54-ой научной конференции аспирантов, магистрантов и студентов БГУИР*, Минск, 2018, с. 84-85.

[9] Signature recognition, a reliable replacement for passwords. Panda Security, 2016. [Online]. Available: https://www.pandasecurity.com/mediacenter/news/signature-recognition-passwords. Accessed on: Aug 10, 2018.

[10] И. Смирнов, и С. Борисова, "Распознавание рукописного почерка при аутентификации пользователей ПЭВМ", *Успехи современного естествознания*, № 6, с. 99-100, 2012.

[11] TLS 1.3 is here to stay. 2018. [Online]. Available: https://www.ssl.com/article/tls-1-3-is-here-to-stay. Accessed on: Dec 20, 2018.

[12] І. Горнійчук, та В. Євецький, "Свідоцтво про реєстрацію авторського права на твір "Комп'ютерна програма реєстрації користувачів для автентифікації засобами системи автентифікації користувачів за їх рукописним підписом – MarMurAuth Registration Module", *Державна служба інтелектуальної власності України №84551*, Січ. 2019.



ІВАН ГОРНІЙЧУК,
ВІКТОР ЄВЕЦЬКИЙ,
ВОЛОДИМИР КУБРАК


## ВИКОРИСТАННЯ МОБІЛЬНИХ ПРИСТРОЇВ В БІОМЕТРИЧНИХ СИСТЕМАХ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧА


Розглянуто використання біометричних характеристик для підвищення ефективності автентифікації користувача. Ідентифікатор, що використовує біометричні характеристики, нерозривно пов'язаний з користувачем, і скористатися ним несанкціоновано практично неможливо. З огляду на це запропоновано використовувати динамічні біометричні характеристики користувачів. Їх перевагою є те, що завдяки наявності динамічної складової

ймовірність їх підробки зловмисником є дуже низькою. В рамках багатофакторної системи автентифікації біометрія може значно зменшити шанси злому облікових записів користувачів, оскільки усуває недоліки класичних парольних систем і систем на основі карт доступу. Як біометрична характеристика користувача використовується рукописний підпис. Рукописний підпис є суспільно і законно визнаною біометричною характеристикою, що використовується для автентифікації людини. Він має достатньо складну структуру і високу деталізацію, все це робить вирішення даної проблеми математичними методами досить складним і потребує великих обчислювальних затрат. Також суттєвим недоліком є те, що системи автентифікації з використанням рукописного підпису вимагають встановлення додаткового спеціалізованого обладнання. Тому використання таких систем як рядового засобу автентифікації є дуже дорогим. Наявність сьогодні практично у всіх користувачів мобільних пристроїв, дозволило сформувати ідею використання їх в системах автентифікації. Завдяки цьому запропоновано схему реалізації системи захисту комп'ютерних даних від несанкціонованого доступу на основі рукописного підпису з використанням мобільних пристроїв на основі ОС Android в якості пристроїв введеня підпису. До того ж запропоновано схему встановлення з'єднання між комп'ютером та мобільним пристроєм. ЇЇ особливість в тому, що з'єднання між мобільним пристроєм і комп'ютеорм встановлюється шляхом сканування QR-коду відображеного на моніторі комп'ютера, модулем на мобільному пристрої. Практичну цінність отриманих результатів підтверджено свідоцтвом про реєстрацію авторських прав на розроблений в ході роботи програмний застосунок.

**Ключові слова**: автентифікація; біометрична автентифікація користувача; біометрирична характеристика; рукописний підпис; система біометричної автентифікації; мобільний пристрій.

**Horniichuk Ivan**, engineer at Research Center, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

ORCID: 0000-0001-6754-4764.

E-mail: horniychuk.ivan@gmail.com.

**Yevetskyi Viktor**, candidate of technical sciences, associate professor, associate professor at the cyber security and application of information systems and technology academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

ORCID: 0000-0002-5364-8076.

E-mail: viktorevetsky@gmail.com.

**Kubrak Volodymyr**, engineer at the state information resources security academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

ORCID: 0000-0001-8877-5289.

E-mail: volodymir.kubrak@ukr.net.

**Горнійчук Іван Вікторович**, інженер науково-дослідного центру, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

**Євецький Віктор Леонідович**, кандидат технічних наук, доцент, доцент кафедри кібербезпеки і застосування інформаційних систем і технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

**Кубрак Володимир Олександрович**, інженер кафедри безпеки державних інформаційних ресурсів, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.