ISSN 2181-3187

# TWO-FACTOR BIOMETRIC AUTHENTICATION SYSTEM[1]

***Zakirova Rufina Ilgizarovna***
*Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti fina82310@gmail.com*

The aim of the work is to develop a specialized service for two-factor authentication of users based on their biometric data namely unique physiological or behavioral person characteristics. This extended authentication method can be used in systems where data security is of particular importance, for example, in financial systems. Some types of biometric data used in modern security systems are discussed in the article namely voice and fingerprints, as well as methods for collecting and processing them. Biometric systems are analyzed, their advantages and disadvantages are considered. Such systems seem to be the most convenient for the user since they do not require additional memorization of any data or possession of physical objects. However, biometric systems are much more expensive for the owners of these systems. The risks of hacking biometric data assets were also noted. Considering the hardware power and avail- ability of interface software, as well as a wide audience of users of modern mobile devices, a mobile version of the two- factor biometric authentication service has been proposed. Fingerprint recognition is performed using standard Android OS tools – Biometric API. A method based on Linear Prediction Coefficients (LPC) is used for voice recognition. To apply of this service for authenticating of users by third-party applications special protocol has been developed. To prevent compromise of biometric data, an encryption method based on Diophantine equations is used.

**Keywords:** information security, authentication, biometric, speaker recognition, fingerprint recognition, two- factor authentication, Diophantine equations


[1] The work was supported by the RFBR grant No 19-01-00596 "Numeric and algorithmic aspects of the development of mathematical models of information security systems containing Diophantine difficulties".

ISSN 2181-3187

## Graphical annotation

**Introduction.** The problems of passwords typical of traditional security systems, the use of which is associated with information security risks, are effectively solved by modern technologies of biometric methods of information protection. Biometric systems are adapted for personal identification without the possibility of transferring a key and are more convenient from the user's point of view.

The introduction of biometric recognition systems into the activities of a modern person can simplify the processes of obtaining access to information, since many modern devices, for example, smartphones, can collect biometric data without additional equipment, which makes such systems more convenient for end users. In addition to traditional security methods, they help automate behavioral analysis processes and detect illegal users.

In recent years, according to Comparitech [3], biometric data collection has been very active in many countries, especially in China, Pakistan, Malaysia, the USA and India. For example, more than 80% of the country's population is registered in the biometric data system of India, biometric data is used in all areas - from finance to education and public services.

Despite these advantages, biometric systems also have drawbacks. Firstly, biometric information, like any other, is vulnerable. Information systems are constantly subjected to hacker attacks, and some of the information falls into the hands of intruders. Law enforcement agencies do not always manage to properly organize control over its safety. For example, a number of cases of biometric data leakage in China have recently been noticed [5]. And the uniqueness of biometric data turns from an advantage into a disadvantage: when it is compromised, an attacker gains access to all assets with biometric authentication. Secondly, biometric systems can also be technologically imperfect. The presence of these vulnerabilities, as well as the lack of reliable security systems, leads to the fact that the majority of potential customer companies are not yet ready for a large-scale transition to biometrics. The widespread use of such systems is currently associated with a high level of risk.

The increasing number of internal and external risks constantly puts pressure on biometric system developers to ensure an adequate level of security. The biometry market is in dire need of new solutions that increase confidence in its products.

To ensure the appropriate level of security, more and more security systems have recently switched to multi-factor authentication, where several different and complementary mechanisms for proving access are used to prove authentication. To prevent the hacking of biometric signature databases, it is necessary to use algorithms that are resistant to quantum computing to encrypt biometric data. For example, cryptoalgorithms based on the theory of Diophantine equations have high cryptographic strength [7].

ISSN 2181-3187

**Basic concepts of biometric authentication.** Authentication is a procedure for verifying that the subject of access has an identifier presented by him. The biometric method of authentication uses the user's biometric data – unique physiological or behavioral characteristics of a person. This method is the most convenient for the user, since there is no need to remember any information or own a certain object for authentication. However, this method has a significant problem: the equipment for biometric authentication must have a sufficiently high accuracy of detection to distinguish people with similar data.

All biometric data can be divided into two classes:

- static – physiological features that are not subject to change over a long period of time;
- dynamic – behavioral characteristics based on the peculiarities of human movement. The term "behaviometrics" is often used to refer to this class of biometrics.

Examples of static biometric data: fingerprints or papillary line drawings; iris; retina of the eye; vein pattern; face; hand geometry; DNA.

Dynamic data, for example, include the following data: handwriting and signature dynamics; voice and rhythm of speech; Gesture recognition dynamics of keystrokes; gait.

Biometric systems can operate in two modes [13]:

- Verification based on a biometric parameter and on a unique identifier that identifies a specific person (one-to-one comparison).
- Identification based on biometric measurements. In this case, the measured parameters are compared with all records from the database of registered users, and not with one of them selected on the basis of an identifier (one-to-many comparison).

**Multi-factor authentication.** Multi-factor authentication is advanced authentication, an access control method in which a user is required to present more than one authentication factor in order to access information. Each authentication factor encompasses a number of elements used to authenticate or verify a person's identity before access is granted.

Authentication methods can be grouped into three main categories [1]:

1. Knowledge factors are what the user knows, for example, a password, a PIN code, the answer to a secret question, etc.
2. Property factors are things that are part of us, such as a fingerprint, a handwriting, a voice, etc.
3. Ownership factors are what the user has, for example, a contactless identity card, a cell phone, a physical key, etc.

The combination of several types of authentication mechanisms can improve both

ISSN 2181-3187

the security and efficiency of security systems, as the number of possible errors inherent in biometric systems in general is reduced.

Multi-factor authentication is not standardized. There are various forms of its implementation. Two-factor authentication is the most common. Two-factor authentication is a method of identifying a user in a service by requesting two different types of authentication data, which provides two-layered, and therefore more effective, protection of the account from unauthorized entry.

To increase reliability and efficiency, access control systems are increasingly using biometric identification. In this paper, a variant of the two-factor authentication system with two biometric factors is presented, and an authentication mechanism in the form of a property is used. To obtain biometric signatures of the user, fingerprint and voice recognition technologies are used [6], the main provisions of which are presented below.

**Fingerprint recognition.** In 1788 [2], the German anatomist J. C. Mayer discovered the uniqueness of fingerprints. For a long time, fingerprints have been a universal source of biometric characteristics.

The compactness of modern fingerprint scanners allows them to be implemented in various input devices. Thanks to the scanners built into smartphones, you can unlock your mobile device and pay for purchases on the Internet. In the near future, it is planned to introduce similar technologies into other public devices, such as ATMs and even ticket replacement facilities. Fingerprints are widely used in forensics to search for and identify criminals. A number of countries require fingerprints when applying for a visa, such as Schengen countries. In Russia, biometric foreign passports contain fingerprints recorded on a chip. Recently, a method of using fingerprints for dermatoglyphic studies (a method of testing the human body, based on the study of signs of patterns on the skin of the palm side of the hands and feet) has been developed.

**Voice recognition.** The use of biometrics based on a person's voice is more complex and interesting than the use of most biometric features. Voice recognition technology falls into the realms of both physiological and behavioral biometric data. From a physiological point of view, such systems recognize the shape of the human vocal tract, including the nose, mouth and larynx, and determine the sound produced. From a behavioral point of view, they record the way a person says something – variations in movements, tone, tempo, accent, etc., which is also unique to each person. Combining physical and behavioral biometrics data creates an accurate voice signature.

However, since a person's voice can change depending on age, emotional state, health, hormonal background and a number of other factors, the method is not completely accurate.

Voice identification is one of the most attractive for identification, but the problems that exist at the moment must be taken into account when implementing in

ISSN 2181-3187

working businesses. Voice recognition is effectively used as a complementary method in multifactorial systems.

**Practical implementation.** The rapid spread of mobile technologies has significantly expanded the audience of mobile device users, which stimulates the development of the market for mobile applications for various purposes. In the development of mobile applications, the power of modern mobile platforms and APIs allows you to use all the capabilities of hardware human characteristics (voice and fingerprint recognition). The developed biometric system is a client-server mobile application for two-factor user authentication through a special protocol (Fig. 1).

Biometric identification is the process of comparing and determining the similarity between the biometric data submitted by a user and the corresponding digital standard reflecting the unique biometric characteristics of this user [4]. A reference model of human biometric characteristics is preliminarily formed on the basis of one or more biometric samples and stored in the database. To work with the biometric database, the proposed authentication service uses the PostgreSQL DBMS. User information and their biometric digital signatures are stored in the database in encrypted form. To encrypt data, the SOLDEEA algorithm is used, based on linear Diophantine equations [12]. According to the works of K. Shannon [11], cryptographic schemes containing Diophantine difficulties are the most resistant to hacking, which will have a positive effect on the security of biometric data and increase the level of user confidence in biometric authentication systems.

The server application of the service, written in the Java language, provides access to user biometric data, user authorization in the service, as well as fingerprint and voice recognition. The service provides the ability to integrate two-factor authentication in third-party applications.


Figure 1 – System structure

ISSN 2181-3187

The server application is divided into 2 main parts:

- the interface for third-party applications allows third-party applications to interact with the service and authenticate;
- The user interface allows users to interact with the service: add a biometric signature of a certain type, confirm authentication.

To set up authentication, the administrator of a third-party application needs to register his application (the so-called project) with the service. To do this, the administrator must specify the name, description of his application, and the domain that the user will see in the future when authenticating using the mobile service. This is necessary so that the user can identify the application in which he wants to authenticate. After creating a project, the administrator receives the project's secret key from the service server, which is then used to create authentication requests.

The client application is written in Java for the Android operating system. It provides basic functionality for users of the service:

- authorization/registration;
- adding/removing biometric data;
- authentication in third-party applications.

The protocol for user authentication in a third-party application is as follows (Figure 2):

- A third-party application sends an authorization request to the service in which it passes a secret key unique to each application and a user ID in the service.
- the service returns an authorization code to the third-party application;
- A third-party app shows the authorization code to the user.
- the user enters this code in the authenticator mobile application;
- the user chooses a method and performs authentication;
- if authentication is successful, the service sends the user an authentication code;
- The user enters an authentication code in a third-party app.
- The third-party app verifies the authentication code.

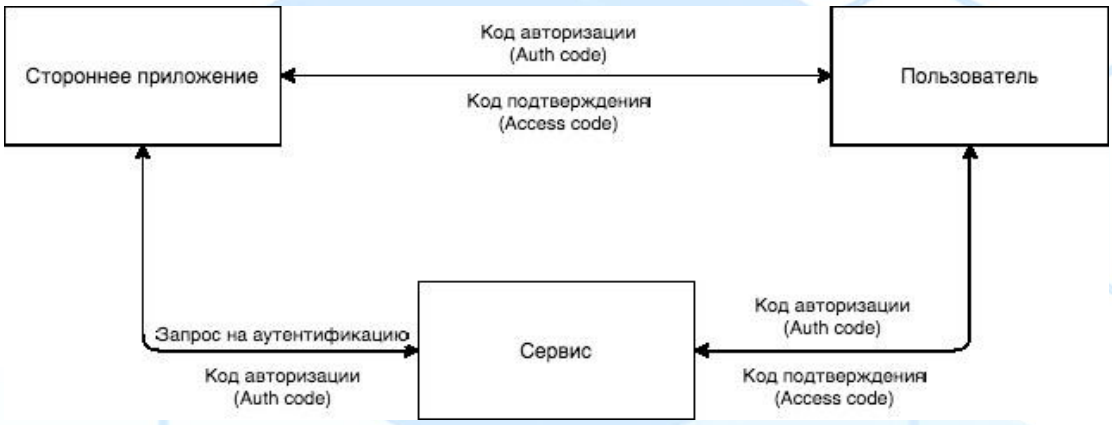


Figure 2 – Authentication protocol

ISSN 2181-3187

After sending a request for user authentication, the third-party application receives an authorization code, which is generated using the Time-based One-Time Password Algorithm (TOTP) to generate one-time passwords for secure one-way authentication.

$AuthCode = TOTP(ProjectSecret + UserID, AuthTime)$,

ProjectSecret is the secret key of the project,

AuthTime is the validity time of the code,

UserID is the user's identifier in the system

This code allows you to simultaneously identify the authorization request and set a time limit for the request.

After that, the third-party application must accept a confirmation code from the user, which is generated by the service upon successful authentication:

$AccessCode = TOTP(ProjectSecret + UserToken, AuthTime)$,

ProjectSecret is the secret key of the project,

AuthTime is the validity time of the code,

UserToken is a special user token in the service.

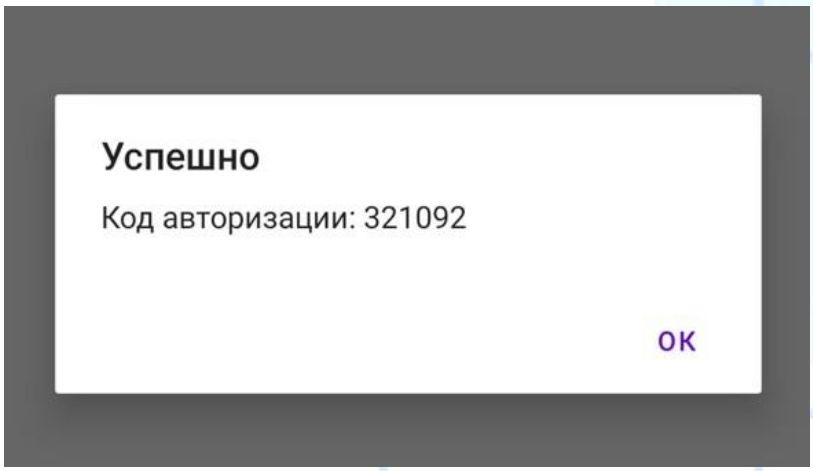


Figure 3 – Successful authentication screen

The confirmation code received from the user can be verified by sending a request to the service by a third-party application.

The voice recognition method implemented in the system allows you to connect the unique characteristics of a person's voice to identify his or her identity. To record audio from microphones to devices, the standard Android OS interface - AudioRecord is used. During the recording process, the voice is saved as an audio file in WAV format (Fig. 4).

ISSN 2181-3187


Figure 4 – Start window for voice authentication

Speaker recognition is performed using the Recognito library [9] on the server. To convert an audio file into a digital code, the Linear Prediction Coefficients (LPC) algorithm is used. Linear prediction coefficients reflect the main vocal characteristics of a person necessary for making a decision about the personality of the announcer: the voice source, the resonant frequencies of the vocal tract and their attenuations, as well as the dynamics of articulation control [10]. Figure 5 shows the steps involved in obtaining a digital voice signature:

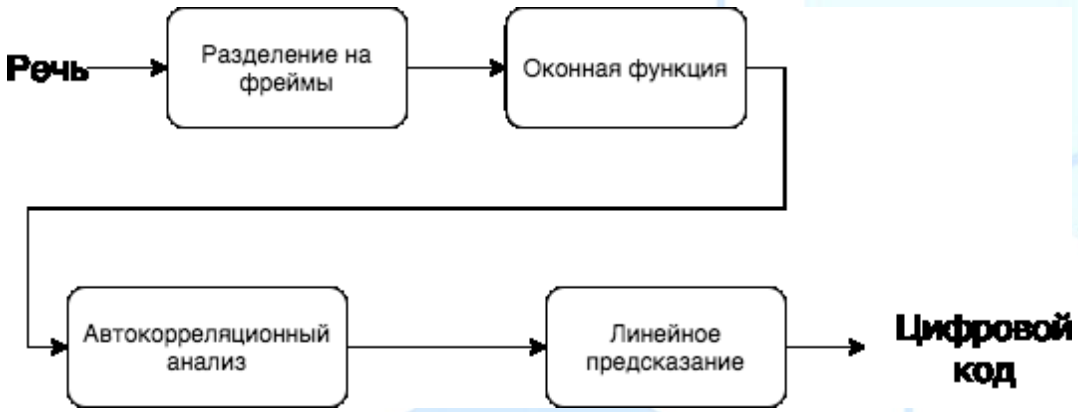


Figure 5 – Diagram of obtaining a digital voice signature

The full algorithm for user authentication by voice in the service:

- receiving an audio file as input;
- Create a digital signature from the resulting audio file.
- Retrieving the user's existing reference voice signature from the database
- Comparison of the obtained sample with the reference and signatures created on the basis of other voices and various noises, based on the results of the comparison, the probability ratio is calculated, which shows the probability that the obtained sample is close to the reference one.
- Authentication is considered successful if the result of the likelihood

ISSN 2181-3187

ratio for the received sample exceeds a certain mark (0-100). In this implementation, the elevation is 90. The digital signature is stored in the database and is used for authentication in the form of an array of

numbers reflecting the characteristics of the voice (Fig. 6).

| Сигнатуры | |
|---|---|
| 1 | 3[illegible] |
| 2 | 1[illegible] |
| 3 | 1[illegible] |

Figure 6 – Example of storing a voice fingerprint in encrypted form

For fingerprint authentication, the application uses the standard features of the Android OS - Biometric API (Automated Biometric Identification System). Once scanned, the unique pattern is transformed into a digital biometric template. Then the interface saves the data necessary for recognition in a special secure storage - Android Keystore. The system guarantees the security of data in this storage from unauthorized access. The app uses Class 3 security, which prevents the user from using the device's password or other methods instead of fingerprinting.

The sequence of actions of the service when using fingerprints for authentication:

- The user enables in-app fingerprint authentication.
- the service generates a random string and sends it to the user, the string is stored in the service database;
- the application encrypts the received string with a special key, the encrypted string is stored in the application's memory, and the decryption key is stored in a special storage;
- When authenticating, the user uses a fingerprint and the application accesses the decryption key, after which the string stored in the application's memory is decrypted and sent to the server for verification.

The digital signature of the fingerprint is represented as a string consisting of English letters and numbers.

**Evaluation of work.** To determine the effectiveness of the presented authentication service, we use the F-measure [14], which is used to assess the accuracy of recognition algorithms:$F\beta$

$$= (\beta 2 + 1) \cdot \frac{Precision \cdot Recall}{\beta 2 \cdot Precision + Recall},$$

ISSN 2181-3187

$0 < F\beta < 1$.

This metric takes into account and combines the measure of accuracy and completeness of the algorithm.

We will calculate the accuracy based on a sample of 100 different users.

To begin with, let's calculate the number of errors of the first and second kinds, i.e. the number of false and false positive results, as well as the number of true positive and true negative results. Let's get the following table.

| Верная гипотеза / результат распознавания | **Верно** | **Неверно** |
|---|---|---|
| **Верно** | 51 (верно принятых TP) | 11 (неверно принятых, ошибки второго рода FP) |
| **Неверно** | 18 (неверно отвергнутых, ошибки первого рода FN) | 20 (верно отвергнутых TN) |

Точность (*Precision*) вычислим по формуле:

$$Precision = \frac{TP}{TP + FP}.$$

В нашем случае имеем:

$$Precision = \frac{51}{51 + 11} \approx 0{,}82.$$

Далее вычислим полноту (*Recall*) по формуле:

$$Recall = \frac{TP}{TP + FN}.$$

Получим следующее значение:

$$Recall = \frac{51}{51 + 18} \approx 0{,}74.$$

F-мера вычисляется на основе значений полноты и точности. Чтобы добавить одной из этих величин определенный вес, то есть увеличить значимость при оценке, используется параметр $\beta$:

$$\begin{cases} 0 \leq \beta < 1, \text{если важна точность} \\ \beta \geq 1, \text{если важна полнота} \end{cases}.$$

В нашем случае большее значение имеет точность, поэтому выберем параметр $\beta = 0{,}5$.

Вычислим F-меру:

$$F_2 = (0.5^2 + 1) \cdot \frac{0{,}82 \cdot 0{,}74}{0{,}5^2 \cdot 0{,}82 + 0{,}74} \approx 0{,}79.$$

Thus, the accuracy of the algorithm implemented in the biometric authentication service rhythm is ~79%.

By using more accurate algorithms, the accuracy of voice recognition can be improved. For example, replace linear prediction coefficients (LPC) with mel-frequency cepstral coefficients (MFCC), and use the Gaussian mixture model (GMM)

ISSN 2181-3187

when creating a voice signature [15].

**Conclusion.** Identity verification is used both in simple systems for enhanced authentication and to confirm the user's identity in various mission-critical operations. The presented mobile service is designed to provide on-demand identity verification to any third-party application that requires high security standards.

The implementation of the service for mobile platforms was carried out in order to improve the ease of use for a wide audience of users. According to a social survey conducted by the analytical company Pew Research Center [8], more than 60% of the adult population use smartphones. The service described in the work is installed as an application on smartphones running the Android operating system. Using a developed specialized protocol, any third-party application can access the service for additional verification of access rights.

The use of modern biometric information security technologies in this service guarantees the reliability of verification due to the uniqueness of biometric data.

The additional combination of several biometric proof of rights mechanisms in a two-factor authentication system has a positive effect on both the level of security and the efficiency of the authentication process.

Encryption of confidential information using a cryptographic method based on Diophantine equations is aimed at reducing the risk of unauthorized access to biometric data in the service. It is known that in the general formulation the problem of solving Diophantine equations in integers is algorithmically unsolvable, which leads to high cryptographic strength of such encryption algorithms.

## Biliography


1. Ometov, Aleksandr. Multi-Factor Authentication: A Survey / Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, Yevgeni Koucheryavy. – 2018.
2. Quantized Convolutional Neural Networks for Mobile Devices. – Regime Access: https://arxiv.org/abs/1512.06473, free. – Title from the screen. –Armenian. (accessed: 24.02.2021).
3. Osipyan, V. O. Development of information security system mathematical models by the solutions of the multigrade Diophantine equation systems / V. O. Osipyan, K. I. Litvinov, R. Kh. Bagdasaryan, E. P. Lukashchik, S. G. Sinitsa, A. S. Zhuk. – ACM Press, 2019. – P. 1–8.
4. Recognito: Text Independent Speaker Recognition in Java. – Mode of access: https://github.com /amaurycrickx/recognito, free. – Title from the screen. – Armenian. (accessed: 16.02.2021).
5. Sabur, Ajibola Alim. Some Commonly Used Speech Feature Extraction / Sabur Ajibola Alim and Nahrul Khair Alang Rashid // Algorithms From Natural to

Artificial Intelligence – Algorithms and Applications. – 2018.

6. Shor, P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring / P. Shor // Foundations of Computer Science : Proceedings of the 35th Annual Symposium – IEEE, 1994. – P. 124–134.
7. SOLDEEA – Encryption algorithm based on system of linear diophantine equations. – Mode of access: https://github.com/CrissNamon/soldeea, free. – Title from the screen. –Armenian. (accessed: 12.04.2021).
8. Sushil, Phadke. The Importance of a Biometric Authentication System / Sushil Phadke // The SIJ Transac- tions on Computer Science Engineering & its Applications (CSEA). – 2013.
9. Yutaka, Sasaki. The truth of the F-measure / Yutaka, Sasaki // School of Computer Science. – University of Manchester, 2007.
10. G. Suvarna, Kumar. Speaker recognition using GMM / G. Suvarna, Kumar // International Journal of Engi- neering Science and Technology. – 2010. – Vol. 2 (6). – P. 2428–2436.

## References

1. Petrunenkov, A. Era biometriki [The Era of Biometrics]. *Direktor informatsionnoy sluzhby* [Director of In- formation Services], 2003, no. 12, December 24.
2. *Istoriya biometrii: ot drevnosti do nachala XX veka* [The history of biometrics: from antiquity to the begin- ning of the XX-th century]. Available at: https://worldvision.com. uk (accessed 13.02.2021).
3. *Biometric data collection by country*. Available at: https://www.comparitech.com (accessed 24.01.2021).
4. Jain, A. K. Ross, Arun, Prabhakar, Salil. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 2004, vol. 14 (1), p. 4–20.
5. Kaspersky reports surge in cyber-attacks on selfies and others biometry. *Biometric technology today. Janu- ary 2020.* Available at: https://www.biometricstoday.com (accessed 15.03.2021).
6. Ometov, Aleksandr, Bezzateev, Sergey, Mäkitalo, Niko, Andreev, Sergey, Mikkonen, Tommi, Koucherya- vy, Yevgeni. *Multi-Factor Authentication: A Survey*, 2018.
7. Osipyan, V. O., Litvinov, K. I., Bagdasaryan, R. Kh., Lukashchik, E. P., Sinitsa, S. G., Zhuk, A. S. *Devel- opment of information security system mathematical models by the solutions of the multigrade Diophantine equation systems.* ACM Press, 2019, pp.1–8.
8. *Quantized Convolutional Neural Networks for Mobile Devices.* Available at:

ISSN 2181-3187

https://arxiv.org/abs/1512.06473 (accessed 24.02.2021).

9. *Recognito: Text Independent Speaker Recognition in Java.* Available at: https://github.com/amaurycrickx/recognito (accessed 16.02.2021).
10. Sabur, Ajibola Alim, Nahrul, Khair Alang Rashid. Some Commonly Used Speech Feature Extraction.

*Algorithms From Natural to Artificial Intelligence – Algorithms and Applications*, 2018.

11. Shor, P. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. *Foundations of Computer Science : Proceedings of the 35th Annual Symposium on – IEEE*, 1994, pp. 124–134.
12. *SOLDEEA – Encryption algorithm based on system of linear diophantine equations*. Available at: https://github.com/CrissNamon/soldeea (accessed 12.04.2021).
13. Sushil, Phadke. The Importance of a Biometric Authentication System. *The SIJ Transactions on Computer Science Engineering & its Applications (CSEA)*, 2013.
14. Yutaka, Sasaki. The truth of the F-measure. *School of Computer Science*. University of Manchester, 2007.
15. G. Suvarna, Kumar. Speaker recognition using GMM. *International Journal of Engineering Science and Technology*, 2010, vol. 2 (6), pp. 2428–2436.