User authentication method information and telecommunication systems based on cascading multimodal biometric identification

Vasyl Trysnyuk[a], Oleksii Lebid[a], Kyrylo Smetanin[b], Ihor Humeniuk[b], Oleksii Samchyshyn[b], Viktor Shumeiko[a] and Taras Trysnyuk[a]

[a] *Institute of Telecommunications and Global Information Space of the National Academy of Sciences of Ukraine, 13 Chokolivsky Blvd., Kyiv, 02000, Ukraine*
[b] *Korolov Zhytomyr Military Institute, 22 Miru Ave., Zhytomyr, 10004, Ukraine*

Abstract

Efficiency of information and telecommunication systems significantly depends on the strong control over the provision of authorized access to them. However, the constant improvement of the technical equipment of these systems requires new approaches creation and user authentication existing method improvement. Biometric identification technologies are one of the significant approaches in the development of methods. Timely detection of unauthorized access to information and telecommunication systems is a necessary component of high stability ensuring and reliability of their operation, especially for cyber-attacks prevention or important information leakage and necessitates the development of intelligent methods of user authentication. Authors proposes a method of user authentication of information and telecommunications systems, based on the use of cascading multimodal biometric identification by voice message and facial geometry, particularly taking into account the physiological characteristics of the person. The results of method verification for users of different sex, physiological condition, and their comparative characteristics were established. The application of the proposed method allows reduces the risk of successful implementation by the violator of unauthorized access to the network of information and telecommunication systems in the absence of means to control access to them.

Keywords

authentication; information and telecommunication system; cascade; multimodal identification; biometrics

1. Introduction and Literature Review

Nowadays passwords are based on unique personal information and attribute identification methods are losing their relevance, but there are in great demand among users. These methods of providing access have significant technological shortcomings, which are becoming increasingly pronounced. One of such problems is the inaccuracy of user identification in the system and the high probability of violation of its security as a result of unauthorized access (UI) to information, information leakage, imitation of a certain attribute or password cracking, and so on. Another important problem of these methods is the lack of functionality to detect the substitution of an authorized ("legitimate") user.

Compared to previous methods, the user's biometric characteristics as authentication method can guarantee an increased level of security, taking into account the individual characteristics of the biometric data of a particular person [1].

ITTAP'2021: 1nd International Workshop on Information Technologies: Theoretical and Applied Problems, November 16–18, 2021, Ternopil, Ukraine
EMAIL: trysnyuk@ukr.net (A. 1); lebid65@gmail.com (A. 2); kiry221982@gmail.com (B. 1); ig_hum@ukr.net (B. 2); samyj123@ukr.net (B. 3); shym1983@ukr.net (A. 3); tryskTar@ukr.net (A. 4)
ORCID: 0000-0001-9920-4879 (A. 1); 0000-0002-4003-8068 (A. 2); 0000-0002-6062-550X (B. 1); 0000-0001-5853-3238 (B. 2); 0000-0002-1542-1065 (B. 3); 0000-0002-0285-4566 (A. 3); 0000-0002-3672-8242 (A. 4)

Standard password (attribute) for security systems is increasingly being replaced or supplemented by biometric personal identification systems. According to the analysis of the scientific literature [2– 5], the most effective and popular methods are the application of identification by facial geometry [6, 7] and voice message [8]. The main advantages of such systems are low price, high security level, user convenience, accessibility, ease of use, remote access etc. Such authorization systems allow to solve problems related to the confidentiality of user credentials, identification and authentication in information and telecommunications systems (ITS).

However, at the current level of development of information technology there is an increase in the frequency of false positives, service failures, artificial (malicious) violations of control systems and access to ITS using cyber-attacks, hardware and software. Therefore, the task of developing and / or improving methods of multimodal biometric authentication to reduce the risk of successful implementation of the NSD violator to the ITS network becomes relevant.

A number of modern methods of ITS information protection using biometric user identification methods have been developed and implemented. The authors in [1] present the results of the analysis of face recognition methods and algorithms for comparing image patterns, as well as trends in the development of biometric identification and authentication of persons by facial geometry; in [2] the analysis of methods of biometric identification was carried out, the advantages and disadvantages of technologies of their realization are resulted; in [3] modern methods of biometric identification of users of computer systems, designed to ensure the protection of confidential information was considered; paper [4] describes general methods and programs of biometric identification; in [5] the classification of models and methods of biometric attendance control is considered, the results of the analysis of human authentication was proposed; in [6] the structure of the biometric template of mobile banking user authentication was developed; in [7] current scientific and technical problem of developing information technology for personnel identification based on a set of biometric parameters using a combination of static-dynamic recognition methods and improving methods of creating reference samples was solved; in [8] the results of using chalk-frequency coefficients of keppra to solve the problem of user identification by voice signal were proposed.

Therefore, the results of the analysis of scientific and practical sources indicate that a sufficient amount of scientific and methodological and practical support was developed to solve the problems of ITS protection. These methods of access control are based on voice and face recognition and have a number of disadvantages. Such methods do not take into account the training sample (computer training) identification data, in particular, standards of target voice and face images, as well as physiological characteristics of the user. This does not ensure the cascading operation of biometric user identification systems and a sufficient level of efficiency of the identification system to prevent the successful implementation of UAA. Based on these prerequisites, the purpose of this article is formulated, which is to develop a method of authentication of ITS users based on cascading multimodal biometric identification and its application in solving problems of timely detection and operational blocking of UAA.

2. Materials and Methods

Biometric identification is a technology for recognizing certain unique specific biometric features (identifiers) that are specific to a particular person or user.

In order to increase the level of ITS security, to prevent the successful implementation of the UAA violator, it is proposed to change the approach to solving the problem of user identification, namely: to solve this problem not in the systematic and simultaneous use of identification systems by voice and facial geometry within the framework of cascading identification of "voice-face" with an increased educational sample of standards, in particular, taking into account the physiological characteristics of the person. In this approach, the problem of user identification is solved separately for identification systems by voice recognition [7] and facial geometry [9] with sequential activation of the second, provided the successful completion of the first. This approach allows to ensure the cascading of the user identification system, which increases the efficiency of the ITS access control systems as a whole [10, 11].

The developed method of authentication based on cascading identification of "voice-face" includes the following steps: the first - by voice message; the second - on the geometry of the face. Therefore, performance of the second step is possible only on condition of successful identification of the first.

The use of face identification systems by voice and facial geometry is the most user-friendly method of authentication, which is based on individual physiological features of the speech apparatus and the shape of the human face. The peculiarity of the application of the selected methods of biometric identification is the computer training of voice classifiers and face primitives of users with increased training sample of target standards, which are stored in the database and taking into account physiological features of the person, namely: different volume levels etc.

The generalized scheme of multimodal biometric identification of ITS users is given in fig. 1

Step 1.1. *Normalization of the input voice signal.* To remove fragments that do not contain a voice imprint, the input speech signal passes through a voice activity detector. The result of such an operation is the selection of a fragment of the voice, reducing computational complexity by eliminating the calculation of fragments of the speech signal that do not contain a voice imprint.

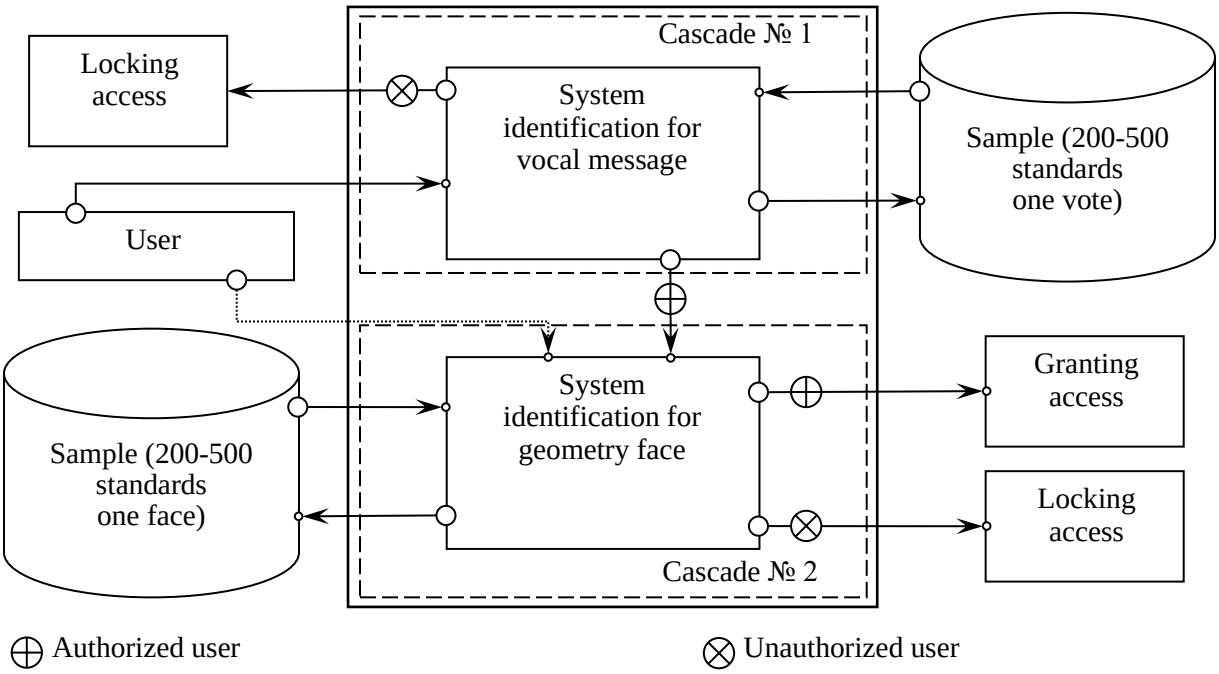


Figure 1. Scheme of operation of multimodal user identification

Consider in detail each of the cascades (steps of the method).

Stage 1. Identification by voice message. A detailed scheme of identification by voice message is given in Fig. 2.

Step 1.2. *Selection of characteristic features of the voice.* The value of the amplitude of the speech signal X, which are outside the range:$X \notin [X(t) - 3 \cdot \delta; X(t) + 3 \cdot \delta]$ (the rule of "three sigma"), are considered as a voice imprint, the rest - as fragments of noise. The speech signal is divided into equal frames of duration (ms), each value of the amplitude of which is estimated according to the rule of "three sigma".

A temporary array of values of logical type is created for each frame:

$$Bool = \begin{cases} true(1), & X \notin [X(t) - 3 \cdot \delta; X(t) + 3 \cdot \delta]; \\ false(0), & X \in [X(t) - 3 \cdot \delta; X(t) + 3 \cdot \delta]. \end{cases} \quad (1)$$

Then the calculation is performed $p_{"1"}$ – the probability of an element with a value $true(1)$ та $p_{"0"}$ – the probability of occurrence of the value $false(0)$. Probabilities are calculated by finding the ratio of the number of occurrences of elements with a value $true(1)$ or $false(0)$ relative to the total number of values in the array.

Provided that value $p_{"1"}$ less than some threshold value α, it is believed that this fragment contains a voice, otherwise - noise or silence.

Parameter α is interpreted as follows: if 65% of the values of the amplitude of the speech signal in the fragment ($\alpha = 0{,}65$) are outside the range $[X(t) - 3 \cdot \delta; X(t) + 3 \cdot \delta]$, the current snippet contains a voice, otherwise noise or silence.

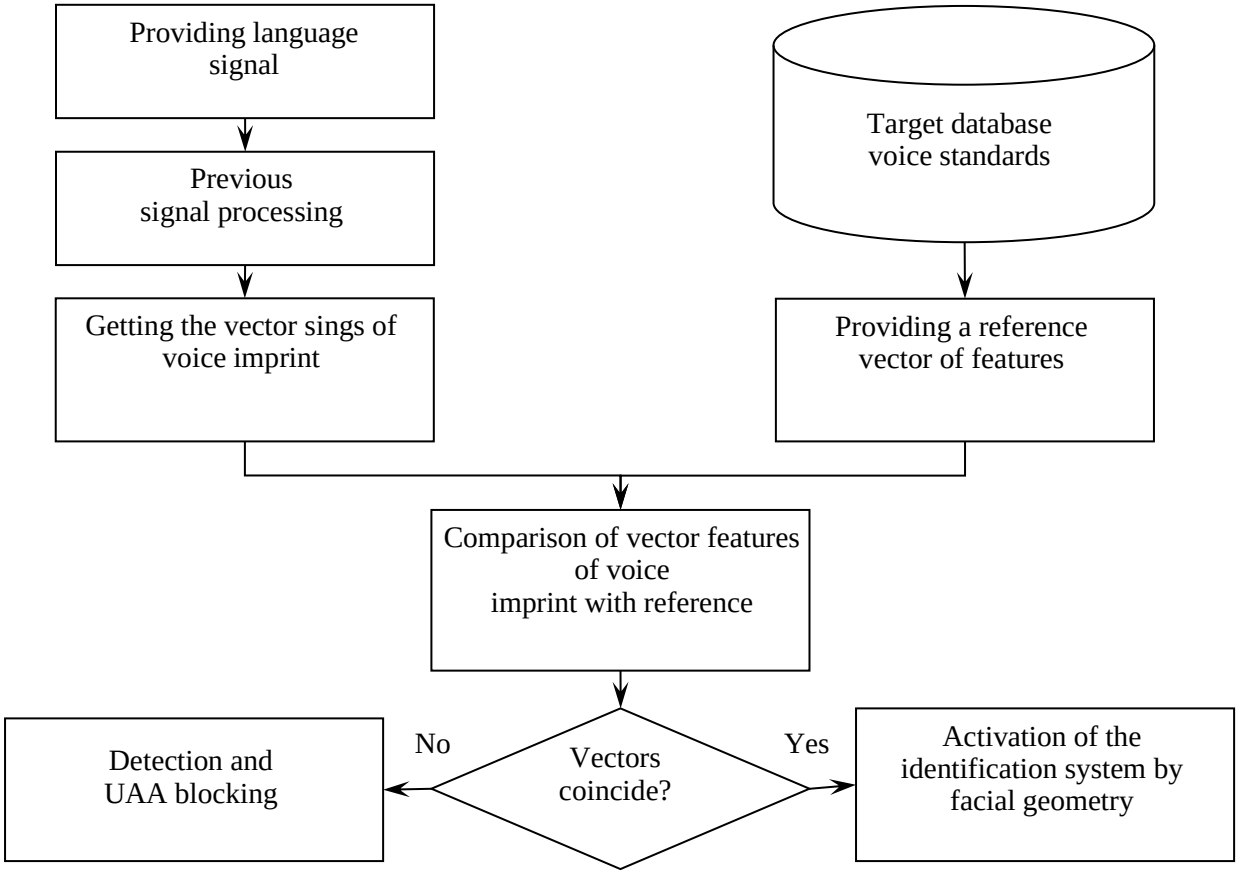


Figure 2. Biometric identification by voice message

Step 1.3. *Comparison of the voice imprint with the reference ones contained in the database***.** The voice imprint is presented as a sequence of feature vectors, each of which describes the characteristics of the speech signal interval. The sequence of vectors is used to build a model of the voice standard of the ITS user. The main parameter used to identify the user is the similarity of the two sound fragments (input voice imprint and the target voice standard contained in the database).

In the authorization mode, the user provides an identifier in the form of a voice message, while the access control system analyzes this voice print, compares it with the target voice standard, identifies the person by voice.

If the user is successfully identified, the access control system activates the next stage of the identification system, in particular, the facial geometry [11, 12]. We will describe the process of facial recognition by this method of identification.

Stage 2. Identification by facial geometry.

Step 2.1. *Detection and localization of facial geometry in the image of the video stream***.** In this article, the Viola-Jones algorithm is used to search for the shape (geometry) of the face in the image of video surveillance systems. The chosen algorithm is the best solution, compared to other algorithms, in terms of efficiency and efficiency of face recognition.

When using this method, the video image is presented in an integrated form (matrix of values of total brightness) to increase the efficiency of analytical calculations and calculations. Each element of this matrix stores the value of the sum of the pixel intensities that geometrically delineate the object on the left and top. The identification scheme is given in Fig. 3.

The elements of the integrated representation are calculated by the formula:

$$L(x,y) = \sum_{i=0}^{i\le x}\sum_{j=0}^{j\le y} I(i,j), \quad (3)$$

where, $I(i,j)$ – the value of the brightness of the pixel in the image.

Each item $L(x,y)$ corresponds to the sum of pixels that are in a certain rectangle. The video image on which the object is searched is presented in the form of a two-dimensional matrix with a dimension (x,y), each pixel of which takes values for a monochrome image and for a color image format RGB – $[0;255^3]$. The search is performed in the active area of the image with rectangular features (description of the user and his facial geometry):

$$RECT = \{(x,y),(w,h),\alpha\}, \quad (4)$$

where, (x,y) – coordinates of the center of the rectangle;

w, h – width and height of the rectangle, respectively;

α – the angle of the rectangle relative to the vertical axis of the image.

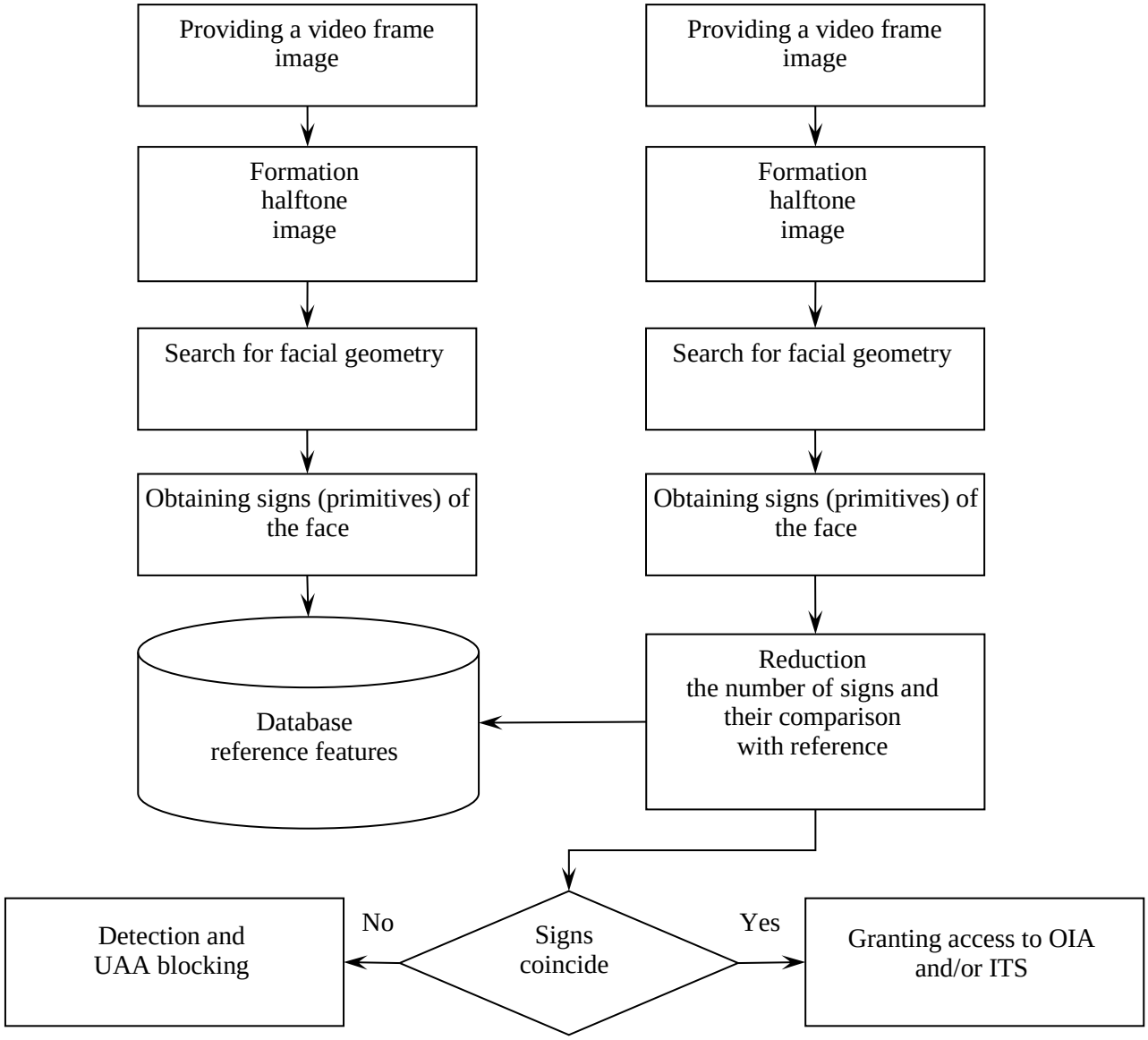


Figure 3. Biometric identification by facial geometry

Step 2.2. *Normalize the image by scale (brightness, etc.).*

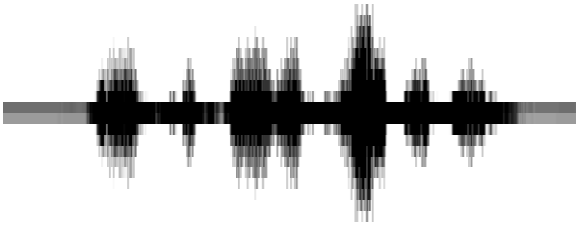
Step 2.3. *Calculation of a set of basic features (characteristics) of the image.* All Haara primitives come to the classifier input and are processed with some boost. In order to achieve the appropriate

efficiency of the algorithm and the reliable operation of the identification system for facial geometry [12], an intellectual training of the classifier using neural networks, which solves the problem of classification of objects by features?

Step 2.4. *Comparison of the calculated features with the reference ones contained in the database.*

3. Experiment, Results and Discussions

The biometric characteristics of the authors of the article are selected as initial data. Authorized is user № 1, the standards of voice imprint and facial geometry are given in Fig. 4. Verification of the proposed method was carried out using the specialized software developed by the authors on voice signals (Fig. 5) and monochrome video images (Fig. 6), obtained using a security camera Infinity SR-DN530SD with a resolution of 800x600 pixels.



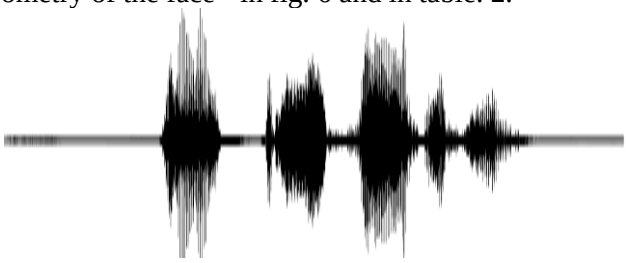
a)

b)

Figure 4. Biometric user standards № 1
a – voice message; b – facial geometry

The results of verification of the proposed method, in particular the identification of users by voice message are presented in Fig. 5 and in table 1, and the geometry of the face - in fig. 6 and in table. 2.

a)



d)

b)

f)

c)

g)

Figure 5 Spectrograms of voice messages:
user № 1 (a – normal voice; b – hoarse voice; c – in the presence of noise);
user № 2 (d – normal voice; f – hoarse voice; g – in the presence of noise)

Table 1
Voice message identification results

Voice message	Comparison of output signals with the template, (%) ([0-20] – blocked; [21-100] – access granted)	
	user № 1	user № 2
fig. 5 a	81	14
fig. 5 b	53	12
fig. 5 c	25	4
fig. 5 d	14	13
fig. 5 f	12	11
fig. 5 g	4	6

a)

d)

b)

f)

c)

g)

Figure 6. Face image:
user № 1 (a – normal; b – indignant; c – turn heads);
user № 2 (d – normal; f – indignant; g – turn heads)

Table 2
The results of identification by facial geometry

Voice message	Comparison of source images with template, (%) ([0-20] – blocked; [21-100] – access granted)	
	user № 1	user № 2
fig. 6 a	90	13
fig. 6 b	72	12
fig. 6 c	31	5
fig. 6 d	13	12
fig. 6 f	11	10
fig. 6 g	5	4

As a result of application of the offered method authentication for the user № 1 is successful, and for another access f is blocked.

The efficiency of the access control system based on voice and face recognition of the analogue (prototype) is $E_{a(n)}(k) = 0.75$ for $k = 10$, where k – number of authorized users. As the number of users increases, the efficiency of such a system decreases exponentially. Accordingly, for the multimodal system proposed in the article, the results of operational efficiency are obtained $E_{м}(k)$ (fig. 7).

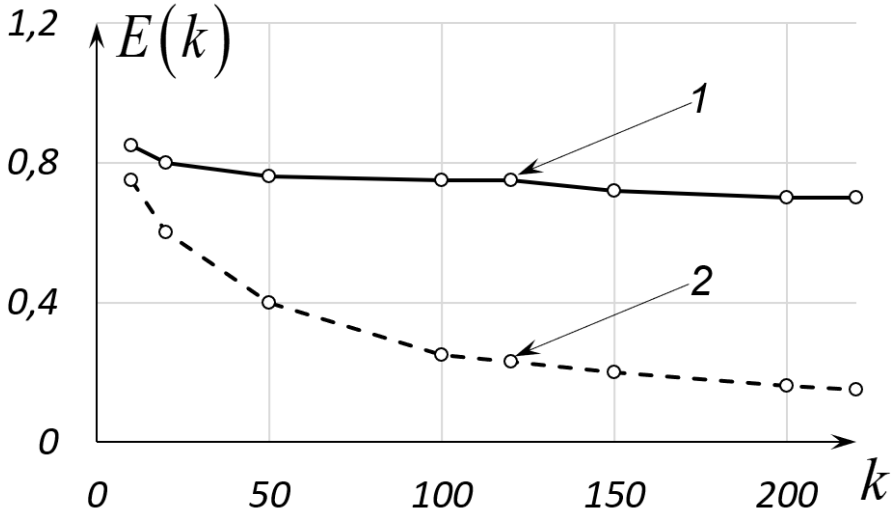


Figure 7 The effectiveness of access control systems:
cascade identification method - 1; prototype (analogue) - 2

4. Conclusions

The article solves the current scientific and practical problem, which is to reduce the risk of successful implementation of the UAA violator to the ITS network by increasing the methods of biometric identification (by voice recognition and facial geometry) and cascading application of identification systems that implement them [13].

From the analysis of the obtained results, it follows that in comparison with the existing [14] the developed method provides increase of efficiency of functioning of identification system (level of ITS protection and prevention of successful implementation by the violator of UAA mode of access to them) by 15–30% by increasing training sample physiological features of the user's condition and cascade application of biometric user identification systems.

The method of multimodal biometric identification of users of the ITS network should be used for the effective operation of systems in special conditions in the interests of counteracting the implementation of UAA by the violator of the access regime and the lack of means of user identification.

5. References

[1] O. V. Nechyporenko, Ya. V. Korpan, Biometric identification and authentication of a person by facial geometry, in: Visnyk of Khmelnitsky National University, technical sciences (4), Khmelnitsky Ukraine, 2016. pp. 133–138.

[2] L. G. Koval, S. M. Zlepko, G. M Novitsky, Methods and technologies of biometric identification based on the results of literature sources, in: Scientific notes of Taurida National V.I. Vernadsky University, series: technical sciences, volume 30 (69) Ch. 1 № 2, Kyiv Ukraine, 2019, pp. 104 – 112.

[3] P. Bidyuk, V. Bondarchuk, Modern methods of biometric identification, in: Legal, normative and metrological support of the information protection system in Ukraine, volume 1 (18), 2009. pp. 137–146.

[4] N Divyarajsinh Parmar, B. Brijesh, P. G. Mehta, Face Recognition Methods & Applications, in: Int. J. Computer Technology & Applications. volume 4 (1), Wadhwan city India, 2015. pp. 84–86.

[5] D. V. Aleksandrovich, A. L. Erokhin, Research of models and methods of biometric control of attendance, in: Information systems. volume 6 (122), 2014, pp. 157–162.

[6] O. A. Nemkova, Biometric identification in cyberspace, in: Information processing systems, issue 7 (132), Kharkiv Ukraine, 2015. pp. 118–121.

[7] Yu. O. Kumchenko Information technology of personnel identification on the basis of a complex of biometric parameters (technical sciences), Ph.D. thesis, 2017, 143 p.

[8] DianaVan Lancker, JodyKreiman, Karen Emmorey, Familiar voice recognition: patterns and parameters Part I: Recognition of backward voices, in: Phonetics Laboratory, Department of Linguistics, University of California at Los Angeles, Los Angeles. California 90024, U.S.A., 2019 URL: https://doi.org/10.1016/S0095-4470(19)30723-5.

[9] V. Trysnyuk, Y. Nagornyi, K. Smetanin, I. Humeniuk, T. Uvarova, A Method for user authenticating to critical infrastructure objects based on voice message identification, in: Modern information systems, science. Magazine, National Technical University "Kharkiv Polytechnic Institute", Kharkiv Ukraine, 2020, volume 4(3) pp. 11–16. doi: https://doi.org/10.20998/2522-9052.2020.3.02.

[10] O. S. Boychenko, I. V. Humeniuk, K. V. Smetanin, O. V. Nekrilov, Method of blocking access to information and telecommunication systems based on biometric identification / user authentication, in: Technical Engineering: Science. View, Zhytomyr Polytechnic State University, Zhytomyr Ukraine, 2020. Volume 1 (85). pp. 171–176. doi: https:// doi.org/10.26642/ten-2020-1(85)-171-176.

[11] V. G. Babenko Methodology of synthesis of information transformation operations for computer cryptography (Computer systems and components), Dr.Sc. thesis, Cherkasy State Technological University, Cherkasy, Ukraine, 2020.

[12] V. Trysnyuk, O. Demydenko, K. Smetanin, A. Zozulia [2020] Improvement of the complex evaluation method of vital activity risks. Geoinformatics - XIXth International Conference "Geoinformatics: Theoretical and Applied Aspects", 17605.
[13] A. B. J. Teoh, A. Goh, and D. C. L. Ngo, "Random Multispace Quantization as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs, " Pattern Analysis and Machine Intelligence, IEEE Transactions on, vol. 28, pp. 1892—1901, 2006
[14] A. A. Ignatovych, Methods of increasing the efficiency of security components of computer systems using masking elements of text and biometric data (Computer systems and components), Ph.D. thesis, Lviv Polytechnic National University, Lviv Ukraine, 2016.