Neural network biometric cryptography system

Alexey Vulfin, Vladimir Vasilyev, Andrey Nikonov and Anastasia Kirillova

Ufa State Aviation Technical University, 12, K.Marks st, Ufa, 450077, Russian Federation
nikonovandrey1994@gmail.com

Abstract. In this paper, an approach to the construction of a neural network system of biometric authentication is proposed, which allows organizing the distributed stor-age of the base of biometric images and using a secret cryptographic key generated on the basis of the input biometric image as an output of the neural network. The object of the research is the biometric authentication system, and the subject of the research is the algorithms for converting parameters into a cryptographic key based on neural network technologies. The structure of a biometric authentication system has been developed, which identifies biometric features of a face image. The main difference between the developed system and existing solutions is the method of constructing a vector of primary biometric features based on neural network models and methods of machine learning and data mining, which allows assigning a unique private cryptographic key to each authentication subject. The mechanism of a distributed neural network representation of private key components significantly reduces the likelihood of compromising the vector of biomedical features. The use of the developed system and algorithms will make it possible to create highly reliable biometric security systems that ensure the ability of users to work with confidential information in open and weakly protected information systems.

Keywords: Information security, Neural network, Biometric, Cryptography, Image analysis.

1 Introduction

A promising trend in increasing the efficiency of authentication systems is the integration of biometric and cryptographic methods in the task of converting biometric parameters into an access key code (cryptographic key). The use of initial biometric features for the generation of cryptographic keys has a number of difficulties: biometric data is not clearly reproducible and does not have a uniform distribution of parameters, while most cryptographic transformations are bijective and require an exact key value [1–7].

Biometric authentication systems, that using machine learning models, approximate a set of multidimensional dividing hyperplanes in the space of selected features of biometric templates, which makes it possible to isolate the templates of each predefined class associated with the authentication subject. Systems whose output vector reproduces the code of a predetermined class are vulnerable to attacks on the "last bit" of the decision rule [8-9]. The use of neural network models in the core of the authentication system is also associated with a number of disadvantages associated with the need to retrain the neural network when adding a user and potential errors of the second kind.

The goal of the research is improvement of biometric authentication algorithms due to neural network transformation of biometric features into a cryptographic key.

To achieve the goal, the following tasks were set:

- development of the structure of a neural network biometric authentication system with the transformation of the vector of biometric features into a cryptographic private key;
- development of an algorithm for converting input biometric features into a cryptographic "private" key in a neural network basis;
- comparative analysis of the effectiveness of biometric authentication systems based on machine learning models.

2 Materials and methods

The algorithm of the neural network biometric authentication system with the transformation "biometrics – code" (NNBA) includes five stages (Figure 1) [10–20].

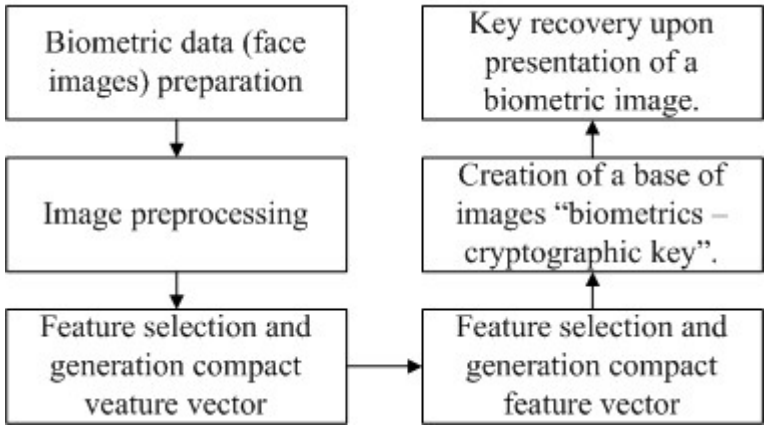


Fig. 1. Basic algorithm for neural network transformation of the original biometric features into a cryptographic private key.

Image preprocessing. Image preprocessing performed as extraction of biometric features from a "raw" biometric image. To train neural networks, a sample of data was created with images of the faces of five users, which are presented in Figure 2.

Image preprocessing is performed according to the diagram in the Figure 3.

5000 images from the video stream were selected for each of the classes. The selected areas have been labeled and scaled to 256x256 pixels to contain the minimum number of pixels outside the face of interest. Additionally, the images were normalized by equalizing the histogram to normalize certain sections of frames with different brightness. Also for some neural networks, color images were converted from a color scheme (RGB) to grayscale with a 255-bit palette (grayscale). The negative sample consists of 5000 images, also reduced to a size of 64x64 pixels.

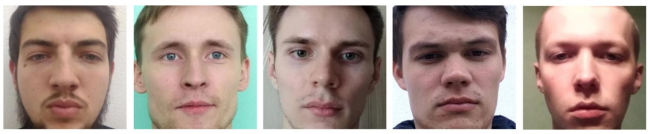


Fig. 2. Sample images from the training set.

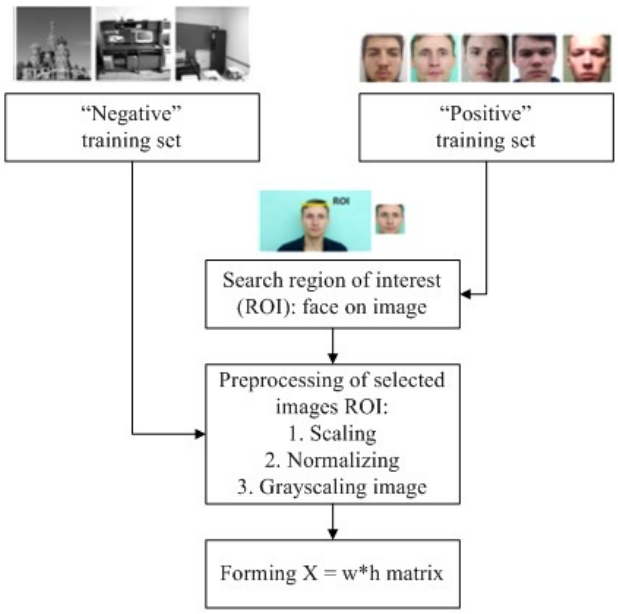


Fig. 3. Scheme of the image preprocessing block.

Coding and selection of features for building a base of biometric images. At the preprocessing stage, two training samples are prepared: positive and negative. A "positive" training set consists of preprocessed images extracted from the video stream and containing the user's face (the subject of authentication). The "negative" training set includes arbitrary images that do not contain fragments of a human face. A sufficiently large number of examples in a "negative" training set in comparison with a "positive" one allows the classifier model to use a larger number of images for constructing dividing surfaces in the feature space and has a beneficial effect on the learning outcomes of such models.

It is proposed to coding features using the following steps:

- images of all classes of positive and negative samples are represented as an integer matrix of uniform size [n, n], in which each pixel is an integer in the range [0, 255], which corresponds to the representation of the image in grayscale;
- the unified matrix is split line by line, and a column vector of size [n*n, 1] is constructed. This step provides an invariant to displacement of the region of interest (ROI) in the vertical direction;
- each element of the column vector can be transformed into a reflective binary 8-bit Gray code [21], and then the resulting matrix is again split into rows. A column vector of size [8 * n * n, 1] is formed again from the received rows. Representation of features in the form of Gray codes is due to the fact that two adjacent values of the color scale differ only in one bit.

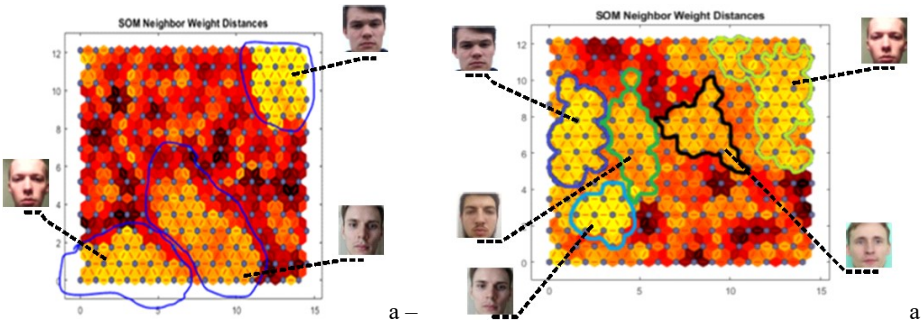
Feature generation consists in projecting the primary vector into a new feature space and forming a compact feature vector of each image for subsequent neural network processing. A binary or integer vector is fed to the input of a neural network unit, which implements a functional mapping of an image into a unique vector, which acts as a private cryptographic key.

It is proposed to use the following approaches for features generation:

Self-organizing two-dimensional Kohonen map (SOM). Figure 4 shows maps of clustering of the feature vectors: user classes are displayed in yellow shades, a noisy samples are displayed in red. The vectors of user attributes are visually divided into three and five groups, which corresponds to the number of users in the system in the first experiment on field data.

Probabilistic principal component analysis (PPCA). The input of the PPCA [22] algorithm is an array with data and the value of the space dimension to which the data should be "compressed".

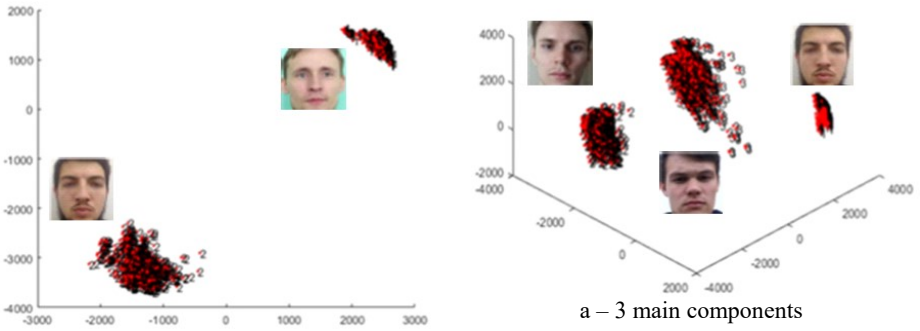
Figure 5 shows an example of highlighting two and three main components. Each point corresponds to the image of the recognition object, in our case – the NNBA users.



a – first experiment with 3 classes

a – first experiment with 5 classes

Fig. 4. Kohonen map with highlighted clusters in the first computational experiment.



a – 2 main components

a – 3 main components

Fig. 5. An example of the selection of compact groups of images based on the use of two and three main components in the image.

Thus, it is proposed to use the first n = 16 ... 32 distinguished main components as a compact vector of features of a human face.

Convolutional neural network (CNN). The outputs of the fully connected layer fc8 of the AlexNet convolutional network [23], consisting of 1000 neurons, providing the integration of information about the facial features of a particular user, are used as a compact vector of features.

Creation of a base of images "biometrics – cryptographic key". For each user of the system, whose images are used to extract biometric features, it is necessary to match a previously generated cryptographic key.

The private key is represented as an integer column vector [m, 1] of length m = 132. Each element of the vector is converted to a reflexive binary 8-bit Gray code. The rows of the resulting matrix are converted to a column vector [8 * m, 1]. This transformation is shown in Figure 6.

For each class of input images of a positive sample, which are facial images of a unique user, a single binary output vector is assigned, which is an encoded private key.

For each negative sample, a random private key in binary representation is assigned.

One of the following options is used as an input vector:

- image as an integer column vector;
- binary representation of the image as an integer column vector;
- binary vector formed by the output neurons of the two-dimensional Kohonen map, the input of which was an image in the form of an integer column vector;
- real-valued vector of activations of the fc8 layer of the AlexNet convolutional network, to the input of which a color image [227, 227, 3] of a person's face was fed in the RGB palette;
- real-valued vector formed by the principal components of the corresponding input image after projection using the PPCA method.

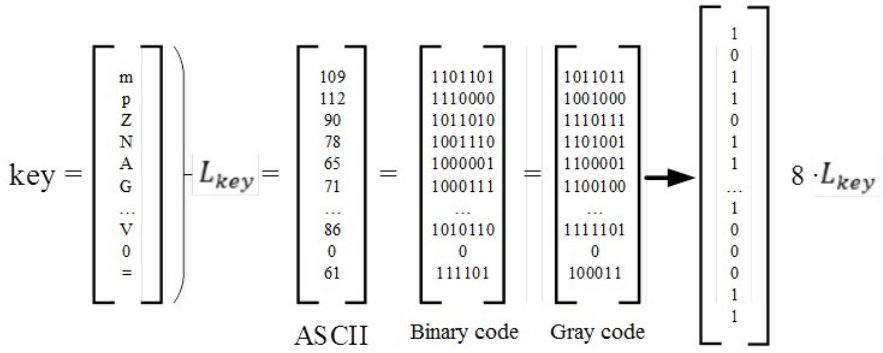


Fig. 6. Converting private key to Gray code.

Thus, the training sample is a set of pairs of input and output vectors.

Neural network matching of compact vectors of biometric images to the cryptographic keys. Matching of compact vectors of biometric images to the cryptographic keys is implemented using the following methods:

- use of bidirectional associative memory (BAM) [24];
- single-layer and multilayer perceptrons.

The algorithm for constructing an extended BAM is shown in Figure 7.

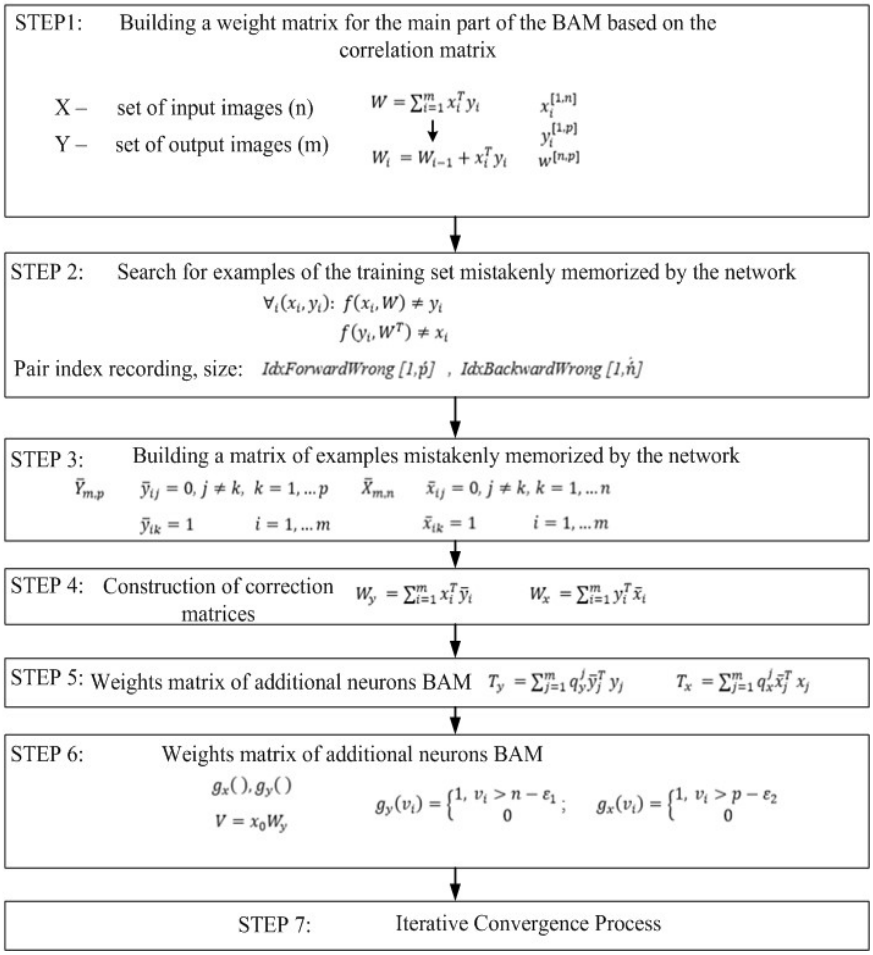


Fig. 7. Algorithm for constructing extended BAM.

Key recovery upon presentation of a biometric image. The final structure of the authentication system with neural network conversion of biometric parameters into a cryptographic “private” key is shown in Figure 8.

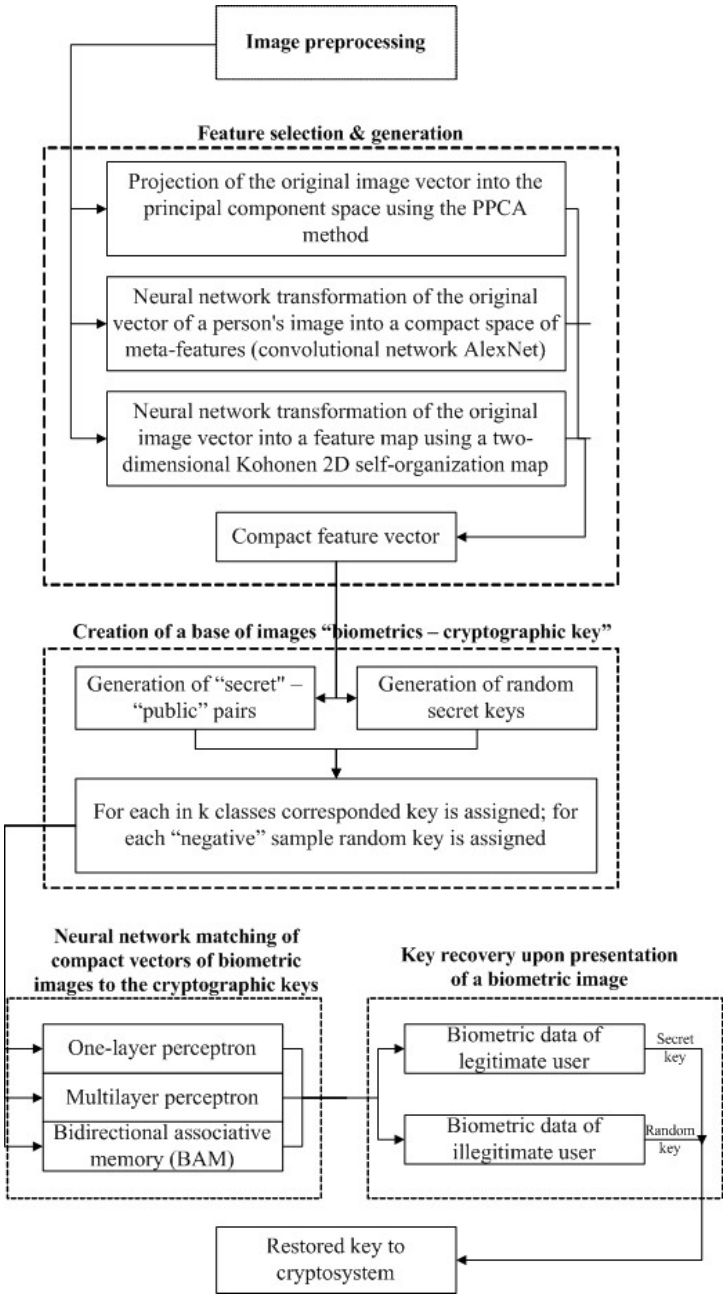


Fig. 8. The structure of a neural network biometric authentication system.

3 Results

To assess the efficiency of the neural network transformation of the initial biometric features into a cryptographic private key, several computational experiments with using following models were carried out on field data (Table 1):

- multilayer perceptron (MP);
- PPCA and multilayer perceptron;
- two-dimensional Kohonen map and multilayer perceptron;
- convolutional neural network AlexNet and multilayer perceptron;
- BAM based on B. Kosko's neural network in the version of Y. Wang.

Table 1. computational experiments.

Parameters	Experiment				
	1	2	3	4	5
	MP	PPCA + MP	Kohonen map + MP	AlexNet + MP	BAM
Source images	[64, 64, 1]	[64, 64, 1]	[64, 64, 1]	[227, 227, 3] in RGB palette	[64, 64, 1]
Compact feature vector generation	No	64 principal components by PPCA	2D Kohonen map, 15*15 neurons with a hexagonal grid	AlexNet (fc8 layer activation neurons)	No
The architecture of the neural network matching unit					
Dimension of the input vector	4096	64	225	1000	4096
Input vector type	Decimal integers [0, 255]	Real numbers	Binary vector of activities of neurons in the output layer of the Kohonen map	Real numbers	Binary Gray code
Dimension of the output vector	132 or 1056	1056	1056	1056	1056
Output vector type	Decimal integers [0, 255] or binary Gray code	binary Gray code	binary Gray code	binary Gray code	binary Gray code
Neural netwok	MP	MP	MP	MP	BAM
Number of neurons by layers	4096, 2018, 1056	64, 1056	225, 1056	1000, 1056	4096, 1056
Activation functions of neurons	elliotsig, elliotsig, satlins	elliotsig, satlins	elliotsig, satlins	elliotsig, satlins	satlins, satlins
Post-processing in network output	no / hardlim	hardlim	hardlim	hardlim	hardlim

The results of experiments on the training set are shown in the Table 2.

Table 2. Training results.

Parameters	Training 1 MP	2 PPCA + MP	3 Kohonen map + MP	4 AlexNet + MP	5 BAM
Absolute number of errors / examples	394 [4500]	362 [4500]	281 [4500]	273 [4500]	23 [450]
Proportion of correctly recognized images,%	91.24	91.96	93.76	93.93	94.89
Sensitivity	0.9688	0.9825	0.9784	0.9729	0.9865
Specificity	0.9727	0.9753	0.9830	0.9811	0.9628
Positive predictive value	0.8794	0.8869	0.9188	0.9101	0.8391
Predictive value of negative results	0.9934	0.9965	0.9957	0.9946	0.9972

Table 3 shows the results obtained during testing on field data.

Table 3. Test results on field data.

Parameters	Training 1 MP	2 PPCA + MP	3 Kohonen map + MP	4 AlexNet + MP	5 BAM
Absolute number of errors / examples	133 [1500]	124 [1500]	95 [1500]	88 [1500]	8 [150]
Proportion of correctly recognized images,%	91.13	91.73	93.67	94.13	94.67
Sensitivity	0.9828	0.9806	0.9808	0.9808	1
Specificity	0.9763	0.9775	0.9774	0.9774	0.9758
Positive predictive value	0.8837	0.9004	0.9011	0.9014	0.8966
Predictive value of negative results	0.9968	0.9959	0.9959	0.9959	1

4 Discussion

The main advantage of the Kohonen maps according to the results of experiments is the best scores of the first kind error. However, to add a new authentication subject, it is necessary to retrain the neural network. The PPCA method performs the transformation of the feature vector without the need for a continuous learning process. The

use of convolutional neural networks allows to achieve the best sensitivity and specificity by extracting complex features from the original images, but training such a network requires significant computing resources.

To match the compact vector of features isolated from the biometric image to the private cryptographic key, multilayer perceptrons and hetero-associative memory based on the BAM neural network were used.

The use of a neural network implementation of BAM makes it possible to effectively implement the mechanism of functional mapping of the feature vector into a private cryptographic key. However, due to the high dimensionality of the input feature vector and the large number of pairs of compared input (n) and output (p) vectors, the total memory capacity is

$$m = \sqrt{\min(n, p)} \tag{1}$$

For feedforward neural networks, one hidden layer is sufficient to match input biometric images and output private keys. Testing the system on a control set of examples demonstrated the possibility of obtaining random output vectors for images of users who are not subjects of authentication. If we refuse the use examples of negative sampling when training the neural network core of the system, 42% of examples of images of users who are not subjects of authentication are assigned by the system to one of the available classes.

5 Conclusion

The paper proposes an approach that allows combining a biometric authentication system module based on a machine learning model and a cryptographic module. The neural network core of the system allows to organize the distributed storage of biometric templates and implements the mapping of the input image into the generated private cryptographic key.

The structure of a neural network system for biometric authentication has been developed, including a digital video stream processing module for extracting an image of the authentication subject's face. A distinctive feature is the way to transform the vector of primary biometric signs into a compact vector using a self-organizing Kohonen map, a convolutional network, a probabilistic principal component algorithm, bi-directional hetero-associative memory, and a multilayer neural network. The next neural network unit implements the process of functional mapping of a compact vector of subject features into a unique private cryptographic key. Thus, it is possible to organize distributed compact storage of the base of biometric images and reduce the probability of compromise, since the whole process takes place in a neural network basis, which is a "black box".

Application of this approach will make it possible to create highly reliable biometric security systems that provide the ability for users to work with confidential information in open and weakly protected information spaces.

6 Acknowledgments

The reported study was funded by Ministry of Science and Higher Education of the Russian Federation (information security) as part of research project № 1/2020.

References

1. Abu Elreesh J.Y., Abu-Naser S.S.: Cloud Network Security Based on Biometrics Cryptography Intelligent Tutoring System (2019).
2. Uludag U., Pankanti S., Prabhakar S., Jain A.K.: Biometric cryptosystems: issues and challenges, 92(6), 948–960, Proceedings of the IEEE (2014).
3. Juels A., Sudan M.: A fuzzy vault scheme. Designs, Codes and Cryptography, 38 (2), 237-257 (2006).
4. Nandakumar K., Jain A.K.: Multibiometric Template Security Using Fuzzy Vault. In: Int. Conf. Biometrics: Theory, Applications and Systems, Arlington, 1–6, Proceedings of the IEEE (2008).
5. Scheirer W. J., Boult T.E.: Cracking fuzzy vaults and biometric encryption. In: Biometrics Symposium, 1-6, Proceedings of the IEEE (2007).
6. Zhou X. et al.: Feature correlation attack on biometric privacy protection schemes. In: Intelligent Information Hiding and Multimedia Signal Processing, 1061-1065, IIH-MSP (2009).
7. David C., Jan Z., Dhinaharan N.: Advances in Computer Science, Engineering & Applications. In: Proceedings of the Second International Conference on Computer Science, Engineering and Applications, 39–41, ICCSEA, New Delhi, India (2012).
8. Barreno, M. et al.: The security of machine learning. Machine Learning, 81(2), 121–148 (2010).
9. Kulikova O.V.: Biometric cryptographic systems and their usage. Information technology security, 16(3), 53-58 (2009).
10. Chuikov A.V., Vulfin A.M., Vasiliev V.I.: A neural network system for converting user biometric features into a cryptographic key. In: Proceedings of Tomsk State University of Control Systems and Radioelectronics, 21(3) (2018).
11. Scheidat T., Vielhauer C., Dittmann J.: Biometric hash generation and user authentication based on handwriting using secure sketches. In: Image and Signal Processing and Analysis, 89-94, Proceedings of 6th International Symposium (2009).
12. Dodis Y., Reyzin L., Smith A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. Advances in Cryptology. In: Cachin C. and Camenisch J. (eds.), 3027, 79–100, Springer, Verlag (2004).
13. Turk M., Pentland A.: Face recognition using eigenfaces. Journal of Cognitive Neuroscience 3, 7286 (2001).
14. Dodis Y., Katz J., Reyzin L., Smith A.: Robust fuzzy extractors and authenticated key agreement from close secrets. Advances in Cryptology, 4117, 232–250, Springer, Verlag (2006).
15. Boyen X., Dodis Y., Katz J., Ostrovsky R., Smith A.: Secure remote authentication using biometric data. Advances in Cryptology. In: Cramer R. (ed.). LNCS, 3494, 147–163, Springer, Verlag (2005).
16. Sahai A., Waters B.: Fuzzy identity-based encryption. Proceedings of EUROCRYP. LNCS, 3494, 457–473, Springer, Verlag (2005).

17. Baek J., Susilo W., Zhou J.: New construction of fuzzy identity-based encryption. Proceedings of the 2nd ACM Symposium on Information, Computer and Communications Security, 368–370, USA, ACM New York (2007).
18. Fang L. et al.: Chosen-Ciphertext Secure Fuzzy Identity-Based Key Encapsulation without ROM. IACR Cryptology ePrint Archive 2008, 139 (2008).
19. Fang L., Xia J. Full Security: Fuzzy Identity Based Encryption. IACR Cryptology ePrint Archive, 307 (2008).
20. Yang P., Cao Z., Dong X.: Fuzzy Identity Based Signature. IACR Cryptology EPrint Archive 2008, 2 (2008).
21. Gray code https://ru.wikipedia.org/wiki/Код_Грея, last accessed 2020/12/24.
22. Tipping M.E., Bishop C.M.: Probabilistic principal component analysis. Journal of the Royal Statistical Society: Series B (Statistical Methodology), 61(3), 611-622 (1999).
23. Yuan Z.W., Zhang J.: Feature extraction and image retrieval based on AlexNet. In: Eighth International Conference on Digital Image, 10033, 100330E, International Society for Optics and Photonics (2016).
24. Kosko B.: Bidirectional associative memories. IEEE Transactions on Systems, man, and Cybernetics, 18(1), 49-60 (1988).