Cognitive security modeling of biometric system of neural network cryptography

Alexey Vulfin, Vladimir Vasilyev, Anastasia Kirillova and Andrey Nikonov

Ufa State Aviation Technical University, 12, K. Marks st., Ufa, 450008, Russian Federation
kirillova.andm@gmail.com

Abstract. The object of the research is a biometric authentication system based on neural network transformation of features into a cryptographic key. The analysis of the security of such systems is carried out using the methods of cognitive modeling. The use of the neural network transformation “biometrics-key” can significantly reduce the likelihood of a number of attacks by external intruders due to the distributed storage of the base of biometric images and allows the use of a secret cryptographic key generated on the basis of the image as the output vector of the neural network. To assess the security of the biometric system based on the ML model, an analysis of current threats, vulnerabilities and potential attack vectors was carried out. A fuzzy gray cognitive map is built for modeling and assessing local relative risks of information security in the event of an attacker without using and using the architecture of the ML model of the neural network transformation “biometrics-key”. The indicators of the local relative risk of a system malfunction and refusal to use it (breach of integrity) and modification of the base and ML model (breach of confidentiality) decreased by 45%.

Keywords: Biometric authentication system, Fuzzy gray cognitive map, Biometrics-key.

1 Introduction

Currently, traditional authentication methods (passwords and IDs) are no longer sufficient to ensure security - they have been replaced by integrated biometric systems embedded in an increasing number of devices (for example, FaceID and TouchID technologies in mobile devices). Today, there are two main areas of application of biometric methods: solving the problem of user authentication and their integration with cryptographic systems [1-3]. Cryptographic systems are much more secure than traditional biometric systems. One of their main disadvantages is the problem of ensuring reliable storage and correct use of secret cryptographic keys [1; 4].

Biometric authentication systems based on the use of artificial intelligence and machine learning technologies approximate a nonlinear functional display that allows the recognized biometric image to be attributed to one of the predefined classes. The machine learning models (ML models) used to solve this problem are very sensitive to changes in input data, which allows an attacker in some cases to influence the result of the biometric system by modifying the presented biometric images. A significant number of services operate on the basis of ML models that process biometric images, which is an important problem in ensuring information security of the system as a whole [5].

The purpose of the work is to provide a cognitive analysis of the security of a biometric authentication system based on a neural network transformation of biometric features into a cryptographic key.

To achieve the purpose, the following tasks were set:

- analysis of existing biometric cryptographic systems;
- security assessment of the neural network biometric authentication system based on cognitive modeling technologies.

2 Analysis of existing biometric cryptographic systems and methods for processing facial images

Existing biometric cryptographic systems using facial images as primary biometric features can be divided into three categories according to the nature of the cryptographic key processing (Table 1).

Table 1. Categories of biometric cryptographic systems.

	“key release cryptosystems”	“key binding cryptosystems”	“key generation cryptosystems”
Features	Biometric reference and key are stored separately	1) the cryptographic key and the biometric reference are linked by an algorithm for replacing a small number of secret bits with a cryptographic key; 2) correction codes are used; 3) fuzzy vault is the most common scheme.	1) the cryptographic key is extracted from the user's biometric data and is not stored in the database; 2) large artificial neural networks; 3) fuzzy extractors.
Advantages	Ease of implementation	The security of the method is due to the secrecy of the key closing and recovery algorithms	Cryptographic key is not stored in the database
Disadvantages	1) biometric standards are stored locally; 2) requires access to locally stored unsecured	1) deterministic key-closing algorithms can be compromised; 2) algorithms are difficult to implement due to the variability of biometric features.	1) high complexity of system implementation; 2) biometric data is inaccurately reproducible, which makes it difficult to use it as the

	and unencrypted biometric templates.		basis for sustainable key generation.
Vulnerabilities and attacks	An attacker has replaced the image comparison module with malware.	1) correlation attacks, attacks via record multiplicity – ARM; 2) surreptitious key-inversion attacks – SKI; 3) blended substitution attacks.	

For the subsequent analysis and application of the ML model in solving the problem of image classification, it is necessary to extract the vector of primary features from the generated biometric templates [6]. A possible taxonomy of methods for constructing vectors of primary formal features with an analysis of advantages and disadvantages is presented in Table 2.

Table 2. Features of methods for extracting and matching features.

Method name	Advantages	Disadvantages	Approach to constructing the primary feature vector
Elastic graph matching [5; 7]	identification accuracy reaches 95-97% even with a head position deviation of 15 degrees and with a change in emotional state	computational complexity; linear dependence of the running time on the size of the database of data images	approaches based on anatomical features
Face recognition techniques in 3D space [8-10]	high recognition accuracy; works independently of natural transformations due to facial features	increased requirements for shooting conditions and system computing resources	
Principal component analysis [11]	identification accuracy up to 95%; reduction in the dimensionality of the feature space	the effectiveness of the method decreases with varying object illumination	a holistic approach is the processing of the entire image area containing the face as a sequence of lines without taking into account individual anatomical features
Linear discriminant analysis [11]	splits images into classes better than principal component method	large training sample required	
Hopfield network	high speed of work; weak dependence of convergence on network dimension	small network capacity	
Convolutional neural network [11]	identification accuracy 96%; resistance to changes in scale, head displacement	it requires a very large training sample and significant computational resources to train a neural	

		network
Self-organizing two-dimensional Kohonen map [11]	resistance to noisy data; high learning rate; reduces the dimension of the input data	only works with real numeric vectors
Multilayer perceptron [11]	high generalizing ability; resistance to noise in the training set; high speed of work after training	the complexity of the selection of hyperparameters and network configuration; the difficulty of creating a good training sample; the likelihood of overtraining and undertraining
Histogram of oriented gradients [11]	does not depend on the size of the object (face)	sensitive to changes in object orientation in space
Support vector machine [11]	high speed of work	sensitive to noise in the training set
Algorithm for enhancing the composition of classifiers	good generalizing ability; simplicity of software implementation; high recognition accuracy	the possibility of retraining; great computational complexity
Methods Using Hidden Markov Models	high recognition accuracy; the possibility of complicating the model;	it is necessary to select the model parameters for each database; inability to track the internal state of the model

To generate keys based on biometric images, two main tools are used (Table 3) that meet the requirements of modern cryptography and have an acceptable estimate of the magnitude of the second type error [12-18]:

- neural network converter “biometrics-code” (Fig. 1, a);
- fuzzy extractors (Fig. 1, b).

Table 3. Key generation tools based on biometric images.

	Neural network converter “biometrics-code” [19, 20]	“fuzzy extractors” [1, 2, 20]
Features	A large artificial neural network of feedforward propagation with a large dimension of inputs and outputs and a small number of hidden layers, which transforms an ambiguous, fuzzy vector of input biometric parameters “our” into a unique code of a cryptographic	Uniquely recover the secret key from the fuzzy biometric image based on the helper data that is public.

	key, any other vector ("alien") into a random signal.	
Advantages	GOST R 52633-2006[†]: protection against attacks on the "last bit" of the decision rule.	the length of the generated key is specified as an algorithm parameter; no need to store a private key, but storage of auxiliary data is required; allows to get a single key from one set of biometric data
Disadvantages	Training requires significant computing resources and makes high demands on the quality of the training sample.	the quality of work corresponds to the quality of the applied error correction codes; fuzzy extractors are susceptible to the same classes of attacks as fuzzy containers

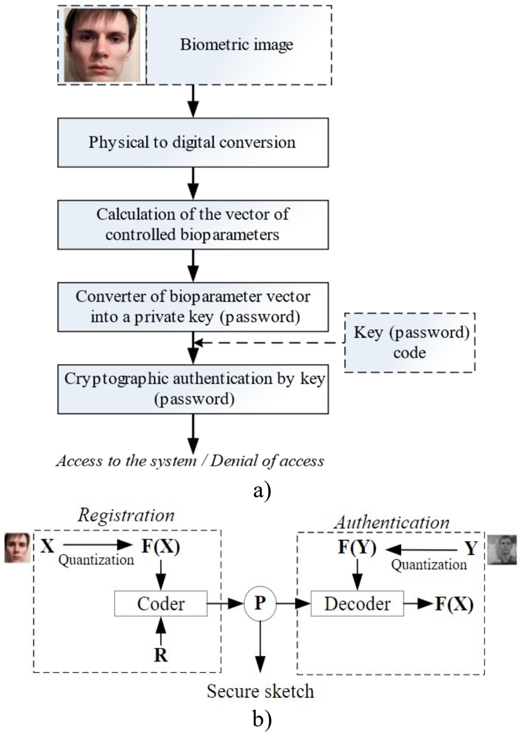


Fig. 1. The scheme of the neural network converter "biometrics-code" (a) and the fuzzy extractor (b).

[†] GOST R 52633-2006 3 Information protection. Information protection technology. Requirements for the means of high-reliability biometric authentication, http://docs.cntd.ru/document/1200048922, last accessed 2021/01/10.

X – the biometric template used during registration, F – the quantization function, R – the random noise introduced into the construction of the secure sketch, P – the generated secure sketch, Y – the biometric template used in the user authentication process.

A generalized scheme of the neural network system of biometric identification and authentication (NSBIA) of a person is shown in Fig. 2 and reflects the main stages of processing biometric information.

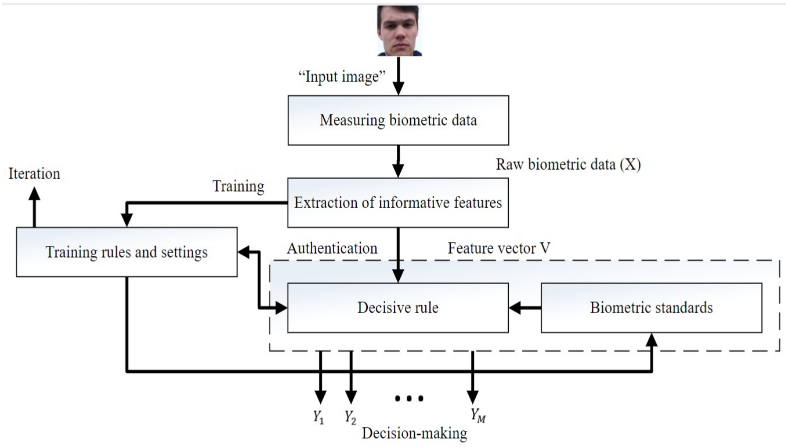


Fig. 2. Generalized scheme of a neural network system of biometric identification.

To store the database of biometric formed, the parameters of the neural network connection weights are used, which makes it possible to ensure the confidentiality of the biometric network system, since even a compromise of the neural network connection weights will not give the intruder information either about the users of the system, or the system itself. The only vulnerable element of the system is the output vector generated by the neural network, which makes it possible to assign the presented biometric image to one of the known classes. This type of attack on a biometric system is called an attack on the "last bit" of the decision rule [19], when an attacker presents an output vector to the information system, in which a unit in a specific line position indicates the class of a legitimate user of the system registered in the NSBIA. An attacker will gain access to the system under the guise of an existing user. A diagram of such an attack is shown in Fig. 3.

Consequently, the use of biometric systems based on this class of neural networks and other ML models with an open vector encoding the belonging of the input image to a certain class becomes problematic in open and weakly protected information systems.

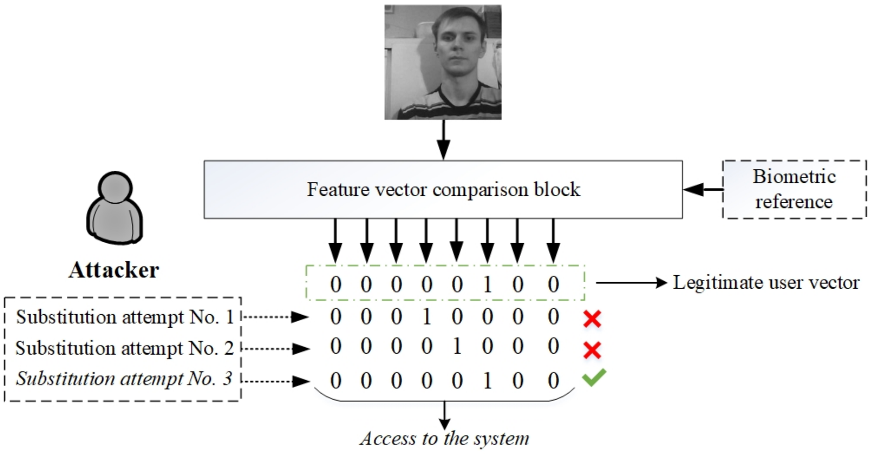


Fig. 3. Fragment of the attack scheme on the "last bit" of the decision rule.

The key for biometric identification and authentication systems are falsification of biometric data presented through the user interface and leakage from the database of biometric images[‡]. Vulnerabilities in the implementations of biometric identification and authentication systems can be divided into:

— vulnerabilities in used libraries and plug-ins;
— vulnerabilities in the program code;
— architectural vulnerabilities.
— Attacks on biometric images presented through the system user interface can be divided into two groups:
— non-targeted attack (a general type of attack when the main target is an incorrect classification result);
— targeted attack (the goal is to obtain a label of the required class for a given input image[§]).
— For systems using machine learning methods and technologies, there are two types of AML attacks (adversarial machine learning)[**]:
— evasion – an attacker causes the model to behave incorrectly. The system is viewed by the attacker as a black box. This type of attack is considered the most common

[‡] How vulnerable are biometric Big Data systems: causes of errors and their measurement metrics, https://www.bigdataschool.ru/blog/biometrics-vulnerabilities-big-data-ml.html

[§] Attacks on biometric systems, https://www.itsec.ru/articles/ataka-na-biometricheskie-sistemy

[**] How to deceive a neural network or what is an Adversarial attack, https://chernobrovov.ru/articles/kak-obmanut-nejroset-ili-chto-takoe-adversarial-attack.html

and includes spoofing attacks on biometric systems, when an attacker tries to disguise himself as another person.

- poisoning – an attacker seeks to gain access to the data and learning process of the ML model in order to disrupt the learning process. Poisoning can be thought of as malicious infection of training data. The attacker possesses information about the system (Adversarial Knowledge, AK): sources and algorithms for processing data for training, training algorithms and resulting parameters.

3 Security assessment of the authentication system with neural network conversion of biometric parameters into a cryptographic "private" key

The final structure of the identification and authentication system with neural network conversion of biometric parameters into a cryptographic "private" key is shown in Fig. 4.

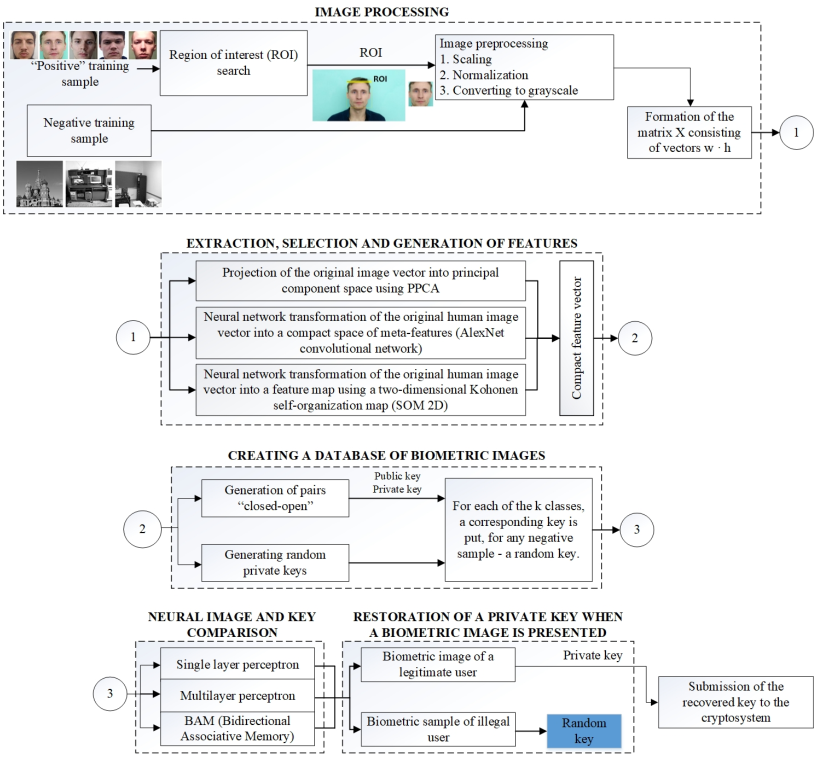


Fig. 4. The structure of a neural network biometric authentication system with a neural network transformation of biometric parameters into a cryptographic "private" key.

To assess the security of the system shall use the methodology for analyzing information security and cybersecurity based on fuzzy gray cognitive maps, detailed in [21].

Fuzzy gray cognitive map (FGCM) is a directed graph defined using a tuple of sets [21]:

$$\text{FGCM} = \langle \text{C, F, W} \rangle, \tag{1}$$

Where C – a set of concepts, which are significant factors (graph vertices), F – a set of connections between concepts (directed arcs), and W – a set of weights of FGCM connections, which can be both positive and negative for "strengthening" and "weakening" the influence of the concept, respectively.

The use of the algebra of "gray" numbers when specifying the set W allows the use of a fuzzy linguistic scale, considering the degree of confidence of the expert in the current assessment (Table 4). The state of concepts X will also be defined as a "gray" number at an arbitrary discrete moment in time $t \in N \cup \{0\}$:

$$X_i(t+1) = f\left(X_i(t) + \sum_{\substack{j=1 \\ (j \neq i)}}^{n} W_{ji} X_j(t) \right), \tag{2}$$

Where $X_i(t)$ and $X_i(t+1)$ – the values of the concept state variable at times t and $t+1$, n – number of concepts in FGCM, $f()$ – nonlinear concept function (hyperbolic tangent).

Table 4. Fuzzy linguistic scale for assessing the relationship between concepts (assessment of mutual influence).

Linguistic meaning	Range	Term designation
Not affect	0	Z
Very low	(0; 0,15]	VL
Low	(0,15; 0,35]	L
Middle	(0,35; 0,6]	M
High	(0,6; 0,85]	H
Very high	(0,85; 1]	VH

Potential threats[††] to information security and cybersecurity breaches and potential vulnerabilities of the neural network biometric authentication system are highlighted in Table 5.

[††] Database of information security threats FSTEC, https://bdu.fstec.ru/threat, last accessed 2021/01/10.

Table 5. Threats to information security and cybersecurity of a neural network biometric authentication system.

Threats from BDU FSTEC	Description	Prerequisites and implementation
UBI.218 Machine learning model information disclosure threat (breach of confidentiality)	Disclosure by the violator of information about the machine learning model used in the information (automated) system.	It is caused by the weaknesses of access differentiation in information (automated) systems using machine learning. Implementation is possible if the attacker has direct access to the machine learning model.
UBI.219 Training data theft threat (breach of confidentiality)	Possibility of theft by the violator of training data used in an information (automated) system that implements artificial intelligence technologies.	It is caused by weaknesses in the differentiation of access to training data used in the information (automated) system. Implementation is possible if the violator has direct access to the training data.
UBI.220 Threat of disrupting the functioning (“bypass”) of means that implement artificial intelligence technologies (breach of confidentiality)	Violation of the functioning (“bypass”) by the violator of the means that implement artificial intelligence technologies.	Due to the following reasons: – lack of necessary data in the training sample; – the presence of weaknesses in the ML model.
UBI.221 Threat of modifying a machine learning model by distorting (“poisoning”) training data (breach of integrity)	The possibility of modifying (distorting) a machine learning model used in an information (automated) system that implements artificial intelligence technologies.	Due to the following reasons: – disadvantages of the machine learning process implementation; – disadvantages of machine learning algorithms. Implementation is possible if the attacker has the ability to influence the machine learning process.
UBI.222 Threat of substitution of a machine learning model (breach of integrity, confidentiality)	The possibility of an intruder replacing a machine learning model used in an information (automated) system that implements artificial intelligence technologies.	It is caused by weaknesses in the differentiation of access in information (automated) systems that use machine learning. Implementation is possible if the attacker has direct access to the ML model.

In Table 6, the main vulnerabilities correspond to the $C_7 - C_9$ FGCM concepts. Threats $C_2 - C_6$ correspond to scenarios of exposure to an external attacker in the course of exploiting one or more system vulnerabilities. The assessment of local relative risks of violation of information security and cybersecurity of the NSBIA system was carried out for the most likely attack vectors. The corresponding FGCM is shown in Fig. 5.

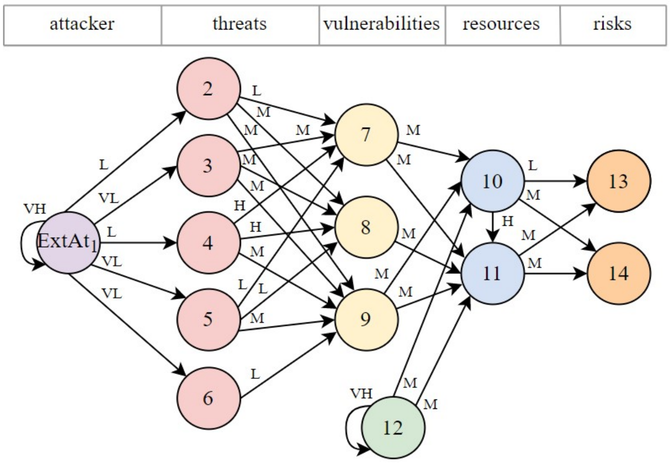


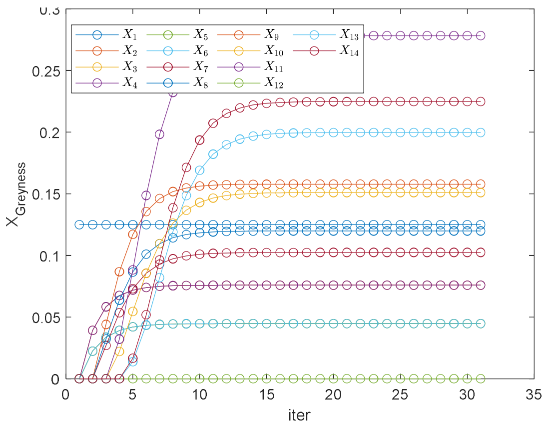
Fig. 5. Fuzzy cognitive map for assessing local relative risks of information security and cybersecurity breach NSBIA.

Table 6. Description of FGCM concepts.

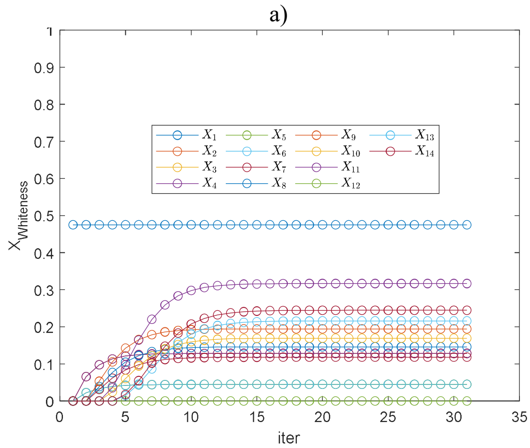
Concept	Name	Concept type
$ExtAt_1$	External attacker	Concept driver
C_2	ML model disclosure threat (UBI.218)	Threats
C_3	Training data theft threat (UBI.219)	
C_4	Threat of malfunctioning ML model (UBI.220)	
C_5	ML model modification threat (UBI.221)	
C_6	Threat of substitution of the ML model (UBI.222)	
C_7	Vulnerability of libraries and models (plugins)	Vulnerabilities
C_8	Vulnerability of the software implementation of the model	
C_9	Architectural vulnerabilities	
C_{10}	Base of biometric images	Target system resources
C_{11}	ML model	
C_{12}	Countermeasure based on the implementation of the neural network transformation "biometrics-key"	Concept driver
C_{13}	Violation of the system's performance and refusal to use it (breach of integrity)	Effects
C_{14}	Modification of the base and ML model (breach of confi-dentiality)	

Let us consider the scenario of an attacker's impact with and without using a countermeasure based on a neural network transformation “biometrics-key” to ensure information security and cybersecurity of the NSBIA.

Fig. 6 andFig. **7** below show the process of changing the state of FGCM concepts in the event of an attacker without using and using the implementation of the neural network transformation “biometrics-key” to ensure information security and cybersecurity of NSBIA as a defensive countermeasure.

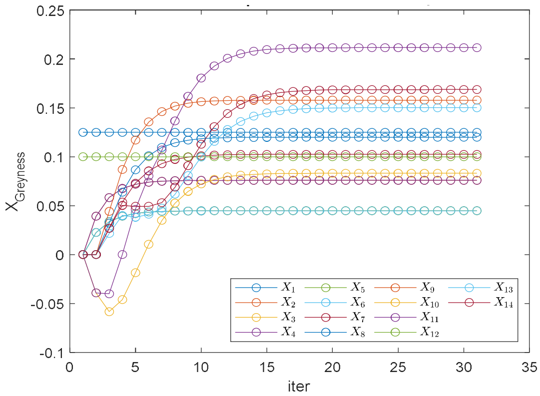


a)

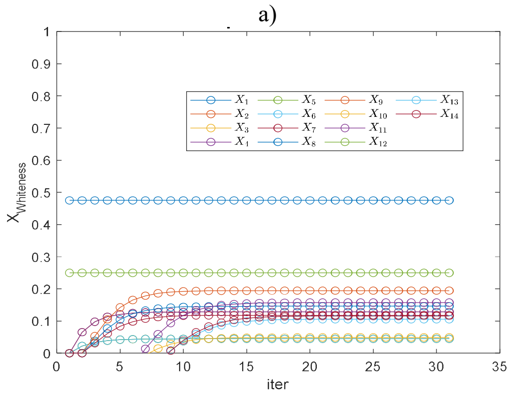


b)

Fig. 6. Change in time of the state of (a) “grayness” – the spread of the assessment, (b) “bleached” – the central meaning of the gray assessment) of concepts under the influence of an attacker without using the implementation of the neural network transformation “biometrics-key”.



a)



b)

Fig. 7. Change in time of the state of (a) "grayness" – the spread of the assessment, (b) "bleached" – the central meaning of the gray assessment) of concepts under the influence of an attacker and the application of a protective countermeasure based on the neural network transformation "biometrics-key".

Local relative risk indicators for target concepts C_{13}, C_{14} are shown in Table 7.

Table 7. Results of risk analysis based on FGCM.

Concept	without the use of neural network transformation "biometrics-key"	after applying the neural network transformation "biometrics-key"
Violation of the system's performance and refusal to use it (breach of integrity)	[0.0162; 0.4156]	[0.0442; 0.2560]
Modification of the base and ML model (breach of confidentiality)	[0.0199; 0.4694]	[0.0527; 0.2846]

4 Discussion

The use of cognitive analysis in the task of assessing information security and cybersecurity risks allows us to consider the range of opinions of experts, as well as the inaccuracy and incompleteness of the data collected during the audit on the state and properties of the information system. Cognitive models allow one to formalize the mutual influence of system elements and the destabilizing effects of internal and external abusers who exploit vulnerabilities of software and hardware components, which are a significant decision-making tool in the process of qualitative and quantitative assessments. Scenarios for modeling the impact of an attacker using a gray fuzzy cognitive map built based on expert data make it possible to assess the effectiveness of the applied protection tools and select the optimal combination of applied solutions, considering the identified threats and potential attack vectors on NSBIA, including ML models for processing biometric data.

5 Conclusion

The paper proposes an approach to the analysis of the security of integrated biometric authentication and identification systems based on gray fuzzy cognitive maps. A feature of the biometric system is the use of a neural network transformation "biometrics-key", which provides distributed storage of the base of biometric images and allows the use of a secret cryptographic key generated based on the image as an output of the neural network.

To assess the security of biometric authentication and identification systems using ML models, an analysis of current threats, vulnerabilities and potential attack vectors was carried out, on the basis of which a fuzzy gray cognitive map was built to assess local relative risks of ensuring information security and cybersecurity in the event of an attacker without using and using neural network transformation "biometrics-key". Local relative risk indicators for key information resources decreased by 45%.

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. Vasilyev, V.I.: Intelligent information security systems. 2nd edn. M.:Mashinostroenie, 199 (2012).
2. Kulikova, O.V.: Biometric cryptographic systems and their applications. Bezopasnost' informacionnyh tehnologij, 16(3), 53–58 (2009).
3. Merkushev, O. Yu., Sidorkina, I.G.: Use of biometric cryptography in a control system of access. Software & System, 4, 172–175 (2012).

4. Abu Elreesh, J.Y., Abu-Naser, S.S. Cloud Network Security Based on Biometrics Cryptography Intelligent Tutoring System. International Journal of Academic Information Systems Research (IJAISR), 3(3), 37–70 (2019).
5. Barreno, M. et al.: The security of machine learning. Machine Learning, 81(2), 121–148 (2010).
6. Turk, M., Pentland, A.: Face recognition using eigenfaces. In Journal of Cognitive Neuroscience, 3, 7286 (2001).
7. Wiskott, L. et al.: Face recognition by elastic bunch graph matching. IEEE Transactions on pattern analysis and machine intelligence, 19(7), 775–779 (1997).
8. Wagner, A. et al.: Toward a practical face recognition system: Robust alignment and illumination by sparse representation. IEEE transactions on pattern analysis and machine intelligence, 34(2), 372–386 (2011).
9. Paul, L.C., Al Sumam A.: Face recognition using principal component analysis method. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1(9), 135–139 (2012).
10. Bhele, S.G., Mankar, V.H.: A review paper on face recognition techniques. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 1(8), 339–346 (2012).
11. Ding, S. et al.: Evolutionary artificial neural networks: a review. Artificial Intelligence Review, 39(3), 251–260 (2013).
12. Dodis, Y. et al.: Robust fuzzy extractors and authenticated key agreement from close secrets. In: Dwork C. (Ed.) Annual International Cryptology Conference CRYPTO 2006, LNCS 4117, 232–250. Springer, Berlin, Heidelberg, (2006).
13. Boyen, X. et al.: Secure remote authentication using biometric data. In: Cramer, R. (Ed.) Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2005, LNCS 3494, 147–163, Springer, Berlin, Heidelberg (2005).
14. Sahai A., Waters B.: Fuzzy identity-based encryption. In: Cramer, R. (Ed.) Annual International Conference on the Theory and Applications of Cryptographic Techniques EUROCRYPT 2005, LNCS 3494, 457–473, Springer, Berlin, Heidelberg (2005).
15. Baek, J., Susilo, W., Zhou, J.: New constructions of fuzzy identity-based encryption. In: Proceedings of the 2nd ACM symposium on Information, computer and communications security, 368–370, ACM New York. NY, USA (2007).
16. Fang, L. et al.: Chosen-Ciphertext Secure Fuzzy Identity-Based Key Encapsulation without ROM. IACR Cryptology ePrint Archive 2008, 139–151 (2008).
17. Fang, L., Xia, J.: Full Security: Fuzzy Identity Based Encryption. IACR Cryptology ePrint Archive, 307 (2008).
18. Yang, P., Cao, Z., Dong, X.: Fuzzy Identity Based Signature. IACR Cryptology EPrint Archive, 2 (2008).
19. Vasilyev, V.I. et al.: Analysis of confidential data protection in critical information infrastructure and the use of biometric, neural network and cryptographic algorithms (standards review and perspectives). Informacionnye tehnologii i sistemy, 193–197 (2019).
20. Juels, A., Sudan, M.: A fuzzy vault scheme. Designs, Codes and Cryptography, 38(2), 237–257 (2006).
21. Salmeron, J.L.: A Fuzzy Grey Cognitive Maps-based intelligent security system. 2015 IEEE International Conference on Grey Systems and Intelligent Services (GSIS). IEEE, 29–32 (2015).