Method of Detecting Special Points on Biometric Images based on New Filtering Methods

Mariia Nazarkevych[a], Volodymyr Hrytsyk[a], Yaroslav Voznyi[a], Andrii Marchuk[a], and Olha Vozna[b]

[a] *Lviv Polytechnic National University, 12 Stepan Bandera str., Lviv, 79013, Ukraine*
[b] *Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies, 50 Pekarska str., Lviv, 79010, Ukraine*

Abstract
Artificial intelligence in the recognition of biometric images has great advantages of use because it works with big data and provides high speed. One of the common tasks of modern artificial intelligence is image recognition, including biometric image recognition and object detection. It is analyzed that the main approaches to fingerprint recognition are comparisons by special points; correlation comparison; pattern matching; pattern comparison, graph-based comparison. Ateb-Gabor filtering and selection of special points were performed. Experiments were performed with the selection of special points and it was shown that the images are better. Filtration results are based on PSNR and MSE. Visual filtering is shown as research results. Ateb-Gabor filters give a strong reaction at those points of the image where there is a component with local features of frequency in space and orientation. An experiment was performed with Ateb-Gabor and Gabor fingerprint filtering based on the freely available NIST Special Database 302. The results of the experiments showed that as a result of correlation, the images change significantly the higher the values of the parameters m, n, σ is laid down. When creating the biometric protection system, the results of filtration by Ateb Gabor showed good time and characteristics and recognition properties

Keywords
Image processing, filtration, biometric images, identification, filtering.

1. Introduction

Artificial intelligence studies methods of solving problems that require human understanding. Evolving from research into pattern recognition and computational learning theory in the field of artificial intelligence, machine learning explores the study and construction of algorithms that can learn and make predictions from data—such algorithms overcome strictly static program instructions, making data-driven predictions or decisions by building models with selective inputs [1].

Speaking of today, the field of artificial intelligence is dominated by such areas as working with big data [2], machine learning, deep learning related to the development of neural networks, training with reinforcement.

Algorithms are the driving forces behind the development of modern artificial intelligence - they are certain mathematical models used in computer science [3]. Another point is the accumulation of big data thanks to the power of modern computers. Companies and each of us have begun to accumulate a lot of data, and they are all food for algorithms that allow us to obtain certain practical solutions and results based on this data. However, all these studies are possible only with good computing power. Cheaper CPUs and the availability of computers as such essentially allow everyone to take certain actions to analyze or work with data.

Cybersecurity Providing in Information and Telecommunication Systems, January 28, 2021, Kyiv, Ukraine
EMAIL: mariia.a.nazarkevych@lpnu.ua (A.1); volodymyr.v.hrytsyk@lpnu.ua (A.2); voznyyy@outlook.com (A.3); camacomua13@gmail.com (A.4); voznaseniv.olha@gmail.com (B.4)
ORCID: 0000-0002-6528-9867 (A.1); 0000-0002-9696-5805 (A.2); 0000-0002-5481-9973 (A.3); 0000-0001-5871-7053 (A.4); 0000-0003-1750-6465 (B.4)

The main engine of modern artificial intelligence is also deep learning and machine learning, which are based on two main principles - pattern recognition (pattern recognition) and multi-iterative learning, ie the creation of a mathematical model that is programmed and learned from data [4]. which she receives. The main task of this principle is to find correlations, ie relationships between different data.

Modern artificial intelligence often works with visual measurements and images. This is explained, firstly, by cognitive-psychological factors, because the visual channel for people is the most important in the perception of reality. In addition, we have a biological plane—the area of the neocortex that is responsible for processing visual information, the most studied by scientists. The creation of modern artificial neural networks essentially reproduces the work of these visual parts. Cognitive sciences have significantly influenced the creation of artificial neural networks, and hence the development of artificial intelligence. Now we see the opposite effect—knowledge of how artificial neural networks work, allows us to deepen our understanding of the functioning of the human brain.

One of the typical tasks of modern artificial intelligence is image recognition - for example, face detection in photographs or posture (pose detection). Another point is the discovery of objects. This approach is now widely used for self-driving car technology, which has to recognize objects on the road in real-time [5]. Artistic style transfer-ring is a very popular approach when we apply the style and patterns of paintings by famous artists to certain images. Artificial image creation is the ability of artificial neural networks to create images at your request, including images of people who never existed [6]. This technology raises perhaps the most ethical questions and debates in society. Derived from this is also the emergence of the phenomenon of Deep Fake—the creation of false content, images, and videos [7]. Such Deep Learning technologies can be used, for example, in various political configurations - when you need, for example, to denigrate a politician or political force.

2. Methods of Highlighting Special Points on Fingerprints

Among the variety of existing approaches for fingerprint recognition, there are several, the most commonly used [8]:

- Comparison on special points.
- Correlation comparison.
- Pattern matching.
- Pattern comparison.
- Comparison based on graphs.

When comparing by special points, a pattern is formed on which the endpoints and branching points are highlighted. The scanned image of the print also highlights special dots, which are compared with the template [9]. The main advantage of this algorithm is the speed of its operation and ease of implementation. The disadvantages of the algorithm for comparison at special points include high requirements for image quality and sensor size.

The essence of the method of correlation comparison is that the obtained fingerprint is superimposed on each standard from the database in turn, after which the difference between them is calculated by pixels [10]. The comparison process should include many iterations, in each of which the image is rotated at a small angle or slightly shifted. Therefore, this method is the slowest and requires high computing power.

The pattern matching algorithm takes into account not only individual points but also the general characteristics of the fingerprint, such as the thickness of the strips, their curvature or density. The advantages of this method are that it can work with a lower quality print. However, this method is not suitable for many searches in the database.

The method of comparison by pattern uses the structure of the papillary pattern. The resulting image is divided into many small axes-rows, in each of which the location of the lines is described by the parameters of the sonic wave. The imprint obtained for comparison is aligned and reduced to the same type as the template. The main advantages of this algorithm are a fairly high speed and low requirements for image quality [11].

3. Development of a Method for Comparing Fingerprints

Comparison of fingerprints is carried out on search of special points on images, a search of the corresponding reference points on images, the definition of values of attributes of special points on images [12]. As a result, we decide that the images are identical if these images have a certain common set M of the same corresponding singular points [13].

The built rule should work on new data to be entered into the system, and the number of corresponding pairs of points is equal to the smaller of the two total numbers of special points in the images. Therefore, search for the corresponding singular points by selecting from the set M the largest subset MO and M spatially compatible pairs of singular points, perform the alignment of the singular points of the first image with the special points of the second image. Subsequently, by coinciding their reference points and rotating the special points of one of the images around the reference point in this image, calculate the total number of special points of the two compared images in the overlap of these images and decide that the two compared images are identical based on the number of corresponding points found. , as well as the total number of special points in the area of overlap of these two images.

There is a way that the two images being compared are fingerprints of one finger by calculating the degree of closeness of these images by the formula:

$$sim = \frac{identical}{\sqrt{k_1 \cdot k_2}} \tag{1}$$

where identical, k_1, k_2 respectively, the number of found corresponding points and the total number of special points of the two images in the area of their overlap, and comparing the calculated degree of proximity with a predetermined limit value.

We can say that the images are identical if their reference points on the two compared images are from the number of special points that correspond to the ends of branches of papillary lines.

You can also search for singular points by searching for the set M of pairs of corresponding points by constructing a complete bipartite graph, the left and right vertices of which correspond to special points of the first and second compared images, and graph arcs—the sum of weighted differences of vertex attributes connected by this arc. and finding the optimal markup of the vertices of this bipartite graph.

You can also define the overlap area of two images that are compared as one that is the overlap of the convex hulls of the sets of singular points in these images.

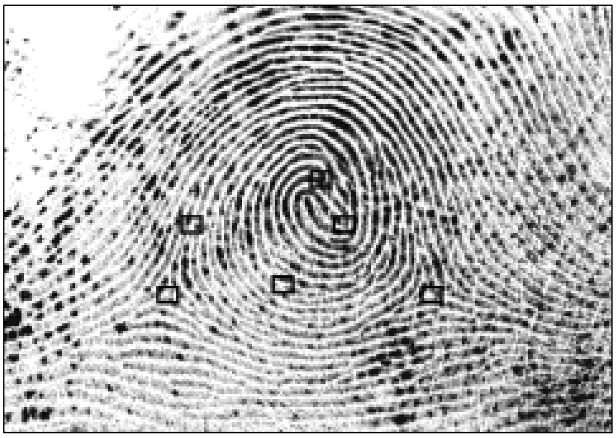


Figure 1: Example of marking special points of a fingerprint

From the points obtained in the previous stages, an array of objects with the following parameters is formed: the coordinates of the point; line type; the angle formed by them. The set of special point parameters obtained from the scanned fingerprint is compared with the set of reference parameters of fingerprints of registered RU users. The next step is to determine the deviations in the values of these parameters. A large deviation threshold will increase the probability of a false match between the biometric characteristics of two users—FAR (False Acceptance Rate). On the other hand, the small value of the tolerance is the reason for the increased probability of failure of the legitimate user RU—

FRR (False Rejection Rate) [14]. The problem of choosing the tolerance threshold is associated with the deformation and displacement of the finger during scanning, which leads to obtaining different parameters of the extracted points [15]. As a result of the research, it was found that it is advisable to keep information about the combination of three special points. Such a structure—called a triplet, is shown in Fig. 2.

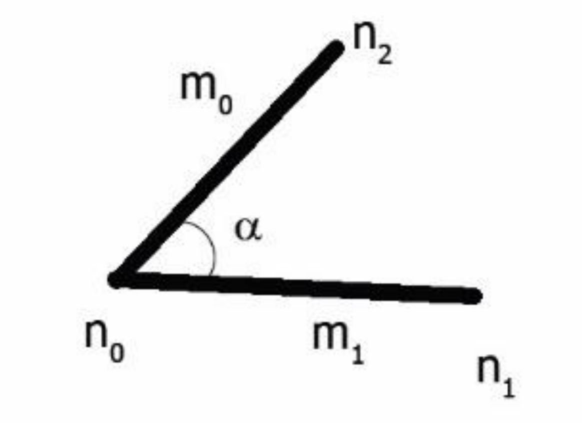


Figure 2: Construction of a triplet

For each central point n_0 (xn_0, yn_0) and two adjacent n_1 (xn_1, yn_1) and n_2 (xn_2, yn_2) a parameter vector is formed, see Fig.3.

Figure 3: Formation of vector parameters

The algorithm shows the mask training procedure for each browser pair [16]. We take a rough search: which is the most effective, but the most effective and complete. Due to the small size of the training data, we realize this brute force is possible and gives the best result. In particular, we first list each pair of browsers and then all possible masks (line 4). For each mask, we review the training data and make sure that we choose a mask that deploys stability between browsers, multiplying the uniqueness [17].

We will form a fingerprint on the server-side based on hashes on the client-side of the task [18]. As already mentioned, a fingerprint is a hash that is calculated from the AND operation of the hash list of all tasks and a mask. The mask is a fingerprint for a single browser and is calculated from two cross-browser fingerprint masks.

4. Comparison of Selected Special Points using Machine Learning

We have at our disposal (Fig. 4) a finite number of data—a training sample. Each element is described by a set of features *x* ("feature vector"). For each vector of parameters *x*, the answer *y* is known.

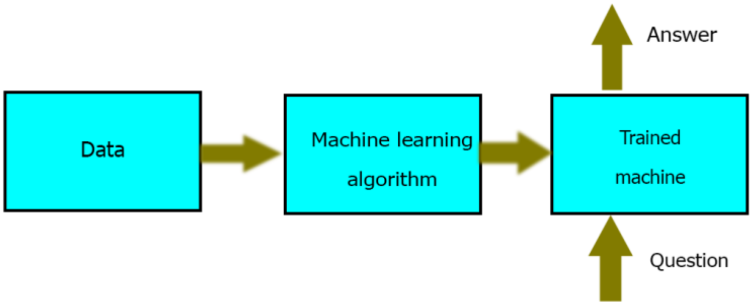


Figure 4: Scheme of machine learning to identify a person from biometric data

The problem of machine learning is that we need to construct a function *y* = *f*(*x*) from the vector of signs *x*, which gives the answer *y* for any possible observation *x*.

5. Ateb-Gabor Filtering and Selection of Special Points

Table 1
Comparison of filtered images by Gabor and Ateb-Gabor filter PSNR and MSE

Ateb filtering	Comparison	Filtration time	PSNR	MSE
		Sample 1		
m1n1 σ=pi	m1n1 σ=pi	1min 54s	361.20	—
m0.9n1 σ=pi	m1n1 σ=pi	1min 55s	38.77	24
m0.8n1 σ=pi	m1n1 σ=pi	1min 54s	33.06	9.15
m0.7n1 σ=pi	m1n1 σ=pi	1min 54s	29.66	8.21
m0.6n1 σ=pi	m1n1 σ=pi	2min 3s	27.08	7.49
m0.5n1 σ=pi	m1n1 σ=pi	1min 57s	24.95	6.91
m0.4n1 σ=pi	m1n1 σ=pi	2min 01s	23.35	6.46
m0.3n1 σ=pi	m1n1 σ=pi	1min 53s	22.20	6.14
m0.2n1 σ=pi	m1n1 σ=pi	1min 55s	20.83	5.77
m0.1n1 σ=pi	m1n1 σ=pi	2min 11s	19.35	5.35
m1n1σ=pi/4	m1n1σ=pi	2min 18s	12.77	3.14
m1n1σ=pi/3	m1n1σ=pi	2min 03s	3.61	3.54
m1n1σ=pi/2	m1n1σ=pi	2min 15s	4.03	14.55
m1n1σ=2*pi	m1n1σ=pi	2min 15s	4.72	17.07
m1n1σ=3*pi	m1n1σ=pi	1min 58s	4.25	15.35
m1n1σ=4*pi	m1n1σ=pi	2min 03s	3.94	14.25

Ateb filtering	Comparison	Filtration time	PSNR	MSE
		Sample 3		
m0.9n1 σ=pi	m1n1σ=pi	1min 56s	37.33	10.34
m0.8n1 σ=pi	m1n1σ=pi	1min 56s	31.71	8.78
m0.7n1 σ=pi	m1n1σ=pi	1min 56s	28.75	7.96
m0.6n1 σ=pi	m1n1σ=pi	1min 49s	26.60	7.36
m0.5n1 σ=pi	m1n1σ=pi	1min 47s	24.98	6.92
m0.4n1 σ=pi	m1n1σ=pi	1min 52s	23.84	6.60
m0.3n1 σ=pi	m1n1σ=pi	—	—	—
m1n1σ=pi/4	m1n1σ=pi	1min 40s	2.65	9.58
m1n1σ=pi/3	m1n1σ=pi	1min 46s	2.73	9.86
m1n1σ=pi/2	m1n1σ=pi	1min 30s	3.27	11.83
m1n1σ=2*pi	m1n1σ=pi	1min 40s	4.76	17.21
m1n1σ=3*pi	m1n1σ=pi	1min 43s	4.28	15.49
m1n1σ=4*pi	m1n1σ=pi	1min 36s	4.50	16.26
m1n1σ=4.4*pi	m1n1σ=pi	1min 36s	4.61	16.67
m1n1σ=4.5*pi	m1n1σ=pi	1min 36s	4.63	16.72
		Sample 5		
m0.9n1 σ=pi	m1n1 σ=pi	1min 36s	31.49	8.72
m0.8n1 σ=pi	m1n1σ=pi	1min 55s	31.49	8.72
m0.7n1 σ=pi	m1n1σ=pi	1min 34s	28.43	7.87
m0.6n1 σ=pi	m1n1σ=pi	1min 34s	26.37	7.87
m0.5n1 σ=pi	m1n1σ=pi	1min 40s	24.86	6.88
m1n1σ=pi/4	m1n1σ=pi	1min 34s	12.51	3.46
m1n1σ=pi/3	m1n1σ=pi	1min 34s	12.52	3.47
m1n1σ=pi/2	m1n1σ=pi	2min 02s	12.70	3.52
m1n1σ=2pi	m1n1σ=pi	1min 25s	22.28	6.17
m1n1σ=3pi	m1n1σ=pi	1min 24s	19.54	5.41
m1n1σ=4pi	m1n1σ=pi	1min 24s	17.59	4.87
m1n1σ=4.1pi	m1n1σ=pi	1min 25s	17.40	4.82
m1n1σ=4.2pi	m1n1σ=pi	1min 24s	17.22	4.76
m1n1σ=4.3pi	m1n1σ=pi	1min 30s	17.04	4.72
		Sample 6		
m1n1σ=3*pi	m1n1σ=pi	1min 31s	38.99	10.79
m1n1σ=4*pi	m1n1σ=pi	1min 34s	33.20	9.19
m1n1σ=4.4*pi	m1n1σ=pi	1min 33s	30.63	8.48
m1n1σ=4.5*pi	m1n1σ=pi	1min 42s	28.34	7.84
m0.5n1 σ=pi	m1n1σ=pi	1min 42s	26.42	7.31
m0.4n1 σ=pi	m1n1σ=pi	1min 48s	25.12	6.95
m0.3n1 σ=pi	m1n1σ=pi	1min 38s	24.02	6.65
m0.2n1 σ=pi	m1n1σ=pi	1min 48s	23.04	6.37
m0.1n1 σ=pi	m1n1σ=pi	1min 38s	22.09	6.11

The Ateb-Gabor filter [20] is a product of the Gaussian and periodic Ateb function, which predicts the improvement of monotonic areas of periodic images. In the case of fingerprints, it is assumed that the periodicity of the lines and the standard deviation is consistent mainly with the local characteristics of the image [21]. Ateb-Gabor filters give a strong reaction at those points of the image where there is a component with local features of frequency in space and orientation [22].

A two-dimensional Ateb-Gabor filter is used for image filtering. It is a harmonic function multiplied by the Gaussian function. The two-dimensional Ateb-Gabor filter has the form

$$G(x, y, \lambda, \theta, \psi, \sigma, \varphi) = \exp\left(\frac{-x'^2+\varphi^2 y'^2}{2\,\sigma^2}\right) ca\left(m, n, 2\prod, \theta, \frac{x'}{\lambda + \psi}\right) \quad (2)$$

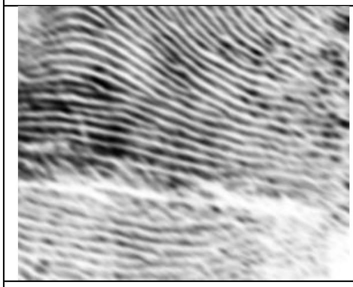
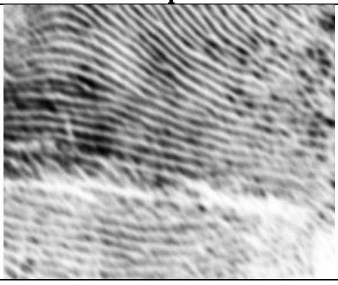
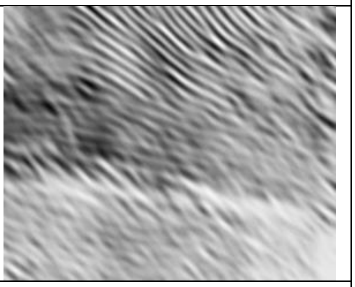
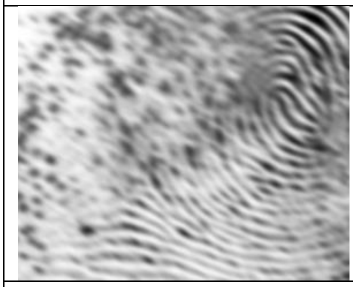
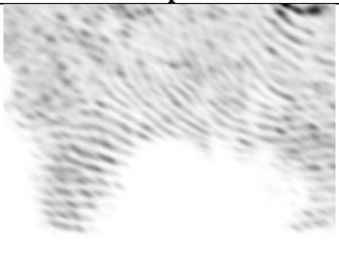
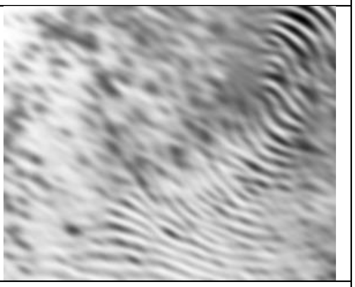
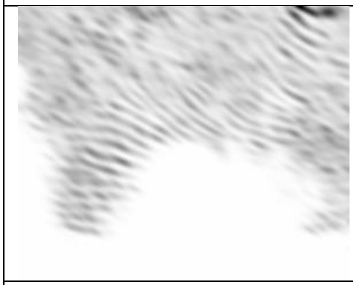
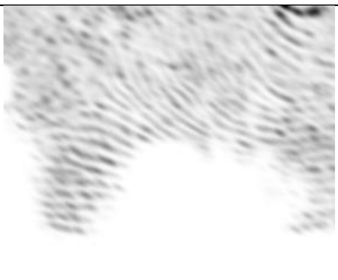
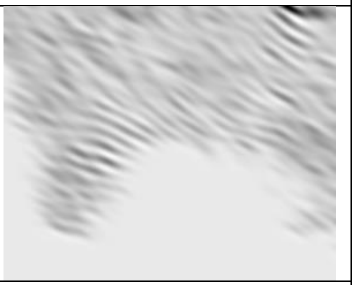
where

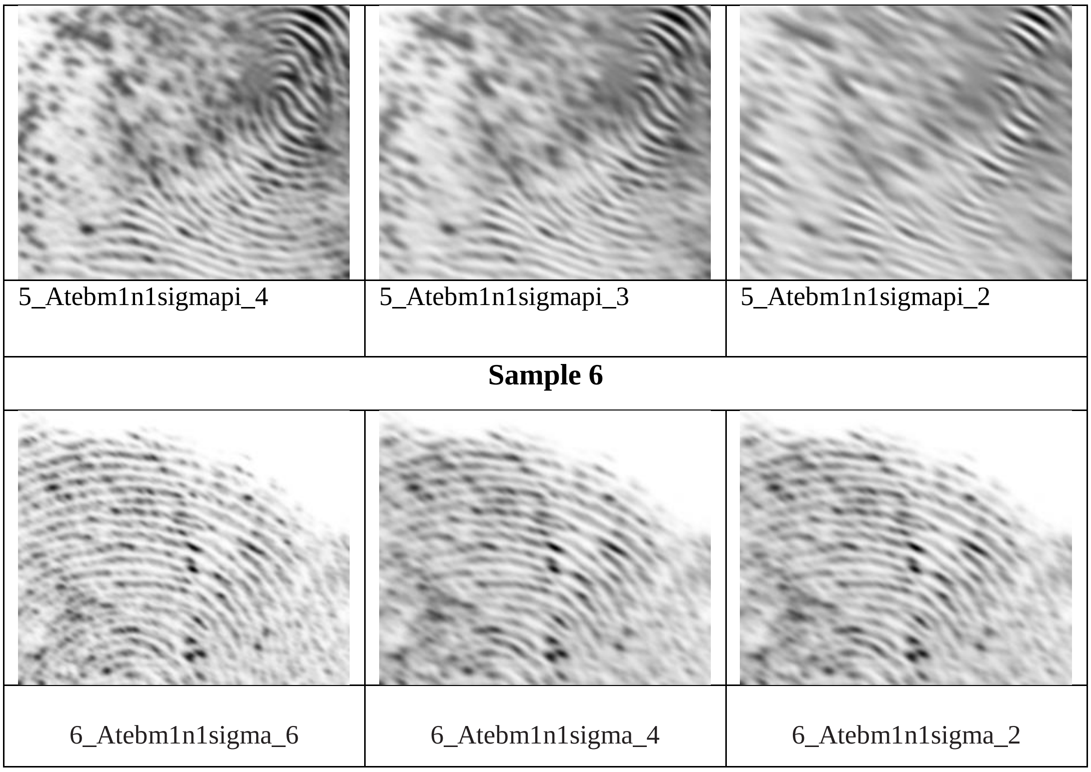
$$x' = x \cos \theta + y \sin \theta$$

$$y' = -x \sin \theta + y \cos \theta /$$

In this equation, λ is the wavelength of the cosine multiplier, θ is in degrees, ψ is the phase shift in degrees, and φ is the compression ratio [23], m, n are the parameters of the Ateb function, 2 is the period of the Ateb function [24].

An experiment was performed with Ateb-Gabor and Gabor fingerprint filtering based on the freely available NIST Special Database 302. The results of the experiments showed that as a result of correlation, the images change significantly the higher the values of the parameters m, n, σ are embedded.

Sample 1		
		
Atebm1n1sigmapi1_3	Atebm1n1sigmapi0_25	Atebm1n1sigmapi0_5
Sample 3		
		
3_Atebm1n1sigma4pi	3_Atebm1n1sigmapi_3	3_Atebm1n1sigma4pi
		
3_Atebm1n1sigmapi_3	3_Atebm1n1sigmapi_4	3_Atebm1n1sigmapi_2
Sample 5		



5_Atebm1n1sigmapi_4 5_Atebm1n1sigmapi_3 5_Atebm1n1sigmapi_2

Sample 6

6_Atebm1n1sigma_6 6_Atebm1n1sigma_4 6_Atebm1n1sigma_2

Figure 5: The results of experiments

6. Conclusions

Artificial intelligence systems for biometric images with deep learning and machine learning, based on the basic principles of pattern recognition and multi-iteration learning, ie the creation of a mathematical model that is programmed and learned from the data it receives, are analyzed.

Comparison of fingerprints is carried out on search of special points on biometric images, a search of the corresponding reference points on images, the definition of values of attributes of special points on images.

The results of the experiments were tested on the freely available NIST Special Database 302. The filtering results are based on PSNR and MSE. Recognition indicators showed good results.

7. References

[1] R. Toorajipour, V. Sohrabpour, A. Nazarpour, P. Oghazi, M. Fischl, Artificial intelligence in supply chain management: A systematic literature review, Journal of Business Research, 122 (2021) 502–517.

[2] J. G. Greeno, H. A. Simon, Problem solving and reasoning (No. UPITT/LRDC/ONR/APS-14), Pittsburgh univ pa learning research and development center 1984.

[3] A. Gomez-Perez, V. R. Benjamins, Applications of ontologies and problem-solving methods. AI Magazine 20 (1999) 119.

[4] W. F. Clocksin, Artificial intelligence and the future. Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences 361 (2003).) 1721–1748.

[5] N. M. Avouris, L. Gasser, (Eds.), Distributed artificial intelligence: Theory and praxis, Springer Science & Business Media 5 (1992).

[6] V. Khavalko, I. Tsmots, Image classification and recognition on the base of autoassociative neural network usage, in: 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2019, pp. 1118–1121.

[7] V. Hrytsyk, A. Grondzal, A. Bilenkyj, Augmented reality for people with disabilities, in: Proceedings of the International Conference on Computer Sciences and Information Technologies, CSIT 2015, pp. 188–191.

[8] E. Zhu, X. Guo, J. Yin, Walking to singular points of fingerprints. Pattern Recognition, 56 (2016) 116–128.

[9] J. Zhou, F. Chen, J. Gu, A novel algorithm for detecting singular points from fingerprint images, IEEE transactions on pattern analysis and machine intelligence 31 (2008) 1239–1250.

[10] D. Peralta, I. Triguero, S. García, Y. Saeys, J. M. Benitez, F. Herrera, Distributed incremental fingerprint identification with reduced database penetration rate using a hierarchical classification based on feature fusion and selection. Knowledge-Based Systems 126 (2017) 91–103.

[11] A. Ross, J. Shah, A. K. Jain, From template to image: Reconstructing fingerprints from minutiae points, IEEE transactions on pattern analysis and machine intelligence 29 (2007) 544–560.

[12] A. J. Jacob, N. T. Bhuvan, S. M. Thampi, Feature level fusion using multiple fingerprints, International Journal on Computer Applications, Special Issue on Computational Science--New Dimensions & Perspectives (2011).

[13] K. Nandakumar, A. K. Jain, S. Pankanti, Fingerprint-based fuzzy vault: Implementation and performance. IEEE transactions on information forensics and security 2 (2007) 744–757.

[14] M. Vatsa, R. Singh, A. Noore, Reducing the false rejection rate of iris recognition using textural and topological features, Journal of Signal Processing 2 (2005).

[15] O. Riznyk, O. Povshuk, Y. Kynash, I. Yurchak, Composing method of anti-interference codes based on non-equidistant structures, in: XIIIth International Conference on Perspective Technologies and Methods in MEMS Design (MEMSTECH), 2017, pp. 15–17.

[16] Q. A. Hadi, Vein palm recognition model using fusion of features. Telkomnika 18 (2020) 2921–2927.

[17] T. Nishimura, H. N. Patel, S. Wang, G. A. Upadhyay, H. L. Smith, C. Ozcan, R. Tung, Prognostic Value of Cardiac Magnetic Resonance Septal Late Gadolinium Enhancement Patterns for Periaortic Ventricular Tachycardia Ablation: Heterogeneity of the Anteroseptal Substrate in Nonischemic Cardiomyopathy, Heart Rhythm 18 (2020) 579–588.

[18] V. Buriachok, V. Sokolov, M. T. Dini, Research of caller id spoofing launch, detection, and defense, Cybersecur. Educ. Sci. Tech. 3 (2020) 6–16. doi:10.28925/2663-4023.2020.7.616.

[19] T. Radivilova, D. Ageyev, N. Kryvinska, (Eds.), Data-Centric Business and Applications: ICT Systems-Theory, Radio-Electronics, Information Technologies and Cybersecurity 5 (2020).

[20] M. Nazarkevych, N. Lotoshynska, I. Klyujnyk, Y. Voznyi, S. Forostyna, I. Maslanych, Complexity Evaluation of the Ateb-Gabor Filtration Algorithm in Biometric Security Systems, in: IEEE 2nd Ukraine Conference on Electrical and Computer Engineering (UKRCON), 2019, pp. 961–964.

[21] M. Nazarkevych, M. Logoyda, O. Troyan, Y. Vozniy, Z. Shpak, The Ateb-Gabor Filter for Fingerprinting, in: International Conference on Computer Science and Information Technology, 2019, pp. 247–255.

[22] M. Nazarkevych, N. Lotoshynska, V. Brytkovskyi, S. Dmytruk, V. Dordiak, I. Pikh, Biometric Identification System with Ateb-Gabor Filtering, in: XIth International Scientific and Practical Conference on Electronics and Information Technologies (ELIT), 2019, pp. 15–18.

[23] M. Logoyda, M. Nazarkevych, Y. Voznyi, S. Dmytruk, O. Smotr, Identification of Biometric Images using Latent Elements, 2010. CEUR-WS.org, online CEUR-WS.ORG/Vol-2488/paper8.pdf

[24] M. Nazarkevych, Y. Voznyi, S. Dmytryk, Wavelet transformation Ateb-Gabor filters to biometric images. Cybersecur. Educ. Sci. Tech. 3 (2020) 115-130. doi:10.28925/2663-4023.2020.7.616.