Identification of Biometric Images using Latent Elements

Mariya Nazarkevych[1][0000-0002-6528-9867] , Mykola Logoyda[1][0000-0002-6528-9867] ,

Serhii Dmytruk [1][0000-0001-6434-2817] Yaroslav Voznyi [1][0000-0002-5481-9973],

and Olga Smotr [2][0000-0003-2767-5019],

[1] Publishing Information Technology Department,
Institute of Computer Science and Information Technologies
Lviv Polytechnic National University
12 Bandery str., Lviv, 79013, Ukraine
mariia.a.nazarkevych@lpnu.ua
[2] Department of project management, information technologies, and telecommunications of
Lviv State University of Life Safety, Lviv, Ukraine

Abstract. The identification method of biometric images is developed where the filtration using Ateb-Gabor was implemented. Attacks that act on a biometric system were analyzed, and an attempt to counter these attacks was made. While applying skeletonization, we proposed to use a wave algorithm. It forms a ridge of minucius in the center of mass. This method of filtering has more opportunities than the traditional Gabor filter. A new filtering method has been developed that extends the existing filtering methods for prints. The method is based on Ateb-filtering, which increases the capabilities of standard filters because it is based on differential equations with degree of nonlinearity. Since it is based on Ateb-functions, which have more extensive properties than classical trigonometry. Such kind of filtration gives a solution to a problem that is clearly defined in specific parts of the area, both in the spatial and in frequency domains.

Keywords: Gabor filter, Ateb function, biometric system, image processing, filtering.

1 Introduction

The most common static method of biometric identification is the comparison of fingerprint [1]. A fingerprint is a unique pattern of a finger of an individual. This feature is the basis of this method. The fingerprint, which was received by a special scanner converted into a digital code and compared with the previously entered standard.

Biometric technologies are very vulnerable to hacking attacks. Because hackers can crack the biometric passport chip and access the information stored on it. Source [2] investigated attacks on the database of biometric passports In [3] it was found that

2019 IDDM Workshops.

45.5% of respondents attacked brute force of attack, therefore, when designing a security system, special attention should be paid to protecting the server system to obtain the database for biometric templates. 33.3% showed password recovery because a hacker could hack and recover a password from a stored system to access unauthorized files. 15.2% indicated that the attack was carried out as a result of eavesdropping. An eavesdropper is a hacker who secretly listens to a communication link and interrupts messages through digital devices such as RFID chips.

Specifically, there were attempts to break and clone a biometric passport of a US citizen. You can record any arbitrary information on the chip or block it completely [4].

Another perspective is medical. Hackers can hack medical devices implanted in a person's body. By breaking, for example, the Merlin @ home system [5] that controls the pacemaker, hackers can send any command, including stopping the heart. One only has to dream that the next generation of implants will be more secure and secure; for example, the patient will carry encryption keys in his body [6].

Thus, today, the effectiveness of biometric technologies in the context of foreign policy security seems controversial. The development of modern information technologies makes it possible to bypass the security system, which puts new tasks before information security [7].

Human control and surveillance [8]. According to human rights activists, biometric technologies are exacerbating human rights issues. The person will carry a document that will allow him to track his movements. The state will know everything - where the person doing it, who its friends are. This technology can become a kind of instrument of total control and monitoring of the person by the state authorities.

Interference with the privacy of citizens [9]. According to human biometrics, specialists can determine a person's health, identify congenital or acquired illnesses, evaluate a person's abilities and aptitudes that can be used for a variety of purposes: from health insurance withdrawal to employment discrimination.

The problem of storing biometric databases of citizens [10]. Numerous cases of theft of such databases by hackers and their subsequent sale to business entities or fraudsters are known to be able to use a person's data, including name and date of birth, place of residence, passport numbers, health insurance cards, fingerprints, etc. for criminal purposes, such as , to access financial information.

Impact of biometric technologies on human health [11]. According to ophthalmologists, the procedure of the retina scan is dangerous: it occurs with the help of infrared light of low intensity, and this can lead to impaired vision.

2 Attacks

Hackers continually have to invent new ways to deceive biometric scanners in order to log on. Therefore, we have synthesized different types of attacks to use them as a means of hackers' counteracting.

Biometrics-Based personal authentication systems, particularly fingerprints, become more popular than traditional systems that are based on tokens (keys or password) [12].

Traditional authentication systems are not prepared to distinguish between impostors who have illegally acquired the privileges to access a system and the genuine user. Furthermore, biometric systems can be more user-friendly because there is no need for the user to remember passwords.

Regardless of these benefits, biometric systems have some disadvantages. That is to say that biometric systems are vulnerable to external attacks, which could reduce their level of security.

In Ratha [13] has identified and classified eight different types (points) of attacks. Fig. 1 shows these attacks along with the components of a typical biometric system that might be affected.

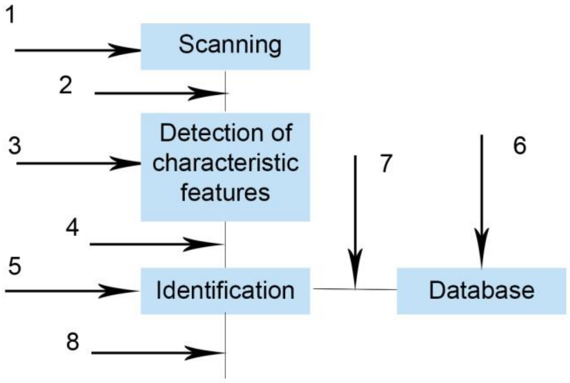

Fig. 1. Types of attacks on a biometric system

The first type of attack involves submitting a fake biometric fingerprint sample for scanning. In other words, the hacker submits pre-intercepted biometric data. The second type is known as “replay attack.” In some way, hackers reproduce a biometric sample and enter the system. In the third type of attack, the recognition module provides false values of the feature which were chosen by the intruder. In the fourth type of attack, the values of a specific function are replaced by those who were selected by the hacker. The set of recognition features can be modified to obtain an artificially high matching score in the fifth type of attack. The attack on the database by adding new templates, modifying existing templates and removing existing templates carry out in attack number 6. The attack in the seventh type carries out when a template is broadcasting through a communication channel between the system database and the matcher module, resulting in a change of templates in the database. Finally, an intruder might redefine the result of the matcher (accept or discard).

3 Fingerprint identification algorithm

The algorithm of segmentation and enhancement of the fingerprint image, which uses a new method of filtering based on Ateb-functions [14] is proposed and consists of the following steps:

Step 1. **Image normalization**. At this stage, we carry out the scaling process of imprint to uniform scale and geometric sizes with a clearly defined resolution.

Step 2. **Computation of the local orientation**. It means the scaling process of imprint to the origin of coordinate and turning the imprint with the setting of the origin of the coordinates and the polar axis. While scanning, we incline fingers at any angle. It is necessary to have an apparent reference to the coordinate system in order to recognize the imprint. We try to find out it in the second step.

Step 3. **Evaluation of the local frequency of the backbones**. Computation of the frequency matrix based on the normalized and orientation image, which was performed in steps 1 and 2.

Step 4. **Imprint segmentation**. The construction of an imprint mask by breaking down the normalized image into blocks and performing the classification task of each block, dividing them into those who contain and not contain backbones. After this, we smooth the mask by Gabor filtering [15].

Filtration of the normalized image. The outlines of parallel ridges and valleys with well-defined frequency and focus on the fingerprint image contain the information that helps eliminate objectionable noise. A bandpass filter [16] uses for it. The bandpass filter is tuned to the appropriate frequency and orientation. It can effectively remove the objectionable noise and maintain a solid structure of the ridges valleys. We have proposed to perform the Ateb-Gabor filtering [17], which has broader properties than the ordinary Gabor filter. Since it is based on Ateb-functions, which have much more extensive properties than classical trigonometry. This kind of filtration gives a solution to a problem that is clearly defined in specific areas of the square, both in the spatial and in frequency domains. This type of filtration is advisable to use as a bandpass filter. The Ateb-Gabor filter is described by the formula:

$$Ateb - G(x, y, \lambda, \theta, \psi, \sigma, \xi) = \exp\left(-\frac{\dot{x}^2 + \psi\,\dot{y}^2}{2\sigma^2}\right) Ateb - ca\left(\frac{2\Pi\,\dot{x}}{\lambda} + \xi\right)$$

$$\begin{cases} \dot{x} = x\cos\theta + y\sin\theta \\ \dot{y} = -x\sin\theta + y\cos\theta \end{cases}$$

where λ is the wavelength of the cosine multiplier, θ is the orientation of the regular parallel bands, ξ is the phase shift, ψ is the compression coefficient [17].

There are three parameters for using Gabor filters to the image: the frequency of the Ateb-function f wave, the filter direction, the mean square deviations of the Gaussian shell x 'and y'.

Step 5. **Filtration of the normalized image**. We apply a set of Gabor filters, Ateb-Gabor [18], which adjust to the local orientation of the ridges and the frequency of the ridges by pixels in a normalized image in order to get an improved fingerprint image.

We use part of the image obtained after filtering the image that has got into the mask constructed in the fourth step, so that construct the pattern of the imprint.

We calculate three values for each pair of such points: the module of the vector, which connects a pair of minucius, the vector orientation relative to the horizontal, and the directions of the papillary lines with minucius relatively to the horizontal. So, the template contains a description of the imprint in relative units, which neglects alters the image orientation.

The algorithm evaluates the percentage of matches between the corresponding three values. The speed of response of systems is determined by the execution of several significant operations - exponentiation, computation of a root, division, calculation of arctangent.

Step 6. **Skeletonization**.

4 Skeletonization

The next stage involves making the fingers of the papules thinner and bringing them to a thickness of one pixel of curves. In this case, the contour is selected, which is highlighted in Fig. 5 in a darker color and the construction of a graphic representation of curves. We will call the contour of the image a collection of its pixels, around which there is a jump-like change in the brightness function. The image contours will be represented by lines in one pixel wide. If, in addition to areas with constant brightness, there are areas with brightness that is smoothly changed in the original image, then there is no guarantee of continuity of the contour lines when specifying the contour lines: the discontinuities in those places where the change of brightness function is not sharp enough will be observed.

On the other hand, noise is present on a piecewise permanent image, and then unnecessary contours may be recognized that are not desirable when creating the boundaries of the domains. The algorithms for selection of contours are developed, and the behavior of contour lines is taken into account. Unique extra algorithms can eliminate gaps and eliminate excess contour lines.

For the selection of boundaries, i.e., brightness variations are made by the wave method [19]. Consider a fragment of an image that is scanned by the waveform and covers several pixels at a time. At the same time, the window contains a small fragment. When moving the window the fragment is changed. The image processing by a wave method is shown in Fig. 2.

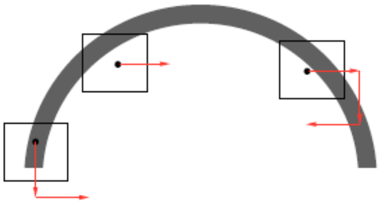

Fig. 2. Wave method for skeletonization

Then, the image is split into individual fixed blocks. On the curve we find the points of maximum or minimum. A skeleton image is created.

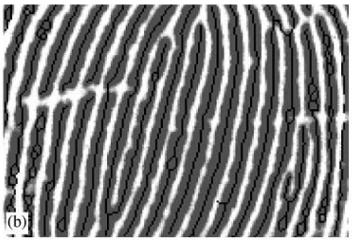

Fig. 3. Creating a skeleton image

By the skeleton of the image, we evaluate the characteristic points that were given in Fig. 2 and 3.

5 Recognition and identification

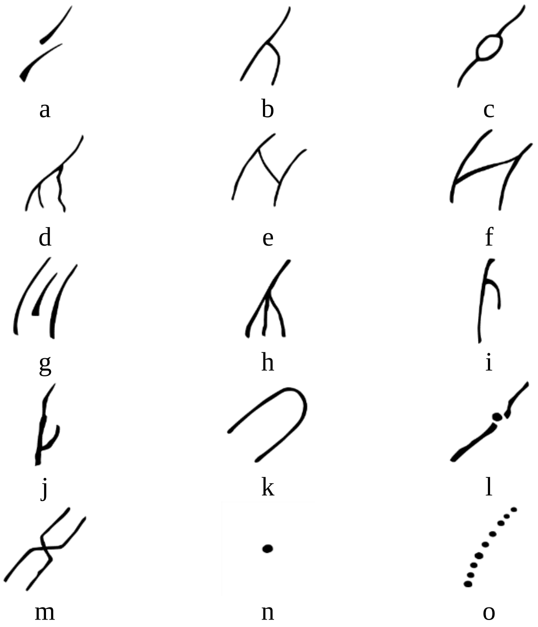

Fig. 4. Classification of minutiae: a - ridge endings, b - bifurcations or fork; c - eye or enclosure; d – bifurcations or fork, which sometimes can form a trifurcation; e - convergence or convergent fork; f - Interjunction or Bridge minutiae; g - fragment or short ridge; h - hook or spur; i - hook or spur right crochet; j - hook or spur left crochet; k - return minutiae; l – Interruption; m - crossovers are formed when two ridges; n - dot is a tiny ridge;o - dotted ridge

It is necessary to highlight the critical points after the formation of the skeleton of a biometric image and compare them to the key points which exist in the database in order to carry out the identification in this way. The main characteristic points highlight the graphic image. We suggest installing them in the range from 12 to 24. In the event of a large number of points, there probably will not be enough computational resources, but when there are few points, there is the probability of admitting someone else's fingerprint. Owing to this, the algorithm has two parameters: FAR - the access error of extraneous user, which should be 0,01%, and FRR - a mistake of genuine objection user 0%. Biometric devices can provide either high-speed recognition or high security of the system. We have used three classes of fingerprints comparison algorithms for the experiments. The algorithm with minutiae (individual points) is the first class. The second is the correlation analysis. The latter ones are hybrid methods. The most common, due to the simplicity and speed of work, is the method of comparison by particular points - endpoints of papillary lines and dots of duplication of papillary lines of minutiae. The description of minutiae was entirely carried out thoroughly in [19].

The classification of minutiae is shown below. [20].

1. Ridge endings. It is a ridge that is located between two almost parallel crests. Ridge ending is the point where the ridge ends suddenly and does not appear again (Figure 4.a).

2. Bifurcations or Fork. A ridge divides the left side of the papillary lines into specific lengths and forms two parallel lines (Fig. 4.b), which sometimes can form a trifurcation (Fig. 4.d and 4.h).

3. Eye or enclosure. These are ellipsoid minutiae, which are formed by a ridge that branch out only for merge or approaching one crest, leaving space within the ridge. The enclosure may be small or large. (Fig. 4.c).

4. Convergence or convergent fork. This is similar to bifurcation, but with reciprocal or mirror image. It is formed by two parallel ridges. (Fig. 4.e).

5. Interjunction or Bridge minutiae. A joint between two parallel crests with a short diagonal of the ridge, which encounters the ridges in a very sharp angle (Fig. 4.f).

6. A fragment or short ridge. The ridge from the ends, which sharply ends, and have varying lengths. The fragment can be small or large (Fig. 4.g).

7. Hook or spur. It is formed at the vertebrae when the ridge divides into two parts (Fig. 4.h). One bifurcation ridge continues further, and another split is added to the ridge, as an appendage of the spine with a certain angle of inclination. The hook can be ascending crochet, and a descendant, hook, right crochet and left hook (Fig. 4.i and 4.j).

8. Return minutiae. One ridge suddenly turns back and forms a rounded loop. (Fig. 4.k).

9. Interruption. Interruptions formes between two crests that are interrupted, suddenly deviating, forming two ridges that end with a furrow between them (Fig. 4.l).

10. Crossovers are formed when two ridges cross each other (Fig. 4.m).

11. Dot is a tiny ridge that is usually found in the middle of the interruption, either delta or between the two ridges (Fig. 4.n).

12. Dotted ridge. This is a ridge that is created by dots (Fig. 4.o) [20].

The algorithm contains the steps of reading the imprint by the optical system, recording to the image buffer, transferring to a convolution buffer, comparing data with the template database, and deciding whether or not to identify. Because of the large volume, we tried to encode biometric images using the RSA algorithm from [21].

The Adafruit fingerprint sensor is used as an optical sensor. The component generates code for the Python programming languages. Programming was carried out on

Python in the PyCharm environment [22]. Processing and decoding of prints were carried out for [23]. The above module enabled fingerprint recognition to be available for 127 different fingerprints. The system has a third level of protection [24]. Time for fingerprint recognition is less than 1 second.

The comparison was carried out using the SSIM metric [25]:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x{}^2+\mu_y{}^2+c_1)(\sigma_x{}^2+\sigma_y{}^2+c_2)} \quad (1)$$

where $\mu(x)$- average scanned fingerprint μ_y - the average fingerprint for which the comparison was made; σ_x – standard deviation for the scanned fingerprint, σ_y - standard deviation fingerprint, for which the comparison was made c_1, c_2 – equalization coefficients.

Figure 5 shows an analysis of the comparison for formula (1) of the originality of the prints and three different attempts to falsify and distort the original fingerprint and attempt to connect to the system. The experiments were carried out for three falsifications, and the results were displayed, the system did not allow any attempt and identified it as a fake.

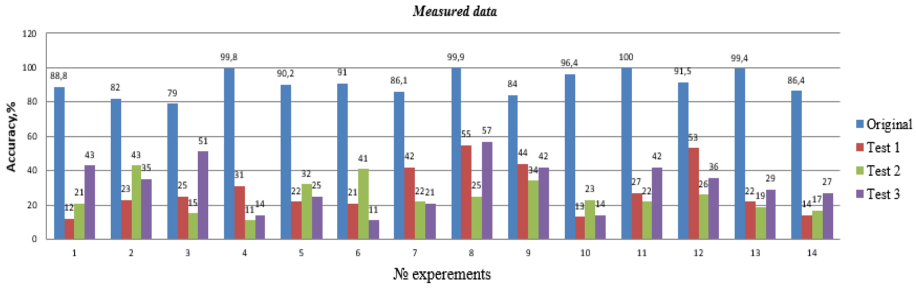

Fig. 5. Testing system for identifying the originality of the fingerprints

Assessment of the local frequency of the ridges. If minutiae wasn't detected locally, the brightness levels along the crests could be modeled as a sinusoidal wave along the normal to the spine orientation. Fig. 6 shows the percentage display of the original fingerprint and failure in the system in 14 experiments.

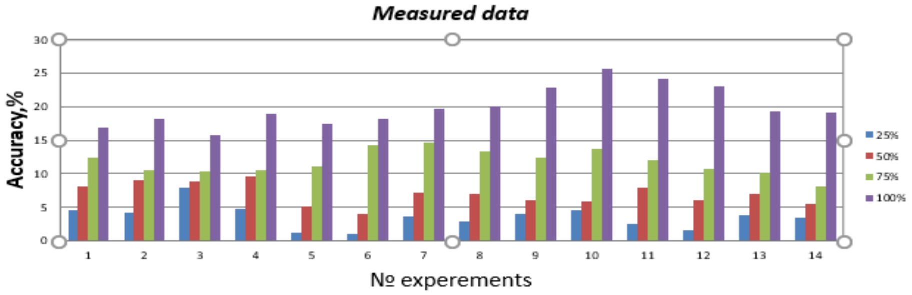

Fig. 6. Testing the percentage of the original concerning forgery

This method was used in the construction of intelligent decision support systems [27] based on adaptive ontology, in which the entry is made on the basis of latent elements with fingerprints. And in [28] a statistical analysis of the coefficients of language diversity, from which the statistical estimates based on which latent elements of system protection were constructed, were taken. In [29], the design and development of the Virtual Library Information System was carried out. To protect the system it is proposed to introduce a developed security system.

Conclusion

An identification system of biometric images using passive elements has been developed. The article analyzed the types of attacks affecting the identification system. Conclusions are made about the vulnerability of the system to attacks on it. Classification of minucius for biometric images has been carried out. We proposed to use of wave algorithm for skeletonization. Besides, experimental studies of the identification of biometric fingerprint are presented.

References

[1] Sun, S., Gu, Y., Wang, L., Gu, P., Li, Y. Key technology research for mobile police terminal fingerprint collection for quick comparison using automated fingerprint identification system. Journal of Forensic Science and Medicine, 5(1), 57. (2019).

[2] Heimo, O. I., Hakkala, A., Kimppa, K. K. How to abuse biometric passport systems. Journal of Information, Communication and Ethics in Society, 10(2), 68-81. (2012).

[3] Habibu, T., Luhanga, E. T., Sam, A. E. Evaluation of Users' Knowledge and Concerns of Biometric Passport Systems. Data, 4(2), 58. (2019).

[4] Petitdidier, S. U.S. Patent Application No. 16/043,289. (2019).

[5] Jackson Jr, G. W., Rahman, S. Exploring Challenges and Opportunities in Cybersecurity Risk and Threat Communications Related To The Medical Internet Of Things (MIoT). arXiv preprint arXiv:1908.00666. (2019).

[6] Chokesuwattanaskul, R., Safadi, A. R., Ip, R., Waraich, H. K., Hudson, O. M., Ip, J. H. Data Transmission Delay in Medtronic Reveal LINQTM Implantable Cardiac Monitor: Clinical Experience in 520 Patients. Journal of Biomedical Science and Engineering, 12(8), 391-399. (2019).

[7] Hsu, K. H., Chiang, Y. H., Hsiao, H. C. SafeChain: Securing Trigger-Action Programming from Attack Chains. IEEE Transactions on Information Forensics and Security. (2019).

[8] 8. Kudret, S., Erdogan, B., Bauer, T. N. Self-monitoring personality trait at work: An integrative narrative review and future research directions. Journal of Organizational Behavior, 40(2), 193-208. (2019).

[9] Yi-Ling, Teo. The Right of Privacy: Death By a Thousand Data Cuts. Rajaratnam School of International Studies. http://hdl.handle.net/11540/10001. (2019).

[10] EDRi, B. An Open Letter to the European Parliament on Biometric Registration of all EU Citizens and Residents. Agenda. (2019).

[11] Ahmed, A. A. Future Effects and Impacts of Biometrics Integrations on Everyday Living. Al-Mustansiriyah Journal of Science, 29(3), 139-144. (2019).

[12] Giobbi, J. J. U.S. Patent Application No. 16/170,234. (2019).

[13] N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 223-228. (2011).

[14] Nazarkevych M., Riznyk O., Samotyy V., Dzelendzyak U. Detection of regularities in the parameters of the ateb-gabor method for biometric image filtration. Eastern-European journal of enterprise technologies. № 1(2). pp. 57–65. (2019).

[15] Ryszard S. Choras Multimodal Biometrics for Person Authentication [Online First], IntechOpen, DOI: 10.5772/intechopen.85003. Available from: https://www.intechopen.com/online-first/multimodal-biometrics-for-person-authentication. (March 14th 2019).

[16] Tapia, J. E., Perez, C. A. Gender Classification From NIR Images by Using Quadrature Encoding Filters of the Most Relevant Features. IEEE Access, 7, 29114-29127. (2019).

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

[18] Dronyuk I., Nazarkevych M., Poplavska Z. Gabor Filters Generalization Based on Ateb-Functions for Information Security. In: Gruca A., Czachórski T., Harezlak K., Kozielski S., Piotrowska A. (eds) Man-Machine Interactions 5. ICMMI 2017. Advances in Intelligent Systems and Computing, vol 659. Springer, Cham (2018).

[19] Kistler, P. M., Roberts-Thomson, K. C., Haqqani, H. M., Fynn, S. P., Singarayar, S., Vohra, J. K., ... Kalman, J. M. P-wave morphology in focal atrial tachycardia: development of an algorithm to predict the anatomic site of origin. Journal of the American College of Cardiology, 48(5), pp.1010-1017. (2006).

[20] Stücker, M., Geil, M., Kyeck, S., Hoffman, K., Röchling, A., Memmel, U., Altmeyer, P. Interpapillary lines—the variable part of the human fingerprint. Journal of Forensic Science, 46(4), 857-861. (2001).

[21] Y. Rashkevych, A. Kovalchuk, D. Peleshko, M. Kupchak, "Stream modification of RSA algorithm for image coding with precize contoure extraction," 10th International Conference - The Experience of Designing and Application of CAD Systems in Microelectronics, Lviv-Polyana, 2009, pp. 469-473. (2009).

[22] Islam, Q. N. Mastering PyCharm. Packt Publishing Ltd. (2015).

[23] O. Riznyk, V. Parubchak and D. Skybajlo-Leskiv, "Information Encoding Method of Combinatorial Configuration," 9th International Conference- The Experience of Designing and Applications of CAD Systems in Microelectronics, Lviv-Polyana, 2007, pp. 370-370. (2007).

[24] Martsyshyn, R., Medykovskyy, M., Sikora, L., Miyushkovych, Y., Lysa, N., Yakymchuk, B. (2013, February). Technology of speaker recognition of multimodal interfaces automated systems under stress. In Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2013 12th International Conference on the (pp. 447-448). IEEE.

[25] Hore, A., Ziou, D. (2010, August). Image quality metrics: PSNR vs. SSIM. In 2010 20th International Conference on Pattern Recognition (pp. 2366-2369). IEEE.

[26] Medykovskyy, M., Lipinski, P., Troyan, O., Nazarkevych, M. Methods of protection document formed from latent element located by fractals. In 2015 Xth International Scientific and Technical Conference" Computer Sciences and Information Technologies"(CSIT). pp. 70-72. IEEE. (2015, September).

[27] Lytvyn, V., Vysotska, V., Dosyn, D., Lozynska, O., Oborska, O. Methods of building intelligent decision support systems based on adaptive ontology. In 2018 IEEE Second International Conference on Data Stream Mining & Processing (DSMP). pp. 145-150. IEEE. (2018, August).

[28] Lytvyn V., Vysotska V., Pukach P.Y, Nytrebych Z., Demkiv I., Kovalchuk R., Huzyk N. Development of the lingummetric method for automatic determination of the author of textual content based on statistical analysis of language diversity coefficients // Eastern-European journal of enterprise technologies. № 5/2 (95). pp. 16–28. (2018).

[29] Rusyn Bohdan, Lytvyn Vasyl, Vysotska Victoria, Emmerich Michael, Pohreliuk Liubomyr. The virtual library system design and development // Advances in Intelligent Systems and Computing (AISC). – Vol. 871: Advances in intelligent systems and computing III. Selected papers from the International conference on computer science and information technologies, CSIT 2018, September 11-14, Lviv, Ukraine. pp. 328–349. (2019).