The Development of Information Technology of Biometric Protection with an Image Filtration Based on Ateb-Gabor

Mariya Nazarkevych
Department of Information Technology Publishing,
Lviv Polytechnic National University,
Lviv, Ukraine, e-mail: mariia.a.nazarkevych@lpnu.ua,
mar.nazarkevych@gmail.com

Yaroslav Voznyi
Department of Information Technology Publishing,
Lviv Polytechnic National University, Lviv, Ukraine,
e-mail: voznyyy@outlook.com

Hanna Nazarkevych
Faculty of Cybernetics Taras Shevchenko National University of Kyiv, Kyiv, Ukraine,
e-mail: h.nazarkevych@gmail.com

Iryna Maslanych
Department of Applied Linguistics, Lviv Polytechnic National University, Lviv, Ukraine,
e-mail: ira.masl.nch@gmail.com

Abstract—**An overview of the systems of biometric protection with image filtering is carried out. Dactyloscopic recognition method takes half of the market access systems. Filtering is based on the developed Ateb-Gabor filter. Good recognition rates are achieved by filtering the papillary lines texture. The best results can be obtained when the direction and frequency of papillary lines are taken into account. For this biometric image is subject to adaptive alignment of histograms, calculation of the local orientation of the image, image frequency and filtration of the Ateb-Gabor. The generalized Ateb-Gabor filter, based on periodic Ateb-functions and Gabor filters, is developed. Ateb-Gabor filtering allows you to use more flexible and multivariate image management. This will allow you to apply many changes to one image to solve the identification problem. The software is developed by Pyton.**

Index Terms—**Image filtering, Ateb-Gabor filter, Ateb-functions.**

I. Introduction

Biometric protection systems have become widespread due to the use of unique, specific physiological characteristics that are inherent to a person. These include the unique characteristics that a person receives at birth: a DNA structure, an eye iris, a retina, a geometry and a temperature face map, fingerprints, a palm geometry. Biometric characteristics also include those that are acquired and change over time a signature, a voice and a walk [1].

The technology of recognizing the unique physiological characteristics of each individual is determined by electronic authentication. Its essence is to determine if a person is really the person he thinks about. The purpose of the authentication is to check whether the person who has the right to log in will get the access to the system, for example, when checking the password. The aim of an authorization is to give the user the access to some resources.

Protecting data that can not be changed or tampered provides the most accurate authentication based on the biometric systems. These benefits are obvious because traditional security systems are not able to discover who, for example, enter the code or insert a smart card.

However, biometric security systems have a big drawback. Security systems work when the system knows the confidential characteristics of a particular person. In addition, supporters of biometric security systems claim that these confidential characteristics actually provide a higher level of secrecy, because during the authentication the information about a person's address, home phone, bank account, etc. is not provided [2]. In most cases, biometric security systems are based on sections of mathematical statistics.

II. The Analisis of the Last Developements

Biometric systems are identified by the following biometric indicators with 58% fingerprints, 18% face geometry, 7% retina, 7% hand geometry, 3% human vein pattern, 5% human voice, 2% other biometric indexes [3].

An identification in any biometric system goes through the four stages: storage - the physical sample is stored by the system; selection - the unique information is extracted from the model and the biometric model is compared; comparison - the model is compared with the available templates; co-existence / discrepancy - the system decides whether biometric models coincide.

The fingerprinting recognition method takes a half of the market access systems. Such systems include laptops, keyboards, computer mice, flash drives, door locks, and so on nowadays. Biometric security systems has become an

important part of our everyday life. The identification of the following characteristics are introduced:

- the probability of a person's access, who does not have the access right (False Acceptance Rate - FAR) is the most undesirable result that needs to be minimized;

- the probability of the person's refusal, who has an access (False Rejection Rate- FRR), this false result can be corrected.

These characteristics are interrelated. The smaller the first one, the bigger the second one. The point in which these two levels of error are equal is called EER (Equal Error Rates). The smaller the EER value, the higher the error rate of the access system [4].

Faking a papillary pattern of a human finger or the retina is very difficult. Therefore, the occurrence of mistakes of the second kind, that is, granting access to a person who does not have this right is practically excluded. However, under the impact of some factors, the biological peculiarities on which the identification of the person is carried out can change. Because of this, there is a high frequency of errors of the first kind in biometric security systems, that is, denial of access to a person who has the right to do so. The system is better, the smaller the value of FRR with the same values of FAR. The point in which these two curves intersect is a comparative EER error (Equal Error Rates) [5]. However, this point is not always representative. There is always a certain degree of system error probability. For access control systems using different technologies, the error may differ significantly. It is important here that the access of someone else to the system, or to skip all of them, is important.

III. Information technology of the biometric protection with the image filtration

To improve the quality of fingerprints, good results are achieved when filtering the texture of papillary lines. The best results can be obtained when the direction and the frequency of papillary lines are taken into account. There are many suggestions for improving image quality, one of which belongs to Hang L. [6]. The researcher identified the following main steps:

1) adaptive alignment of histograms
2) calculation of the local the image orientation
3) calculation of the local frequency of the image
4) Gabor filter

1) Adaptive aligment of histograms

Contrast-limited adaptive histogram alignment (CLAHE) [7] is used to improve image quality. To implement it, the OpenCV library createCLAHE method is used. Adaptive alignment of histograms - an image processing technique designed for local contrast and sharpening of edges. In contrast to the usual alignment of histograms, the image is split into sectors and each of them is calculated by its own histogram. This allows you to more accurately distribute the light throughout the image. But despite its effectiveness in this method, there are its disadvantages, including excessive contrast and excessive noise.

2) Calculation of the local image orientation

The local orientation of the image is the property of the image, which describes the coordinates of the papillary lines. To represent the image as an oriented texture, the method of least squares is used (the method of finding an approximate solution of an over-defined system [6].

The main steps of the algorithm include:
Split image into blocks of size w x w (16 x 16)
Calculate the gradients in each dx (i, j) and dy (i, j) in each pixel (i, j) using the Sobel operator.

3) Calculation of the local frequency of the image

Another important feature of the fingerprint is the analysis of the frequency of papillary lines. In the local neighborhood, where there are no special points or details, the brightness levels of gray can be modeled in the form of a sinusoidal wave along the normal direction to the local orientation of the papillary line (see Fig. 1 [6]).

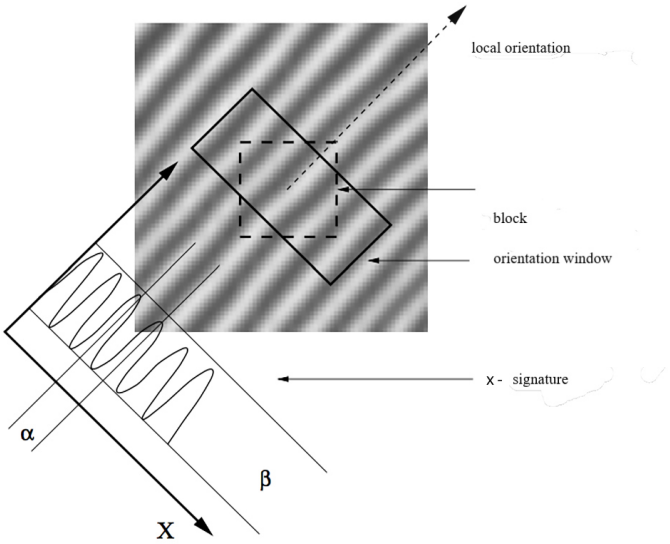

Fig.1 Analysis of the frequency of papillary lines

In order to calculate the local frequency of the image, we will mark the normalized image - G and the orientation image - O, and take the following steps:

Split image G into blocks of size w x w (16 x 16).

For each block centered in the pixel (i, j), an orientation window with the size l x w (32 x 16) is calculated, which is determined by the coordinate system of the line.

Most fingerprint identification algorithms work mainly on comparing branching and ending papillary lines. The end of the papillary line is the place where it is severely ends. Branching of a line is considered to be a place where it branches out and forms two independent lines. From high-quality images 40-100 unique characteristics (breaks and divisions of papillary lines) can be distinguished. With low-quality images, the whole process becomes a little bit more complicated.

Among many ways to improve the low-quality fingerprint images, the Gabor filter is considered to be the most common and effective.

4) Gabor filter

Usually the Gabor filter is applied to the image by applying a mask. And it is necessary that several lines of the pattern should fall under the mask, for this purpose the size of a mask of the order of 15 × 15 pixels is chosen. Thus, it turns out that significant computational costs are required. Taking into account the foregoing, one can make a certain modification of the algorithm of Gabor filtering.

IV. Biometric protection with the filthration based on the Ateb-Gabor filter

The fingerprint enhancement algorithm receives an initial image on the input, and then runs a set of intermediate steps that are based on the Ateb-Gabor filter and, as a result, we get an improved image.

V. The Ateb-Gabor one-dimensional filter developement

A generalized one-dimensional Gabor filter based on Ateb-functions [8, 10]. It will look like:

$$g(m,n,\omega) = e^{-\frac{\omega^2}{2\sigma^2}} \mathrm{ca}(m,n,2\Pi,\theta,\omega) \qquad (1)$$

where σ is the standard deviation of the Gaussian nucleus, which determines the amplitude of the function, ω is the frequency of oscillations, which is defined as ω = 1 / T, where T (m, n) is the period of the function ca (m, n, 2Π, θ, ω).

The graphical representation of the generalized Gabor filter is shown in Fig. Unlike the well-known Gabor filter, Ateb-based filtration has more control actions due to the parameters m n that can take rational numbers. These control actions will be shown in this research. In the case of m = n = 1, the Ateb-Gabor becomes equivalent to the Gabor filter. Since the Ateb-Gabor function is even and symmetric, the values for parametres (0.1, 1, ω) will be identical to parametres (1, 0.1, ω).

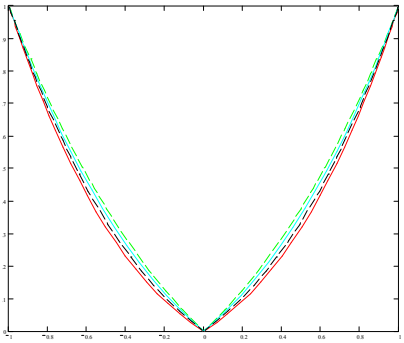

Fig. 2. The graphic representation of the Ateb-Gabor at m = 0.1, 0.5, 0.7 and 1, with n = 1, σ = 1;

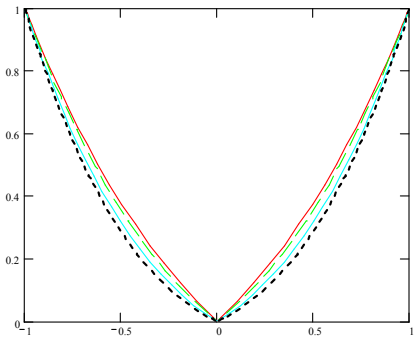

Fig.3. The graphic representation of the Ateb-Gabor with parameters m = 0.1, 0.5, 0.7 and 1, n = 1, σ = 3.

Based on the Ateb-Gabor filter, it is possible to filter images with a large number of crests. This can provide better characteristics than the well-known Gabor filter. The one-dimensional Gabor filter based on the Ateb-functions makes it possible to obtain more flat shapes, as it is shown in Fig. 1, 2, 3. Thus, the filtration can be realized with a larger spectrum of curves and a larger set of governance parameters. In particular, the four parameters for the Ateb-Gabor filter - m, n, σ, θ, as opposed to two for the previously known Gabor filter - σ, θ.

VI. The Ateb-Gabor two-dimensional filter developement

Filtration Ateb-Gabor occurs according to the formula:

$$AtebG(x,y,\lambda,\theta,\psi,\sigma,\zeta) = = \exp\left(-\frac{x'^2+\psi y'^2}{2\sigma^2}\right)\mathrm{ca}\left(2Pi\frac{x'}{\lambda}+\zeta\right)$$

$$x' = x\mathrm{Cos}(\theta) + y\mathrm{Sin}(\theta)$$

$$y' = -x\mathrm{Sin}(\theta) + y\mathrm{Cos}(\theta) \qquad (2)$$

where λ – the wavelength of the cosine - multiplier, θ – prallel bandwidth normal orientation, ζ – lagging (phase transmition ; phase shift) , ψ – data compression ratio.

The modulation Ω and the phase shift θ. The expansion on the Gabor's functions is the expansion on the modulated fragments of the sinusoid. The length of the fragments for all frequencies is constant, which gives a different number of oscillations for different harmonics. There is thus a sufficiently well localized in t and k-space Gabor's function can not be a basis wavelet transformation, since the basis on which it is based does not have the properties of self-similarity.

Received 3d graphs of two-dimensional Ateb-Gabor. In fig. 4 shown two-dimensional filter Ateb- Gabor (2) with parameters m=n=1, σ=10, in fig. 5 - two-dimensional filter Ateb- Gabor with parameters m=n=0.2, σ=10, but in fig. 6 - two-dimensional filter Ateb-Gabor with parameters m=3, n=3, σ=10.

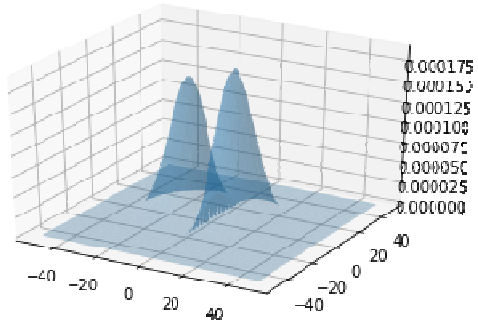

Fig. 4. Two-dimensional filter Ateb- Gabor with parameters m=n=1, σ=10

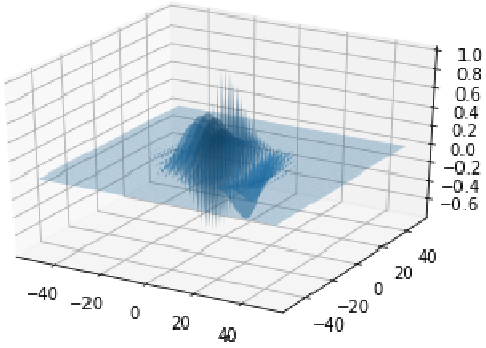

Fig. 5. Two-dimensional filter Ateb- Gabor with parameters m=n=0.2, σ=10

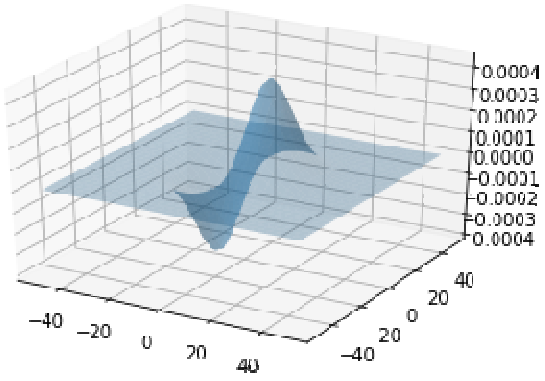

Fig. 6. Two-dimensional filter Ateb- Gabor with parameters m=3, n=3, σ=10

After performing the actions, described above, we get the following result (Fig. 7). The program is written in Python.

Such an organization of information security technology will enable to reduce the time to enter the security system, through the indicators FRR, FAR and make the accessible access point EER [9].

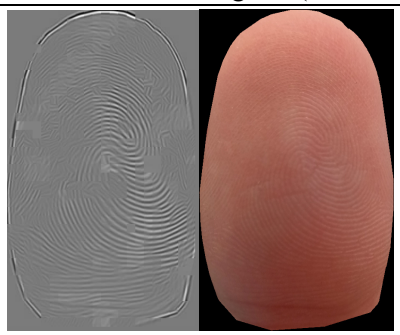

Fig. 7. The graphical representation of Ateb-Gabor filtration taking into consideration the local orientation of the image and the local frequency of the image

VII. Conclusion

The problem of automatic image processing and image filtration. It has been determined that technologies that are associated with text recognition, identification of biometric indicators and others are rapidly developing. Typically, images that fall into the auto-processing system have poor-quality appearance because of the influence of the noise. The new Ateb-Gabor filtration method is considered, which allows to reduce noise and interference, as well as to expand the effective filtration methods. The new filtering method has wider capabilities. The Gabor filter for biometric images has been developed. A new Ateb-Gabor's filter has been investigated. Its efficiency in application to biometrics has been proved as well.

Research for images filtering and studying their characteristics based on one-dimensional and two-dimensional Gabor filter is carried out. The use of the generalized Gabor filter will allow a better filtration and a large number of governance parameters from which to select the best samples for the filtration. The change of the m and n parameters provides different values of the period, which makes it possible to expand the number of filter options.

To solve the problem of fingerprint identification, the Ateb-Gabor function allows you to improve identification, and, based on it, to filter images with a large number of crests. This provides better characteristics than the usual one-dimensional Gabor filter.

References

[1] R. Jiang, S. Al-maadeed, A. Bouridane, D. Crookes, and A. Beghdadi, Biometric Security and Privacy, Springer International Publishing AG, 2017. https://doi.org/10.1007/978-3-319-47301-7

[2] Wayman, James, et al. "An introduction to biometric authentication systems." Biometric Systems. Springer, London, 2005. 1-20.

[3] Gomez-Barrero, Marta, et al. "Predicting the vulnerability of biometric systems to attacks based on morphed biometric information." IET Biometrics (2018).

[4] Ortiz, Nicolas, et al. "Survey of Biometric Pattern Recognition via Machine Learning Techniques." (2018).

[5] Akin, Cihan, Umit Kacar, and Murvet Kirci. "A Multi-Biometrics for Twins Identification Based Speech and Ear." arXiv preprint arXiv:1801.09056 (2018).

[6] Hang L, Wan Y, Jain A "Fingerprint image enhancement: algorithm and performance evaluation" Chapter 2.1

[7] J. Alex Stark, "Adaptive Image Contrast Enhancement Using Generalizations of Histogram Equalization" IEEE Trans. On Image Processing, vol. 9, no. 5, pp. 889-896, May 2000

[8] Nazarkevich M. Methods for increasing the efficiency of printing by means of Ateb-functions / M.Nazarkevich. Monograph. Lviv: Publishing House of the Lviv Polytechnic National University, 2011. - p.188.

[9] Yudin, O. K., Korchenko, O. G., & Konahovich, G. F. (2009). Information security in data networks. K: TOV "NVP" INTERSERVIS.

[10] Nazarkevych M. Data protection based on encryption using Ateb-functions / M. Nazarkevych, O. Troyan, R. Oliarnyk, H. Nazarkevych. The XI International Scientific and Technical Conference CSIT 2016, 06-10 September, Lviv 2016. P.30-32.