IEEE Second International Conference on Data Stream Mining & Processing
August 21-25, 2018, Lviv, Ukraine

Investigation the Ateb-Gabor Filter in Biometric Security Systems

Mariya Nazarkevych
Lviv Polytechnic National University,
Lviv, UKRAINE,
mariia.a.nazarkevych@lpnu.ua

Ivanna Klyujnyk
Technical College,
Lviv Polytechnic National University
Lviv, UKRAINE,
ivanna.klyujnyk@gmail.com

Hanna Nazarkevych
Faculty of Cybernetics Taras Shevchenko National University of Kyiv
Kyiv, UKRAINE,
h.nazarkevych@gmail.com

***Abstract*—Biometric information security systems are analyzed. One of the most important characteristics is the high reliability, which corresponds to the ability of the system to distinguish between biometric characteristics that correspond to different people on also it is safe to find a match. To implement this, at the filtration stage, it is proposed to use the Ateb-Gabor filter, which extends the usual filtering. With this filtering, you can improve the gradation characteristics of biometric models. The Ateb-Gabor filter was constructed and studied, graphs of the new function and corresponding frequency graphs are presented. Filtration experiments are performed. The SNR filtration quality is estimated.**

Keywords—Image filtering, Ateb-Gabor filter, Ateb-functions.

I. Introduction

Biometric technologies have become the most significant of the latest achievements in the area of identification and control of the information access. Biometric technologies are based on the biometric characteristics of a single person [1]. These include the unique characteristics that a person receives at birth: DNA structure, eye iris pattern, eye retina, geometry and temperature card of the face, fingerprints, palm geometry. Biometric characteristics include those that are acquired and change over time - signature, voice, walking [2].

Biometric systems are divided by the following biometric indicators [3] - 58% of the are fingerprints, 18% - facial geometry, 7% - retinal eye, 7% - hand geometry, 3% - human vein pattern, 5% - human voice, 2% - other biometric Indexes..

All biometric systems consist of two parts - hardware and specialized software.

There are four stages of identification in any biometric system[4]:Зберігання – фізичний взірець зберігається системою

Selection - the unique information is extracted from the model and the biometric model is compared to it.

The model is compared with available models. Match/ mismatch - the system decides whether biometric models match.

The purpose of this work is to review modern biometric methods of identification of a person and the level of their development, as well as the possibilities of using modern technologies in information security systems and the development of a new filtration method.

One of the most important information security characteristics based on the biometric technologies is high reliability. It can be defined as the ability of the system to reliably distinguish between biometric characteristics belonging to different people and to reliably find coincidences [5].

Dactyloscopic recognition method takes half of the market access systems [6]. Nowadays such systems include laptops, keyboards, mice, flash drives, door locks, etc.

Biometric security systems are frequently used in the modern society. Identification of the following characteristics are introduced:

- the probability of a False Acceptance Rate (FAR) [3] is the most undesirable result that needs to be minimized.

- the probability of a False Rejection Rate (FRR) refusal [3], this false result can be corrected.

These characteristics are related. The smaller the first, the bigger the second. The point in which these two errors are equal is called EER (Equal Error Rates) [3]. The lower the EER value, the higher the error rate of the access system. The first number characterizes the probability of denial of access to the person having access, the second is the probability of false coincidence of the biometric characteristics of two people. Forging a papillary pattern of a person's finger or a rainbow of an eye is very difficult. So the emergence of "second kind errors" (that is, granting access to a person who does not have this right) is practically excluded. However, under the influence of some factors, the biological characteristics that make identification of the personality can change. Therefore, the frequency of occurrence of "errors of the first kind" (denial of access to a person having this right) in biometric systems is large enough. The better the system is, the lower the value of FRR with the same FAR values is. EER (Equal Error Rate), which defines the point in which the FRR and FAR graphs cross, are sometimes used. But it is not always representative.

II. Analysis of Recent Developments

Using biometric systems, especially facial recognition systems, even after introducing correct biometric characteristics, the authentication decision is not always correct. This is due to a number of features and, first of all, with the fact that many biometric characteristics can change. There is a certain degree of system error probability. And with the use of different technologies, the error can vary significantly. For access control systems using biometric technologies, it is necessary to determine what it is more important not to miss a "stranger" or skip all "own" examples [3].

Many firms and state institutions are currently developing biometric security systems. Among them, the most well-known are Ekey biometric systems and ZKTeco, which introduced biometric systems for implementation [7].

Ekey biometric systems is an Austrian company, a leader in the development and implementation of biometric systems in Europe. ZKTeco - The Chinese company produces budget devices for access control while taking into account working time, which scans fingerprints and facial geometry [8]. Such equipment is in demand in various financial and public organizations.

The developed Ateb-Gabor filter has several significant advantages compared with the known ones. Among the parameters that you can modify the image, there are two independent ones that accept the values of rational numbers. Additionally, filtering can be done not for the whole image, but for some kind of slabs that look noisy. The filtering developed by the filter showed good results. The Gabor function [9] is a Gauss modulated. Gaussian function with four parameters: displacement t_0, standard mean square deviation σ, modulation frequency Ω, and phase shift θ:

$$G(t) = e^{i\Omega(t-t_0)-i\theta} e^{\frac{(t-t_0)^2}{2\,2\sigma}}$$

Decomposing on the Gabor functions is a decomposing 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. It follows that a sufficiently well localized in the t and *k*-space function of the Gabor cannot be a basis of the wavelet transform, since the basis based on it does not have the properties of self-similarity [9].

We will solve the system of differential equation:

$$\dot{x}+\beta y^m=0,$$
$$\dot{y}+\alpha x^n=0. \qquad (1)$$

where α ,β – some real constants and where *m*, *n* is:

$$n=(2\theta'_1+1)/(2\theta''_1+1)$$

$$m=(2\theta'_2+1)/(2\theta''_2+1),\ (\theta'_1, \theta''_1, \theta'_2, \theta''_2=0, 1, 2, \ldots). \qquad (2)$$

Let's solve this system graphically and solution for parameters m=1, n=1, α=1, β=1 are shown on Fig. 1, a m=7, n=7, α=1, β=1 are shown on Fig. 2 Solutions of this systems are Ateb-functions [10].

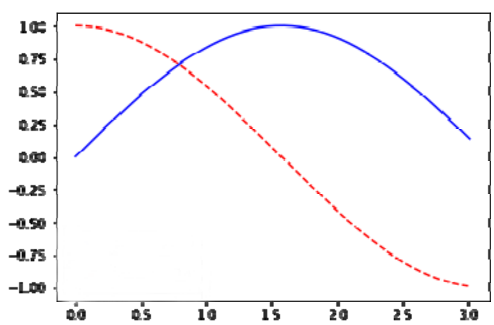

Fig. 1. Ateb-ca (red) and Ateb-sa (blue) with parametres m=1, n=1, α=1, β=1.

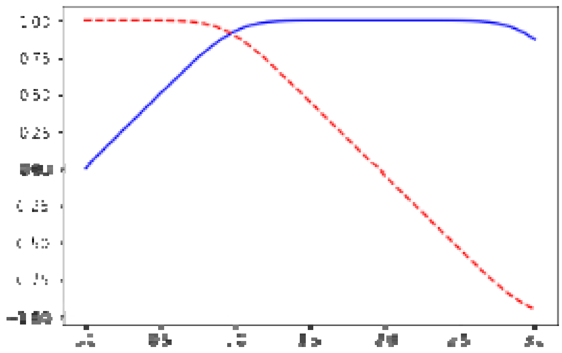

Fig. 2. Ateb-ca (red) and Ateb-sa (blue) with parametres m=7, n=7, α=1, β=1.

III. TWO-DIMENSIONAL ATEB-GABOR FILTER

Filtration of the two-dimensional Ateb-Gabor is implemented by formula:

$$\text{Ateb-G}(x,y,\lambda,\theta,\psi,\sigma,\zeta) =$$
$$\exp(-(x'^2+\psi\cdot y'^2)/2\sigma^2)\ \text{Ateb-ca}(2\Pi\cdot x'/\lambda+\xi). \qquad (3)$$
$$x'=x\cdot \mathrm{Cos}(\theta)+ y\cdot \mathrm{Sin}(\theta)$$
$$y'= - x\cdot \mathrm{Sin}(\theta)+ y\cdot \mathrm{Cos}(\theta),$$

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

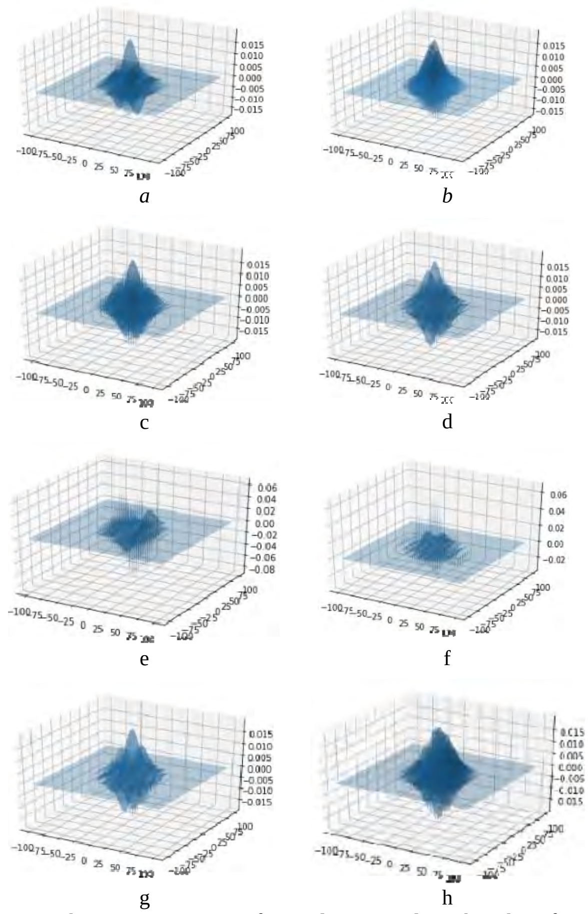

Fig. 3. Graphic representation of two-dimensional Ateb-Gabor for a) m=0.1, n=1; b) m=0.5, n=1; c) m=1, n=1; d) m=3, n=1; e)m=2, n=1; f) m=4, n=1; g) m=5, n=1; h) m=1, n=5.

Fig. 3 shows graphs of the Ateb-Gabor two-dimensional filter for various Ateb-function parameters. As you can see from the drawings, you can pick up the values that would most closely match the figures with biometric data. Experiments (except Fig. 3h) are performed with the parameter n = 1. The parameter m changes its value to the side of the increase. In graph c, we can observe the parameters m = n = 1, which corresponds to the well-known Gabor filter.

Fig. 4 shows the frequency graphs corresponding to the charts of the two-dimensional Ateb-Gabor. The experiments were carried out with the same parameters of the Ateb function as shown in Fig. 3. On the graphs depicted in Fig. 3 it can be observed that the maximum of the Ateb-Gabor function in Fig. 3 are displayed on the frequency chart with white curves. When filtered, this will allow you to draw out the contours of the figure with a biometric. On graph 4c we can observe the parameters m = n = 1, which corresponds to the frequency pattern of the Gabor filter.

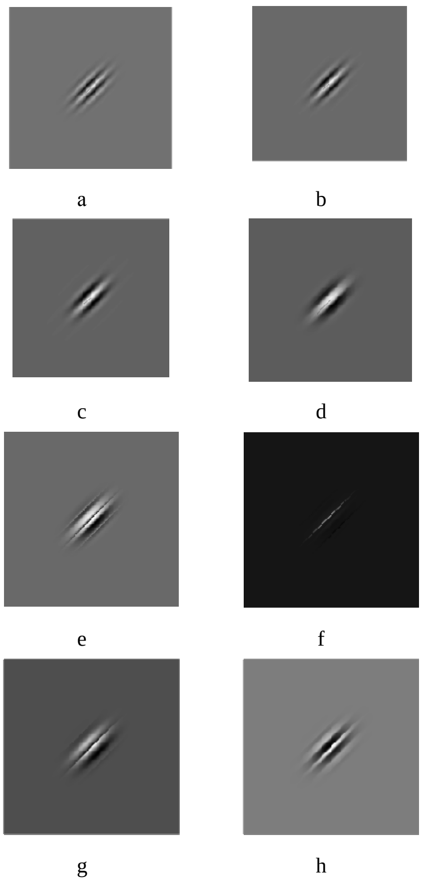

Fig. 4. Graphic representation of frequency two-dimensional Ateb-Gabor for a) m=0.1, n=1; b) m=0.5, n=1; c) m=1, n=1; d) m=3, n=1; e) m=2, n=1; f) m=4, n=1; g) m=5, n=1; h) m=1, n=5.

IV. Experimental Data

Fig. 5 shows the representation of the *Ateb*-Gabor filtration of the fingerprints *Ateb-G*($x,y,\lambda,\theta,\psi,\sigma,\zeta$) at different values of the sinusoidal wave frequency θ, see (3). The experiment was carried out with values $m = n = 1$. The value of σ of the mean-deflection of the Gabor rotation is selected as 1, in order to see the visual differences in the filtration. As it can be seen from Fig. 5e and 5f look more contrasting than other images. In Fig. 5f and 5g on the papilla of the fingers small details are visible more clearly.

We are evaluating the effectiveness of using different filtration and filtration with different characteristics, comparing characteristics that describe the invisibility (distortion level) and bandwidth. The study of image quality based on enhanced image resolution is devoted [11]. Method image superresolution from two frames is based on the aggregate divergence matrix elements of the theory and genetic algorithms [12].

Evaluation of the image distortion level is based on PSNR [13]:

$$P_{SNR} \tag{4}$$

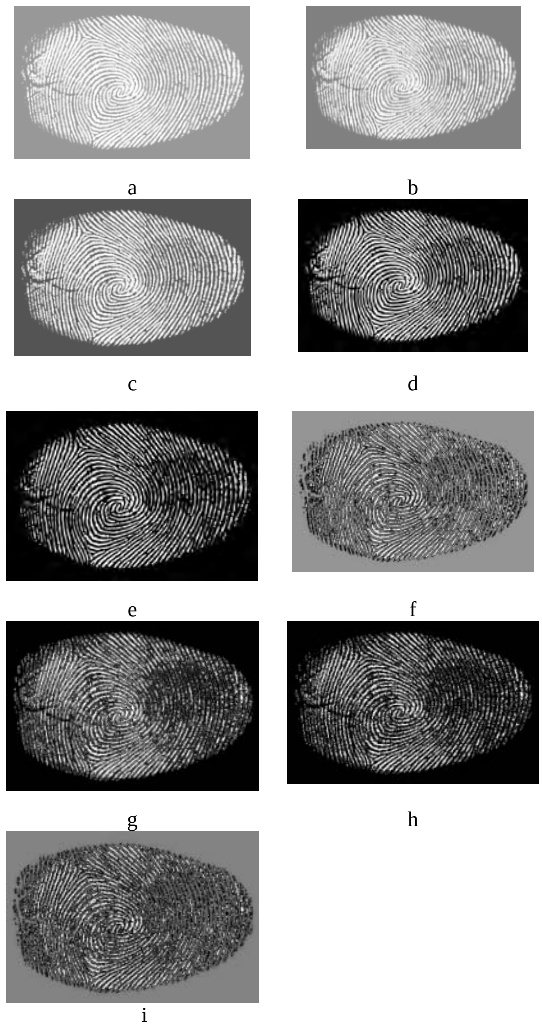

Fig. 5. Results of the image processing by the *Ateb*-Gabor filter at different frequency values of the sinusoidal wave θ :a) 0.1/p, b) 0.3/ p, c) 0.5/ p, d) 1/ p, e) 2/ p, f) 3/ p, g) 4/ p, h) 5/ p, i) 6/ p.

During the research, images of the jpg format, which was undelivered and with a size of 466x311 pixels, were used. The study was conducted in the following way. Two images were compared. The first image is called the original, and the second image is the filtered image. In order to make the equal-sized images which vary slightly among themselves, both of them are filtered out. However, the first image was changed based on the habitual Gabor filter, and the second one was replaced with the Ateb-Gabor filter. Then, on the basis of (4), these two images were compared. The comparison results are presented in Table I. From the comparison results, it can be noted that the larger the parameter m, n, the more the filtered image differs from the same picture filtered with Gabor filter.

TABLE I. EVALUATION OF BIOMETRIC IMAGE DISTORTION WITH ATEB-GABOR FILTERING

Original image	Filtered image	SNR
m1 n1	m3 n3	20,63 dB
m1 n1	m7 n7	19,04 dB
m1 n1	m11 n11	16,01 dB

Models of systems and pattern recognition using the SNR signal-to-noise ratio are described in [14]. Mathematical approaches to the recognition of biometric images are taken from [15]. The graphical representation of the change in the gradation characteristics of biometric images during filtration by the Ateb-Gabor is shown in Fig. 6. As can be seen from the graph, with the increase of the parameters of the Ateb-Gabor, the image substantially changes, this corresponds to a curve which value decreases with increasing x coordinat.

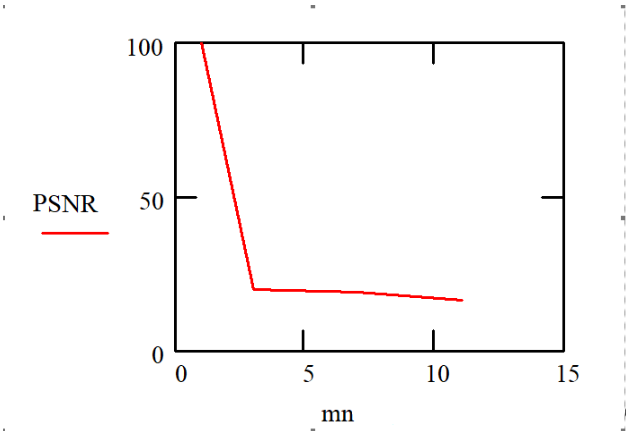

Fig. 6. Estimation of changes in the characteristics of the PSNR image from parameters m, n Ateb-Gabor

V. Conclusions

The properties of the Ateb-Gabor filter are studied. Usually the images which come to the system of processing have low quality due to noise action. Filtration of Ateb-Gabor is to reduce effects of noise and obstacles, This is actually expand methods of filtration.

The Ateb-Gabor filter has been developed, it extends the functions of controlling the conventional Gabor filter through. This allows developing a new image processing method.

The change of the parameters m and n provides different values of the period, which gives a possibility to expand the number of filter options.

Ateb-Gabor function gives a possibility to solve the problem with identification of finger's papilloma by improving the identification process. And on its basis, it is possible to conduct the image filtration with a big amount of combs. All this guarantees better characteristics than usual one-dimensional Gabor filter.

The efficiency-proving experiments of SNR-based filtration based on signal-to-noise ratio are carried out. It is shown that when entering the parameters m and n of the Ateb-garbage, it is possible to modify and extend the results of the filtration.

References

[1] S. Pankanti, R.M. Bolle, and A. Jain. "Biometrics: The future of identification [guest eeditors' introduction]," Computer society, 33.2 pp. 46-49, 2000.

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

[3] A. Ross, and A. Jain. "Information fusion in biometrics." Pattern recognition letters 24.13 (2003): 2115-2125.

[4] U. Umut and A.K. Jain. "Attacks on biometric systems: a case study in fingerprints," Security, Steganography, and Watermarking of Multimedia Contents VI, vol. 5306. International Society for Optics and Photonics, 2004.

[5] X. Liu, M. Tanaka, and M. Okutomi. "Noise level estimation using weak textured patches of a single noisy image," Image Processing (ICIP), 2012 19th IEEE International Conference on. IEEE, 2012.

[6] W.F. Lane, "Self-authenticating identification card with fingerprint identification," U.S. Patent No. 5,623,552. 22 Apr. 1997.

[7] J.E. Thurman, "Biometric security now and in the future," East Carolina University, 2016.

[8] T. Murakami and K. Takahashi. "High security biometric authentication system," U.S. Patent Application No. 13/706,854.

[9] J.P. Jones, and L.A. Palmer. "An evaluation of the two-dimensional Gabor filter model of simple receptive fields in cat striate cortex," Journal of neurophysiology, 58.6, pp. 1233-1258, 1987.

[10] M. Nazarkevych, R. Oliiarnyk, H. Nazarkevych, O., Kramarenko, and I. Onyshschenko, "The method of encryption based on Ateb-functions," IEEE First International Conference Data Stream Mining & Processing (DSMP), pp. 129-133, August 2016.

[11] Y. Rashkevych, D. Peleshko, O. Vynokurova, I. Izonin and N. Lotoshynska, "Single-frame image super-resolution based on singular square matrix operator," 2017 IEEE First Ukraine Conference on Electrical and Computer Engineering (UKRCON), Kiev, pp. 944-948, 2017. doi: 10.1109/UKRCON.2017.8100390.

[12] D. Peleshko, T. Rak, M. Peleshko, I. Izonin and D. Batyuk, "Two-frames image superresolution based on the aggregate divergence matrix," 2016 IEEE First International Conference on Data Stream Mining & Processing (DSMP), Lviv, Ukraine, pp. 235-238, 2016. doi: 10.1109/DSMP.2016.7583548

[13] O. K. Yudin, O. G. Korchenko, G. F. and Konahovich, Information security in data networks. K: TOV "NVP" INTERSERVIS, 2009.

[14] O. Riznik, I. Yurchak, E. Vdovenko and A. Korchagina, "Model of stegosystem images on the basis of pseudonoise codes," 2010 Proceedings of VIth International Conference on Perspective Technologies and Methods in MEMS Design, Lviv, pp. 51-52, 2010.

[15] O. Riznyk, I. Yurchak and O. Povshuk, "Synthesis of optimal recoverysystems in distributed computing using ideal ring bundles," XII International Conference on Perspective Technologies and Methods in MEMSDesign (MEMSTECH), Lviv, pp. 220-222, 2016. doi: 10.1109/MEMSTECH.2016.7507545.