# Ateb-Gabor Filtering Simulation for Biometric Protection Systems

Mariia Nazarkevych[1[0000-0002-6528-9867]], Andrii Marchuk[1[0000-0001-5871-7053]], Lesia Vysochan[2[0000-0002-8978-5005]], Yaroslav Voznyi[1[0000-0002-5481-9973]], Hanna Nazarkevych[3[0000-0002-6528-9867]], and Anzhela Kuza[4[0000-0002-3937-6449]]

[1] Lviv Polytechnic National University, Ukraine
[2] Vasyl Stefanyk Precarpathian National University Ivano-Frankivsk, Ukraine
[3] Taras Shevchenko National University of Kyiv, Ukraine
[4] Lviv National Agrarian University, Ukraine
mariia.a.nazarkevych@lpnu.ua

**Abstract.** Personal authentication by fingerprint recognition depends on the correct identification of characteristic points of biometric images. This paper presents a scheme for identifying characteristic points. However, poor fingerprint input quality is generally observed due to unstructured patterns, unclear spine structures, and various background noises that have resulted in poor fingerprint recognition. Therefore, improving the input image is a crucial step for more accurate recognition. This paper proposes a new method of image filtering by filtering by non-periodic Ateb-functions. The functions of hyperbolic sine, cosine, tangent, cotangent are considered. The method of calculation of non-periodic Ateb-functions is shown. To identify the characteristic points, a set of bifurcation patterns was constructed, oriented along with different directions. The proposed method is implemented and tested on fingerprints The reliability results were tested based on NIST Special Database 302. A data set for estimating the parameters that verify fingerprints obtained from 162 samples of different quality. Experimental results show the effectiveness and accuracy of the method.

**Keywords:** Image Processing, Filtration, Biometric Images, Identification, Filtering.

## 1 Introduction

The world is developing in the direction of greater informatization of both individual sectors of the economy and society as a whole. The problem of information security is especially acute in connection with the rapid introduction of computer technology in the field of banking, insurance, medicine. The need to address the issue of information security is also due to various increases in the level of malicious crime, the result of which is to lead to significant material losses, whether it is a virus attack.

Information security is a young industry that is at the intersection of information technology and information security [1].

## 2 Information Technologies in Biometric Protection Systems

One of the common security technologies is biometric information security. These systems are convenient because they do not require storing complex passwords or carrying special identifiers (keys, cards, etc.), and it will be enough to say a code word, put a finger or brush, or substitute a face for the scan to access. It should be noted that in the theoretical variety of possible biometric methods are many and applied in practice among them quite a bit. The advantages of biometric systems include unique human qualities that cannot be forged: to leave a fake fingerprint with your own or to make the iris of your eye look like someone else's. Passport, driver's license, identity card from a password or personal identification number, biometric characteristics cannot be forgotten or lost [2].

One of the areas of protection of information systems is to equip the premises with computer equipment and procedures for opening software and databases with access devices [3]. Recommendations for the application of these methods in information security systems are offered.

Various approaches to machine learning and neural networks have been proposed for the collection, detection, classification, and analysis of fingerprints. First, let's look at the characteristics of fingerprints and their use in a criminal investigation. Also, we analyze and compare machine fingerprint learning algorithms in terms of classification, matching, feature extraction, fingerprint and vein fingerprint recognition, and counterfeit detection [4].

The quality of recognition is the high reliability of recognition—more in-formation than a normal image, it is the resistance of recognition to the deviation of the face from the front, it is also the resistance of recognition to the heterogeneity of lighting. But the most important sign is the absence of the need to contact the device.

Fingerprints are unique features of the skin. We can use it to identify a person through his unique ridges and formations. The fingerprint begins to form during the third to four months when the person is not yet born but is a fetus during pregnancy. Ridges are formed to hold in the fetus, not to slide when we squeeze an object [5]. They made a regular arrangement of patterns and have the location and combination of models of the characteristics of the spine. These structures of the ridges consist of many pores. Fingerprints are formed when sweat touches another substance on a smooth surface [6]. Scanning reliability does not depend only on the sensor. Further processing of the received data is the key to successful fingerprint recognition. In a fingerprint scanner with an optical sensor, essentially a monochrome matrix, the image comes in the form of a photograph. In the simplest scanners, the image is simply compared to a reference. Further processing is often based on working with several templates [7].

The digital code received from the scanner in a system with a linear thermal sensor is always a different pattern. The scan from the fingerprint is always different, the recognition quality depends on the angle under. swabbing your finger against moisture from the finger or the scanner surface [8]. The data supplied by such a scanner is a collection of points. No matter how you put your finger on the surface of the scanner, these points will always have the same bend.

It should be noted that when recognizing fingerprints by any type of sensors and algorithms, errors are inevitable [9]. Errors are usually divided into 2 types—not recognizing the correct print and recognizing the wrong print as correct.

# 3 Image Quality Requirements in a Biometric Security System

The fingerprint scan is converted into a template, which is then used for comparison. Currently, ANSI and US FBI standards are mainly used [10].

They define the following requirements for the imprint image:

- Each image is presented in an uncompressed TIF format.
- The image must have a resolution of at least 500 dpi.
- The image should be grayscale with 256 levels of brightness.
- The maximum angle of rotation of the print from the vertical is no more than 15 degrees.
- The main types of minutiae are ending and bifurcation.

Usually, more than one image is stored in the database, which improves the recognition quality. Images can be distinguished from each other by shift and rotation. The scale does not change, since everything from the seal is received from one device.

## 3.1 Properties of Aperiodic Ateb-Functions

Aperiodic functions include sine of Ateb-hyperbolic function $sha(n,m,\omega^*)$, the cosine of Ateb-hyperbolic function $cha(m,n,\omega^*)$, tangent of Ateb-hyperbolic function $tha(n,m,\omega^*)$, cotangent of Ateb-hyperbolic function $ctha(m,n,\omega^*)$, secant of Ateb-hyperbolic function $she(m,n,\omega^*)$, cosecant Ateb-hyperbolic function $chse(n,m,\omega^*)$.

For aperiodic Ateb functions, the identity is valid, which is a generalization of the basic identity for ordinary hyperbolic functions.

$$cha^{m+1}(m,n,\omega^*) - sha^{n+1}(n,m,\omega^*) = 1$$

Taking into account the relationship (2.18)–(2.21) we obtain the formulas for differentiation of hyperbolic Ateb-functions.

$$\frac{d}{d\omega^*} sha^{n+1}(n,m,\omega^*) = \frac{2}{n+1} cha^{m}(m,n,\omega^*)$$

$$\frac{d}{d\omega^*} cha^{n+1}(m,n,\omega^*) = \frac{2}{m+1} sha^{n}(n,m,\omega^*)\cdot$$

An important practical task is to calculate aperiodic Ateb-functions. To do this, Table 1 presents the domains and sets of values of aperiodic Ateb-functions.

**Table 1.** Properties aperiodic Ateb functions.

| Function | Area of definition | Set of values |
|---|---|---|
| $sha(n, m, \omega)$ | $(-\Pi^*(m, n); \Pi^*(m, n))$ | $(-\infty;+\infty)$ |
| $cha(m, n, \omega)$ | $(-\Pi^*(m, n); \Pi^*(m, n))$ | $[1;+\infty)$ |
| $tha(n, m, \omega)$ | $(-\Pi^*(m, n); \Pi^*(m, n))$ | $(-\infty;+\infty)$ |
| $ctha(m, n, \omega)$ | $(-\Pi^*(m, n);0) \cup (0;\Pi^*(m, n))$ | $(-\infty;0) \cup (0;+\infty)$ |
| $cshe(m, n, \omega)$ | $(-\Pi^*(m, n);0) \cup (0;\Pi^*(m, n))$ | $(-\infty;0) \cup (0;+\infty)$ |
| $she(n, m, \omega)$ | $(-\Pi^*(m, n); \Pi^*(m, n))$ | $(0;1]$ |

These properties were used to plot aperiodic Ateb-functions with different values of min parameters. The properties of aperiodic or hyperbolic Ateb-functions generalize the properties that ordinary hyperbolic functions have.

### 3.2 Method for Numerical Representation of a Periodic Ateb-Function based on a Taylor Series Expansion

The numerical representation method [7] describes the example of the function $cha(m, n, \omega)$. At the beginning we declare variables and assign values to constants, namely: we set accuracy for calculation of full *Beta*-functions; declare cycle variables. In the first stage, we create a text file to record the calculated numerical data. In the second stage, we calculate constant values for $cha(m, n, \omega)$, these include the period of the Ateb-function by formula (2.15), the value *a*, *b*, *c* according to formula (2.28). The calculation is performed with accuracy $\varepsilon = 10^{-10}$. The next stage—the basic calculation. We will describe it in detail. We organize a cycle on $\omega$ the segment (0;1] with a step of 0.01.

## 4 Proposed Method

Filtering based on Ateb functions Select the optimal parameters of Ateb-functions described in [11] and filter the image. The image was taken from the database.

The schedule of Ateb-Gabor functions is a schedule of modulated fragments of these functions. The length of the fragments for all frequencies of the Ateb-function is a constant value, which gives a different number of oscillations for different harmonics. It follows that a sufficiently well-localized Gabor function cannot be a basic wavelet transform [12].

In this study, Ateb-Gabor Filter filtering with hyperbolic functions was implemented, which expands the known filtration values [13].

The surface with the filter data is shown in Fig. 1. An image was taken from the freely available NIST Special Database (Fig. 2). The filtered image is shown in Fig. 3.

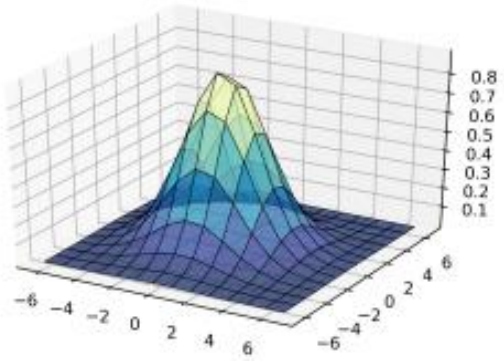


**Fig. 1.** Prezentation Ateb-Gabor filter with some parameters.

**Fig. 2.** Input image from NIST Special Database.

**Fig. 3.** Filtered image Ateb-Gabor filter with some parameters.

# 5 Classification of Biometric Images

Typically, fingerprint patterns can be found for three categories loops, *whorls*, and arches and rights loops, left loops, double loop (see Fig. 4–6).

**Fig. 4.** Classification of biometric images—whorl.

**Fig. 5.** Classification of biometric images—double loop.

**Fig. 6.** Classification of biometric images—right loop.

Fingerprint shaped arch. The arch pattern is found in 5% of all fingerprints. There are four categories of arch designs: plain arches, radial arches, elbow arches, and tent

arches. The ridges of the plain arches constantly flow from one surface to another pattern. The ridges begin on one side of the imprint and then slide. As for the radial arches, the spine is bent towards the thumb but not bent. In elbow sprains, the spines are placed to the little finger. However, tent arches have an angle, shape with an upward direction. They do not have the same type of flow as the plain arches, and, in particular, have an upward direction, directing upward the pattern on the bridges. In the loop pattern, at least one ridge remains inside the imprint, re-bends or crosses the line joining from the delta to the heart-fault, and ends at the side where the bridges begin. The pattern of the radial loop is concentric, the pattern is inclined to the radial bone, the thick bone from the top of the finger. The direction of the radial loop leading to the thumb. Radial loops are rare. But in general, we can find it on the index fingers.

The central pocket loop, which rotates in this pattern, the bridges create one incomplete scheme. This pattern can be spiral, oval, or take any type. Rectangles with a flow line have one or more twisted ridges. An example of the central pocket shown in Fig. 5.

Loops. The ridges rotate to form one complete contour with two deltas. Therefore, monochromatic loops have a round or spiral shape. In random curls, it has two patterns, as well as two or more deltas. Patterns of random twists are not the same. The ridges correspond to the characteristics of a specific subgroup. An example of a circular pattern is shown in Fig. 5.

Double-loop curls. This pattern consists of two different separate curls. A complete circuit is created with one or more bridges. An example of a double loop, which is shown in Fig. 6.

During this fingerprint analysis process, if the collected fingerprint is not clear, inaccurate, and incomplete, it can create problems in the recognition process. For this reason, fingerprint experts decide whether or not there is enough information on the printed material to identify.

The analysis involves determining the characteristics of the class and individual characteristics by comparing one point by one point until they find a match.

The collected seal falls into one of these three groups by analysis. After grouping, it again narrows to individual characteristics. Individual characteristics are unique characteristics for each person. They are very small discrepancies among the fingerprints. They are also known as details of Galton. They consist of three main types: ridges, bifurcations (dividing spine), and points. Fingerprint recognition is based on matching the pattern by identifying certain characteristics of the spine. If there are unclear differences between the two fingerprints, they remove the unknown fingerprints from the database. Otherwise, if the characteristics of the class are different, the imprint may be excluded. If the first characteristics and individual characteristics are the same between two fingerprints, the system skips them. In some cases, neither of these two options may be available.

Yes, it may not be possible to make it cheaper to compare effectively, that is, three potential outcomes may be available when examining fingerprints: exclusion, recognition, and ineffectiveness.

## 6 Conclusions

The filtration method based on aperiodic Ateb-Gabor functions is proposed in the work. The properties of Ateb-Gabor filtration were investigated for different rational parameters and their influence on filtration was carried out.

The classification of biometric prints concerning the characteristic distribution points of the ridges is shown.

Due to the low quality of the input images, poor recognition properties are observed. Filtration is used to improve these properties. We offer our method, which we consider universal, and which combines multiple filtering. So, improving the input image is a crucial step for more accurate recognition.

To identify the characteristic points, a set of templates in the form of bifurcations oriented along different directions was constructed. The proposed method is implemented and tested on fingerprints from the NIST Special Database 302. Experimental results show the effectiveness and accuracy of the method.

## References


1. Buriachok, V., et al.: Information and Cybersecurity: Sociotechnical Aspect (2015). [Publication in Ukrainian]
2. Lakhno, V., et al.: Clustering network attack features in information security analysis tasks. Cybersecur. Educ. Sci. Tech. **1**(9), 45–58 (2020). https://doi.org/10.28925/2663-4023.2020.9.4558. [Publication in Ukrainian]
3. Buriachok, V., Sokolov, V., Mahyar, T. D.: Research of caller ID spoofing launch, detection, and defense. Cybersecur. Educ. Sci. Tech. **3**(7), 6–16 (2020). https://doi.org/10.28925/2663-4023.2020.7.616
4. Hryshchuk, R., Hryshchuk, O.: A generalized model of fredholm's cryptosystem. Cybersecur. Educ. Sci. Tech. **4**(4), 14–23 (2019). https://doi.org/10.28925/2663-4023.2019.4.1423. [Publication in Ukrainian]
5. Nazarkevych, M., Voznyi, Y., Dmytryk, S.: Wavelet transformation Ateb-Gabor filters to biometric images. Cybersecur. Educ. Sci. Tech. **3**(7), 115–130 (2020). https://doi.org/10.28925/2663-4023.2020.7.115130. [Publication in Ukrainian]
6. Manickam, A., et al.: Bio-medical and latent fingerprint enhancement and matching using advanced scalable soft computing models. J. Ambient Intell. Humaniz. Comp. **10**(10), 3983–3995 (2018). https://doi.org/10.1007/s12652-018-1152-1
7. Huang, X., Qian, P., Liu, M.: Latent fingerprint image enhancement based on progressive generative adversarial network. IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops: 800–801 (2020). https://doi.org/10.1109/cvprw50498.2020.00408
8. Chhabra, M., Shukla, M. K., Ravulakollu, K. K.: Bagging- and boosting-based latent fingerprint image classification and segmentation. International Conference on Innovative Computing and Communications: 189–201 (2020). https://doi.org/10.1007/978-981-15-5148-2_17
9. Kim, J., et al.: Hand classification from fingerprint image using deep neural network. Comp. Mater. Contin. **63**(1): 17–30 (2020)
10. Brislawn, C. M., et al.: FBI compression standard for digitized fingerprint images. Applications of Digital Image Processing XIX **2847**: 344–355 (1996)

11. Nazarkevych, M., et al.: Detection of regularities in the parameters of the Ateb-Gabor method for biometric image filtration. East.-Eur. J. Enterp. Technol. **1**(2): 57–65 (2019). https://doi.org/10.15587/1729-4061.2019.154862
12. Nazarkevych, M., Yavourivskiy, B., Klyuynyk, I.: Editing raster images and digital rating with software. The Experience of Designing and Application of CAD Systems in Microelectronics: 439–441 (2015). https://doi.org/10.1109/cadsm.2015.7230897
13. Nazarkevych, M., et al.: Complexity evaluation of the Ateb-Gabor filtration algorithm in biometric security systems. IEEE 2nd Ukraine Conference on Electrical and Computer Engineering: 961–964 (2019). https://doi.org/10.1109/ukrcon.2019.8879945