UDC 004.056.55 DOI: 10.26565/2519-2310-2019-1-01

MATHEMATICAL MODEL OF THE BIOMETRIC SYSTEM OF FINGERPRINT AUTHENTICATION

Serhii Rassomakhin[1], Kateryna Budianska[1], Anna Uvarova[2], Mykhaylo Bagmut[1]

[1] V. N. Karazin Kharkiv National University, Svobody Sq., 4, Kharkiv, 61022, Ukraine
rassomakhin@karazin.ua, budyanskaya96@gmail.com, sapsanmiha@gmail.com

[2] Yuzhnoye State Design Office, 3, Krivorozhskaya St., Dnipro, 49008, Ukraine
annet.uvarova@gmail.com

Reviewer: Serhii Toliupa, Doctor of Sciences (Engineering), Full Prof., Taras Shevchenko National University of Kiev, 81 Lomonosova St., Kyiv, 03189, Ukraine.
tolupa@i.ua

Received on February 2019

Abstract: *This paper considers mathematical models of biometric fingerprint images, as well as basic computational procedures for fingerprinting. The main stages of processing dactyloscopic portraits based on the selection of local features, their filtering and digital processing are investigated. The developed software implements the transformation of fingerprint images with the subsequent formation of a cryptographically strong password sequence based on them. This allows you to simulate a dactyloscopic authentication system for the purpose of studying certain of its properties, estimating probabilistic performance indicators (error probabilities of the first and second kind), and so on.*

Keywords: *fingerprints; biometric image; password authentication; biometric system.*

1 Introduction

To date, biometric technologies are actively used in many areas of everyday life that are related to providing access to information in the tasks of identification and authentication of personality. Biometrics use the following features that are inherent to each individual: a papillary finger pattern, a pattern of the iris, voice parameters, a blood vessel pattern and so on.

All people have a unique fingerprint pattern, so everyone can be identified. Identification algorithms use points on fingerprints: the end of the pattern line, line branching, single points [1]. Also, the morphological structure of the fingerprint is considered, namely, the relative position of the closed, arched and spiral lines of the papillary pattern. The features of fingerprint portraits are transformed into a unique code that preserves the informative image of the imprint [1].

Thus, the actual formation of a model of a biometric fingerprint portraiture system and subsequent authentication is relevant. The purpose of this work is to develop a mathematical method and algorithm for converting fingerprint portraits for reliable authentication on fingerprints.

2 Formation of the model of fingerprints

Dactyloscopy is a subdiscipline of traosology that studies the configuration of papillary lines of the skin on the palms, fingers, legs and special techniques for their investigation in order to establish the identity of the person in the process of identification and authentication of users for access to a secure system, etc. [2]. There are two types of attributes: global and local. The global features include the core (center), the point "delta" (*starting point*), line type, counter line, types of patterns. Local signs are also minutias that are unique for each imprint of signs that determine the points of change in the structure of papillary lines (ending, splitting, rupture, etc.), the orientation of the papillary lines and the coordinates in these points. Each imprint can contain from 16 to 70 minutias [3].

Classification of all fingerprints is based on the existence of singular points - global fingerprint signs [4]. Although the fingerprints of different people may have the same global characteristics, it is completely impossible to have the same local characteristics. Therefore, global attributes are used to

classify the database into classes - the authentication phase. At the next stage, local identification is used to identify.

Papillary patterns on the human fingertips form three types of patterns, namely: "*loop*" (left, right, central, double), *delta* or arc (simple and acute), "*spiral*" (central and mixed) (Fig. 1).

a) *b)* *c)*

Fig. 1 - Types of fingerprint patterns (*a – loop; b – delta; c - spiral*)

The fundamental distinction between identification and authentication is the level of trust to the user. At the previous stage of system identification, the level of trust to the user being logged is a priori high. In a multi-user system, biometric identification must be carried out under the direct control of its owner or its representative, which confirms the user's authority and correctness of the behavior during the system training.

The biometric authentication mode, conversely, implies a low level of confidence in the identity that is authenticated. When biometric authentication, the applicant must prove the authenticity of his claimed name by presenting his unique biometric images. It should be noted that biometric authentication is potentially vulnerable if it is used regardless of the methods of classical authentication based on protocols using passwords and keys. An adequate level of information security can only be achieved by combining methods of classical and biometric authentication.

Any biometric system can accept errors of the first and the second kind. In biometrics, the most constant notions are FAR (*False Acceptance Rate*) and FRR (*False Rejection Rate*). The first number characterizes the probability of a false coincidence of the biometric characteristics of two people. The second is the likelihood of denial of access to a person with a tolerance. The system is considered to be better when the value of FRR is smaller with the same FAR values [5]. Fingerprint has a characteristic FAR of 0.001%, and FRR of 0.6% [6].

As matters currently stand, it can be identified three basic methods for comparing fingerprint images: comparing patterns of prints, correlation comparisons and a method that uses key points - minutias.

In the algorithm of pattern comparison, the peculiarities of the structure of the papillary pattern are used directly. The image of the fingerprint obtained from the scanner is divided into a large number of small particles, while the size of such cells depends on the required accuracy (the smaller the size of the cell, the more accurate the result is obtained).

The disposition of the lines in the cell is described by parameters of some sinusoidal wave: the initial phase shift, the wavelength and the direction of its propagation are determined. Accordingly, to receiving a fingerprint for comparison, it is aligned and is reduced to the same kind as the template. Then the parameters of the wave representations of the corresponding cells are compared.

The main advantages of this algorithm are quite high speed and low requirements for the quality of the resulting image. The method of comparison on the pattern has not yet become widespread because of the complexity of implementation, as well as high requirements to the mathematical base.

It should be noted separately that in the automated identification, there are several problems associated with the difficulty of scanning and recognizing some types of fingerprints.

In the algorithm that uses a correlation comparison, the received fingerprint is superimposed on each of the standards of the prints of the database and the calculation of the pixel difference between the input fingerprint and the reference.

The main advantage of this method is the low requirement for the quality of the received imprint. Disadvantages: the need for a large amount of memory to store the database, low speed algorithm. Every time a person places his finger at different angles and different places of the scanner's working area. This means that the process of comparing its fingerprint with the standards should include a lot of iterations, each of which the image obtained from the scanner returns at a small angle or slightly shifts [7]. Because of the duration of the comparison procedure, especially when solving the identification problem, the "one to many" comparison, this method is extremely rarely used for solving identification and authentication tasks.

The algorithm of a method that uses minutias describes a template that is formed on the basis of the fingerprint image on which the end points and branch points are marked. When comparing the key points at the input fingerprint image are also marked. After that, the minutias of the given imprint are compared with the templates. By the number of concurrency points, a decision is made on the identity of the images [8]. The advantage of this algorithm is the high speed of operation. That is why the algorithms of this class are the most common.

To work the algorithm for comparing fingerprints from key points, high quality images with low noise are required. Therefore, special image processing algorithms are used to improve the quality of the fingerprint images. In particular, as a model of noisy biometric imaging, the most commonly used normal distribution law with random variables. In this paper, the method of taking the inverse function is used to implement this model. This method is especially convenient to use in the case when the integral law of probability distribution is given analytically and a possible analytical take of the inverse function from it.

3 Modeling of normally distributed random variables in the processing of biometric images

The random variable means the value, which as a result of the trial takes a certain value, and it is unknown in advance, which is exactly [9].

According to the central limit theorem of probability theory, by adding a sufficiently large number of equally distributed independent random variables, we obtain a random variable with a normal distribution law [10] (1).

$$F\left(x\right) = P(X < x) = \sum_{x_i < x} P(X = x_i) = \sum_{x_i < x} p_i \,. \tag{1}$$

Due to the addition of more than ten random variables with uniform distribution in the interval $(0;1)$, we obtain a random variable, which with the accuracy sufficient for most practical problems can be considered as distributed according to the normal law [10].

For the quantitative characterization of the distribution law it is convenient to use the probability of an event $X < x$, where x- a certain variable. The probability of this event obviously depends on x. This dependence is given by the distribution function of a random variable X (2):

$$F(x) = P(X < x). \tag{2}$$

Properties of the distribution function are:

- the distribution function $F(x)$ does not decrease, that is, when $x_2 < x_1$ the $F(x_2) \geq F(x_1)$ inequality is performed;
- $F(-\infty) = 0$;
- $F(+\infty) = 1$.

Knowing the law of the distribution of random variables, we can construct the distribution function by the following rule.

The function of the distribution of a random variable always is a discontinuous step function, the jumps of which occur at points corresponding to the possible values of the random variable, and are equal to the probabilities of these values [11]. The sum of all jumps is equal to one (Fig. 2).

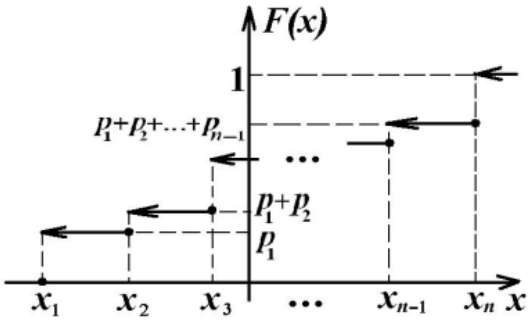

Fig. 2 - Bursting step function

Normal distribution law is found in nature very often, therefore, effective methods of modeling for it are developed. The formula for the probability distribution of the values of random variable x under the normal law has the form (3):

$$y = \frac{1}{\sigma_x \cdot \sqrt{2\pi}} \cdot e^{-\frac{(x-m_x)^2}{2\sigma_x^2}}, \quad (3)$$

Where x - a random variable; $y(x)$ - probability of acceptance of a random value of value x; m_x - mathematical expectation; σ_x - mean square deviation.

As you can see, a normal distribution has two parameters: the mathematical expectation m_x and the mean square deviation σ_x of the value x from this mathematical expectation.

Normalized normal distribution (Fig. 3) is called a normal distribution, which has $m_x = 0$ and $\sigma_x = 1$ [12]. With a normalized distribution, you can get any other normal distribution with given m_x and σ_x by the formula: $z = m_x + x \cdot \sigma_x$.

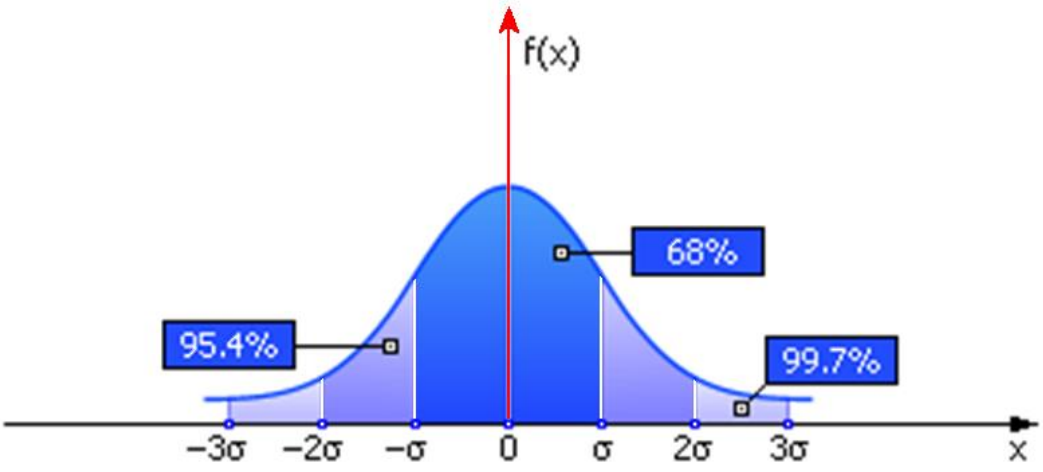

Fig. 3 - A graphical representation of the normal distribution law of a random variable x

The graph of the normal distribution law shows that in the interval $-\sigma < x < \sigma$ of the graph, 68% of the distribution area is concentrated, in the interval $-2\sigma < x < 2\sigma$ 95.4% of the distribution area is concentrated, and in the interval $-3\sigma < x < 3\sigma$ - 99.7% of the distribution area (the "rule of three sigmas").

Consider the question of simulating random variables given by the normal distribution law. In this paper, the method of taking the inverse function will be used.

In the case of continuous random variables, their probabilistic characteristics are determined by the distribution density. The density of the distribution of a random variable [13] X is called a function $f(x)$ that (4):

$$f(x) = F'(x), \tag{4}$$

where $F(x)$ is the distribution function of the quantity X.

Assume that the integral law of probability distribution $F(x)$ is given to us (5):

$$F(x) = \int_{-\infty}^{x} f(x)\,dx. \tag{5}$$

Then it is enough to play a random number, evenly distributed in the range from 0 to 1. Since the function F also varies in this interval, then the random event x can be determined by taking a reciprocal function graphically or analytically: $x = F^{-1}(r)$. Here r - the number generated by the reference *Random Number Generator* in the range from 0 to 1, x - generated as a result a random variable. Graphically, the essence of the method is depicted in Fig. 4, namely the probability density graphs and the integral probability density of x.

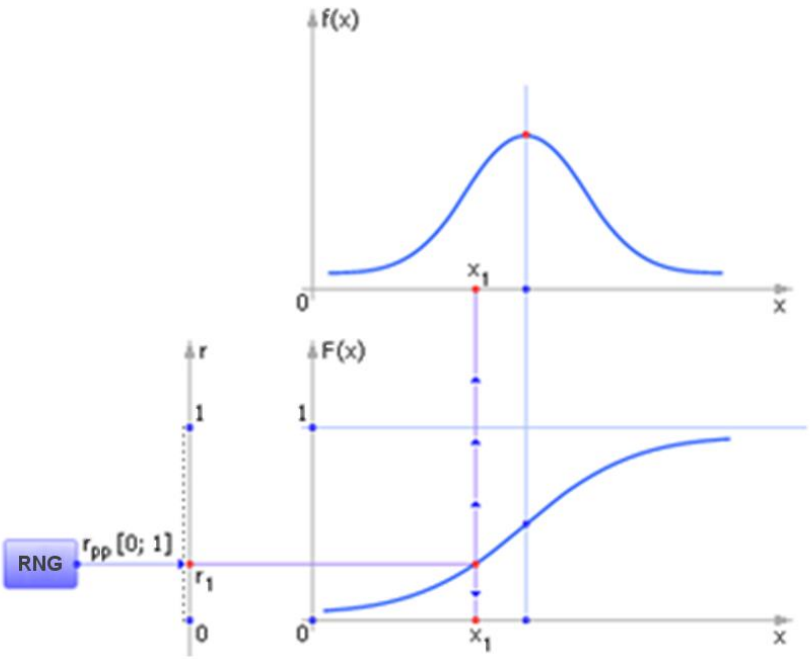

Fig. 4 - Illustration of the reverse function method for generating random events x

By the density distribution property $f(x) > 0$ for all x of the interval (a,b), the function $y = F(x)$ increases strictly in this interval (Fig. 3). Therefore, the function $F(x)$ has an unambiguous inverse function $x = G(y)$ with a range of values $y \in (0,1)$ and a definition area $x \in (a,b)$ on the interval (a,b). The function $x = G(y)$, as well as the function $y = F(x)$, is increasing (Fig. 5).

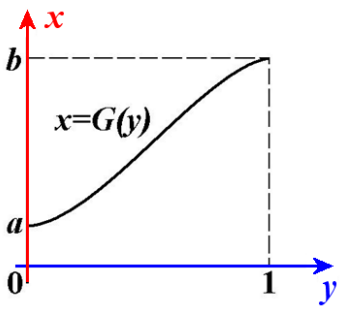

Fig. 5 - Graphic display of the function $x = G(y)$

This function also has an unambiguous reverse function on its interval of definition $(0,1)$. Obviously, this reverse function is $y = F(x)$. This method is especially convenient to use in the case when the integral law of probability distribution is given analytically and a possible analytical take of the inverse function from it.

4 Handles dactyloscopic portraits

4.1 Selection of key points in the image

Image processing is an important part in creating automated biometric identification systems.

Usually, the image obtained with the scanner is of low quality. The quality of this image is influenced by many factors: the strength of the finger pressure when scanning, the humidity of the air, the cleanliness of the finger and the scanner itself. Therefore, different methods of filtering are used to improve the quality of the original image. At the stage of thinning operation, the binary image of the image of the fingerprint is throttled to the skeleton.

The skeleton of the line is called a simple chain *(u,v)* passing near the geometric center of the line, and for each vertex p_1 there are exactly two adjacent to it vertices p_2 and p_3, thus, the vertices p_2 and p_3 are not adjacent.

Thinning operation is a morphological operation that brings a binary image to its skeleton. The thickness of all lines in the skeleton has a thickness of 1-2 pixels. For such a result, it is necessary to remove the extreme points from the black lines. The method pulls the line into the center, without making any breaks.

After that, in the skeleton of the image is searched for minutias - key points. In most algorithms for recognition, only two types of minutias are used: ending and branching.

The ending is called the top of the skeleton such that for it there is exactly one vertex adjacent to it. The branching is called a vertex of the skeleton, for which there are exactly three adjacent vertices and are pairwise noncontiguous.

For each key point, its type, their coordinates in the image and the orientation are determined.

To correctly determine the minutias, it is needed to process the image and then lead to a special format. The image processing can take place in two scenarios. Such scenarios are conditional, that is, it is possible to combine them.

The first scenario:

1) calculation of orientation of lines;
2) improving the quality of the lines;
3) binaryization of the image;
4) thinning operation to the image.

Second scenario:

1) adaptive filtering, allocation of interest zone;
2) binarization, the allocation of homogeneous areas;
3) morphological treatment;
4) thinning;
5) vectorization;
6) vector post-processing.

4.2 Digital fingerprint image processing

To date, there are several fingerprint filtering algorithms.

Smoothing filter

The smoothing filter is widely used to remove noise in the image in general and in the form of a fingerprint in particular. It consists in scanning the entire image of the window N - dimensionality $n*n$ and converting the intensity value for each pixel. The new value is calculated as the arithmetic mean of the value of all the pixels that fall into the window (6):

$$I(i,j) = \frac{\sum_{(x,y)}^{N} I(x,y)}{n^2}, \quad (6)$$

where $I(i,j)$ - the new value of the pixel intensity with coordinates (i,j), $I(x,y)$ - the initial intensity value for the pixel with coordinates (x,y).

Median filter.

Similarly, the method of removing noise in an image is widespread. The image is scanned by the $n \times n$ dimension window, the value of the intensity of the pixels inside each window is sorted ascending (descending); the output value is the intensity of the pixel located in the middle of the list.

The method of spatial filtration of the image.

The method of spatial filtration of the image is to realize the physical process of absorption and reflection of light. The algorithm is implemented in several stages:

1) The input of the algorithm receives a grayscale $n \times n$. Then the threshold processing of the fingerprint image is performed to obtain a binary image.

Let $R(i,j)$ - the value of the pixel with coordinates (i,j) in the binary image, then $R(i,j) = 1$ with $G(i,j) > R_0$, in all other cases $R(i,j) = 0$.

2) At this stage, the binary image is scanned by the $n \times n$ dimension window, for the central pixel of the window with coordinates (i,j), and the reflection coefficient is calculated, which is equal to the ratio of the number of $N(i,j)$ white pixels caught in the window to the dimension of the window (7):

$$k(i,j) = \frac{N(i,j)}{n^2}, \quad (7)$$

where $k(i,j)$ - the reflection coefficient of the pixel with coordinates (i,j).

3) Next, a new intensity value for each pixel is calculated. The new value of the intensity of the pixel is equal to the product of the reflection coefficient on the maximum intensity of light (8):

$$I(i,j) = k(i,j) \cdot I_{max}, \quad (8)$$

where I_{max} - the maximum value of intensity, $I(i,j)$ - the value of the intensity of the pixel with coordinates (i,j).

Gabor filter.

Processing of the image of a fingerprint by the given algorithm is carried out in several stages:

1) Normalize the image. Required to set the previous mean values and deviations. A normalized image G is defined as an image where $G(i,j)$ - the value of the normalized brightness of the pixel with coordinates (i,j).

The normalized image is calculated based on the mean and root mean square deviation of the original image, where M and VAR - the output values of the mean and the mean square deviation, are calculated by the formulas (9) (10):

$$M = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} I(i,j), \quad (9)$$

$$VAR = \frac{1}{N^2} \sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \left(I(i,j) - M\right)^2. \quad (10)$$

2) Orientation image is calculated from the normalized image. It is defined as an image where $O(i,j)$ - the local orientation (angle of inclination) of the projection in the pixel with the coordinates (i,j) (11):

$$O(i,j)=\frac{1}{2}arctg\left(\frac{d_x^2(i,j)d_y^2(i,j)}{2d_x(i,j)d_y(i,j)}\right), \quad (11)$$

where $d_x(i,j)$ and $d_y(i,j)$ - gradients of the pixel with the (i,j) coordinates on the axes X and Y respectively.

3) From the normalized image, the frequency image F is calculated. Frequency image is an image where $F(i,j)$ - the local frequency of the protuberance, which is defined as the frequency of papillary lines of the image of the fingerprint. If due to the features of the papillary pattern, it is not possible to determine the pixel frequency, then its frequency is defined as the average value of the frequency of adjacent blocks.

Let I - the number of pixels between two adjacent vertices of the crests in the dimension block $W\times W$ with the center of which is a pixel with coordinates (i,j), then the frequency in this pixel will be (12):

$$F(i,j)=\frac{1}{I}., \quad (12)$$

4) Binaryization of the image. We will define a binary image R as an image $N\times N$ showing the (i,j) pixel category. The pixel may be a pixel of the hollow or pixel of the ridge.

$R(i,j)=1$, if $G(i,j)>R_0$, in all other cases $R(i,j)=0$ where $G(i,j)$ - the threshold of masking, R_0 - the intensity of the pixel of the normalized image.

5) The use of Gabor filters configured for the local orientation of the speeches, applies to the normalized input image (13):

$$G(x,y)=exp\left(-\frac{1}{2}\left(\frac{x_\varphi^2}{\sigma_x^2}+\frac{y_\varphi^2}{\sigma_y^2}\right)\right)cos\left(2\pi\theta x_\varphi\right), \quad (11)$$

where $x_\varphi=x\cos(\varphi)+y\sin(\varphi)$; $y_\varphi=-x\sin(\varphi)+y\cos(\varphi)$; φ - the orientation of the Gabor filter, θ - the frequency of the sinusoidal plane wave, σ_x^2 and σ_y^2 - the space constants of the Gaussian bypass along the axes x and y, respectively. These constants are established and adjusted on the basis of empirical data on the operation of the algorithm.

For the Gabor filter, you need to set up a Fourier transform, which gives the frequency information contained in the signal, that is, what the content of each frequency in the signal is. The integral is taken from $-\infty$ to $+\infty$ to the entire time axis. For the Fourier transform, it is equally true whether there is a certain frequency throughout the signal being studied, or it arose at a certain time, its contribution will still be the same.

Fourier transform is not suitable for the analysis of nonstationary signals, with one exception, when we are interested only in frequency information, and the time of existence of spectral components is not important. To correct these shortcomings Gabor's transformation can be used. Let (14):

$$g_a(t)=\frac{1}{2\sqrt{pa}}e^{\frac{-t^2}{4a}}, \quad (12)$$

where a is a fixed parameter. The function g_a is used as the time window.

Fig. 6 shows the Gabor function, which is a composition of the cosine and exponentials.

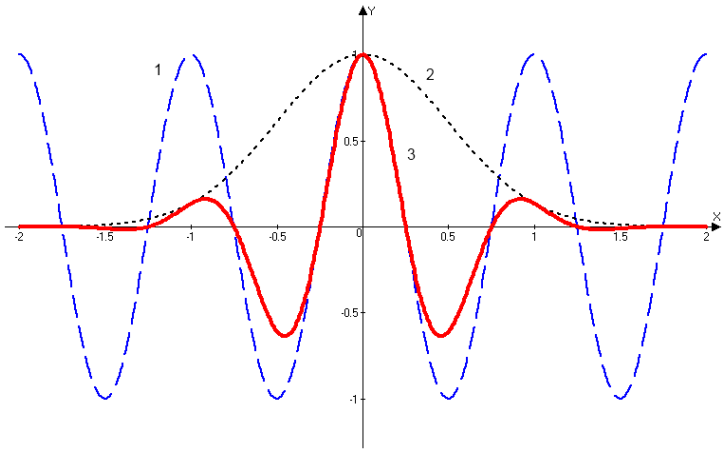

Fig. 6 - The function of the Gabor (3), which is a composition of the cosine function (1) and exponent (2)

Indeed, Gabor's transformation localizes the Fourier transform around a point $t = b$. To construct a one-dimensional Gabor filter, we use the formula (15):

$$G(x) = exp\left(-x^2 / 2\sigma^2\right) \times cos(2\pi\theta x), \quad (13)$$

where σ - the standard deviation of the Gaussian nucleus, which determines the amplitude of the function, θ is the frequency of oscillation, defined as $\theta = \frac{1}{T}$, where T - the period of function $cos(2\pi\theta x)$. The more is σ, the more gentle the form will accept the function.

5 Modeling and analysis of local features

Consider a heuristic approach based on the method of structural and statistical analysis. The main idea of the proposed model lies in the formation of the space of independent attributes when recognizing images given in the form of images. To describe each source image, methods are used to search the main components of the element (that is, the definition of structural features) and to calculate the statistical characteristics of this image of the fingerprints.

The proposed model of operators for identifying the characteristic features of fingerprint images when identifying a person includes the stage of determining the set of fingerprint features. At this stage, a set of characteristic features of fingerprints is formed, which are determined using both the structural method and the statistical method of determining the characteristic features of the images. In determining the structural features of fingerprints (for example, capillary lines of the imprint and special points of the prints), the structural method is used, and when calculating the various statistical characteristics of the image under consideration (for example, texture characteristics based on statistics of the first order), the statistical method. As a result of this stage we will get a set of features that characterize fingerprints. At the next stage there is a selection of subsets of strongly related features. At this stage, the system of "independent" subsets of attributes is determined. The following is a definition of representative features in each subset of characteristic strongly related features. At this stage, from each subset of such signs a single sign is determined and as a result of the implementation of this stage a set of representative features is distinguished. As a result of this stage we get a reduced space of signs, the dimension of which is much smaller. The final step is to identify the desired features. As a result of this stage, the best signs of fingerprints are formed.

Thus, a model of operators of the formation of the space of signs on the images of fingerprints is constructed. In the process of solving the practical problem it is determined that the stages of formation of subsets of "independent" features, namely, the question of determining the number of these subsets and a set of attributes on the image of fingerprints, as well as choosing a model of recognition, are important in solving the problem. Therefore, it is necessary to continue the study based

on the identified features. The developed model can be used in the compilation of various software complexes, focused on solving tasks of classification of objects, given in the form of images.

To solve the problem of identifying local features in this work it is proposed to apply a mathematical model of the salesman problem.

The mission of a salesman is important and difficult to solve. It represents the problem of finding the shortest Hamiltonian path in a complete finite graph with N vertices. In order to apply a mathematical device in solving a problem, it is necessary to present it as a mathematical model. The salesman's task can be presented as a graph using the vertices (minutias) and edges (the distance between the minutias). Let i, j - the vertices, and ribs (i, j) - the paths of communication between the points. In this case, for each of the edges you can match the criterion of the utility of the route $c_{ij} \geq 0$.

The Hamiltonian cycle can be called a route that involves passing through each vertex of the graph exactly once. In order to simplify the task and guarantee the existence of such a route, it is necessary that the model graph is fully connected. All known methods for finding the exact solution include searching for a space of decisions, which expands exponentially depending on N. The mission of a salesman can be solved with heuristic, search and precise algorithms.

Exact algorithms include the algorithm of full-fledging and the method of branches and boundaries.

The exhaustive search algorithm searches for $N!$ space solutions by scrolling through all the options. The result of the algorithm is the exact solution. The disadvantage of this algorithm is its temporal complexity - the search space grows exponentially, so when N is heuristic and search algorithms are not significantly less used.

Experimentally, the complexity of this algorithm was evaluated as $t = 0{,}0056 \cdot e^{(1{,}3789 \cdot N)}$ [14].

The advantages of this algorithm include the possibility of parallelization and the exact solution of the problem.

The method of branches and boundaries is the development of exhaustive search algorithm. Its essence is to add a test of the criterion that limits the functions and proceeds from the task at which, at a certain level, you can pause the construction of this branch of the permutation tree.

It retains all the positive properties of the exhaustive search algorithm, but nevertheless is not suitable for tasks where N is not very small. Experimentally, the complexity of this algorithm was evaluated as $t = 0{,}0745 \cdot e^{(0{,}8485 \cdot N)}$ [14].

In the case of use as a minimal initial solution, a solution obtained by the "greedy" method is used. The complexity of the algorithm will be $t = 0{,}3164 \cdot e^{(0{,}7469 \cdot N)}$ [14]. The advantages of this algorithm include the possibility of parallelization and the exact solution of the problem.

Heuristic algorithms include the method of incorporating a remote and BV-method.

The idea of incorporating a remote method is that the minutias, which are as far apart as possible, will never be adjacent to the chain. These two points will be the basis for further resolution. Then again there is a vertex that is as far removed as possible from the vertices already enclosed in the chain. There is a minimum sum of the lengths of the edges between the vertex found and the pair of adjacent vertices in the chain, which sets the place in the chain of the found vertex. This algorithm has a linear complexity, gives an approximate solution to a problem and can not be parallelized. His temporal complexity was appreciated as $t = 28{,}0600 + (-1{,}6069 \cdot N) + (0{,}0227 \cdot N^2)$ [14].

The BV method is based on an analysis of the existing reference route and its optimization. The decision can be divided into two stages: obtaining the original reference solution and optimizing the initial solution. The initial solution is the best of all decisions made on the basis of the "greedy" method. The second stage is to modernize the resulting initial reference route with the help of BV modifiers, which allow to identify non-optimal areas and convert them. This algorithm has a quadratic complexity, gives an approximate solution and can be parallelized at the 2nd stage [15]. His temporal complexity was appreciated as $t = -169{,}40 + (15{,}5786 \cdot N) + (-0{,}4104 \cdot N^2) + (0{,}0040 \cdot N^3)$ [14].

Search algorithms. The Genetic Algorithm and the Ant Colony System (ACS) algorithm are "leaders" among search algorithms [14].

The most optimal (result / time) among search algorithms is Genetic Algorithm. However, it also has its disadvantages associated with premature convergence (it is not always possible to find a way out of the local minimum). Experimentally its temporal complexity was estimated as $t = 683 + (-42{,}467 \cdot N) + (1{,}0696 \cdot N^2)$ [14].

Ant Colony System (ACS) is the development of the Ant System (AS) algorithm. Its main differences are:

- in the function of choosing a new point the balance between the use of accumulated knowledge and the study of new possible solutions is clearly set;
- at global renewal of pheromone (at the conclusion of each iteration) its addition occurs only to the arcs belonging to the global shortest path.

Heuristic algorithms are found much faster than the search algorithms. This is connected, as a rule, with the linear organization of the method itself and allows them to be used in those tasks, when computing time is a critical parameter. Exact methods are little suitable for solving problems of large size (unable to solve a task in a reasonable time), and search algorithms are a compromise between heuristic and precise methods [14].

6 Conclusion

Thus, the mathematical models and operations investigated allow us to formulate a list of unique biometric features that can be applied in user authentication systems. Structurally, the proposed model of the biometric fingerprint authentication system consists of the following steps.

In **the first stage**, it is necessary to generate normally distributed random variables. Since the normal distribution law is encountered in nature very often, so for it effective methods of modeling have been developed. In this paper, we propose using the method of taking the inverse function. This method is especially convenient to use in the case when the integral law of probability distribution is given analytically and a possible analytical take of the inverse function from it.

At the next, the **second stage**, it is necessary to process the data from the matrix formed at the previous stage. Since we are only interested in key points (they will correspond to "1" in the matrix), then at this stage the task of finding the shortest path will be solved, that is, a chain of points, sorted by minimum distances between the points, will be created.

In the **third stage**, the algorithm "Method of branches and boundaries" will be used to solve the salesman problem. Such an optimization algorithm is one of the effective polynomial algorithms for finding approximate solutions of the salesman problem, as well as solving similar problems in finding routes in graphs. The general idea of the method can be described in the example of finding the minimum of a function $f(x)$ on the set of valid variable x values. For the method of branches and boundaries, two procedures are required: branching and finding the marks (boundaries). The branching procedure consists in splitting the set of permissible variable x values into subsets of smaller sizes. The procedure can be applied recursively. The resulting subsets form a search tree or tree of branches and boundaries. The nodes of this tree are constructed subsets of values of a variable x. The procedure for finding estimates is to find the upper and lower bounds for solving the problem on a subset of admissible values. Discrete optimization methods, in particular branches and boundaries, allow finding optimal or approximate solutions for quite large tasks. The result of this stage is an integer expression, which is the optimal way in the graph, with vertices of which there are minutias.

On the last, fourth stage, the formation of a passive sequence occurs. To do this, as one of the options, the SHA-256 hexing algorithm will be applied to the integer expression. With regard to the use of hexing during the formation of a passive sequence, such a method requires additional research in the further development of work. Technical characteristics of the SHA-256 hex function: The length of the message digest is 256 bits, the length of the internal state is 256 (8×32) bits, the block length is 512 bits, the iteration cycles are 64.

The scheme of the computational algorithm of the developed software implementation of the biometric fingerprint authentication system is shown in Fig. 7.

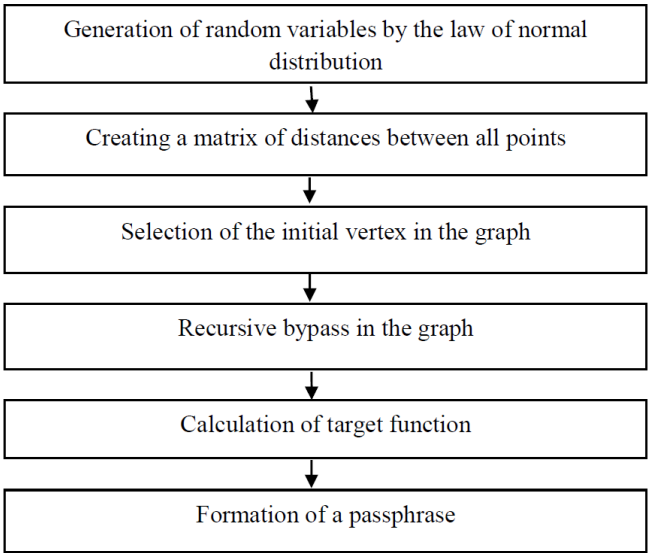

Fig. 7 - Scheme of computational algorithm

The developed software performs the transformation of fingerprint images, formed by the normal law of random variables, with subsequent transformation into a passive sequence. Consequently, it can be provided for modeling the fingerprint authentication system in order to investigate certain properties of it, to evaluate the probability indicators of efficiency (probabilities of the first and second kind errors), etc. These and other studies are a promising direction for our further scientific works.

References

[1] Дактилоскопия и генотипоскопия в судебной медицине. URL: http://www.forens-med.ru/book.php?id=105

[2] Криміналістичне дослідження слідів рук (дактилоскопія). URL: http://pidruchniki.com/2015060965282/pravo/ kriminalistichne_doslidzhennya_slidiv_ruk_daktiloskopiya

[3] Shvets V., Fesenko A. Basic biometric characteristics, modern systems and technologies of biometric authentication. *Ukrainian Scientific Journal of Information Security*. 2013. Vol. 19. P. 2 – 103.

[4] Рыканов А.С. Анализ методов распознания отпечатков пальца. *Системи обробки інформації*. 2010. Вип.6 (87). С. 164 – 171.

[5] Chernychenko I.V. Separate aspects of the formation of fingerprinting until 1900. *Bulletin of criminal justice*. 2005.№ 3. P. 136.

[6] Romanov V. O., Galelyuk I.B., Klochan P.S. Technologies of person's authentication by biometric characteristics. *Computer means, networks and systems*. 2010. № 9. P. 54 – 61.

[7] Зайцев В.Г., Степенко К.С. Спосіб контролю доступу на підставі розпізнавання відбитків пальців. URL: http://pmk.fpm.kpi.ua/arhive_2009/36-Stepenko.pdf

[8] Moroz A.O. Biometric Technologies. Methods of fingerprinting. *Mathematical Machines and Systems.* 2011. P. 3 – 64.

[9] Медична інформатика URL: http://intranet.tdmu.edu.ua/data/kafedra/internal/informatika/classes_stud/uk/med/biol/ptn.htm

[10] Вітлінський В.В. Моделювання економіки. Моделювання випадкових величин як системотвірна імітаційного процесу моделювання. URL: http://ecolib.com.ua/article.php?book=17&article=1540

[11] Вихман В.В., Якименко А.А. Биометрические системы контроля и управления доступом в задачах защиты информации: учебно-метод. пособие. Новосибирск: Изд-во НТГУ, 2016. 54 с.

[12] Руденко В.М. Математична статистика. URL: http://pidruchniki.com/18421120/statistika/normalniy_rozpodil

[13] Випадкові величини. Робоча навчальна програма дисципліни «Теорія ймовірностей та математична статистика» для підготовки бакалаврів за спеціальністю 6.091500 – Комп'ютерні системи та мережі. URL: http://elib.lutsk-ntu.com.ua/book/knit/vm/2011/11-47/page6.html

[14] Борознов В.О. Исследование решения задачи коммивояжера. *Вестник Астраханского государственного технического университета. Сер. Управление, вычислительная техника и информатика.* 2009. С. 147–151.

[15] Борознов В.О. Исследование эвристического метода решения задачи коммивояжера. *Электронный журнал "Исследовано в России»*. 2008. С.322 – 328. URL: http:// zhurnal.ape.relarn.ru/articles/2008/028.pdf

Рецензент: Сергій Толюпа, д.т.н., проф., Київський національний університет імені Т. Шевченка, м. Київ, Україна. E-mail: tolupa@i.ua

Надійшло: Лютий 2019.

Автори:

Сергій Рассомахін, д.т.н., зав. кафедри Безпеки інформаційних систем і технологій, Харківський національний університет ім. В. Н. Каразіна, майдан Свободи 6, Харків, 61022, Україна. E-mail: rassomakhin@karazin.ua

Катерина Будянська, студентка факультету комп'ютерних наук, Харківський національний університет імені В.Н. Каразіна, майдан Свободи 4, Харків, 61022, Україна.
E-mail: budyanskaya96@gmail.com

Ганна Уварова, провідний інженер, Конструкторське бюро «Південне» ім. М.К. Янгеля», вул. Криворізька 3, Дніпро, 49008, Україна. E-mail: annet.uvarova@gmail.com

Михайло Багмут, аспірант, факультету комп'ютерних наук, Харківський національний університет ім. В.Н. Каразіна, майдан Свободи 6, Харків, 61022, Україна. E-mail: sapsanmiha@gmail.com

Математична модель біометричної системи автентифікації відбитків пальців.

Анотація. У роботі розглядаються математичні моделі біометричних образів відбитків пальців, а також основні обчислювальні процедури дактилоскопії. Досліджено основні етапи обробки дактилоскопічних портретів, засновані на виділенні локальних ознак, їх фільтрації і цифровій обробці. Розроблене програмне забезпечення реалізує перетворення образів відбитків пальців з подальшим формуванням на їх основі криптографічно потужної парольної послідовності. Це дозволяє моделювати систему дактилоскопічної автентифікації з метою дослідження її певних властивостей, оцінки імовірнісних показників ефективності (ймовірностей помилки першого і другого роду), тощо.

Ключові слова: відбитки пальців, біометричний образ, парольна автентифікація, біометрична система.

Рецензент: Сергей Толюпа, д.т.н., проф., Киевский национальный университет имени Т. Шевченко, г. Киев, Украина. E-mail: tolupa@i.ua

Поступила: Февраль 2019.

Авторы:

Сергей Рассомахин, д.т.н., зав. кафедры Безопасности информационных систем и технологий, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина. E-mail: rassomakhin@karazin.ua

Екатерина Будянская, студентка факультета компьютерных наук, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина. E-mail: budyanskaya96@gmail.com

Анна Уварова, ведущий инженер, Конструкторское бюро «Южное» им. М.К. Янгеля», ул. Криворожская 3, Днепр, 49008, Украина. E-mail: annet.uvarova@gmail.com

Михаил Багмут, аспирант факультета компьютерных наук, Харьковский национальный университет им. В. Н. Каразина, пл. Свободы 6, Харьков, 61022, Украина. E-mail: sapsanmiha@gmail.com

Математическая модель биометрической системы аутентификации по отпечаткам пальцев.

Аннотация. В работе рассматриваются математические модели биометрических образов отпечатков пальцев, а также основные вычислительные процедуры дактилоскопии. Исследованы основные этапы обработки дактилоскопических портретов, основанные на выделении локальных признаков, их фильтрации и цифровой обработке. Разработанное программное обеспечение реализует преобразование образов отпечатков пальцев с последующим формированием на их основе криптографически сильной парольной последовательности. Это позволяет моделировать систему дактилоскопической аутентификации с целью исследования определенных ее свойств, оценки вероятностных показателей эффективности (вероятностей ошибки первого и второго рода), и тому подобное.

Ключевые слова: отпечатки пальцев; биометрический образ; парольная аутентификация; биометрическая система.