Biometrics Statistical Data Evaluation in the Access Systems

M.Zilys, A.Valinevicius, A.Viluckis

Department of Electronic Engineering, Kaunas University of Technology
Studentu 50, 3031 Kaunas, Lithuania,
e-mail: mindaugaszilys@takas.lt, algimantas.valinevicius@ktu.lt

Abstract: *When the information technologies are improving, the security systems are increasingly developing, too. The higher requirements of safety and higher degree of integration are emphasized. In addition to the functional, schemotechnical, and systemic integration, the integrated security is developing. It consists of a variety of technical safety measures that are aggregated into the integral complex of information computing and functioning according to a single algorithm [1]. The procedure of control of persons' access to certain data plays an important part in the structure of the integrated security system. Now many access control systems that function according to various algorithms of identification has been created. In addition, it is being searched for new ways how to deal with this problem. The biometric identification is one of the new methods of controlling the access system. The objective of this work is to evaluate reliability of use of biometric data, namely, a fingerprint, in the access systems, considering the quality of a fingerprint and appropriate conditions of its approbation.*

1. Introduction The integrated security system consists of: physical protection; network protection; software protection and data protection.

Security of an object depends on the particular conditions and degree of reliability that is wanted to achieve. Subject to a required degree of safety, components of the security system [2] or just their parts are chosen.

Under necessity to control flows of personnel, i.e. in order to increase a safety degree in certain areas, one more component, the access control system, is used. A required access control system may be compounded of a simple mechanical lock or of a maximum integrated security system containing various methods of person identification.

The main purpose of any entrance system is to let automatically in those who are permitted to enter and not to let in those who are prohibited to enter. The system enables to control the situation, order, safety of personnel and customers, inviolability of property and tangibles, to restrict a flow of visitors or employees in certain zones of a building. It is not just the equipment and software; it is also a well thought - out and organized control system.

Many access control systems have one fundamental disadvantage: after having lost a code or card, the system does not notice a trespasser or it restrains the entrance. There is a variety of ways to solve this problem: enter of a personal code before submission of a card, video or audio verification; checking of additional physiological parameters of a person[1-3]:.

2. Biometric access control systems. The biometric identification is the user's identification by comparing the biometric data presented by him with the biometric data existing in a database [4].

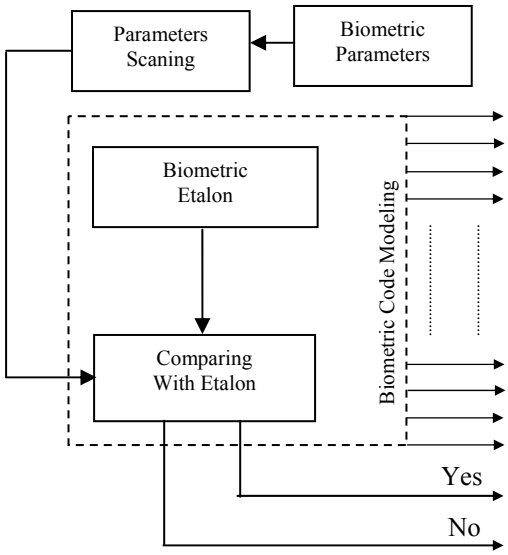

Fig 1. The structure of biometric identification system

A biometric system consists of three main parts: device identifying the parameters of a person who is being checked; device of computing and comparison of received data; device of transmission of received data.

A checked subject is identified if his parameters match the ones in the database. In order to ensure the selection of a relative biometric etalon out of the database and to ensure a higher degree of safety, additionally, a classical identification is also used, i.e. a subject must submit his personal data. All devices of biometric identification function under a similar principle. First of all, a user must register in the system, i.e. the primary scan of his biometric characteristics (a few of them), personal data recording, etc., are performed. For further use, an electronic sample (etalon) is formed of the received biometric data. Usually, a file of biometric data consists of a certain array of elements which present various characteristics of data or of their interrelationship that are received during computation of the biometric image Fig 1.

As the other entrance control systems, the biometric one functions under the algorithm created according to the particularity of the used biometric data.

3. Algorithms and modelling of identification of biometric data (a fingerprint). During the procedure of identification, the biometric data submitted by a user are computed according to an algorithm of identification of biometric data, that is formed in the security system. The classification of data into subgroups according to certain characteristics is a principle of many algorithms.

The algorithms used in contemporary access control systems are developed on the grounds of various methods (mathematical, graphical, etc.) [5].

They are classified as theory of taking a decision; structural, neural networks.

Here, the simplified model of the algorithm is presented:

A user is identified when the following conditions are met: $S_1 \geq T_1$; $S_2 \geq T_2$; $S_3 \geq T_3$, where S_1 the control coefficient of data comparison; S_2 means the control coefficient of comparison of nodes' positions; S_3 means the control coefficient of comparison of nodes' types. T_1, T_2, and T_3 mean the coefficients received during the procedure of identification.

If any of the inequalities is not met, a negative decision is adopted.

The algorithms of biometric identification systems are formed after having created a mathematical schedule of the biometric process. This mathematical description of the biometric model is based on the statistical mathematic theory.

The main characteristics of any biometric access system are the following: FRR (identification of a wrong image as a right one) and FAR (identification of a right image as a wrong one) [4]. It will be attempted to evaluate probabilities under which a chosen model would be identified and the security system would surely function.

First of all, one of the fundamental problems, a choice of a scanning device and fixing of its parameters, should be singled out. The choice should be determined by the resolution coefficient, i.e. what resolution device must be used in order to ensure the resolution of parameters necessary to the biometric identification.

It will be tried to assess the chosen model of a fingerprint: parameters of the image elements- the position (x,y); the orientation angle- (θ). The amount of image elements- n. r_0- the toleration of an image element, that occurs due to the error of a scanning devise. A- the size of the tolerance of a whole image. Mathematical model is shown in Fig 2.

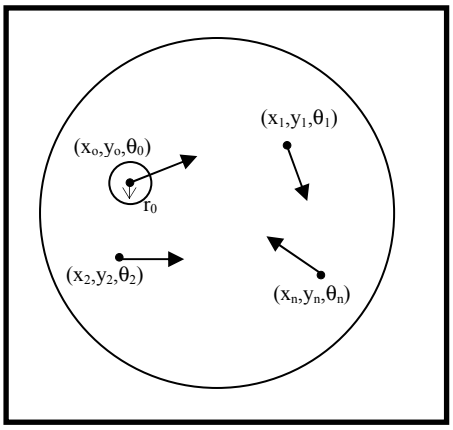

Fig 2. .Mathematical model of image elements

The probability, under which a complete set of the image elements, a pattern, should match a primary image, will be assessed.

The set of elements of a primary image is:

$$I = \{(x_1', y_1', \theta_1'), (x_2', y_2', \theta_2'), ..., (x_n', y_n', \theta_n')\} \quad (1)$$

the set of elements of a pattern is:

$$T = \{(x_1, y_1, \theta_1), (x_2, y_2, \theta_2), ..., (x_n, y_n, \theta_n)\} \quad (2)$$

then, let's set a condition that an image element j of the set of primary image will match an image element i of the set of pattern on the case if:

$$\sqrt{(x_i' - x_j)^2 + (y_i' - y_j)^2} \leq r_0, \quad (3)$$

$$\min(|\theta_i' - \theta_j|) \leq \theta_0. \quad (4)$$

The probabilities that the image elements will match are:

$$P(d \leq r_0) = \frac{\pi r_0^2}{A} \quad (5)$$

$$P(\min(|\theta_i - \theta_j|) \le \theta_0) = \frac{\theta_0}{360}; \quad (6)$$

If supposing that we have n elements of a primary image, then the probability that at least one of them will match an element of a pattern is n times higher:

$$P(d \le r_0) = \frac{n\pi r_0^2}{A}; \quad (7)$$

The evaluation of orientation of a node in relation to the other nodes makes a great impact on the process of identification.

The orientation of nodes is determined with the help of gradients' analysis of the binary model of the image in the image block. The orientation of the block itself is calculated by the method of statistical computation (averaging, etc.) of nodes' gradients.

In order to evaluate the orientation, the following algorithm is used [6]:

1) Bringing an image under W x W blocks;
2) Evaluation of the gradients G_x and G_y of the nodes' orientation in relation to a block;
3) The orientation of each node in relation to a block is evaluated by:

$$V_X(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} 2G_X(u,v)G_Y(u,v); \quad (8)$$

$$V_Y(i,j) = \sum_{u=i-\frac{W}{2}}^{i+\frac{W}{2}} \sum_{v=j-\frac{W}{2}}^{j+\frac{W}{2}} (G_X^2(u,v) - G_Y^2(u,v)); \quad (9)$$

$$\theta(i,j) = \frac{1}{2}\tan^{-1}\left(\frac{V_X(i,j)}{V_Y(i,j)}\right); \quad (10)$$

where W x W means the size of a block (e.g. 32 pixels); G_x and G_y- the meanings of gradients in the directions x and y, accordingly.

4) The average evaluation of the orientation of the block's nodes in a block:

$$C(i,j) = \frac{1}{N}\sqrt{\sum_{(i',j')\in D} |\theta(i',j') - \theta(i,j)|^2}, \quad (11)$$

$$|\theta' - \theta| = \begin{cases} d & if\ (d = (\theta' - \theta + 360) \bmod 360) < 180 \\ d - 180 & \text{In the opposite case} \end{cases} \quad (12)$$

where D means the size of a node in a block; N means the amount of nodes in a block.

If C(I,j) is calculated greater than a certain predetermined coefficient T_e, then, a negative decision is taken. The whole procedure is performed anew after having changed the size of the blocks, i.e. after having changed the resolution coefficient of a scanner.

Thus, the conclusion that reliability of the identification process depends much on the resolution capacity of a chosen scanner and on the conditions of scanning may be drawn. The higher the resolution coefficient of a scanner is, the smaller image blocks may be used, and higher reliability may be ensured.

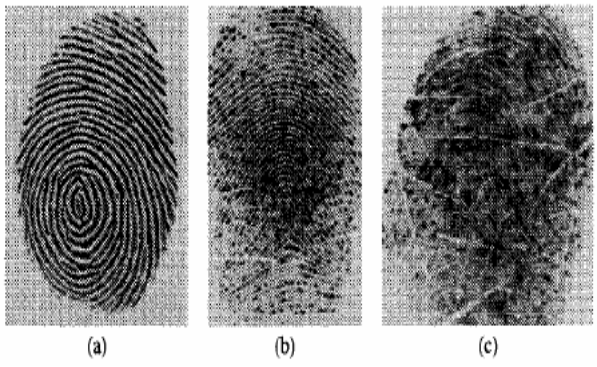

Fig 3. The samples of a fingerprint:(a) good quality; (b) medium quality;(c) bad quality.

4. Scanning speed of a fingerprint and analysis of reliability. The objective of the research: by imitating the change of the resolution of a scanner (or by changing the quality of an image), to explore the possibilities of identification of a fingerprint in relation to the quality and light Fig 3. While changing the quality of an image (while making it worse), it is automatically necessary to use a scanner of higher resolution. By increasing the resolution of a scanner, a possibility to reduce the image blocks would occur what would protect from images of bad quality. In the course of the investigation, the program package of finger identification examination "FingerCell 1.0 Evaluation version" was used.

The fingerprints were computed with the help of the program package "Adobe Photoshop 7.0" by using the functions of the filters of the program package, i.e. an image is treated by random noises.

Conditions of the research- FAR- 0.1%; possible rotation angle of an image- 360°. It means that the program allows the orientation 360° of a whole image, i.e. the rotation of a whole image by any angle makes no impact on the reliability of identification.

The method of the research: changing quality of a biometric image (a fingerprint). The dependence of computing speed and reliability of a biometric image on the quality is determined.

The quality of a fingerprint is determined by: the external factors (the emergence of the so called refractions, characteristics of the skin, etc.) and systemic factors (the capacities of a scanner, light, etc.)

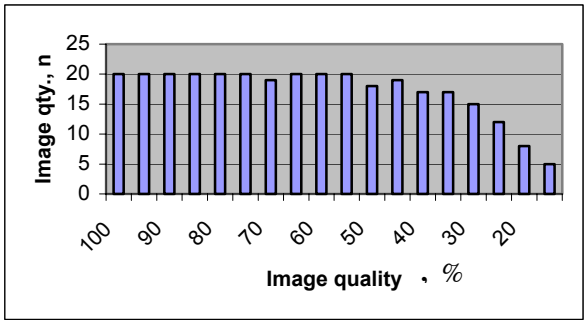

Fig 4. Frequency of image recognition, when the distinctness of refractions is equal 50%.

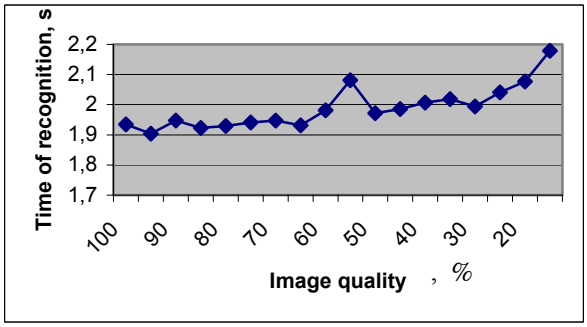

Fig 5. Time of image recognition, when the distinctness of refractions is equal 50%.

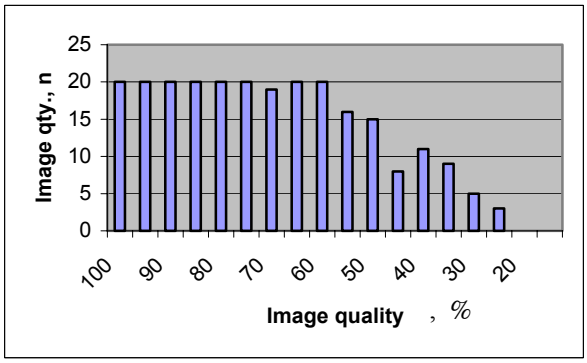

Fig 6. Frequency of image recognition, when the distinctness of refractions is equal 100%

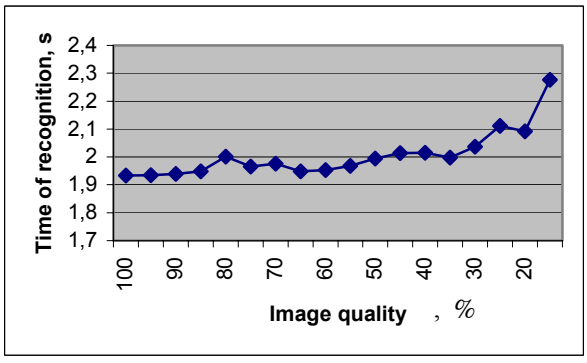

Fig 7. Time of image recognition, when the distinctness of refractions is equal 100%.

The research is conducted in two stages: when the distinctness of refractions is equal to 50% and 100%. In both cases, light- 50%. In this case, the quality of an image is expressed in percentage, too: 100%- clean image; 0%- maximum image impurity.

5 Conclusions. The use of biometric parameters in the access systems is a reliable part of the security system. The use of individual characteristics of a person enables to approbate a totally new conception of the security system. According to the graphs, it is seen that the computation time of data of a fingerprint varies from 1.9 to 2.4 seconds.

The tendency that by imitating the decrease of the resolution coefficient of a scanner, i.e. when the quality is getting worse, the computation time increases is observed. This process can be explained by the following: the higher the resolution coefficient of a scanner is, the smaller image blocks can be used, and therefore, the higher reliability is ensured. A smaller image block enables to avoid mistakes, thus, the greater amounts of information occur, and in general the information is more precise. In order to improve the quality of identification, the resolution of scanners and conditions of scanning must be improved. The research has been conducted having in mind that in such system the possibilities of data storage are unlimited, besides, there is no need to compress additionally an image. Given the low possibilities of storage or rather great amount of biometric data, additional problems occur in a large integrated security system. The necessity of transmission or compression of images or other biometric data occurs. Then, the amount of errors introduced by the compression algorithm must also be evaluated.

6 Literature

1. **D.Eidukas, M.Žilys, A.Valinevičius** Apsaugos sistemų analizė // Elektronika ir elektrotechnika. – Kaunas:Technologija, 2001. – Nr.2(31). – P 13-18.
2. **Волхонский В.В., Засыпкин А.В., Коротких В.Е** Структура технических средств обеспечения безопасности //
3. **M.Deltuvas** "Įeinančių ir išeinančių asmenų kontroliavimo ir registravimo sistemos" // Rizikos faktorius. – Vilnius. 1998. Nr.6. – P.31-32
4. **Simon Liu, Mark Silverman** A Practical Guide to Biometric Security Technology // 2000
5. **Carl G. Looney** Pattern recognition using neural networks // Oxford:University press, 1997. – P 8-9.
6. **A.K.Jain, S.Pankanti** Fingerprint Classification and Matching // January 1999