IRSTI 50.37.23; 50.41.25

UDC 51-76; 004.11

BIOMETRIC IDENTIFICATION OF A PERSON USING A MULTI-PARAMETER AUTOMATED SYSTEM

T. Mazakov[1,2], Erika Lorents (Matsak)[3] M. Aliaskar[1,2], A. Abzhalilova[2], D. Montaeva[2], A. Turlybekova[2]

[1]RSE Institute of Information and Computational Technologies MES RK CS,
Almaty, Kazakhstan
[2]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[3]Tallinn University of Technology IT College, Tallinn, Estonia
[1]tmazakov@mail.ru, [2]87019931011@mail.ru
[1]ORCID ID: https://orcid.org/0000-0001-9345-5167

Abstract. The article is devoted to the development of a system for biometric identification of a person by face, fingerprints and voice. Two-dimensional and three-dimensional characteristics of a person's face, taking into account area and volume, were used as informative signs of biometric identification of a person by face. For biometric identification of a person by fingerprints, an FPM10A scanner and an Arduino microcontroller were used.

Another type of signs is local. They are also called minutiae (features or special points) - unique features inherent only in a specific imprint, determining the points of change in the structure of papillary lines (ending, bifurcation, rupture, etc.), the orientation of the papillary lines and coordinates at these points. Each print can contain up to 70 or more minutes. For biometric identification of a person by voice, the MFCC and PLP algorithms are used for digital processing and analysis of audio recordings. Various algorithms are used for acoustic analysis of speech: hidden Markov models, a model of a mixture of Gaussian distributions. The result of determining the tone of speech and the content of speech for the purposes of identification by voice is obtained.

On the Visual FoxPro DBMS, a “Multiparameter automated system for biometric identification of a person” has been developed.

Keywords: information security, two-dimensional and three-dimensional image, identification, papillary patterns, voice characteristics, human speech, acoustic modeling.

Introduction

The problem of information protection and information security is one of the most important aspects of the development of modern society. Currently, the solution to this problem in the development and operation of information systems for various purposes is associated with the development of all sorts of requirements for ensuring their security and the creation of software and hardware from unauthorized access [1-2].

Automatic person recognition for identification has a large number of applications in various fields. Public security problems, the need for remote authentication, the development of human-machine interfaces are causing increased interest in this technology [3].

Methods of biometric identification of a person are increasingly used in access control systems to workplaces, mobile devices, local and global information resources. Since the implementation of the systems does not require specialized equipment, and the biometric feature cannot be lost, forgotten or transferred, the most promising are systems, the principle of which is based on recognition of a person's face.

Authentication methods based on the measurement of human biometric parameters provide 100% identification. At the moment, the following biometric characteristics are successfully used in biometric systems for user authentication: iris, fingerprint, palm print, vascular patterns, face geometry, voice print, signature, DNA comparison, which have properties without which their practical application is impossible [4]:

Universality: each person has biometric characteristics.

Uniqueness: there are no two people with exactly the same biometric characteristics.

Consistency: biometric characteristics must be stable over time.

Measurability: Biometric characteristics must be measurable by some kind of physical reading device.

Acceptability is also a very important property. It is least of all associated with any specific biometric parameter, however, without taking it into account, it is impossible to create a complete picture of the effectiveness of the use of biometric systems. The combination of all of the above properties determines the effectiveness of biometric authentication systems.

Currently, there are no biometric parameters that would combine all these properties at the same time, especially when considering acceptability. Therefore, the application of multi-parameter biometric authentication is becoming relevant.

Implementation. Main part

For the software implementation of the AS «Biometric Information Security System» was chosen the VisualFoxPro DBMS. Starting with the ninth version of VisualFoxPro, a set of classes GDIPlus and MCI are supplied.

GDIPlus supports both raster (BMP, GIF, PNG, etc.) and vector (WMF, EMF) images. The graphical device interface (GDIPlus) allows the developed applications to use graphics and formatted text for displaying on a monitor screen or printing to a printer [5].

With MCI, you can record, play back audio and video files of various formats.

On the basis of the VisualFoxPro 9 DBMS, the interface part is implemented, which includes the following modes: 1) biological characteristics, 2) characteristics parameters, 3) initial databases, 4) database configuration, 5) simple identification, 6) complex identification, 7) classification [6-8].

After calling the AWP, the main screen of the program appears, shown in Figure 1.

Currently included as biological characteristics are «face video», «fingerprint» and «voice».

Mode - «source databases». Portraits in the following graphic formats can be used as initial data for images: bmp, gif, jpeg, tiff and png. For the «face video» mode, the main information is a volumetric 3d-model, presented as a regular height matrix.

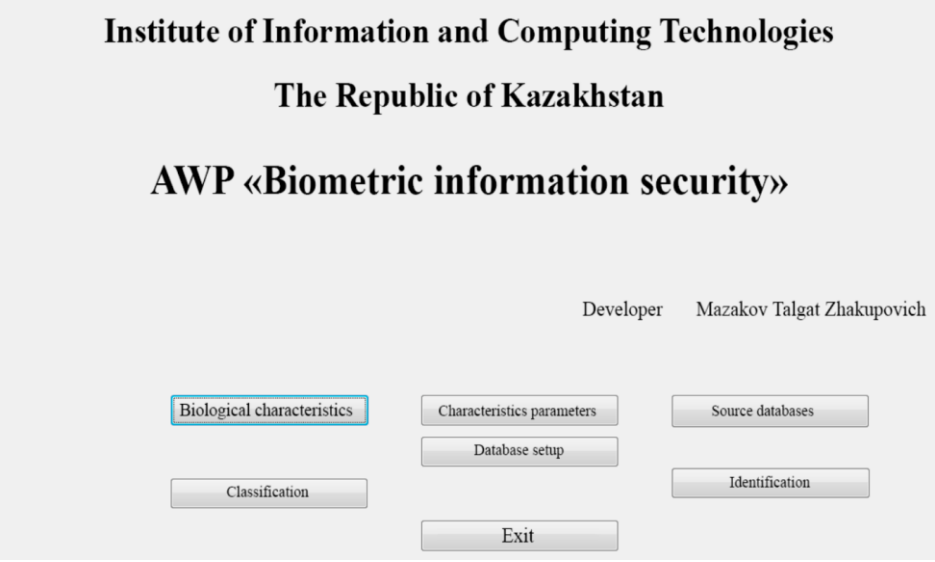

Figure 1 – AWP main screen

The following types are introduced for characteristics parameters:

1 - point coordinate; 2 - distance (number); 3- area; 4 - volume.

Mode - «classification». The program implements classification according to one or several parameters. In this case, the task of classification is to simplify a data matrix that is too extensive for direct human analysis. There is no single “correct” classification for any dataset. Different numerical strategies usually lead to very different results. Consequently, the help of a numerical consultant is needed to characterize the types of classification available, and it is up to the expert to

choose the type that suits him.

Basic algorithm. The initial steps in all agglomerative systems are the same. For n individuals, all $n(n-1)/2$ measures of difference are calculated and the pair of individuals with the smallest measure is combined into one group. It will then be necessary to determine an appropriate measure of difference between this group and the remaining $n-2$ individuals, and in later stages it will obviously be necessary to determine the measure between the individual and the group of any size, as well as between any two groups. At each step of the classification, a union is carried out (between two individuals, between individuals and a group, or between two groups), for which the measure of difference is minimal among all those remaining to this step. The measure must be such that the individual can be regarded as a group of one element. The unification strategy is determined precisely by the measure of differences between the groups. In total, the algorithm calculates $(n-1)^2$ measures. It was shown in [9] that (i, j)-measures can usually be considered from the standpoint of a single linear model. Let there are two groups i and j with ni and nj elements, respectively; the measure of the difference between these groups is denoted by dij. Suppose that dij is the minimum measure of all the remaining ones, so that i and j combine and form a new group k with nk = ni + nj elements. Consider some other group h with nh elements. The values dhi, dhj, dij, nh, ni, and nj are known before joining. Let's put

$$d_{hk} = \alpha_i d_{hi} + \alpha_j d_{hj} + \beta d_{ij} + \gamma \left| d_{hi} - d_{hj} \right|$$

where parameters α_i, α_j, β and γ define the essence of the strategy.

The flexible strategy is applicable for any measure of difference and is determined by four constraints: $\alpha_i + \alpha_j + \beta = 1, \alpha_i = \alpha_j, \beta < 1, \gamma = 0$. The strategy is monotone, and its properties completely depend on β. If β = 0, then the strategy preserves the metric of the space. If β is positive, then the strategy shrinks the space, and if negative, it stretches. The program used the value β = -10.25 as recommended for practice.

The program implements various classification algorithms, the so-called merging strategies (agglomerative systems): flexible strategy, nearest neighbor strategy, far neighbor strategy, group mean strategy, centroid strategy, sum-of-squares strategy.

Face video

For the characteristic «video image of the face», a number of parameters are defined, which are:

1) point - coordinates of the pupils of the eyes, bridge of the nose, tip of the nose,

2) distance - between the eyes, between the bridge of the nose and the tip of the nose, the base of the nose,

3) perimeter - triangle (pupils of the eyes and tip of the nose), triangle (bridge of the nose and base of the nose),

4) area - isolines of the eye sockets, isolines of the nose,

5) volume - eye sockets, nose.

A volumetric 3d-model, presented as a regular height matrix, is used as the initial data for the «face video».

Algorithms for processing information parameters for identifying a person by face:

1. Coordinates of the center of the pupil of the left eye - (P1x, P1y): determined from a graphic file with a photo of a person;

2. Coordinates of the center of the pupil of the right eye - (P2x, P2y): determined from a graphic file with a photo of a person;

3. The distance between the pupils - P3: calculated using data (P1x, P1y) and (P2x, P2y);

4. Area of the second contour of the left eye socket - P6: a file with 3d data of a person's face is calculated by approximating the contour with an ellipse;

5. Volume of the left eye socket - P8: calculated using the data P5, P6, P7 and the distance (step) between the isolines;

6. Area of the first contour of the right eye socket – P10: calculated similarly to the parameter P5;

7. Coordinates of the left base of the nose – (P15x, P15y): determined from a graphic file with a photo of a person;

8. The height of the tip of the nose – P17: determined from file with 3d data of human face;

9. the Area of the third contour of the left nose – P21: the file with 3d data of the human face is calculated by approximating the contour with a trapezoid;

10. The ratio «distance between pupils» / «Distance between the bridge of the nose and the base of the nose» –P25: calculated using the data (P1x, P1y), (P2x, P2y) and (P14x, P14y).

Fingerprint

The FPM10A module with the Adafruit Arduino library was used to create a block of the biometric fingerprint identification system [10]. Figure 2 shows the elements of the image acquisition and fingerprint identification block. The specified block is implemented on the basis of the Arduino UNO controller. The Arduino is a device based on the ATmega 328 microcontroller. [11] It includes everything you need for convenient operation with the microcontroller: 14 digital inputs/outputs (6 of them can be used as PWM outputs), 6 analog inputs, a 16 MHz quartz resonator, a USB connector, a power connector, a connector for in-circuit programming (ICSP) and a reset button.

Figure 2 – fingerprint Scanner: 1-FPM10A optical fingerprint scanner; 2 – Arduino UNO; 3 – wires for connecting the scanner to Arduino; 4-USB cable for Arduino

When using a fingerprint sensor, there are two main steps. First, data is recorded in the sensor memory, that is, a unique ID is assigned to each fingerprint, which will be used for comparison in the future. After recording the data, you can proceed to «search», comparing the current image of the fingerprint with those recorded in the sensor memory. With the help of SFGDemo and ArduinoIDE, new fingerprints are loaded, assigning each of them a new ID #. All uploaded fingerprint images are encrypted (figure 3).

Figure 3 – Uploading a fingerprint to the database

In figure 4, you can see the percentage of matches. Fingerprints that do not match the fingerprints stored in the database are ignored by the scanner.

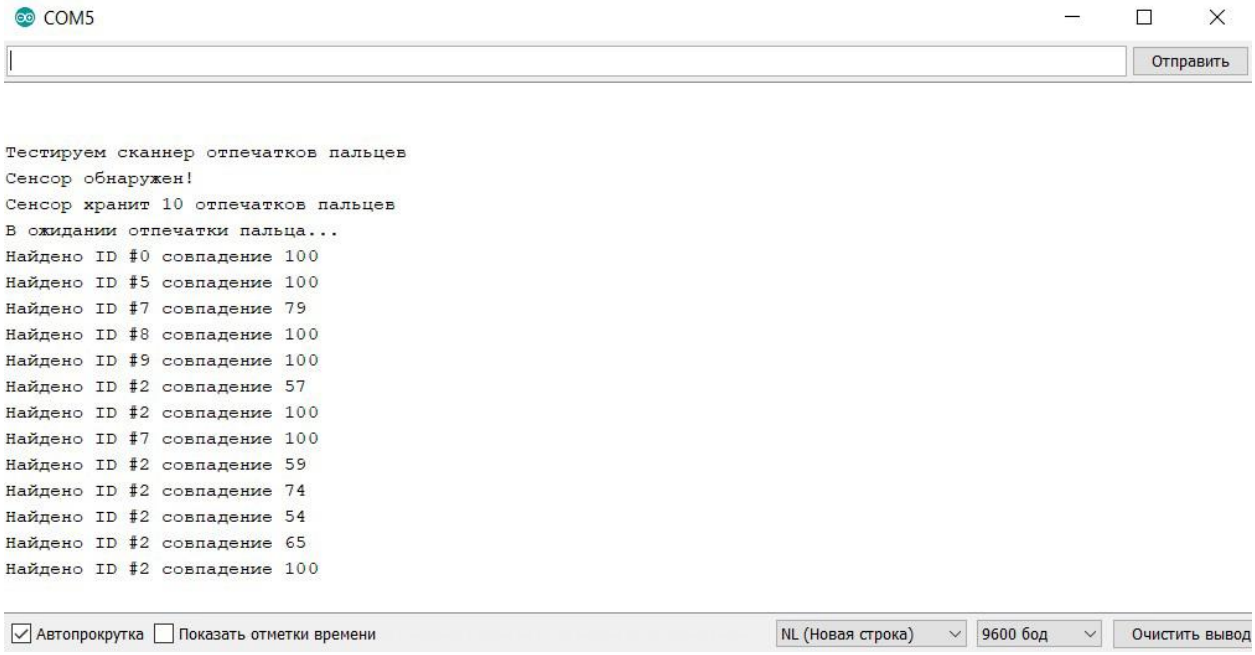

Figure 4 – Fingerprint recognition

Identification signs of the structure of papillary patterns on the fingers are usually subdivided into global and local signs [12-13].

Global signs include signs that can be seen with the naked eye. These features include: type and type of papillary pattern; direction and steepness of streams of papillary lines; the structure of the central pattern of the pattern; delta structure; the number of papillary lines between the center and the delta and many other signs.

Another type of signs is local. They are also called minutiae (features or special points) - unique features inherent only in a specific imprint, determining the points of change in the structure of papillary lines (ending, bifurcation, rupture, etc.), the orientation of the papillary lines and coordinates at these points. Each print can contain up to 70 or more minutes.

In this study, several types of descriptors were used: SIFT, SURF and ORB [14]. SURF / SIFT algorithms have the best classifying ability when solving everyday search problems on textured images. For fingerprint identification tasks, they have «excess power».

Voice

One of the parameters of biometric identification of a person is the voice, but the voice of a

person can change depending on age, emotional state, health or other factors, which makes the identification process more difficult to implement. The oral speech of a person is an ordered system of acoustic signals that are perceived as a sound image, and the oral speech of a person reflects its individual characteristics and features. The acoustic characteristic of the voice is relatively stable over time and remains individual even with pathological changes in the speech organs. The task of voice identification consists in selecting human speech from the input audio stream, its classification and recognition.

The rate of speech is a subjective measure related to the speed of pronunciation of certain segments of speech over time. The tempo can be related to the content, usually the most important words are pronounced slower. The volume and tempo of speech are individual for each person.

The difference in the timbres of different voices is described by different frequency spectra. The mathematical apparatus for analyzing the frequency spectrum is the Fourier transform, as a way to describe a complex sound wave with a spectrogram. Taking into account the peculiarities of human hearing (its non-linear nature in relation to the perception of sound frequencies), the transformation from the Hertz scale to the chalk scale (chalk is a psychophysical unit of sound pitch) is used for this task. The following is the formula for the transition frequency in Hertz (Hz) and the pitch of the sound the Mela

$$m = 1127 * ln(1 + f/700)$$

the calculated spectrum is superimposed with a set of M Mel scale filters, usually M=20 or M=24, usually the more filters the higher the accuracy, while the filters are shifted to those frequencies in which the most in the audio recording:

$$x_i = \sum_{k=0}^{N-1} |X_k| * H_i(f_k), i = 1..M$$

The mel h scale filter has a triangular shape, an example of such a filter is shown below (figure 5).

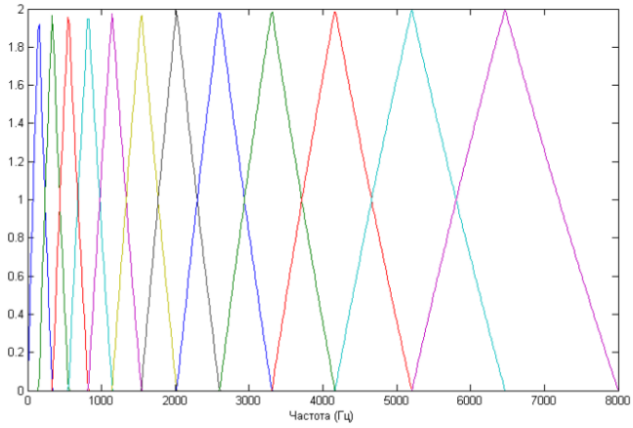

Figure 5 – example of a mel filter

For acoustic speech analysis, a variety of algorithms are also used, the most common are hidden Markov models (SMM or HMM in the English version), as well as a model of a mixture of Gaussian distributions (SGR or GMM in the English version), neural networks have been actively used in recent years [15].

Conclusion

The AWP «Biometric information security system» was developed. Based on the application

of multi-criteria optimization methods, different coefficients are calculated for each class, which allow ranking the criteria by importance. The properties of the proposed mathematical algorithm are investigated. For the first time, the human recognition algorithm takes into account such parameters as the volume of the nose, the volume of the eye socket, and other three-dimensional characteristics. A complex identification algorithm has been developed to take into account such phenomena as portrait shift, different photo scale and tilt of the identified face.

Based on the Arduino microcontroller and the FPM10A scanner, a recognition system has been developed for storing data, further processing it, identifying and displaying fingerprint images. The structure of papillary patterns on the fingers was chosen as identification features. The result of matching fingerprints with different rotation through the scanner is obtained. An experimental study of biometric fingerprint identification created on the basis of sift, SURF and ORB descriptors showed that the developed software system has invariance to image rotations. The system has developed three algorithms for analyzing audio recordings to solve the problem of biometric identification by voice.

Acknowledgements. The work was carried out at the expense of grant funding of scientific research for 2018-2020 under the project AP05131027 «Development of biometric methods and information protection tools».

References

[1] Buzov G.A. Practical guide to identifying special technical means of unauthorized receipt of information. – M.: Hotline-Telecom, 2010. 240 p. (in Russian)

[2] Katrin Y.F., Razumovsky, A.V., Spivak A.I. Protection of information by technical means. St. Petersburg: ITMO National Research University, 2012. 416 p. (in Russian)

[3] Bolle R.M., Connel J.H., Pankanti S., Ratha N.K., Senior A.W. Guide to Biometrics, Sprinter-Verlag. – New York, 2004.

[4] Crihalmeanu S., Ross A. Multispectralsclera patternsfor ocularbiometric recognition. – Pattern Recognition. Lett, 2012. 1860–1869.

[5] Klepinin V.B., Agafonova T.P. Visual FoxPro 9.0. The most complete guide. – St. Petersburg: BHV-Petersburg, 2007. 1216 p. (in Russian)

[6] Jomartova Sh.A., Isimov N.T., Bayrbekova G.S., Ziyatbekova G.Z., Abdrazak Zh. Personal identification based on 2D and 3D images. Bulletin of the National Engineering Academy of the Republic of Kazakhstan, 2018. 2 (68). 16-20. (in Russian)

[7] Mazakov T.Zh., Abzhalilova A.A. Authentication and identification of a person by biometric parameter: fingerprint. Bulletin of KazUTB. 2020. 4. 26-33. (in Russian)

[8] Shormanov T.S., Mazakov T.Zh., Ziyatbekova G.Z., Aliaskar M.S. Algorithms for identification of a person by voice. Bulletin of KazUTB. 2020. 1. 58-68. (in Russian)

[9] Aivazyan S.A., Bukhshberger V.M., Enyukov I.S., Meshalkin L.D. Applied statistics. Classification and dimensionality reduction. – M.: Finance and statistics, 1989. 607 p. (in Russian)

[10] Petin V.A. Projects using the Arduino controller. – St. Petersburg: BHV-Petersburg, 2016. 464 p. (in Russian)

[11] A.V. Belov Arduino. From the basics of programming to the creation of practical devices. – SPb.: NiT, 2018. 480 p. (in Russian)

[12] Tan and B. Bhanu. “Robust fingerprint identification” in International Conference on Image Processing, 2002. 1. 1-277.

[13] Polyakov A.V. Algorithms and secure systems for biometric identity authentication // Auth. Cand. Dissertation. Moscow, 2018. 28 p.

[14] Ethan Rublee, Vincent Rabaud, Kurt Konolige, Gary Bradski. ORB: an efficient alternative to SIFT or SURF, Computer Vision (ICCV), IEEE International Conference on. IEEE, (2011). 2564–2571.

[15] Dzmitry Bahdanau, Kyunghyun Cho, and Yoshua Bengio. Neural machine translation by jointly learning to align and translate. CoRR, abs/1409.0473, 2014.