Mathematical and information maintenance of biometric systems

Z Boriev, S Sokolov, A Nyrkov and A Nekrasova
Admiral Makarov State University of Maritime and Island Shipping, 5/7, Dvinskaya st., Saint-Petersburg, 198035, Russia
E-mail: za_mir_b@mail.ru

Abstract. This article describes the different mathematical methods for processing biometric data. A brief overview of methods for personality recognition by means of a signature is conducted. Mathematical solutions of a dynamic authentication method are considered. Recommendations on use of certain mathematical methods, depending on specific tasks, are provided. Based on the conducted analysis of software and the choice made in favor of the wavelet analysis, a brief basis for its use in the course of software development for biometric personal identification is given for the purpose of its practical application.

1. Introduction
Biometric systems are increasingly popular in society. This is due to the problem of accurate personal identification, and, as a result, reliable protection of personal data.

In practical sense, the biometry is considered as a method for identifying a person, based on his/her physiological or behavioral characteristic.

Such biometric parameters as fingerprints or hand geometry are physiological characteristics, which are measured at a specific point of time. It should be noted that there is a variety of non-unique characteristics among physiological characteristics that cannot be used in the personal identification process. For example, such characteristics include weight and growth of a person, because they are subjected to a strong change over time [1-2].

2. Biometric characteristics
Behavioral characteristics are connected with subconscious movements in the course of reproduction or repetition of any common action. Such characteristics include voice, step, signature of a person, and even dynamics of typing [3].

One of the most important characteristics of biometric identification methods is an accuracy, which means an ability of the chosen method to distinguish reliably biometric characteristics, belonging to different people.

More and more biometric parameters, with use of which personal identification and authentication is possible, appear every year. But a lot of time is spent for their study, search of processing methods and algorithms. Therefore, a level of knowledge of biometric parameter directly influences a level of its use.

Having carried out the analysis of personal identification systems, it was revealed that the following biometric parameters are used more often today: fingerprint, iris, hand veins, voice and signature [4-5].
3. Signature identification

An issue of personal identification by means of a signature is considered in this work. Today, there are two main directions of the signature identification:
- a static signature recognition;
- an analysis of dynamic characteristics.

It is possible to get a two- or three-dimensional (if to consider additional characteristics, such as pressing on a pen, pen slope angle, signature rate) signature model by means of a scanner or a media tablet.

Today, there is no single approach to image identification, irrespective of the number of considered signature parameters. A static signature can be transferred to third parties and is not copy-protected: an original picture is copied on a transparent paper, which is then put on a tablet, and this signature is simply outlined. As a result, we have a completely identical copy of the original signature [6][7].

Figure 1.1. Original signature

Figure 1.2. Outlined signature copy

We can see in these figures that the original and copy are almost indistinguishable that means an unreliability of a static signature. Authentication by dynamic characteristics is a solution of this issue of accurate image recognition and protection against a forgery [8].

Biometric systems, based on analysis of dynamic characteristics, can operate according to a general chart:

Figure 2. Generalized chart of dynamic biometric systems.

The following general order for dynamic authentication systems can be allocated on the basis of this chart:
- transformation of non-electrical values (coordinates of pen point, noise pressure) to electric signals;
- digitization of input electric signals;
- scaling of input amplitudes, resulting them in a certain reference value;
- adjustment of signals to a single time scale;
- computation of a vector (matrix) for measured biometric parameters;
- the system operation mode (instruction or authentication) determines a set of operations, carried out with a pre-formed parameter vector.

4. Mathematical methods

Mathematical solutions of a dynamic authentication method are more complicated than a method of static signature recognition. It allows reading signature parameters in real-time mode, for example, a
speed of hand movement at different sites, a writing order of particular lines, a line form and a direction, the pressure force and duration of all signature stages. The opportunity of a forgery reduces to zero, because it is almost impossible to repeat the smallest nuances when affixing a signature.

In this case, the input data will be $X(t)$, $Y(t)$, $Z(t)$, where $X(t)$, $Y(t)$ - coordinates of pen tip, $Z(t)$ - an additional parameter (pressure force, slope angle, etc.). All three functions are time-dependent. One-dimensional mathematical models, based on one of parameters, provide an error probability 0,1. The error probability in bi-dimensional mathematical models decreases to 0,01. The error probability for the three-dimensional model respectively will be equal to 0,001.

It is required to compute a biometric parameter vector after receiving an original data and its digitizing. Until recently, the most common method of vector formation was a discrete Fourier transformation. This method is a good enough for recognition of a static signature, as the Fourier coefficient represents a signal behavior for all time of its existence that, in case of dynamic authentication, is unjustified. In this case, the best solution of this issue will be a wavelet transform [8][9].

To refer to wavelets, a class of functions should meet the following requirements:

1. **Tolerance.** Analyzing wavelet $\psi(t)$, also called a mother wavelet, should have a zero-mean value:

   $$\int_{-\infty}^{+\infty} \psi(t) dt = 0$$

2. **Similarity.** All class functions are obtained from the analyzing a wavelet by scaling transformation and shift:

   $$\psi_{a,b}(t) = \psi\left(\frac{t - b}{a}\right)$$

The two-parameter class of functions appears as the following: ‘a’ parameter – a function scale (extension), ‘b’ parameter – a function position (shift).

3. **Inversability.** An existence of inverse transform, which definitely restores an initial function, based on its wavelet - transform.

4. **Regularity.** The $\psi(t)$ function should be well localized both in a physical and in Fourier space.

The wavelets' important feature is a possibility to describe non-stationary signals, consisting of different components, operating in different time intervals. Thus, the $X(t)$, $Y(t)$, $Z(t)$ functions can be arranged, according to its wavelets. As a result, we get a coefficient matrix, which can be used for return to an original function. Besides, the wavelet coefficients tend to zero quicker than the Fourier expansion coefficients, and it is possible to store more information about signature with rather equal data volumes. [10]

A matrix of average coefficients is accepted as a standard in this case. An example of dependence of one of coordinates on time and its approximation using wavelet expansion is shown in the following figure.

![Figure 3. Generalized chart of dynamic biometric systems](image)

It is also possible to use different bases of wavelet expansions, for example, DOG-wavelet, MHAT-wavelet, Gaussian wavelet of the 1st order.
5. Conclusion
The conducted analysis allowed forming a common vision of an issue of mathematical and information maintenance in biometric personal recognition systems. Wavelet transforms proved to be an effective method to solve problems of signature recognition. In the course of work it has been found that processing of biometric signs by means of wavelet transform allows achieving an error reduction. We can say that a computational complexity of algorithms is a lack of use of wavelet transforms. But this problem is easily solved owing to the high development level of mathematical packages. A software, which consists of an instruction and comparison modules, is also developed for the analysis of this method.

References
[1] Boriev Z, Sokolov S 2015 *Materials of the VI International research and practice conference ‘Modern tendencies and prospects of the Russian water transport development’* 6 6–37
[2] Umnov A 2006 *Collection of scientific papers of the 1st International research and practice conference ‘World Experience of biometric solutions in complex security systems’* 52–57
[3] Solomatin A 2015 *The St. Petersburg National Research University of Information Technologies, Mechanics and Optics*
[4] Clark R 1994 Personal *Information technologies and people* 3 6–37
[5] Boriev Z, Sokolov S 2015 *VI International Scientific Practical Conference on Innovative Technologies and Economics in Engineering* 91
[6] Leus A 2009 *The ‘SKUD. Antiterrorism’ booklet* 28–29
[7] Chernyi S 2015 *Metallurgical and Mining Industry* 7(3) 60–65
[8] Nyrkov A, Sokolov S, Chernyi S, Mamunts D 2015 *Metallurg. and Mining Industry* 7(6) 521–524
[9] Nyrkov A P, Belousov A S, Sokolov S S 2015 *Modern Applied Science* 10(5) 162–176
[10] Chernyi S, Zhilenkov A, Sokolov S, Titov L 2015 *Metallurgical and Mining Industry* 7(3) 66–73