Alternative Biometric as Method of Information Security of Healthcare Systems

Ekaterina Andreeva
Saint-Petersburg State University of Aerospace Instrumentation
Saint-Petersburg, Russia
eandreeva89@gmail.com

Abstract

As information technologies develop, there appear more and more medical devices for diagnosis of human condition and maintenance of life-support. Such devices as insulin pumps, implanted pacemakers and defibrillators are used for diagnosis, treatment and monitoring of the patients' condition. These devices operate using sensors interacting with the human body. The increasing complexity of such devices induced development of a Body Area Network technology which makes it possible to arrange the sensor network on the human body and perform continuous monitoring of the organism's condition.

The possibility to continuously record the patient's data is useful not only in the treatment and diagnosis but also for design of the information security system for life-support medical devices.

In this article discuss the problem of human authentication in BASN. Biometric technology using heart sounds applied in approach; moreover it has a number of benefits compared to the standard methods of biometrics.

I. INTRODUCTION

Every year appear more and more telemedicine systems and m-health applications, for diagnosis of human condition and maintenance of life-support. According to Russian law "About Personal Data" and international standard of processing medical information like HL7, medical human personal data have high level of privacy, so that it must be protected. With the advent of Body Area Sensor Network technology it became possible to build more flexible information security systems, given the specificity of medical devices. Network security achieved by the fact that human body itself can form an originally secure communication which is unavailable to all other kinds of wireless networks [1].

This article focuses on the problem authentication in BASN. Biometric technology using heart sounds applied in this technology, moreover it has a number of benefits compared to the standard methods of biometrics. A lot of parts of human body had already been use in biometric technologies, and heart is not an exception. But the heart is a life support organ of the body, so that information security system will work in any human body condition and regardless of the user actions. In next section will be illustrate methods of using heart sounds as biometric characteristics for secure medical personal data in healthcare devises.

II. ARCHITECTURE BODY AREA SENSOR NETWORK TECHNOLOGY

In 2012 a standard 802.15.6 was adopted which regulates the development and use of wireless Body Area Networks.

Body Area Network consists of implants and wearable sensors that offer unprecedented opportunities to monitor state of health during normal daily activities for

prolonged periods of time. BAN is classified into Off-body, On-body and In-body communication:

- Off-body communication is the communication from the base station to the transceiver on a human side.
- On-body communication is the communication within on-body networks.
- In-body communication is the communication between invasive or implantable device.

The development of the BASN is derived from the recent development of the BAN technology, and description of the BASN is preferred when referring to the type of BAN in telemedicine and m-health where each node comprises a biosensor or a medical device with a sensing unit.

Fig. 1 shows system architecture of medical data transmission from BASN to medical server or personal professional's computer.

The system consists of 4 levels:

- Level 1 – consists in-body and on-body nodes;
- Level 2 – contains a Personal Processing Devises that gathers patient's information from the sensors of BASN and communicates with the Database Server;
- Level 3 – contains of Remote Database Server that keep patient's medical/non-medical records;
- Level 4 – contains a number of professional`s computer which are get patient's data from database server and provides relevant (diagnostic) recommendations.

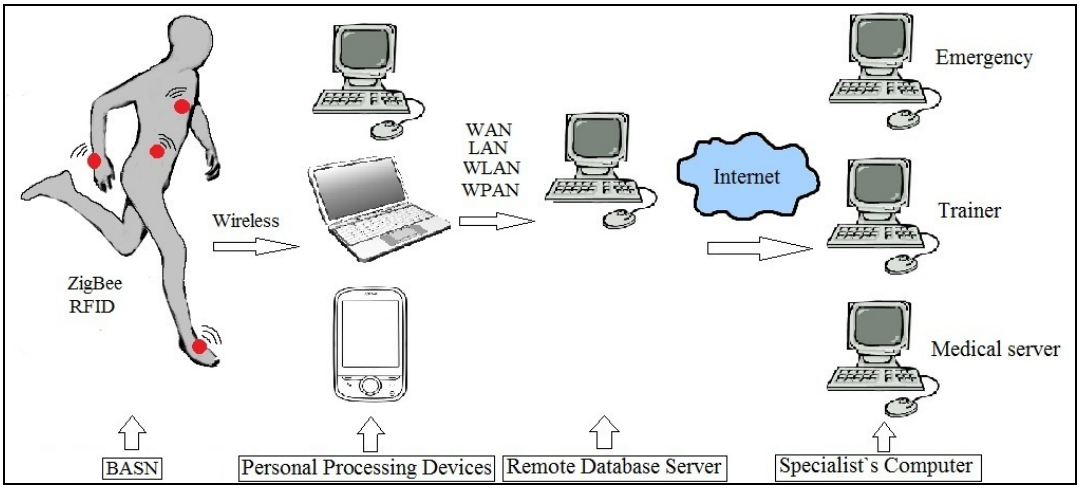

Fig 1. System architecture of medical data transmission

III. AUTHENTICATION SOLUTION

Human authentication during the work with the device is one of the ways for information security. Biometric authentication methods are considered as the most reliable and effective in use [2]. But as applied to medical devices, one should take into consideration the acceptability degree of the selected authentication method. The possibility to pass authentication procedure irrespective of user's actions is of special importance in medical devices. An authentication method providing such possibility is

authentication using human heart sonic signals.

This technology differs from other ones in the following properties:

- heart sonic signals cannot be lost during the life;
- heart sonic signals are difficult to be falsified;
- access control may be performed without user's actions and continuously during operation of medical devices;
- heart sonic signals allow to diagnose the human physical and psychological condition.

The use of heart sonic signals as the authentication method is possible due to availability of a melody which is typical of every specific man. This feature was revealed when studying the heartbeats sonic signal spectrum. The characteristics of human heart sounds may change in time depending on the human physical or psychological condition but the frequency change sequence remains unchanged during a certain period. Just the frequency change sequence produces the musical pattern of the heart sonic signal.

A technique for extracting individual characteristics of heartbeat sound signal was developed in order to extend studies on this issue [3]. Standard speech recognition algorithms were applied in this approach, also taking into account heartbeat sound specificity.

Authentication mechanism using heart sounds consists of three important parts:

- Creating and working with database.
- Extracting individual characteristic of heartbeat sound signal.
- Creating classification of individual characteristic for making a decision.

The database is formed on a personal user's device through the accumulation and processing of data received from the BASN. During authentication procedure BASN applies to personal devise, so that there is no need to store large amounts of information within the network.

Algorithm of extracting individual characteristic of heartbeat sound signal illustrated in Table I.

After receiving the individual characteristics of the signal, it is necessary to classify them in order to make decisions about pass or fail the authentication procedure [4, 5]. At the Fig. 2 you can see classification scheme of authentication procedure. Here binary encoder works on the MIN/MAX principle. The system sets the upper and lower limits.

Upper admissibility limit defines a value to which the difference is compared between reference and new signal entered into biometric system during authentication. If the difference between signals is more than the upper limit, access for this user is denied for the signal is recognized as unauthorized person's heartbeat.

Lower admissibility limit defines maximum value of differences in one person's heartbeat signals. If the value obtained is less than the lower limit, the person passes authentication procedure, which may be followed by analysis of person's state in order to determine its physical and psychological condition.

Upper limit value is defined during investigation, and it can be applied to a wide set of signals. However, lower limit value can be defined only since the statistic is collected for any specific person, because heart sound characteristics variability in particular persons significantly differs.

TABLE I
METHOD OF EXTRACTING INDIVIDUAL CHARACTERISTIC OF HEARTBEAT SOUND SIGNAL

Hamming Windows Transform	As in the case of speech signals, we will assume a short-time stationary property for heart sounds, limit the range of research. $newData[i] = Data[i]\left(0{,}54-0{,}46\cos\frac{2\pi i}{N-1}\right)$
Fast Fourier Transform	The result of Hamming transformed undergoes discrete Fourier transform on the fast Fourier transform algorithm. Fast Fourier transform algorithm - the calculation of the Fourier transform for the discrete case. The transformation is obtained amplitude spectrum and phase information signal.
Filtering	In this block, the signal spectrum will pass through a filter-bank set. The usage of these filter-banks is motivated by the fact that, the sound spectrum has some special shapes and is distributed by a non-linear scale in frequency domain. After successful filtering further calculations are made on the frequency range from 0 to 2000Hz
Logarithmic Compression	Since the information content of the different parts of the spectrum is not the same, it makes sense to reduce the considered area of the spectrum to those frequencies, which contain more information. These areas are the low-frequency part of the spectrum. To highlight important parts of the spectrum algorithm logarithmic compression. $f_{new} = 2595 \cdot \log_{10}(1+f_{base})$
Extracting Individual characteristics	The last and most important step of the algorithm it is extracting the individual characteristics of the human heart sound, that is executed by the following formula $c_i = f_i \cdot \cos\left(\frac{2\pi i}{N}\right)$

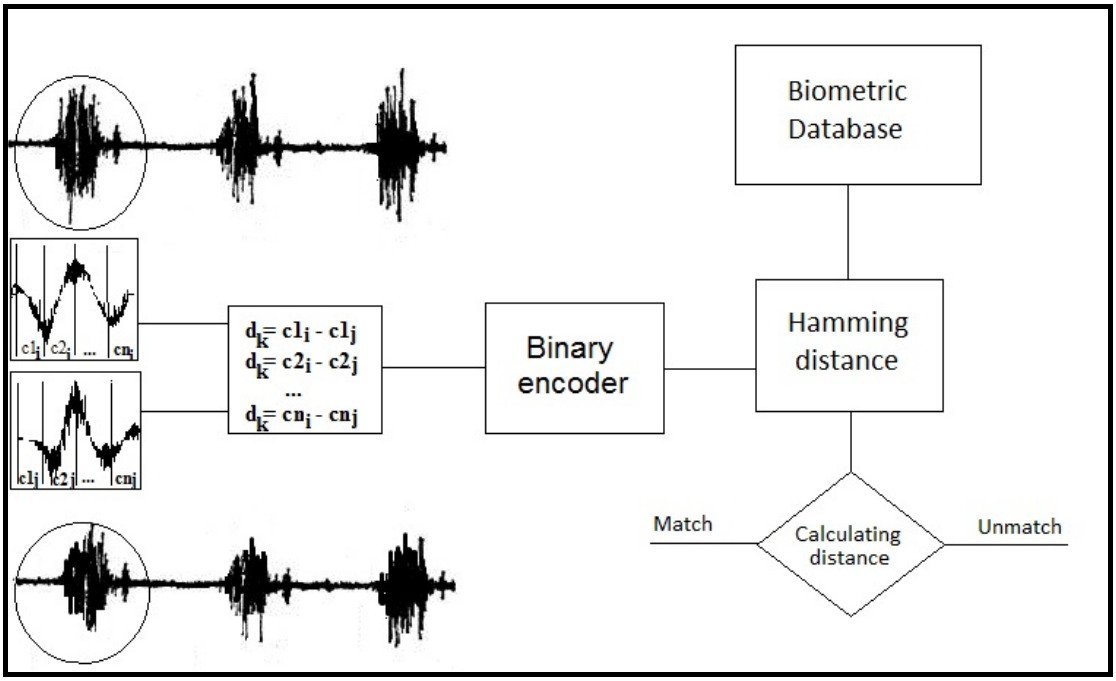

Fig 2. Method classification of extracting individual characteristic of heartbeat sound signal

IV. TESTING AND RESULTS

For testing system, was creating database which include 50 heart sounds from 20 persons. Upper admissibility limit value was chosen as *MAX = 400000*, and lower limit

one as *MIN = 4000*. These values were obtained in our studies. Relative system operating characteristic at the defined values is shown on diagrams.

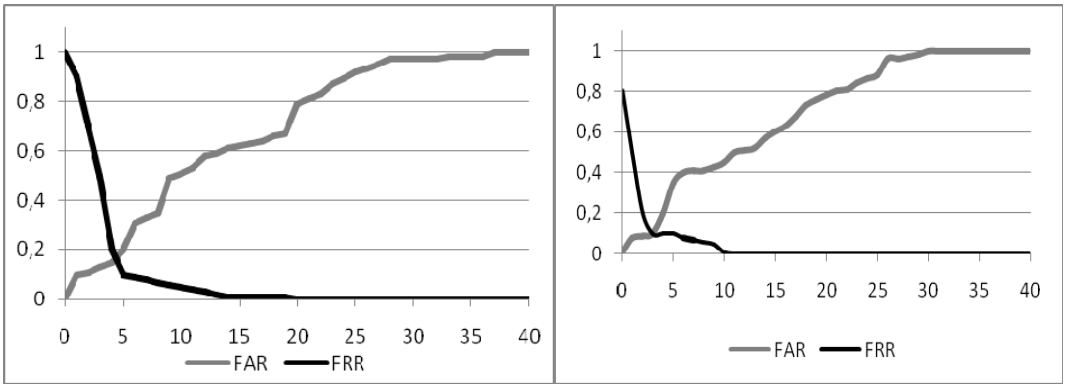

Fig. 3. Receiver operating characteristic for vector

False accept rate (FAR) – the probability that the system incorrectly matches the input pattern to a non-matching template in the database.

False reject rate (FRR) − the probability that the system fails to detect a match between the input pattern and a matching template in the database

The graphs show that the selected parameters can achieve a compromise between system performance and minimize errors in the system.

V. CONCLUSION

This paper presents the method for use of Wireless Body Area Sensor Networks as applied to authentication systems. The method for division of the heart sonic signal into separate, independent informative portions is suggested. The reliability of the authentication system using the heart sonic signals may be increased with the help of this technology.

REFERENCE

[1] Carmen C. Y. Poon and Yuan-Ting Zhang. “A Novel Biometrics Method to Secure Wireless Body Area Sensor Networks for Telemedicine and M-Health”, *The Chinese University of Hong Kong,* 2006, pp. 73-81.

[2] Beritelli F, Spadaccini A., “Human Identity Verification Based on Heart Sounds: Recent Advances and Future Directions”, *University of Catania, Italy* 2010, pp.1–18.

[3] Phua K, Dat T H, Chen J, Shue L., “Human identification using heart sound”, *Institute for Infocomm Research*, Singapore 2008, pp. 1-8.

[4] Andreeva E., “Authentication system using heart sounds”, *Proceedings of the Tomsk State University of Control Systems and Radioelectronics*, 1(25), part 2, 2012, pp. 153-157.

[5] Andreeva E., “System of continuous authentication using cardiology methods”, *Ryazan State Radio Engineering University*, part 2, 2012, pp. 176-179.