Information security of healthcare systems: using a biometric approach

E. Andreeva
Department of Information Security Technologies,
Saint-Petersburg State University of Aerospace Instrumentation, Russia

Abstract

Information security in healthcare and medical privacy is the current issue in modern society. The increase in technological complexity of medical devices and systems does not only improve efficiency, but also influences the risks of loss and change of personal health information. The most important problems of information security in healthcare are the access control to medical personal data and security data transmission. In this paper it is illustrated how these two problems can be solved with a biometric approach.

The biometric technology using heart sounds and acoustic characteristics of the circulatory system allows for construction of flexible information security systems, adapted to the specific characteristics of medical electronic devices. Unlike other biometric technologies, the system of human authentication using heart sounds does not require active data input and provides a reliable working system. In this approach the information security system uses the data that a medical device gets during human condition monitoring. This feature does not complicate a medical device by system information security.
Keywords: information security, healthcare, biometrics, authentication system, heart sound.

1 Introduction

Every year there appear more and more telemedicine systems and m-health applications for the diagnosis of human condition and maintenance of life-support. According to the Russian Law “On Personal Data” and international standard of processing medical information like HL7, medical human personal data have a high level of privacy, so that it must be protected. With the advent of


WIT Transactions on Biomedicine and Health, Vol 17,
www.witpress.com, ISSN 1743-3525 (on-line)
doi:10.2495/BIO130101

Body Area Sensor Network Technology it becomes possible to build more flexible information security systems, given the specificity of medical devices. Network security is achieved by the fact that the human body itself can form originally secure communication which is unavailable to all other kinds of wireless networks [1].

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

2 Architecture of body area sensor network technology

In 2012 the standard 802.15.6 was adopted which regulates the development and use of Wireless Body Area Networks.
The Body Area Network consists of implants and wearable sensors that offer unprecedented opportunities to monitor the 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.

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

The system consists of 4 levels:

- Level 1 – consists of in-body and on-body nodes;
- Level 2 – contains Personal Processing Devices that gather patients' information from the sensors of BASN and communicate with the Database Server;
- Level 3 – contains the Remote Database Server that keeps patients' medical/non-medical records
- Level 4 – contains a number of professional's computers which get patient's data from the database server and provide relevant (diagnostic) recommendations.

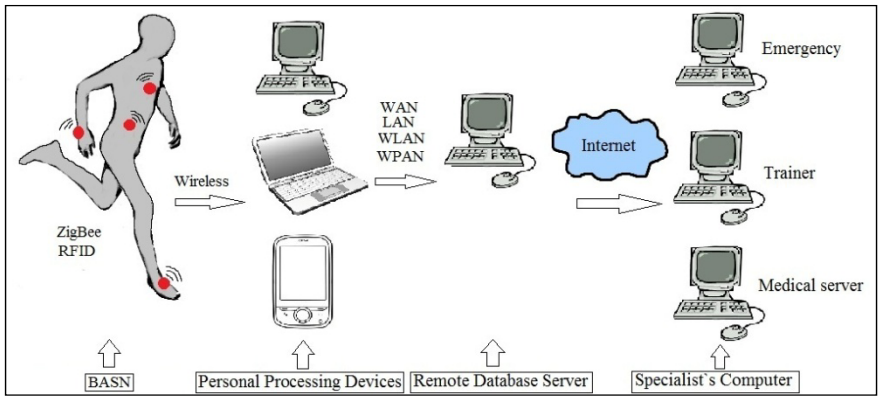

Figure 1: System of medical data transmission architecture.

3 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. The authentication method providing such possibility is the 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 the operation of medical devices;
- heart sonic signals allow us to diagnose the human physical and psychological condition.

The use of heart sonic signals as the authentication method is possible due to the availability of a melody which is typical for 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. Only the frequency change sequence produces the musical pattern of the heart sonic signal.

The technique for extracting individual characteristics of the 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 the heartbeat sound specificity.

Authentication mechanism using heart sounds consists of three important parts:

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

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

The algorithm of extracting individual characteristics of the heartbeat sound signal is illustrated in Table 1.

Table 1: Method of extracting individual characteristics of the 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. $$newData[i] = Data[i]\left(0{,}54 - 0{,}46cos\frac{2\pi i}{N-1}\right)$$
Fast Fourier transform	The result of Hamming transform 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 by the 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 the frequency domain. After the successful filtering further calculations are made on the frequency range from 0 to 2000Hz.
Logarithmic compression	Since the information content of 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 the 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 is extracting individual characteristics of the human heart sound, that is executed by the following formula $$c_i = f_i \cdot \cos\left(\frac{2\pi i}{N}\right)$$

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

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

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

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

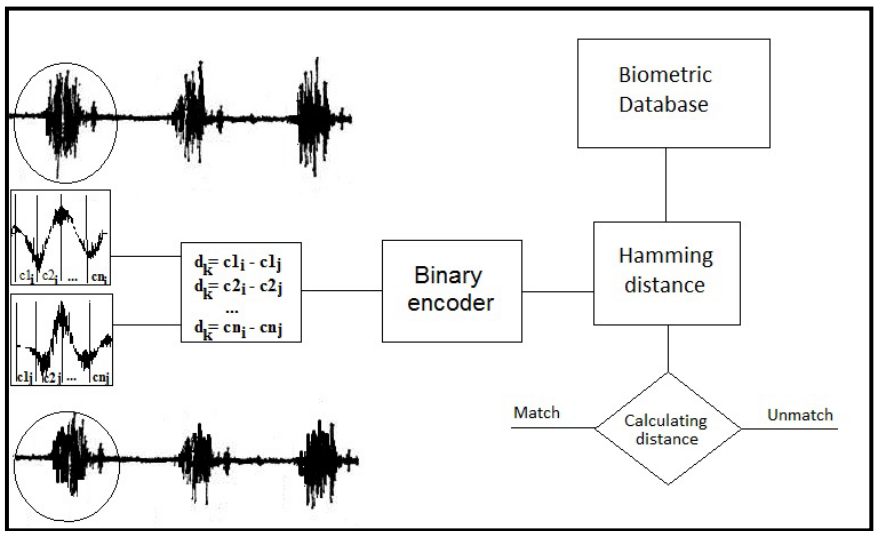

Figure 2: Method of classification of extracting individual characteristic of the heartbeat sound signal.

4 Testing and results

For the testing system, the database which includes 50 heart sounds from 20 persons was created. The upper admissibility limit value was chosen as MAX = 400000, and the lower limit one as MIN = 4000. These values were

obtained in our studies. The relative system operating characteristic at the defined values is shown in the diagrams.

False accept rate (FAR) – the probability that the system matches incorrectly 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 matching template in the database.

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

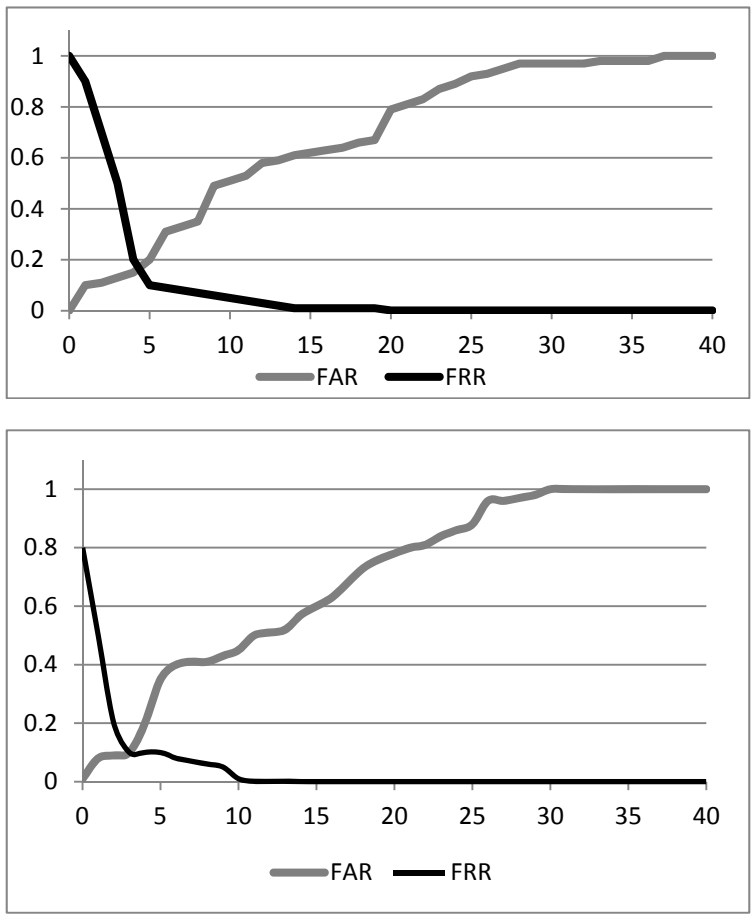

Figure 3: Receiver operating characteristic for vector.

5 Conclusion

This paper presents the method for the 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.

References

[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, 2012.0020 pp. 176–179.