Chapter 2
Chaotic Function Based ECG Encryption System

Butta Singh
Guru Nanak Dev University, India

Manjit Singh
Guru Nanak Dev University, India

Dixit Sharma
Guru Nanak Dev University, India

ABSTRACT

Remote health-care monitoring systems communicate biomedical information (e.g. Electrocardiogram (ECG)) over insecure networks. Protection of the integrity, authentication and confidentiality of the medical data is a challenging issue. This chapter proposed an encryption process having a 4-round five steps -encryption structure includes: the random pixel insertion, row separation, substitution of each separated row, row combination and rotation. Accuracy and security analysis of proposed method for 2D ECG encryption is evaluated on MIT-BIH arrhythmia database.

INTRODUCTION

The technology advancements in health care systems have dramatically increased the number of elderly patients. Remote health care monitoring of patients can decrease the traffic at specialized medical centers and provide reliable emergency services. The applications of remote healthcare technologies have also reduced the medical costs as well. In remote health care monitoring, body sensors acquire biological signals and other physiological parameters of the patient. The recorded signals and confidential side information or any urgent alerts are sent to the specialized hospital servers or medical cloud via the Internet. The security and privacy threats as well as crucial biomedical data integration issues are introduced with internet as a communication channel. Secure transmission of confidential biomedical data has become a common interest in both research and applications (Leeet al., 2008; Li et al., 2013; Hu et

DOI: 10.4018/978-1-7998-1763-5.ch002

al., 2007). Accordingly, it is essential to employ a security protocol which will have powerful information security. One method to protect information from unauthorized eavesdropping is to use an encryption technique. The encryption is the process by which the information is transformed into intelligible form to construct the encrypted data/cipher data. Decryption is the process to reconstruct the original information from encrypted data.

An electrocardiogram (ECG) is an important physiological signal required to transmit in remote health care system used not only to analyze cardiac diseases, but also to provide crucial biometric information for identification and authentication. The ECG signal which monitors the electrical activity of heart is usually characterized by its various set points (P, QRS, T) and intervals (PR interval, QT interval and RR interval) that reflects the rhythmic electrical depolarisation and repolarisation of atria and ventricles (Singh et al., 2014). With an ECG signal, various arrhythmias, degree of myocardial damage and the structure of the atrium and ventricle can also be analyze and identified. While transmitting biomedical information such as ECG through the internet, protection of patient's privacy and confidentiality is a challenging issue (Jero et al., 2015). The methods of computer software should guarantee the information security on the server and inside the communication channels. Several researchers have proposed various security protocols to secure patient confidential information (Enginet al., 2005; Ibaida et al., 2013). The Encryption algorithms based techniques are commonly used to secure data during the communication and storage. As a result, the final data will be stored in encrypted format (Wang et al., 2010; Maglogiannis et al., 2009).

In 1998, Fridrich proposed the chaos-based approach for image encryption (Fridrich 1998), since then there have been increasing researches on chaotic encryption techniques. Chaos based algorithms are developed and considered as the core of encryption processes due to ergodicity, mixing property, the high sensitivity of chaotic systems to parameters and initial conditions (Zhu et al., 2011; Fu et al., 2011; Zhu et al., 2012). Recently, conventional logistic map and tent map based1D chaotic maps, and coupled map lattice based 2D chaotic maps have been developed for substitution-only encryption methods (Soma et al., 2013; Radwan et al., 2016). Chaos-based algorithms have shown exceptionally superior properties in aspects such as security, speed and complexity and computational cost.

Many researchers have proposed ECG signal processing techniques by treating 1D ECG signal as a 2D image and exploiting the inter- and intra-beat correlations by encoder (Chou et al., 2006; Wang et al., 2008). The "cut and align beats approach and 2D DCT" and "period normalization and truncated SVD algorithm" are available preprocessing techniques to get good compression results in ECG (Wei et al., 2001; Lee et al., 1999). This kind of preprocessing are also often associated with the use of state-of-the-art image encoders, like JPEG2000. In (Chou et al., 2006), the authors proposed a lousy compression technique based on converting the 1D ECG signal into 2D ECG image. A period sorting preprocessing technique was introduced, which consists of a length-based ordering of all periods. The authors exploited inter and intra-beat dependencies to compress irregular ECG signals. The technique is based on the supposition that periods with similar lengths tend to be highly correlated, which is not a very strong assumption and may not be valid for pathological ECG signals. Another preprocessing technique consists of QRS detector, period length normalization, period preprocessing and image transform was proposed in (Filho et al., 2008).

This chapter introduces a simple and efficient chaotic system approach using a combination of two existing 1D chaotic maps to encrypt 2D ECG signal. Security analysis reveals the performance of proposed method for 2D ECG encryption. ECG is encrypted in a lossless manner so that after reconstruction there will be zero difference between the original and the reconstructed ECG signal.