Chapter 36
Secured Transmission of Clinical Signals Using Hyperchaotic DNA Confusion and Diffusion Transform

S. J. Sheela
https://orcid.org/0000-0001-6793-1182
Siddaganga Institute of Technology, Tumakuru, India

K. V. Suresh
Siddaganga Institute of Technology, Tumakuru, India

Deepaknath Tandur
ABB, Bengaluru, India

ABSTRACT

Secured transmission of electrophysiological signals is one of the crucial requirements in telemedicine, telemonitoring, cardiovascular disease diagnosis (CVD) and telecardiology applications. The chaotic systems have good potential in secured transmission of ECG/EEG signals due to their inherent characteristics relevant to cryptography. This article introduces a new cryptosystem for clinical signals such as electrocardiograms (ECG) and electroencephalograms (EEG) based on hyperchaotic DNA confusion and diffusion transform (HC-DNA-CDT). The algorithm uses a hyperchaotic system with cubic nonlinearity and deoxyribonucleic acid (DNA) encoding rules. The performance of the cryptosystem is evaluated for different clinical signals using different encryption/decryption quality metrics. Simulation and comparison results show that the cryptosystem yield good encryption results and is able to resist various cryptographic attacks. The proposed algorithm can also be used in picture archiving and communication systems (PACS) to provide an efficient sharing of medical image over the networks.

DOI: 10.4018/978-1-7998-7705-9.ch036

INTRODUCTION

Telemedicine provides sophisticated health care services remotely by using advanced communication technology. It is proven to be the most cost-effective way of extending proper diagnosis, treatment planning and disease prevention utilizing the expertise of specialists and services of local health care workers (WHO, 1998). ECG and EEG signals are the most commonly used clinical signals in telemedicine to resolve patient's abnormalities. An electrocardiogram is a signal generated by the electrical activity of the heart which is used to diagnose the cardiovascular diseases. The electrical signal generated by the brain which is used to detect epilepsy or cognitive functions such as memory loss or concentration is called EEG. Telemedicine presents potential security risks in the exchange of multimedia data, since personal information and clinical data is transmitted over the public internet (Lin, 2016; Murillo-Escobar et al., 2017). Nowadays clinical signals are used to identify the person as they contain patient's sensitive private health information. This necessitates the development of a reliable, fast and robust security system to provide data confidentiality of patient's health information and identification for ethical and legal reasons.

Encryption is one of the convenient strategies which guarantee the secured transmission of clinical signals over an insecure communication channel. In this regard, many novel schemes based on watermarking and generic cryptographic algorithms have been proposed in order to suite the evolvement in wireless communication technologies. However, these algorithms require more computational time and high computing power. It is necessary to explore simple encryption techniques to ensure secure communication in telemonitoring of critical, acute and chronic patients. Many researchers have identified the positive relationship between chaos and cryptography. Chaotic systems have significant properties such as high sensitiveness to initial conditions/system parameters, topological transitivity, erratic behavior, ergodicity and simplicity (Chen, 2015). These outstanding features are equivalent to the counterparts of cryptography which offer good trade-off between security and performance. Hence, these chaotic systems are the perfect candidates in providing the secure communication. In 1998, Fridrich (Fridrich, 1998) first proposed chaos-based image encryption scheme which consists of two stages: confusion and diffusion. These stages are applied to scramble the pixel positions randomly and to change the pixel values respectively. This basic architecture is known as confusion–diffusion or permutation–substitution architecture which guides in the design of chaos-based ciphers. Based on this architecture, numerous chaos-based cryptosystems for multimedia applications have been proposed (Chen, 2015; Hua, 2015; Tong, 2015). Some of them have utilized lower dimensional chaotic maps in the development of security system because of their exceptional features, high speed encryption and simple structures (Prateek, 2006; Ye, 2012). But the authors in (Kocarev, 2001; Wang, 2011) have revealed that lower dimensional chaotic maps result in single simple predictable chaotic orbits. As a result, the initial states and/or system parameters of the chaotic map can be obtained easily. This weakness has degraded the security performance of the cryptosystem. In order to overcome these drawbacks, authors have suggested and proposed encryption schemes based on hyperchaotic systems (Liu, 2016; Tong, 2015; Yuan, 2017) due to their dynamic properties such as higher unpredictability, expansion of complex dynamics more than one direction and more than one positive Lyapunov exponent (Kocarev, 2001). In addition, hyperchaotic systems provide strong confidentiality and large key space.

Further, it has been proved that the encryption schemes using only chaos are less secure which necessitates the introduction of new mechanism to enhance the security of the cryptosystem (Bechikh, 2015; Cokal, 2009; Xie, 2017). In order to make chaos-based cryptosystem more efficient and secure, DNA technology has been infiltrated due to its exclusive characteristics such as huge parallelism, enormous