International Journal of
Scientific Engineering and Technology Research

www.ijsetr.com

ISSN 2319-8885
Vol.05,Issue.12
May-2016,
Pages:2323-2327

An Intelligent Technology for Protecting Patient Security Information Based on ECG Wavelet Transform

ZAINAB QAHTAN MOHAMMED[1], DR. E. SREENIVASA REDDY[2]
[1]PG Scholar, Dept of CSE, Acharya Nagarjuna University, College of Engineering & Technology, AP, India,
E-mail: altmimi104@gmail.com.
[2]Professor, Dept of CSE, Acharya Nagarjuna University, College of Engineering & Technology, AP, India,
E-mail: esreddy67@gmail.com.

Abstract: In the current open society and with the growth of human rights, people are more and more concerned about the privacy of their information and other important data. This study makes use of electrocardiography (ECG) data in order to protect individual information. New technologies in multimedia and communication fields have introduced new ways to transfer and save the medical image data through open networks, which has introduced new risks of inappropriate use of medical information. Electrocardiograms as personal data are being applied more and more as a biometric and deserve to be protected. In this paper, a wavelet based steganography technique has been introduced which combines encryption and LSB embedding technique to protect patient confidential data. Huge amount of ECG signal collected by Body Sensor Networks (BSNs) from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level etc. and diagnosed by those remote patient monitoring systems. The proposed method allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the rest. To evaluate the effectiveness of the proposed technique on the ECG signal, some distortion measurement metrics have been used: the Percentage Residual Difference (PRD) , the root mean square Error (RMSE), peak to peak signal to noise ratio (PSNR) and correlation coefficient. It is found that the proposed technique provides high security protection for patients data with low distortion and ECG data remains diagnosable after watermarking (i.e. hiding patient confidential data) and as well as after watermarks (i.e. hidden data) are removed from the watermarked data.

Keywords: ECG Steganography, Lifting Wavelet Transform, Chaos Encryption, Performance Analysis.

I. INTRODUCTION

An ECG reflects the process of the electrical activity of the heart, which can be taken as a reference for the study of cardiac function and cardiac pathology. With an ECG signal, we can analyze and identify various arrhythmias, and understand the degree and development of myocardial damage, as well as the structure and function of the atrium and ventricle. Besides, it is necessary to decrease the demand for the ECG data storage capacity and data transmission bandwidth. ECG Steganography provides secured transmission of secret information such as patient personal information through ECG signals. This paper proposes an approach that uses discrete wavelet transform to decompose signals to embed the secret information into the decomposed ECG signal. In this model, body sensor nodes will be used to collect ECG signal, glucose reading, temperature, position and blood pressure, the sensors will send their readings to patient's PDA device via Bluetooth. Then, inside the patient's PDA device the stenography technique will be applied and patient secret information and physiological readings will be embedded inside the ECG host signal. Finally, the watermarked ECG signal is sent to the hospital server via the Internet. As a result, the real size of the transmitted data is the size of the ECG signal only without adding any overhead, because the other information are hidden inside the ECG signal without increasing its size. At hospital server the ECG signal and its hidden information will be stored. Any doctor can see the watermarked ECG signal and only authorized doctors and certain administrative personnel can extract the secret information and have access to the confidential patient information as well as other readings stored in the host ECG signal.

The widespread and easy access to multimedia content has motivated development of technologies for digital steganography or data hiding, with emphasis on access control, authentication, and copyright protection. Steganography deals with information hiding, as opposed to encryption. Steganography is defined by Markus Kahn [3] as follows "Steganography is the art and science of communicating in a way which hides the existence of the communication as shown in Fig.1. Cryptography is the technique of transforming information to more secured form. Digital encryption of medical images before transmission and storage is proposed as an easiest way to protect the patient information. Cryptography technique can be divided into symmetric encryption needs secret key and asymmetric encryption which needs private and public keys. An encryption technique [4] is used which is a blend of symmetric key encryption and steganography with a variable length key derived from the encrypted text itself to have better security. Chaotic systems [5] [6] can be used for medical images to achieve robust system as shown in Fig.2.

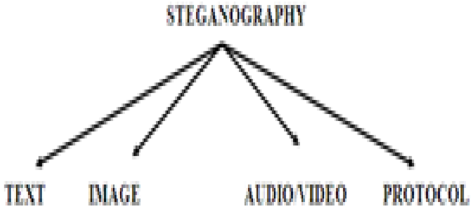


Fig.1.Different types of steganography.

The goal of Steganography is to mask the very presence of communication making the true message not discernible to the observer. As steganography has very close to cryptography and its applications, we can with advantage highlight the main differences. Cryptography is about concealing the content of the message as shown in Fig.3. At the same time encrypted data package is itself evidence of the existence of valuable information as shown in Fig.4.

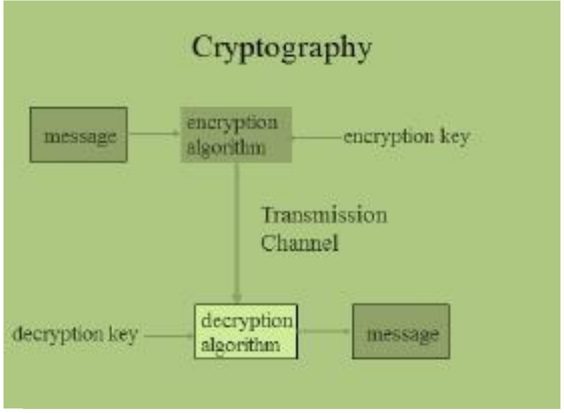


Fig.2. General structure of Chaos algorithm.

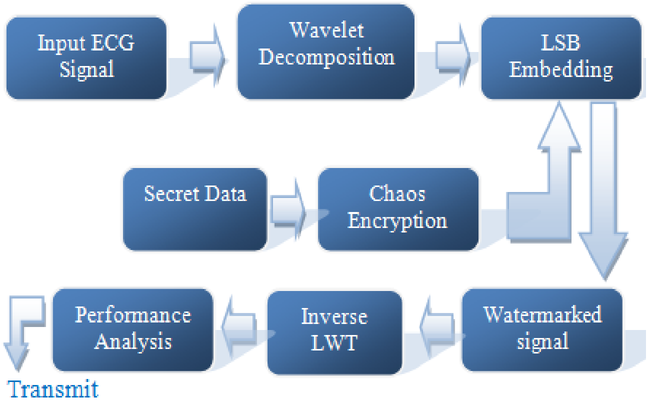


Fig.3. Block Diagram of the sender steganography which encryption, wavelet decomposition and secret data embedding.

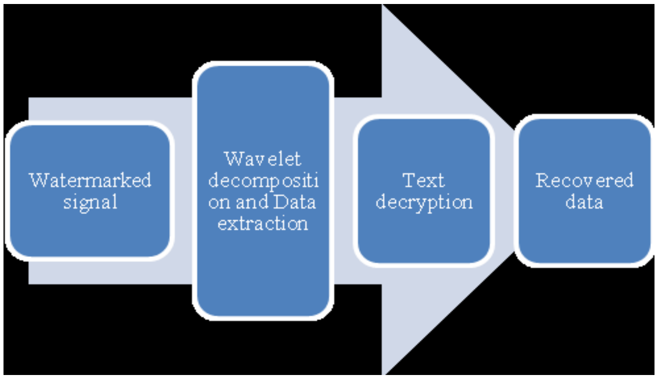


Fig.4. Block Diagram of the receiver which includes wavelet decomposition, extraction, decryption.

II. METHODOLOGY

A. Wavelet Transform

In order to hide the data we should convert the time domain signal into the frequency domain. The transformation of a signal is nothing but representing the signal in a different form. There is no change in the information inside the signal. For the correct analysis it takes multistage wavelet decomposition. The fig.5 shows „h‟ is low-pass filter, „g‟ is high-pass filter, and ↓2 ‟is down sampling. Wavelet transform is a process that decomposes the given signal into high frequency and low frequency coefficients. Wavelet transform can be defined as shown in following equation 1.

$$C(S,P) = \int_{-\infty}^{\infty} f(t)\Psi(S,P)dt \quad \textbf{(1)}$$

Where Ψ represents wavelet function. S and P are positive integers representing transform parameters. C represents the coefficients which is a function of scale and position parameters. Wavelet transform is a powerful tool to combine time domain with frequency domain in one transform.

In most applications discrete signals are used. Most of the important features of the ECG signal are related to the low frequency signal. Therefore, this signal is called the approximation signal (A). On the other hand, the high frequency signal represents mostly the noise part of the ECG signal and is called detail signal (D). As a result, a small number of the sub-bands will be highly correlated with the important ECG features while the other sub bands will be correlated with the noise components in the original ECG signal. Therefore, in our proposed technique different number of bits will be changed in each wavelet coefficient (usually called steganography level) based on its sub-band. As a result, a different steganography level will be selected for each band in such a way that guarantees the minimal distortion of the important features for the host ECG signal. in a wireless communication network which is employed for data transmission, long term ECG guardianship generates a huge amount of data that will make wireless communication costs unacceptable, and raise issues of transmission speed and bandwidth. ECG signal compression technology will guarantee that none of the information of the ECG signal is lost and will minimize the amount of data that needs to be transmitted, reduce transmission costs, and increase transmission speed. That's why using wavelet transform.

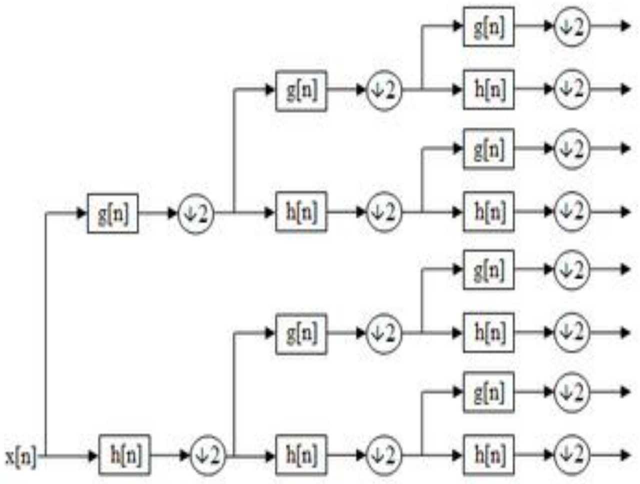


Fig.5. Wavelet transform.

B. Encryption

To encrypt the patient confidential information in such a way that prevents unauthorized persons who does not have the shared key- from accessing patient confidential data. In this stage XOR ciphering technique is used this techniques works on the following principles:

- 0 + 0 = 0
- 0 + 1 = 1
- 1 + 0 = 1
- 1 + 1 = 0
- A + (B + C) = (A + B) + C

The effective acceleration of chaos-based cryptosystem is thus achieved. Theoretical analysis and experimental results show that the proposed algorithm has large key-space, high efficiency, and satisfied security, suits for signal data transmission as shown in Fig.6.

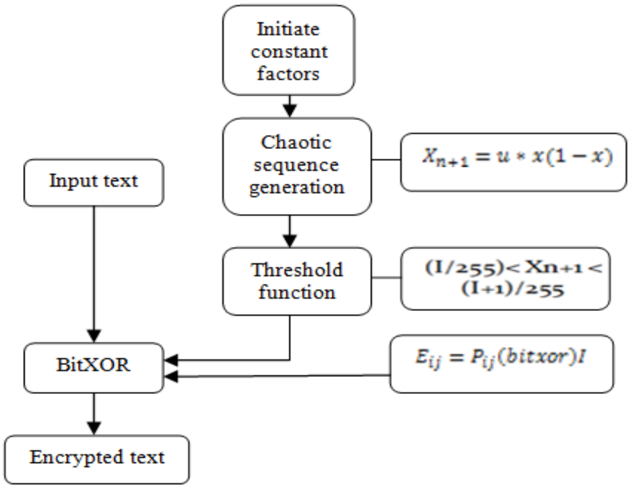

Initiate constant factors
Chaotic sequence generation
$X_{n+1} = u * x(1-x)$
Input text
Threshold function
(I/255)< Xn+1 < (I+1)/255
BitXOR
$E_{ij} = P_{ij}(bitxor)I$
Encrypted text

Fig.6. Block Diagram showing the detailed construction of the chaotic encryption operation.

C. Water Marking Process

Watermarking is the process that embeds data called a watermark into an image or audio or video [10]. The watermark can be detected and extracted later from the carrier (cover). It can contain information such as copyright, license, authorship etc. Any watermarking algorithm consists of three parts: The watermark, which is unique to the owner.

- The encoder for embedding the watermark into the data.
- The decoder for extraction and verification

At this stage the proposed technique will use a special security implementation to ensure high data security. Encrypted data is hidden onto the ECG signal via LSB embedding. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. A detailed coefficients obtained from wavelet domain are used here for concealment process and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first bit selected coefficient and the second bit of message is embedded into the second bit location and so on. The resultant watermarked signal which holds the secret message with original form and difference between the input signal and the watermarked signal is not visually perceptible.

D. Inverse Wavelet Recomposition

In this final stage, the resultant watermarked sub-bands are recomposed using inverse wavelet packet re-composition. The result of this operation is the new watermarked ECG signal. The inverse wavelet process will convert the signal to the time domain instead of combined time and frequency domain. Therefore, the newly reconstructed watermarked ECG signal will be very similar to the original un water marked ECG signal.

E. Extraction Process

The extraction starts by extracting the secret bits in the correct order from the LSB .Finally, the extracted bits are decrypted. The extraction process is almost similar to the embedding process except that instead of changing the bits of the selected coefficients, it is required to read values of the bits in the selected coefficients, and then resetting them to zero.

III. RESULTS

In these paper three different types of ECG signals are used for experimentation. A test bed of ECG samples is used for experimentation. To evaluate the proposed model, the PRD (percentage Residual difference) is used to measure the difference between the original ECG host signal and the resulting watermarked ECG signal. For find out the psnr and mse values AND CC and results as shown in Figs.7 to 10.

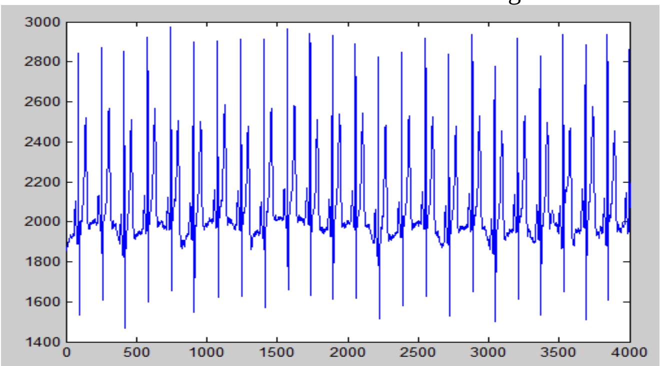
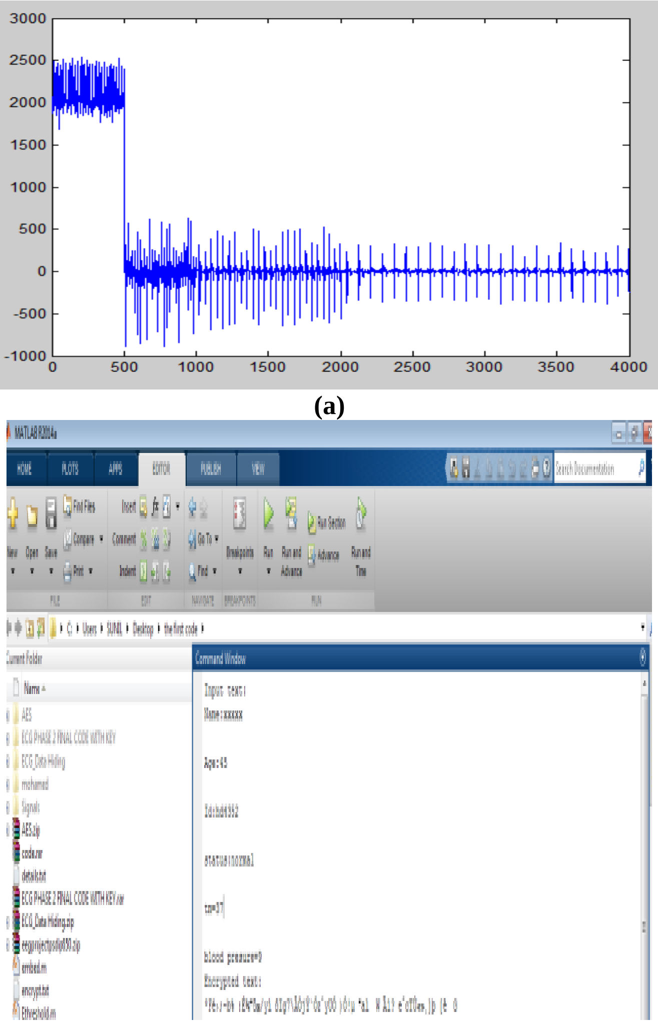


Fig.7.input signal.



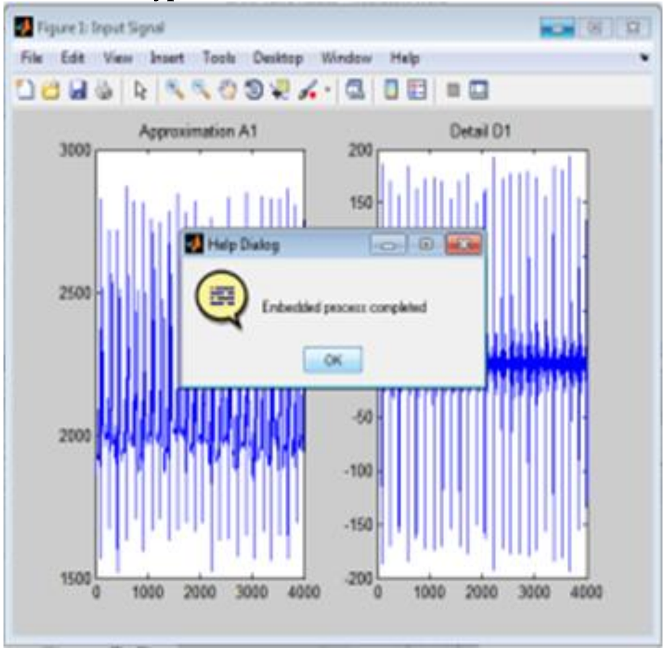
(a)

```
Input text:
Name:xxxxx

Age:45

Id:hd4352

status:normal

tm=37

blood pressure=9
Encrypted text:
[illegible]
```

(b)

Fig.8. Multi level wavelets transform.

A. Data Encryption



Embedded process completed

Fig.9. Embedded Process Completed.

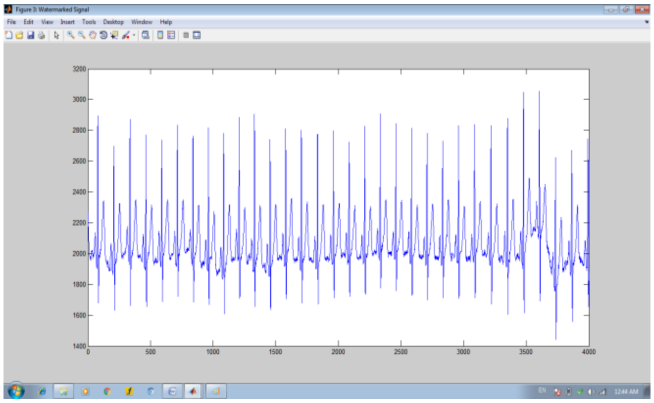


Fig.10. Water Marked Signal.

IV. EVALUATION

In this section, we evaluate the performance of the method. In this paper, three different types of ECG signals are used for experimentation. A tested of 4 ECG samples is used for experimentation. The set of samples consist of (2) normal (NSR) ECG samples, (1) Ventricular fibrillation ECG samples and (1) Ventricular Tachycardia ECG samples. . Each sample is 10 seconds long with 250 Hz sampling frequency. To evaluate the proposed model, the PRD (percentage residual difference) is used to measure the difference between the original ECG host signal and the resulting watermarked ECG signal. To validate diagnosability of the digitally processed ECGs,. 4 ECG Segments for both normal and abnormal cases

TABLE I: Performance Analysis for Normal ECG

Sample no.	PRD	RMSE	PSNR	COR –COF
1	0.2415	4.9932	62.4830	0.9997
2	0.2452	5.0611	63.6887	0.9996

TABLEII: Performance Analysis for Abnormal ECG

Sample no.	PRD	RMSE	PSNR	COR –COF
1(VT)	0.2456	5.0638	62.6526	0.9995
2(VF)	0.1923	4.1105	64.6827	0.9999

Finally, these tables show the PRD measured after extracting the watermark. It is obvious from the tables that removal of the watermark will have a small impact on the PRD value. As a result, the ECG signal can still be used for diagnoses purposes after removing the watermark.

V. CONCLUSION

This paper discusses an innovative idea using the CHOAS encryption TO ENCRYPTION confidential data. A novel steganography algorithm is proposed to hide patient information as well as diagnostics information inside ECG signal. This technique will provide a secured communication and confidentiality in a Point-of-Care system. This algorithm can be used to hide confidential data inside the ECG signal. The suggested technique provides an authentication technique to prevent unauthorized persons from gaining access to the confidential data. Thus this algorithm can be used for secure transmission in cardiac monitoring systems and also for storage of patient information in the cloud. It can also be used for secure transmission of user identification data for validation using biometric wrist bands where data privacy is critical. In this paper we tested the diagnoses quality distortion. It is found that the resultant watermarked ECG can be used for diagnoses and the hidden data can be totally extracted.

VI. REFERENCES

[1] K. Malasri and L. Wang, “Addressing security in medical sensor networks,” in Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments. ACM, 2007, p. 12.

[2] J. C. Lin, “Applying telecommunication technology to health care delivery,” IEEE Eng. Med. Biol. Mag., vol. 18, no. 4, pp. 28–31, Jul./Aug. 1999.

[3] D. Hailey, R. Roine, and A. Ohinmaa, “Systematic review of evidence for the benefits of telemedicine,” J. Telemed. Telecare, vol. 8, pp. 1–7, 2002.

[4] K. Zheng and X. Qian, “Reversible Data Hiding forElectrocardiogram Signal Based on Wavelet Transforms,” in International Conference on Computational Intelligence and Security, 2008. CIS’08, vol. 1, 2008.

[5] H. Golpira and H. Danyali, “Reversible blind watermarking for medical images based on wavelet histogram shifting,” in IEEE International Symposium on Signal Processing and Information Technology (ISSPIT),2009. IEEE, 2010, pp. 31–36.

[6] I. Maglogiannis, “Design and implementation of a calibrated store and forward imaging system for teledermatology,” J. Med. Syst., vol. 28, no.5, pp. 455–467, 2004.

[7] A. Kollmann, D. Hayn, J. Garcia, B. Rotman, P. Kastner, and G. Schreier, “Telemedicine framework for manufacturer independent remote pacemaker follow-up,” in Proc. Comput. Cardiol., 2005, pp. 49–52.

[8] V. Traver, E. Monton, J. L. Bayo, J. M. Garcia, J. Hernandez, and S. Guillen, “Multiagent home telecare platform for patients with cardiac diseases,” in Proc. Comput. Cardiol., 2003, pp. 117–120.

[9] A. De la Rosa Algarin, S. Demurjian, S. Berhe, and J. Pavlich-Mariscal, “A security framework for xml schemas and documents for healthcare,” in Bioinformatics and Biomedicine Workshops (BIBMW), 2012 IEEE International Conference on, 2012, pp. 782–789.

[10] F. Hu, M. Jiang, M. Wagner, and D. Dong, “Privacy-preserving telecardiology sensor networks: toward a low-cost portable wireless hardware/ software codesign,” IEEE Transactions on Information Technology in Biomedicine,, vol. 11, no. 6, pp. 619–627, 2007.