International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 02 Issue: 06 | Sep-2015 www.irjet.net p-ISSN: 2395-0072

SECURE SHARING OF SENSITIVE HEALTH DATA USING WAVELET STEGANOGRAPHY

Swapnil S. Tambatkar[1], S. O. Rajankar[2]
[1]*Student, Department of E&TC, SCOE, Pune, Maharashtra, India,*
[2]*Professor, Department of E&TC, SCOE, Pune, Maharashtra, India,*

Abstract - *The paper proposes the new steganography technique for securing the physiological reading like Temperature, Glucose level, Blood Pressure in host signal. Due to significant development in information and communication technologies, the scope of healthcare delivery and medical data management has considerably changed over last few years. Hence complementary or alternative solutions are required to overcome the new challenges, especially regarding security and full access control on the widely distributed sensitive health data. Also according to Health Insurance Portability and Accountability Act (HIPAA),patient's sensitive medical data should be secure and protected from unauthorized access. This proposed system used Electrocardiogram (ECG) signal as a host signal. The steganography is art of hiding secret information inside another type of data i.e. cover. Electrocardiogram (ECG) signal is a used for diagnosis of various cardiovascular diseases, hence it important to have less amount of distortion. So that host signal (ECG) should be diagnosable. The proposed technique used DWT and DCT based system scrambling with security key. Finally the Peak signal to noise ratio (PSNR) is used to evaluate the diagnosability and distortion occurred in system. The average PSNR obtained for system is more than 60 db.*

Key Words: *ECG, DWT, DCT, Watermarking, Steganography*.

1. INTRODUCTION

The advancement in medical sciences and information technologies have led to a new age in healthcare delivery and it's management system. New challenges have face up, especially concerning about security of sensitive health data for easier access and distribution of digital data. The researchers seeks complementary or alternative solutions to overcome these security problem and to effectively deal with patients full control access on their sensitive medical data.

The steganography is art of hiding secret information inside another type of data called host. The information may be image, text or signal and also the host data may be other signal, image or text etc. The privacy protection of patient's confidential data is important according to Health Insurance Portability and Accountability Act. Patient can manage that who can access his/her health record. Accordingly, it is crucial important to implement security protocol which will have powerful communication and storage security [1].

The proposed method used steganography technique to hide patient physiological signal such as Temperature signal, Glucose level, Blood pressure etc into host signal. The host signal used is Electrocardiogram signal. Electrocardiogram (ECG) signal is a used as diagnosis for various cardiovascular diseases. It is recorded by electrode as electrical activity of heart. The cardiac health of patient is reflected by morphology and heart rate of that patient, which is used in recognition of the heart diseases. Any change in heart rate, rhythm, or the morphological pattern is a sign of cardiac arrhythmia. The recorded ECG waveform is used to identify disorder. Hence it is useful to protect characteristics of host ECG signal during steganography process. That means it can be used for analyzing cardiac health after processing.

For providing high security to the system, the proposed technique use double transform i.e. Discrete Wavelet Transform and Discrete Cosine Transform. Prime importance is given to provide security and control access to system. And hence scrambling with security key is used. For embedding data Amplitude scaling method is used. The distortion level is analyze, so that host signal should be used for diagnosis purpose.

Several approaches have been proposed to protect patient sensitive data. Basically there are two main method to hide the data first is spatial domain and second is transform domain. In spatial domain the confidential data are directly embedded into the host data by shifting bit and it is easy method. In transform domain, data bit is embedded after having transform of host data or signal. The security level of transform domain is very high as compared to spatial domain. Also there are some techniques that are depends on encryption and cryptographic algorithms. In encryption technique, the data are used to encrypt in such way that without having proper decryption key, it is difficult to have secret data. As

a result, the final sensitive data will be obtained in encrypted format These techniques are used to protect patient confidential data during the storage and communication but it has large calculation overhead. Another approaches [3],[4],[5],[6],[7] are proposed to protect confidential medical data based on steganography and bit shifting method for embedding data bit. They used medical images like MRI as host. Some approaches [8],[9],[10] are proposed watermarking based protection of data based on transform domain.

The rest of paper is formulated as follows: In section II, Methodology and proposed approached of system in briefs. In section III, Simulation of system is done. the results and discussion are shown in tabular form, in section IV, final conclusion.

2. METHODOLOGY

The flow diagram for proposed steganography system is shown in Fig 1.

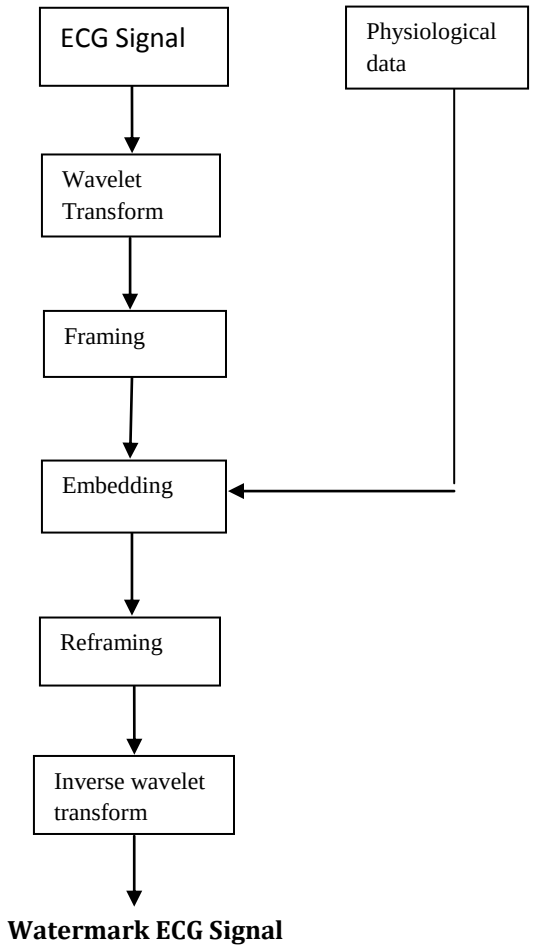

Fig -1: Flow diagram of proposed system

Steps for embedding data are,

1) ECG signal is collected from database.

2) Wavelet transform of ECG signal is obtained.

$$w(i,j) = \sum_i \sum_j X(i)\varphi_{i\,j}(n) \ldots (1)$$

$$\varphi_{i\,j}(n) = 2^{\frac{-i}{2}}\varphi\left(2^{\frac{-i}{2}}n - j\right) \ldots . (2)$$

where W(i,j) represent coefficient of DWT and $\varphi_{i\,j}(n)$ is wavelet basis function.

3) The physiological signal of patient are scrambled using scrambler and converted into binary form.

4) The approximation coefficient u(n) obtained from wavelet transform are segmented into block called framing. It depends on number of sample and data to embedded.

5) At the embedding, DCT of each block is calculated using Eq.(3). u (n) is approximation coefficient and v (k) is DCT coefficient obtained after transform.

$$v(k) = \alpha(k)\sum_{n=0}^{N-1} u(n)\cos\left[\frac{\pi(2n+1)k}{2N}\right] \quad 0 \le k \le N-1 \quad \ldots (3)$$

$$u(k) = \alpha(k)\sum_{n=0}^{N-1} v(k)\cos\left[\frac{\pi(2n+1)k}{2N}\right] \quad 0 \le k \le N-1 \quad \ldots .. (4)$$

where, $\alpha(k) = \sqrt{\frac{1}{N}} \quad for\ k = 0;$

$$\alpha(k) = \sqrt{\frac{2}{N}} \quad for\ k \neq 0;$$

The binary bits obtained from physiological signal are embedded into DCT coefficient. For embedding, Amplitude Scaling Algorithm method is used. After embedding, The inverse DCT transform of coefficient is obtained using Eq. (4) .

6) The re- framing of DCT coefficient is done.

7) For converting signal into original time domain from time-frequency domain ,the inverse wavelet transform is done. Hence watermark ECG signal is obtained.

Steps used for extracting data at receiver is similar as, Fig 1 flow diagram. After receiving signal, DWT of signal is obtained. So that, to have Approximation and Detailed coefficient of received signal. Then at Extraction step, DCT of Approximation coefficient is calculated and data bits are obtained from embedded bit location by amplitude re-scaling algorithm and inverse DCT. Obtained Data bits from extraction step are converted into original signal form by conversion process. Fig 2 shows extraction step used for the collection of data bits from received signal.

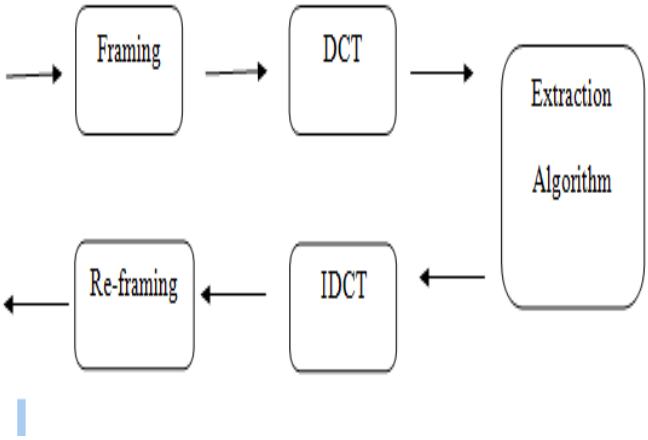

Fig -2: Extraction Process

3.SECURITY ANALYSIS AND SIMULATION

Some parameter shared between transmitter and receiver are used for security analysis of system. The extraction process of proposed method affected by small change in these parameter, which are level of decomposition, position of embedding framing structure and scrambling matrix. This parameter should agreed by both transmitter and receiver. If little change occurred in these factor or parameter, it directly affects the extraction of data.

MATLAB-Simulink Software is used to simulate this proposed system. Three physiological readings i.e. Temperature signal, Glucose level of patient and their Blood pressure are embedded into ECG signal. Fig 2 and Fig 3 shows simulation result. It shows Original ECG signal, Watermark signal and Reconstructed ECG signal.

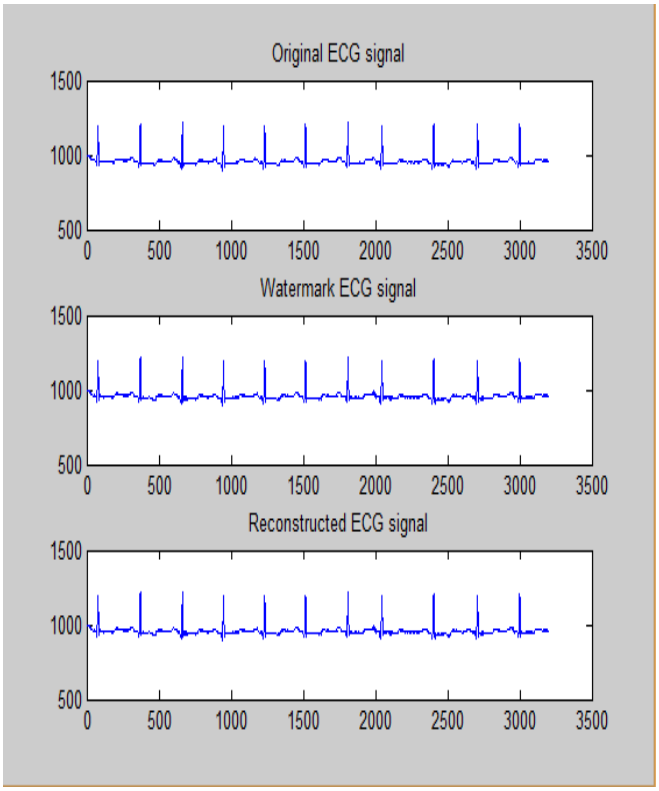

Fig -3: Original, Watermark and Reconstructed ECG Signal

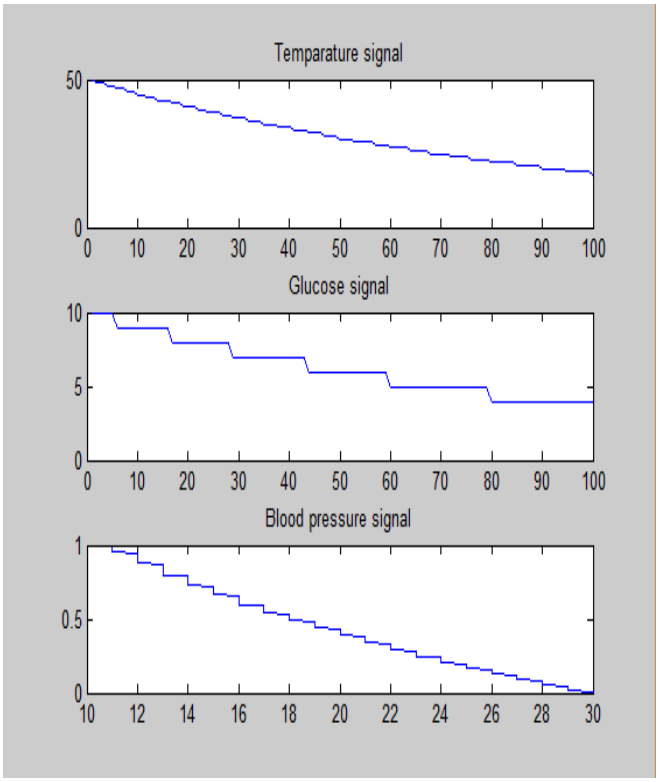

Fig -4: Physiological Signal

In Fig 3, sub fig. 1 shows original ECG signal collected from database. Watermark ECG signal and reconstructed ECG signal is shown in sub fig 2 and 3 respectively. From fig 3, it is observed that original, watermark and reconstructed signal are look similar i.e. distortion is very less. Fig 4 shows Physiological signal like Temperature, Glucose level and Blood Pressure of patient, which is used for embedding in host signal i.e. in ECG signal. The Peak Signal to Noise Ratio (PSNR) is used to calculate the performance of proposed system performance and PSNR of system is calculated using Eq. No. 5.

$$PSNR = 10log_{10}\frac{(MAX)^2}{MSE} \quad \ldots.(5)$$

The Peak signal to noise ratio (PSNR) is measure often used to compare the performance of reconstructed ECG signal. Peak signal-to-noise ratio, often abbreviated PSNR is an engineering term, which is the ratio between the maximum probable power of a signal and the power of corrupting noise that affects the fidelity of its representation. The PSNR is expressed in dB. It is good to have a greater value of PSNR. where MAX is maximum value of signal and MSE is Mean Square Error which is defined as.

$$MSE = \frac{1}{m}\sum_{i=0}^{m-1}(X(i) - R(i))^2 \quad \ldots..(6)$$

where X(i) and R(i) are original and watermark signal coefficient.

Table I shows comparison table for embedding process with two technique. first one is embedding data bit into host signal after applying DCT transform to the approximation coefficient of obtained from DWT. Second technique is directly embedded data into approximation coefficient obtained from DWT. The parameter used for comparison is Peak Signal to Noise Ratio and Total Time required to complete the process of embedding and extraction.

Table -1: Embedding comparison with and without DCT

Record No.	System with DCT		System without DCT	
	PSNR	Time Required	PSNR	Time Required
101_s2	62.21	9.037	11.25	4.669
103_s1	59.92	9.140	13.33	4.646
103_s2	60.69	9.173	12.38	4.607
105_s1	61.01	9.216	13.12	4.533
105_s2	61.41	9.336	12.28	4.578
106_s2	60.01	9.013	11.69	4.542
109_s1	60.51	9.146	12.92	4.583
109_s2	61.98	9.108	11.61	4.543
111_s1	61.70	9.208	12.28	4.579
111_s2	63.04	9.141	13.52	4.569
114_s1	61.47	9.029	11.90	4.508

It is observed from the Table I that average PSNR ratio obtained for proposed system is 61 db and the maximum PSNR obtained is 63 db. Hence maximum PSNR value , less distortion in signal i.e. both signal appear like same. The execution time for proposed system is around 9 Sec. The max PSNR ratio for system without DCT is 14 db, which is quite less. And hence watermark signal obtained are distracted due embedding process. It is not used for diagnosis purpose as PSNR is minimum. The execution time required is around 5 second. As signal diagnosis is important, hence this factor can not affect system much.

4. CONCLUSIONS

The proposed approach provide the new technique for steganography. The proposed technique used transform domain steganography i.e. Wavelet transform and DCT for hiding patient confidential data such as Glucose level, Temperature, Blood Pressure value into host signal. The proposed system follow the Health Insurance Portability and Accountability Act policy, that system should provide security and protection to patient sensitive information. In this system, the diagnoses quality of host signal i.e. ECG signal is analyze using Peak Signal to Noise Ratio (PSNR) after watermark and reconstruction. The average PSNR ratio is obtained greater than 60db. As PSNR ratio is more, the distortion occurred in signal is less. And hence ECG signal is diagnosable. From comparison of system with DCT and without DCT shows that, PSNR obtained for DCT system is very high as compared to 14 db in without DCT system. Though the time requirement is more but similarity of original and reconstruction of signal is maximum.

ACKNOWLEDGEMENT

I welcome this opportunity to express my heartfelt gratitude and regards to Prof. S. O. Rajankar, Department of E&TC, Sinhgad College of Engineering, Vadagaon (Bk), Savitribai Phule Pune University, Pune, Maharashtra, India, for his unconditional guidance.

REFERENCES

[1] Y. Lin, I. Jan, P. Ko, Y. Chen, J.Wong, and G. Jan, "A wireless PDA-based physiological monitoring system for patient transport," *IEEE Trans. Inf. Technol. Biomed.*, vol. 8, no. 4, pp. 439–447, Dec. 2004.

[2] W. Lee and C. Lee, "A cryptographic key management solution for HIPAA privacy/security regulations," *IEEE Trans. Inf. Technol. Biomed.*, vol. 12, no. 1, pp. 34–41, Jan. 2008.

[3] L. Marvel, C. Boncelet, and C. Retter, "Spread spectrum image steganography," *IEEE Trans. Imag. Process.*, vol. 8, no. 8, pp. 1075–1083, Aug. 1999.

[4] M. Li, S. Yu, Y. Zheng, K. Ren, andW. Lou, "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[5] S. Kaur, R. Singhal, O. Farooq, and B. Ahuja, "Digital watermarking of ECG data for secure wireless communication," in *Proc. Int. Conf. Recent Trends Inf. Telecommun. Comput.*, Mar. 2010, pp. 140–144.

[6] H. Golpira and H. Danyali, "Reversible blind watermarking for medical images based on wavelet histogram shifting," in *Proc. IEEE Int. Symp. Signal Process. Inf. Technol.*, Dec. 2009, pp. 31–36.

[7] K. Zheng and X. Qian, "Reversible data hiding for electrocardiogram signal based on wavelet transforms," in *Proc. Int. Conf. Comput. Intell. Security*, Dec. 2008, vol. 1, pp. 295–299.

[8] A.Al-Fahoum, "Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure," *IEEE Trans. Inf. Technol. Biomed.*, vol. 10, no. 1, pp. 182–191, Jan. 20.

[9] Ayman Ibaida and Ibrahim Khalil ''Wavelet-Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems,'' IEEE Transactions on Biomedical Engineering, vol. 60, no. 12, December 2013.

[10] Hwai-Tsu Hu, Ling-Yuan Hsu," Perceptual-based DWPT-DCT framework for selective blind audio watermarking," Science Direct, Signal Processing 105. (2014) pp.316–327.

[11] John G. Proakis and Dimitris de Monolaskis "Digital signal processing, principles, algorithms and applications," Third edition, Prentice Hall International Pub.