ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

DCT based ECG Steganography for Protecting Patient's Confidential Data in Point-of-Care Systems

Dr. K.V.Padmaja[1], Ankitha.O.P[2], Anshu Singhania[3], Preethi.M.R[4], Rashmi R Nayak[5]

Professor & Associate Dean, Dept. of IT, R.V. College of Engineering, Bangalore, Karnataka, India[1]

UG Students, Dept. of IT, R.V. College of Engineering, Bangalore, Karnataka, India[2,3,4]

ABSTRACT: With the increasing number of aging population and a significant amount suffering from cardiac diseases, a need for monitoring ECG from a remote place arises. Since Point-of-Care systems involve the transmission of patient's confidential information, a proposal is made to encrypt the patient's personal data-name, medi-care number, and telephone number etc. to ensure security of the data and embed the encrypted data onto the ECG signal and transmit. Since personal information is being sent on a public network, it is prone to misuse; hence it is important that patient's data remains confidential throughout the process. Here, DCT (Discrete Cosine Transform) is used to decompose the ECG signal and a novel encryption algorithm is proposed to encrypt the confidential data, the result of which is embedded onto the decomposed ECG using the LSB Algorithm. The method produces acceptable results with minimal distortion to the ECG and the signal remains diagnosable.

KEYWORDS: DCT, ECG, Confidential data, Steganography, Encryption, LSB Steganography.

I.INTRODUCTION

Based on the conclusions of a recent study conducted by DrPrabhatJha, director of the Centre for Global Health Research at the University of Toronto and lead researcher of the study in collaboration with the Registrar General of India (RGI) and the Indian Council of Medical Research (ICMR) cardiac diseases have replaced communicable diseases and have emerged as the number one killer in both urban and rural zones of the country. Point-of-Care systems provide a drastic relief with regards to the growing traffic at hospitals and provide high reliability in times of emergencies, as the patients information is immediately transmitted to the concerned medical professional who is well versed with the patient's medical conditions [1].Remote monitoring proves advantageous as the number of hospitals and care centers are considerably few in number and are at times quite distant and the patient may not be able to make it to the center. Internet provides the main form of communication for the exchange of information [2].

However, using Internet as the main communication channel introduces a higher risk of data hacking and misuse of patient's data. Also, according to the HIPAA (Health Insurance Portability and Accountability Act), any information sent through the Internet needs to be secured and protected from unwanted threats. HIPAA decrees that any information that's related to the patient, when transmitted via the Internet, needs to satisfy the following conditions:

1) The patient gets to decide who can access his/her personal information thereby providing patient's privacy.

2) The programs that are used to provide secure transmission of data needs to guarantee security of the information.

There have been several protocols (or techniques) that have been researched and implemented to provide secure transmission of the information. These protocols can be classified into two broad categories, the first being encryption and cryptographic algorithms and the second being Steganography. This paper uses Steganography as well as cryptographic algorithms to accomplish the HIPAA specifications [3]. The encryption algorithm ensures who can access the data while the Steganography method to hide the patients encrypted confidential data into the patient's biomedical signal [4].The ECG signal is used as the host signal as the size of an ECG signal is large compared to the information that needs to be embedded within. The watermarked ECG signal is now transmitted to the hospital server (where it is stored) via the Internet. The size of the signal transmitted is the size of the ECG as the additional data that has been embedded will not act as an overhead to the whole package. Any person can see the watermarked ECG signal but only the person with the shared key can access the confidential data that has been hidden inside the ECG signal.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

II. LITERATURE SURVEY

H. Wang et al. [5] and K C Wu and Wang [6] proposed a reversible stenographic algorithm using texture synthesis and also proposed BSN architecture and its corresponding algorithms for medical monitoring applications, in particular ECG based applications. Given an original source texture, the program can generate a large Stego synthetic texture to hide the secret information. This can exquisitely weave the steganography into a traditional patch-based texture synthesis. The method is novel and provides reversibility to retrieve the original source texture from the Stego synthetic texture, making it possible for a second round of texture synthesis, if necessary However, the quality of the image is greatly compromised.

Kaur et al. [7], [8] proposed a new digital watermarking of ECG data for secure wireless communications. Each ECG sample is quantized using 10-bits and is divided into segments. The Segment size is equal to the chirp signal that they use. Patient ID is used in the modulation method of the chirp signal. The modulated chirp signal is multiplied by a windowdependent factor and then added to the ECG signal. In this paper, the confidential data of the patient is hiding inside the ECG signal, thus ensuring the confidentiality and privacy of patients using the Discrete Cosine Transform .However, the use of DWT increases the complexity there are several researches present on Steganography in the literature. All the methods in literature are with some drawbacks such as low capacity, security issues.

III.METHODOLOGY

The block diagram of the process is shown in Fig. 1.

The sender side Steganography basically consists of 3 stages.

1) Data Encryption

A novel encryption algorithm is developed on MATLAB. The flow of the algorithm is shown in the flow chart 1.

2) Decomposition

The ECG signal is compressed using Discrete Cosine Transform. Decomposition of a signal using this transform involves 4 critical steps, which are: dividing the signal into n subparts; DCT computation for each block; thresholding & Quantization of the DCT coefficients; and encoding of the quantized DCT coefficients. DCT is defined as:

$$X(n) = \left(\frac{1}{N}\right)^{1/2} \sum_{i=0}^{N-1} x(i) \cos\left[\frac{\Pi n}{2N}(2j+1)\right]$$

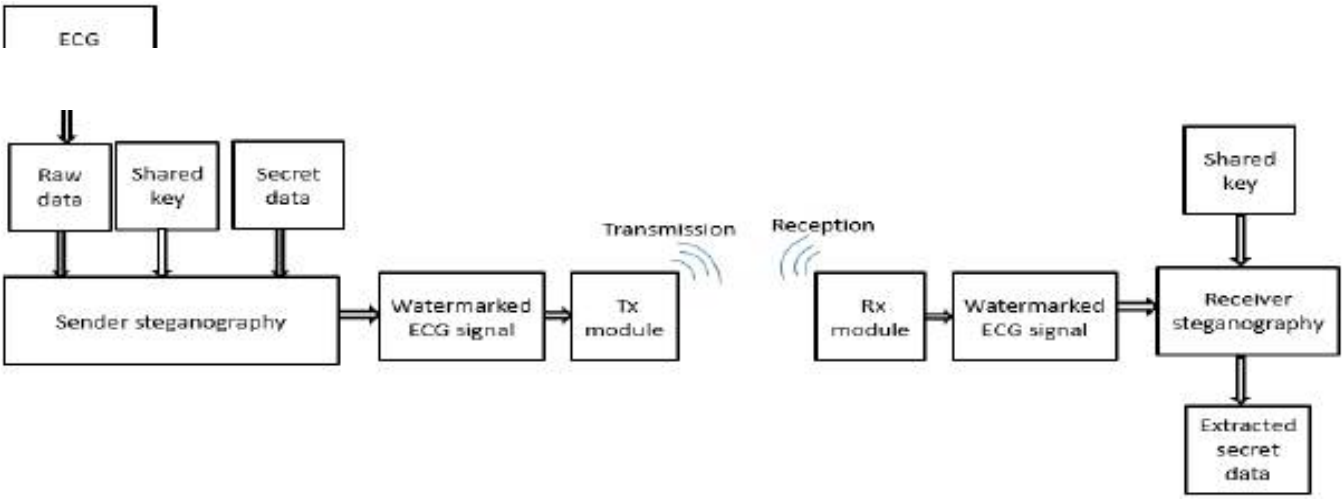


Fig 1: Block Diagram

We have used the MATLAB inbuilt function (Eq. 1) to perform the decomposition

y = dct(a)

$$y = dct(a,n) \quad (1)$$

Where, a=ECG Samples

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

n=the number of subparts

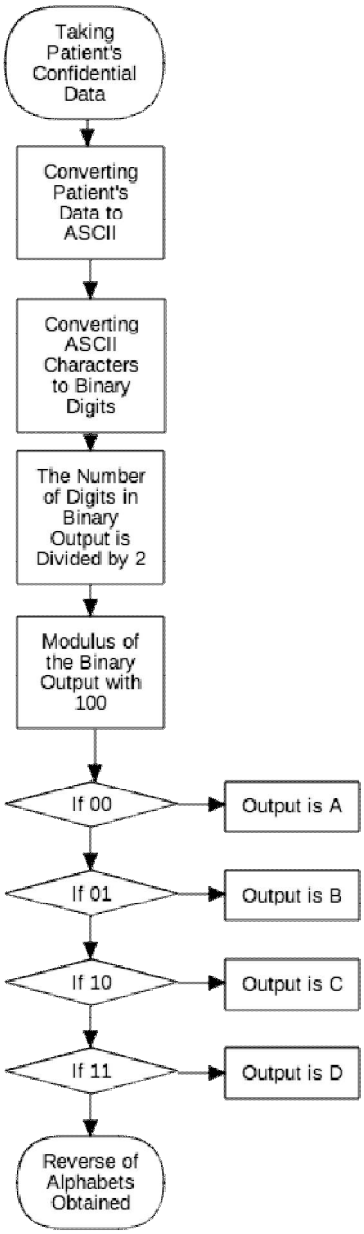
DCT is used for the compression as it gives the decomposed coefficient of the original signal and it gives more weight to low-pass coefficients than high-pass coefficients.

3) Data Embedding

Steganography basically involves hiding the essential data into a cover image and obtaining the Stego image at the receiver end. The Steganography equation is shown below (2) and the block diagram for data embedding is shown in Fig. 2

Stego-medium = Cover medium + Secret message + Stego key (2)

We have used the pure form of steganography where it is assumed that nobody but the sender and the receiver is aware of the communication taking place.



Flow Chart 1: Encryption Algorithm

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

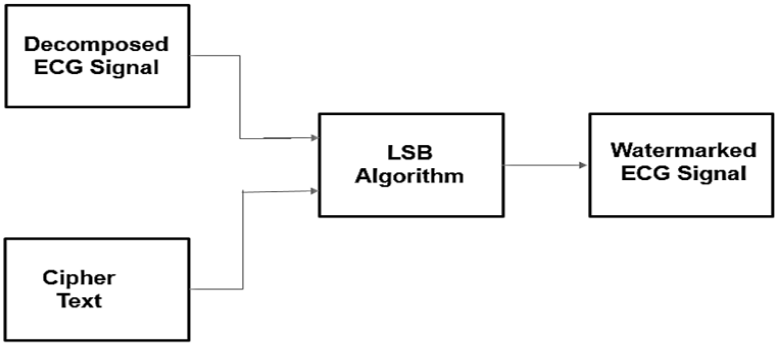


Fig 2: Block Diagram for Data Embedding

To accomplish the embedding operation, we have developed a GUI that would take the input from the user and complete the data embedding and retrieval process. The data embedding process is completed using the LSB algorithm. The brief idea of the algorithm is shown in Fig. 3.

The receiver side Steganography involves the exact opposite of what was done in the sender's side. The first step is to de-watermark the ECG and bring back to its original non-compressed state. The extracted data is now decrypted using the key that's been shared between the sender and the receiver and the original message which is, in this case, the patients' confidential information is obtained.

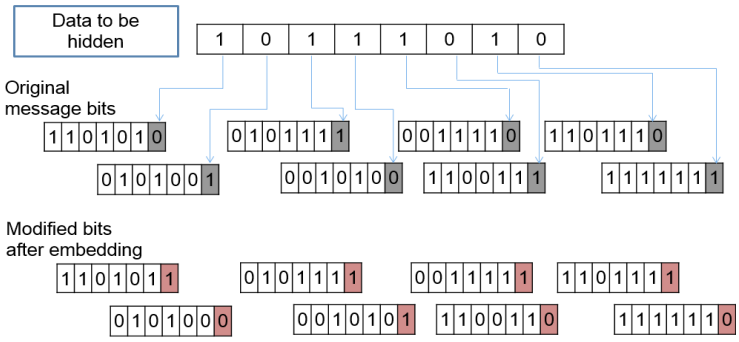


Fig. 3: LSB algorithm

IV. SIMULATION AND RESULTS

50 ECG samples from a database[13] was taken and fed onto MATLAB as input and the DCT of the samples is obtained as shown show in Fig. 4.

GUI developed for the steganography process is shown in the Fig. 5 on the left side and the GUI after the completion of steganography is shown in the Fig. 5 on the right side. The image obtained after the DCT decomposition is used for the process.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

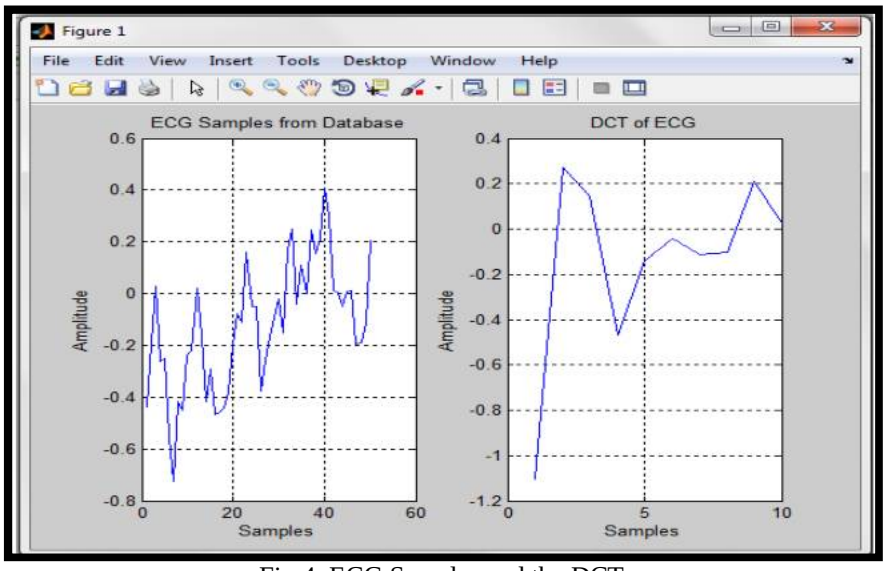


Fig 4: ECG Samples and the DCT

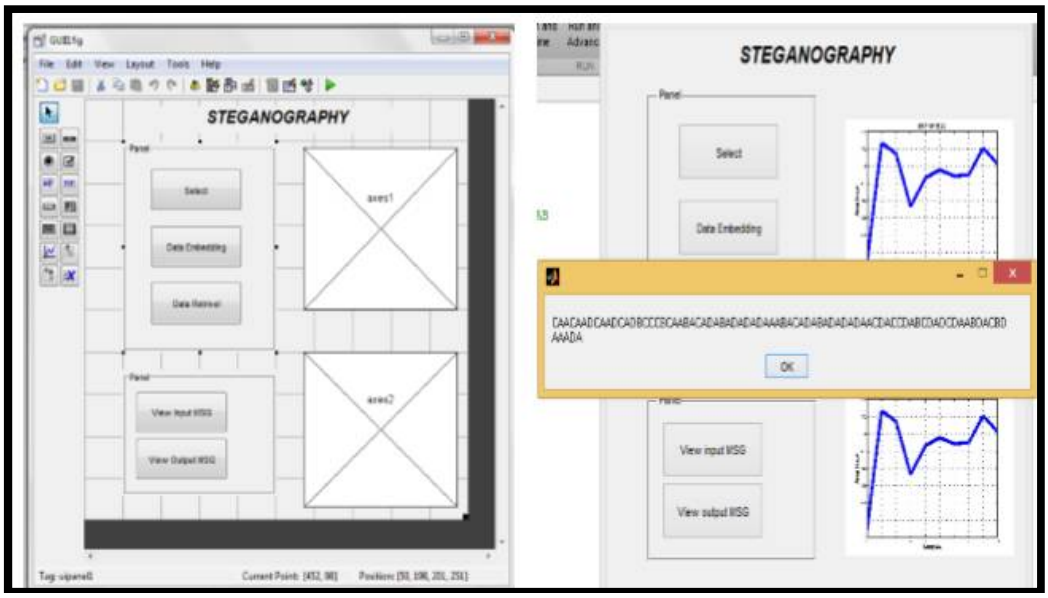


Fig 5: GUI (left) and GUI on Completion.

V.CONCLUSION

In this paper, a novel encryption algorithm is proposed that is used to encrypt the patient's confidential data that is embedded into the ECG signal. The technique provides an effective way to secure the information when transmitted over a public network. It is observed that the ECG remains undistorted after the watermarking process and remains diagnosable.

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] F. Hu, M. Jiang, M. Wagner, and D. Dong, "Privacy-preserving telecardiology sensor networks: Toward a low-cost portable wireless hardware/

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

software codesign," IEEE Trans. Inf. Technol. Biomed., vol. 11, no. 6, pp. 619–627, Nov. 2007.
[3] 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.
[4] A. Ibaida, I. Khalil, and F. Sufi, "Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA)," in Proc. 5th Int. Conf. Intell. Sens. Netw. Inf. Process., pp. 207–212, Dec. 2010.
[5] Wang H, Peng D, Wang W, Sharif H, Chen H, Khoynezhad A. Resource-aware secure ECG healthcare monitoringthrough body sensor networks. IEEE Wireless Comm.;17(1):12–9, 2010.
[6] K. Wu and C. Wang, "Steganography Using Reversible Texture Synthesis", vol. 24, no. 1, pp. 130 – 139, 2015.
[7] Kaur S, Singhal R, Farooq O, Ahuja B. Digital watermark- ing of ECG data for secure wireless Communication. IEEE International Conference on Recent Trends in Informa- tion, Telecommunication and Computing; p. 140–4, 2010.
[8] Ms. PawarKshetramalaDilip, Prof. V. B. Raskar Hiding Patient Confidential Information in ECG Signal Using DWT Technique International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015.
[9] K. Zheng and X. Qian"Reversible Data Hiding for Electrocardiogram Signal Based on Wavelet Transforms," in International Conference on Computational Intelligence and Security, 2008. CIS'08, vol. 1, 2008.
[10] Alauddin Al Omary ,Wael El Medany ,Riyad Al Hakim, "Heart Disease Monitoring System Using Web and Smartphone", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering (An ISO 3297: 2007 Certified Organization), Vol. 3, Issue 4 , pp. 23-43, Saudi Arabia, April 2014.
[11] Clifford G.D., Azuaje, F., McSharry P.E., "Characterisation of Noises affecting ECG", "Advanced Method s and Tools for ECG Analysis", Artech House Publishing, October 2006.
[12] SmitaKasar, Abbhilasha Mishra , Madhurijoshi, "Performance of digital filters for noise removal from ecg signals in time domain", 2014 international journal of innovative research in electrical, electronics, instrumentation and control engineering vol. 2, issue 4, april 2014.
[13] BIT Arrhythmia Database