International Journal of Humanities and Social Science Invention (IJHSSI)
ISSN (Online): 2319 – 7722, ISSN (Print): 2319 – 7714
www.ijhssi.org ||Volume 7 Issue 04 Ver. II ||April. 2018 || PP.54-62

An Audio Steganography Using DWT and Triple DES Technique

Chethan M.D, Anitha Devi M.D , Dr. M Z Kurian
PG Scholar,SriSiddharthaAcademyofHigherEducation Tumakuru,India
Assistant professor,SriSiddharthaAcademyofHigherEducation Tumakuru,India
HOD, Dept. of ECE, SSIT, Tumkur,India,572105
Corresponding Author: Chethan M.D

ABSTRACT—*Point of care testing (POCT) in patients withischemic heart disease is impelled by the time critical need for quick, specific and accurate results for initiation of therapy instantly. The driving force behind POCT using ECG signals is to provide test immediately and conveniently to cardiac patients. This will intensify the probability of patient, physician and care team receiving the results faster, which facilitate immediate clinical management decisions to be taken. In wireless communication the biomedical data may be susceptible to potential attacks leading to following security challenges.*

- *To safeguard the privacy and integrity of biomedical data.*
- *To make sure that only authorized people can have the access to secret information.*

This paper proposes a five level wavelet decomposition based steganography technique applied to ECG signals along with RSA encryption and scrambling matrix based encoding technique to protect confidential information related to patient hidden inside ECG signals. To assess the efficiency of the proposed algorithm on the patient ECG signal, the two distortion measurement metrics like percentage RMSE difference(PRD) and PSNR(peak signal to noise ratio) have been compared with existing algorithm results and energy of watermarked ECG signal is compared with original ECG for Coiflet , Bioorthogonal and symlet wavelets. It is found that the proposed algorithm provides very high security protection for information related to patient and as well as with very less distortion of ECG signal, so that it remains diagnosable even after retrieval of patient related secret information.. (Abstract)

KEYWORDS— *Steganography, POCT, ECG, PRD, PSNR, DES, Coiflet, Bioorthogonal, Symlet.*

Date of Submission: 24-03-2018 Date of acceptance: 08-04-2018

Professional time being optimally used. The communication of medical related information through signals requires both security as well as authentication. Hiding of secret information in these signals can cause distortion in these signals, which is not acceptable since these signals convey very important information required for diagnosis and any kind of distortion could result with erroneous diagnosis. Embedding the secret information related to patient in ECG signal could compromise with important information conveying diagnostic values of medical signals. Hence to develop a high secure medical steganography algorithm is a challenging task. Thus identifying the main security challenges fronting a sensor network for wireless health monitoring, main focus is on developing a steganography algorithm with enhanced security, privacy, authentication and integrity of data with less cost and energy efficient mechanisms.

Hiding techniques have been proposed and has gained huge importance. Reversible data hiding is one of the technique of data hiding, which is lossless i.e. we will be able retrieve the entire original cover information with very less distortion from the marked data after extraction of entire hidden data.

More recently, a significant amount of research is done to improve the effectiveness in data hiding has been conducted. These developed techniques typically intend to strengthen their effectiveness by increasing the amount of data being embedded while maintaining good quality of reconstruction for the host media.

In our proposed method, the following mechanisms are incorporated to provide a novel secured algorithm with minimum distortion for ECG signals used in wireless health monitoring systems, which includes

I. INTRODUCTION

POCT is well established worldwide and play a vital role in public health monitoring. It is one of the standards of care in disastrous situation. Major benefits of POCT include more quick decision making and triage, rapidly reducing operating times, with greater reduction in high dependency, post operative care time, reduction in emergency room time, reduce number of outpatient clinic visits and ensure medical

1. A five level discrete wavelet decomposition technique for data hiding in ECG signals.
2. Triple DES cryptographic algorithm and scrambling matrix based asymmetric encryption and decryption for protecting data confidentiality and integrity.

To weigh up the effectiveness of proposed algorithm on the ECG signal, various distortion measurement metrics like percentage mean square error difference (PRD) for differentscrambling matrix combination and the other evaluation metrics such as peak signal to noise ratio for various embedding capacity.

The organization of this paper is as follows. In section 2, we discuss the related research based on the data hiding approaches in medical related information. Section 3 deals with our novel proposed method. Section 4 then demonstrates the simulation results. Section 5 deals with the performance evaluation of proposed method for text data being secret information. Section 6 deals with the performance evaluation of proposed method for image data being secret information. conclusion and future scope are given in section 7.

II. RELATED WORK

In Literature, a lot of very good data hiding techniques are available by considering various aspects of data security and quality of cover information restored. Ever since the researchers have realized the importance of lossless data hiding techniques for medical and military applications with highly confidential cover content, they have put forward various lossless information hiding techniques related to lossless retrieval of both secret as well as cover data information. There are many approaches to secure patient sensitive information as well.

AymanIbaida and Ibrahim khadil[1] proposed a wavelet based steganography for ECG signals to hide patient information as well as diagnostic information inside ECG signals with XOR ciphering technique to encrypt the patient confidential information. The challenging task here was to retain originality of ECG signal data to remain diagnosable after retrieving patient secret information from ECG signal.

PawanKshetramaladilip and V.B.Raskar[2] have suggested an algorithm to hide patient data inside ECG signals using discrete wavelet transform . But encryption is carried through less secure XOR ciphering and is only tested for text information being the secret data.

Anusha T. Karthikkumar B, ThilakaK[3] have proposed an algorithm for secret data communication through ECG signals. The data hiding technique uses the LSB replacement algorithm for concealing secret message bits into high frequency coefficients. But algorithm is verified for single wavelet decomposition technique as well as single scrambling matrix combination and only text data being the secret information.

M.SabarimalaiManikandan and S. Dandapat[4] have put forward an objective distortion measure for compressed electrocardiogram signals, with less security being the major limitation , since even unauthorized person can view the medical records sent via network.

NilanjanDey , sayantan et.al[5] have proposed a watermarking technique within ECG for authentication , but fails to retain the originality of ECG signal due to strong security aspects. But major concern in point of care system is to retain the important information in ECG signal for it to be diagonasable.

Hamid.A.Jalad, A.A.Zaidan et.al [6] have discussed a new design for hiding information hiding (data file) within image page of Execution file(EXE file) to ensure that the changes made to the file will not be detected by hackers. But the hidingtechnique is applied for general information rather than medical data, where lossless retrieval of cover data information is not mandatory.

III. PROPOSED MODEL

The source side of proposed steganography algorithm consists of four unified stages

- Encryption of secret information
- Wavelet decomposition of host ECG signals
- Embedding and scrambling of secret data
- Inverse wavelet recomposition.

Assume that the host ECG signal is a one dimensional array of coefficients having 7200 samples sampled at a rate of 360Hz. The host ECG is first decomposed into 32 sub bands by applying 5 level wavelet packet decomposition as shown in fig(1). Then the text information is encrypted using RSA technique, finally the encrypted text is embed into the wavelet sub bands.

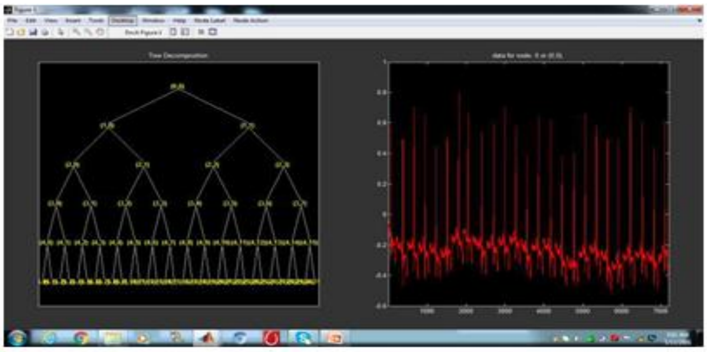


Fig 1: A Fivelevel Wavelet Decomposition of ECG Signal

1. Triple DES Algorithm

The main aim of this stage is to encrypt the patient confidential information in such a way that it prevents unauthorized persons who does not have the shared key from accessing patient confidential information.

- As a first step, we need to choose two large distinct prime numbers *p* and *q*.
- The product of p and q, we call *n* as a component of the “public key”. It must be big enough such that the numbers *p* and *q* cannot be extracted from it - 512 bits minimum i.e. numbers greater than 10. ^154.
- Later we generate the encryption key *e* which should be co-prime to the number *m* = *f* (*n*) = (*p -1*) (*q* -1).
- We will then create the decryption key *d* such that *demod m* = 1. Now we have both public and privatekeys.
- let *y* = *E*(*x*) be the encryption parameter where *x* is an integer and *y* is the encrypted form of *x*
  y = x. ^e mod n
- let *X* = *D*(*y*) be the decryption parameter where *y* is an encrypted integer and *X* is the decrypted form of y
  X = y. ^d mod n

2. Embedding Algorithm

After generation of cipher text by using Triple DES algorithm, we embed the encrypted secrete information in the sub bands obtained after decomposing the ECG signal.

- Convert the cipher text into stream of binary digits.
- The shared key known to both the sender and the receiver.
- Second is the scrambling matrix as shown in fig (2) which is stored at both the sender and the receiver side. Each sender/receiver pair has a same scrambling matrix.
- Scrambling matrix is of 128X32 dimension and the elements of matrix should lie between 1 and 32, with following conditions being met

1. Duplicate elements should not be present in the same row
2. The same row must not be duplicated.

- Apply the scaling operation on each coefficient in the sub bands.
- Access each coefficient from the sub band depending on the sub band number obtained from scrambling matrix .Embed the information bits into the LSB’s of sub band coefficients.
- The steganography level selected for bands from one to seventeen is 5 bits. Since more information is carried in these bits.
- The steganography level selected for rest of the bands is 6 bits
- Apply the inverse scaling operation on each stego coefficients in the sub bands.
- Apply the inverse wavelet recomposition on watermarked sub band to obtain the watermarked ECG Signal.

$$\begin{pmatrix} S_{1.1} & S_{1.2} \;\dots\dots\dots\dots & S_{1.32} \\ S_{2.1} & S_{2.2} \;\dots\dots\dots\dots & S_{2.32} \\ | & | & | \\ | & | & | \\ | & | & | \\ S_{128.1} & S_{128.2} \;\dots\dots\dots & S_{128.32} \end{pmatrix}$$

IV. SIMULATION RESULTS

Fig2: Scrambling matrix

$$\begin{pmatrix} S_{1.1} & S_{1.2} \;\dots\dots\dots\dots & S_{1.32} \\ S_{2.1} & S_{2.2} \;\dots\dots\dots\dots & S_{2.32} \\ | & | & | \\ | & | & | \\ | & | & | \\ S_{128.1} & S_{128.2} \;\dots\dots\dots & S_{128.32} \end{pmatrix}$$

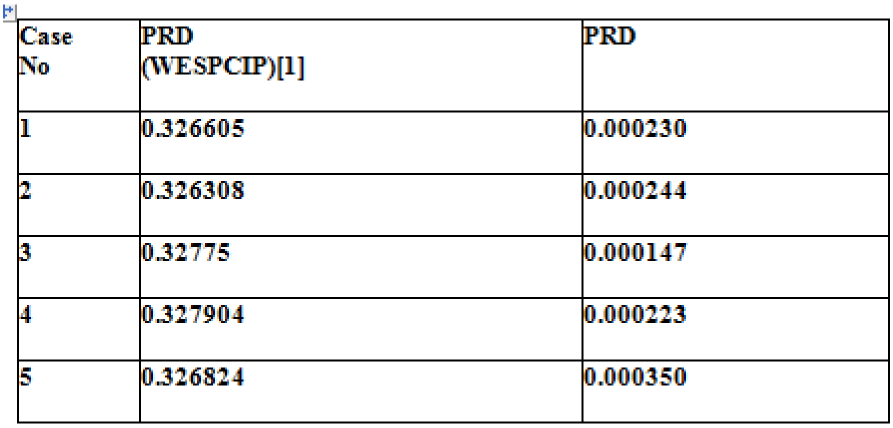
Extraction Algorithm:

- Apply wavelet decomposition on Stego ECG signal.
- Perform the scaling operation on each coefficient in the sub bands.

- Access each coefficient from the sub band depending on the sub band number obtained from scrambling matrix.
- Extract the information bits into the LSB's of sub band coefficients.
- Perform Triple DES decryption to obtain the original information.

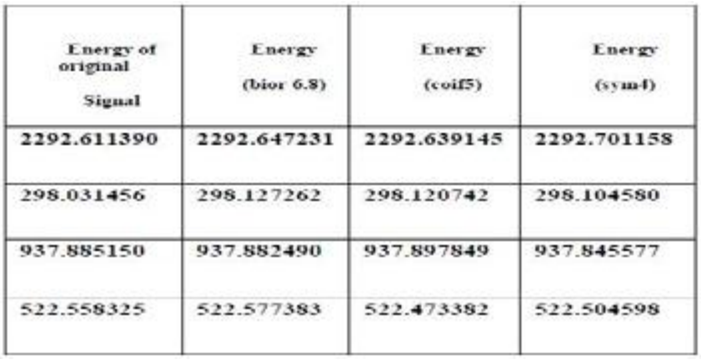
V. PERFORMANCE EVALUATION OF PROPOSED

METHOD WITH RESPECT TO TEXT DATA BEING
THE SECRET INFORMATION.



Case No	PRD (WESPCIP)[1]	PRD
1	0.326605	0.000230
2	0.326308	0.000244
3	0.32775	0.000147
4	0.327904	0.000223
5	0.326824	0.000350

TABLE1: PRD COMPARISON OF PROPOSED METHOD WITH EXISTINGTECHNIQUE



Energy of original Signal	Energy (bior 6.8)	Energy (coif5)	Energy (sym4)
2292.611390	2292.647231	2292.639145	2292.701158
298.031456	298.127262	298.120742	298.104580
937.885150	937.882490	937.897849	937.845577
522.558325	522.577383	522.473382	522.504598

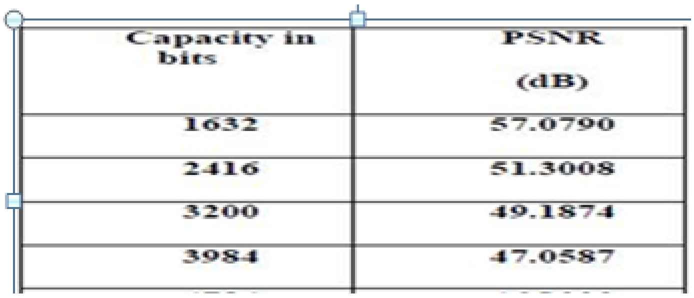
TABLE II: ENERGY COMPARISON OF ORIGINAL ECG SIGNAL

WITH WATERMARKED ECG SIGNAL FOR THREE DIFFERENT WAVELETS

In Table 1: The PRD in percentage for the proposed algorithm is tabulated for different combination of Scrambling matrix and is compared with existing technique(WESPCIP)[1]. Proposed algorithm is found to be more efficient resulting in less distortion, so that ECG signal remains diagnosable even after retrieval of secret information.

In Table 2: The energy of different ECG signals is compared with watermarked ECG signal(with text data being the hidden information) is compared by using Coiflet, Bioorthogonal and symlet wavelets. It is found from the tabulated results that Coiflet wavelet based decomposition method results with less distortion as compared with rest two.

In Table3: PSNR for various capacities of text data being the secret information is being tabulated. It shows that as the number of secret data bits increases , the variations in ECG signal also increases, which results in decrease in peak signal to noise ratio(PSNR).

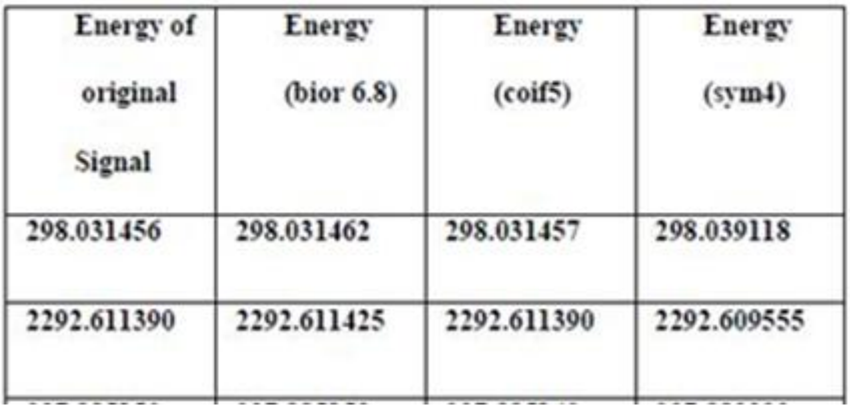


Capacity in bits	PSNR (dB)
1632	57.0790
2416	51.3008
3200	49.1874
3984	47.0587

TABLE III: CAPACITY IN BITS VERSUS PSNR

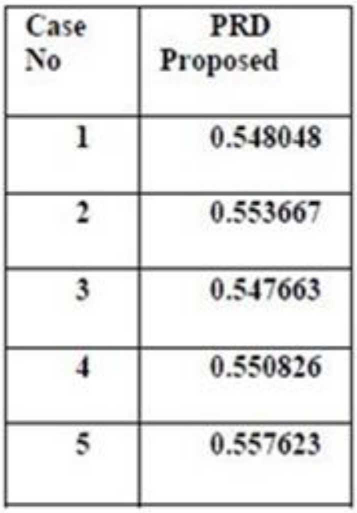
VI. PERFORMANCE EVALUATION OF PROPOSEDMETHOD WITH RESPECT TO IMAGE DATA

BEING THE SECRET INFORMATION.



Energy of original Signal	Energy (bior 6.8)	Energy (coif5)	Energy (sym4)
298.031456	298.031462	298.031457	298.039118
2292.611390	2292.611425	2292.611390	2292.609555

TABLE IV: ENERGY COMPARISON OF ORIGINAL ECG SIGNAL WITHWATERMARKED ECG SIGNAL WITH IMAGE DATA BEING SECRET INFORMATION FOR THREE DIFFERENT WAVELETS.



Case No	PRD Proposed
1	0.548048
2	0.553667
3	0.547663
4	0.550826
5	0.557623

TABLE V: PRD IN % FOR DIFFERENT COMBINATION OF SCRAMBLING MATRIX

VII. CONCLUSIONS

The proposed algorithm allows ECG signal of the cardiac patient to hide corresponding patient confidential data(both text and image) and other various physiological information, thus assuring the integration between ECG and the rest of the parameters. In order to evaluate the effectiveness of the proposed technique on the ECG signal, two distortion measurement metrics have been used: the percentage residual difference and the wavelet weighted PRD. It is found that the novel proposed technique provides high security protection for patient data with very less distortion and ECG data will remain diagnosable even after retrieving secret information from watermarked data.

REFERENCES

[1]. AymanIbaida and Ibrahim Khalil,” Wavelet based ECG steganographyfor protecting patient confidentialinformation in point of care systems,” IEEE Trans.Biomedical Engineering, vol. 60, no. 12, December 2013.

[2]. Ms. PawarKshetramalaDilip, Prof. V. B. Raskar “ Hiding Patient Confidential Information in ECG Signal Using DWT Technique”

[3]. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 4 Issue 2, February 2015

[4]. Anusha.T, Karthikkumar.B, Thilaka.K “DWT Based Secured Patient Monitoring System” International Journal of Engineering Trends and Technology (IJETT) – Vol 9 Number 14 - Mar 2014

[5]. M. SabarimalaiManikandan, Student Member, IEEE, and S. Dandapat,

[6]. Member, IEEE “Multiscale Entropy-Based Weighted DistortionMeasure for ECG Coding” IEEE SIGNAL PROCESSING LETTERS, VOL. 15, 2008 page no:829

[7]. NilanjanDey, SayantanMukhopadhyay, Achintya, and Sheli Sinha Chaudhari, “Analysis of P-QRS-T components modified by blind watermarking technique within the ECGsignal for authentication in wireless telecardiology using DWT”.International Journal of Image,Graphics, SignalProcessing, vol. 4, no 7, July 2012.

[8]. Hamid.A.Jalab,A.A.Zaidan,B.B.Zaidan” New Design fo InformationHidingwithinSteganographyUsingDistortionTechniques” IACSIT International Journal of Engineering andTechnology Vol.2, no.1, February ,2010, ISSN:1793-8236

[9]. L. Brechet, M. F. Lucas, C. Doncarli, and D. Farina, Compressionof biomedical signals with mother wavelet optimization and best-basiswavelet packet selection,” IEEE Trans. Biomed. Eng., vol. 54, no. 12,pp. 2186–2192, Dec. 2007.

[10]. Z. Lu, D. Y. Kim, and W. A. Pearlman, “Wavelet compression of ECG signals by the set partitioning in hierarchical trees method,”IEEE Trans. Biomed. Eng., vol. 47, no. 7, pp. 849–856, Jul. 2000.

[11]. H. wang, D. Peng, W. Wang, H. Sharif, H. chen, and .Khoynezhad, “Resource- aware secure ECG healthcare monitoring through body sensor networks,” IEEE WirelessCommun., vol. 17, no. 1, pp.12-19, Feb. 2010.

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

[13]. [11] K. Zheng and X. Qian, “Reversible Data Hiding for ElectrocardiogramSignal Based on Wavelet Transforms,” in International Conference onComputational Intelligence and Security, 2008. CIS’08, vol. 1, 2008.

[14]. [12] S. Kaur, R. Singhal, O. Farooq, and B. Ahuja, “Digital Watermarking ofECG Data for Secure Wireless Commuication,” in 2010 InternationalConference on Recent Trends in Information, Telecommunication and Computing. IEEE, 2010, pp. 140–144.

[15]. Y. Zigel , A. Cohen, and A. Katz, “The weighted diagnostic distortion(WDD) measure for ECG signal compression,” IEEE Trans. Biomed.Eng., vol. 47, no. 11, pp. 1422–1430, Nov. 2000.

[16]. Anitha Devi M.D,DrK.B.ShivaKumar “Protection of Confidential Color Image Information Based on Reversible Data Hiding Technique (PCCIRT)”International conference on computing and network communications(CoCoNet’15), Dec 16-19,2015.

[17]. 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.2006.

[18]. O. Rosso, S. Blanco, J. Yordanova, V. Kolev, A. Figliola, M.

[19]. Schurmann,and E. Basar, “Wavelet entropy: A new tool for analysis of Short duration brain electrical signals,” Neurosci. Meth., vol. 105, pp.65–75,2001.

Chethan M.D. "An Audio Steganography Using DWT and Triple DES Technique." International Journal of Humanities and Social Science Invention (IJHSSI) 7.04 (2018): 54-62.