RESEARCH ARTICLE OPEN ACCESS

AES Encrypted Wavelet Based ECG Steganography

Prof. Kshetramala Pawar[1], Prof. Dhanshri Naiknaware [2]
1(Department of E&TC, JSPM's ICOER, Pune)
2 (Department of E&TC, JSPM's ICOER, Pune)

Abstract:

The patient's confidential data should be safe and secure this is Act by Health Insurance Portability and Accountability Act (HIPAA). At the same time, there is a significantly growth in population. Numbers of patient care canters are used usually around the world in a Point - Of - care (PoC) applications. The Security systems are implemented to provide data integrity, privacy, and accessibility. Therefore, ECG signal of the patients and other physiological data of the patient's like body temperature, glucose level, blood pressure, position, etc., are collected by Body Sensor Networks (BSNs) at home. After that it will transmitted over network and then stored at hospital server. In this paper, it used the steganography method which is depending on discrete wavelet transform to accomplish HIPAA act. DWT technique is applied on the ECG signal to hide confidential information of the patient which provides privacy to confidential information. High degree privacy is provided to patient, also Stego ECG remains diagnosable. In this paper the steganography technique is used to provide the three tire securities to patient's data. Our system also ensures safety, scalability, and effectiveness.

Keywords — ECG, Wavelet, Steganography, Encryption, Watermarking.

I. INTRODUCTION

It is said by HIPAA regulations act that, there should be a security and safety is given to the patient's secret info, which is then sent through the public network. As the patient secrecy is significant so patient can control his/her private health info. If anyone can access or control the information like name, ID no., adders then he or she will not allowed to access that info without permission [6]. To hide patient's secret info and other patient's physiological info in ECG signal is the aim of the work. Provide secrecy, honesty and convenience to confidential info. Hiding the info decrease the chance of the information being detected. ECG signals are better size than medical image so it is use for steganography. ECG signal is used to hide the patient's data like name, age, blood pressure, temperature, glucose level etc., which are getting with Body Sensor Networks (BSNs) at patient's home and kept on hospital server.

To protect patient confidential info from destruction by using steganography method is our first objective. From the offered model, we then express novel steganography technique using ECG and present their respective algorithms, which are wild and scalable, but are also capable of providing high-quality and consistent performance. Information Security is to prevent the illegal access, misuse of data, content modification, or denial of access, facts (data), etc., the primary goal is to provide confidentiality, availability and integrity. The good security in reality is compiling of these solutions. The solid physical security is crucial to guard substantial assets like approach, records. Communication security (COMS) is crucial to guard info in transmit. Network security (NET) is vital to safe the local area network and Computer security (COMPS) is crucial to control access over others computer systems. Together, these concepts offer Information security (INFOS). Amongst these, an essential sub discipline of hiding info is steganography. Information beating is recent techniques have become essential in a number of applications. It is essential that communication must be safeguarded by encrypting the stealthy messages. Cryptography guards the content of the messages and steganography secreting the secret message. Usually means beating information in other information [1][2][3].

II. LITERATURE SERVEY

To provide safety to patient confidential info, there are no. of methods [1], [4], [5].

XuQian and Kai-meiZheng [8] proposed a technique for data beating which is reversible wavelet transform. Additionally, secret key is not used in this algorithm, so the safety is rest only on proposed algorithm. At last, as QRS complex is lacking in ECG this algorithm is not suitable in abnormal ECG signal. However this algorithm is dependent only on usual ECG signal were QRS complex is present.

H. Danyali and H. Golpira [9] proposed a new method in which medical images are used as host signal. So this technique is not suitable for ECG signal. Also, this algorithm has little capacity. Furthermore, the encrypted key is not used in its watermarking process.

Our method used ECG signal for data beating process. ECG signal is decayed using discrete wavelet transform technique. The patient's confidential info is embedded with share or encrypted key within decayed ECG signal. The key with the XOR ciphering process is used. The key is ASCII coded. First security is given here with a common key. Second security is given at embedding operation and last security is giving at inverse wavelet transform process by selecting steganography level vector. So here three tier safeties are given to the patient's secret or confidential information.

III. IMPLEMENTATION DETAILS

There are two parts of the work. First is the sender side ECG steganography and second is the receiver side ECG steganography. The sender side of the offered steganography procedure consists of four combined stages and receiver side as shown In Fig 1. The offered technique is designed to ensure protected information beating with minimal alteration of the host signal. Additionally, this technique holds an authentication stage to prevent unauthorized users from mining the hidden info.

A. Sender Steganography

This side steganography contains data encryption, then wavelet decomposition and stealthy data embedding. Firstly, secrete info are first encrypted and then embedded with scrambling matrix in to ECG signal. Level vector and scrambling matrix are main parts which are used in the process of embedding. Shared key is used for security purpose. stego ECG signal is send via network to hospital server. The block diagram of sender side ECG steganography is displayed in fig. 2.

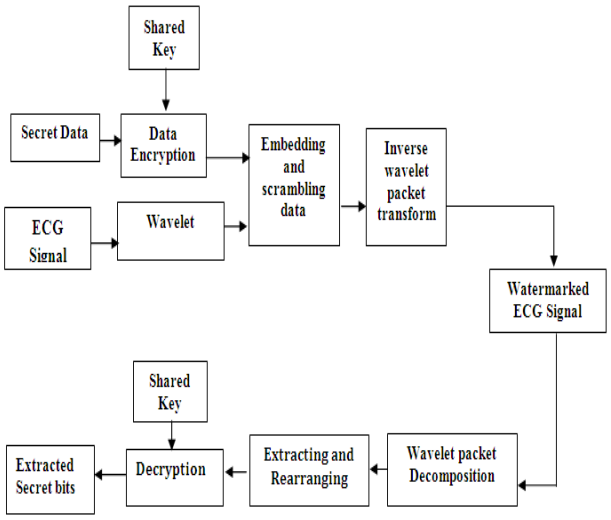

Fig.1 Block diagram of AES Encrypted ECG Steganography

B. Sender Steganography

This side steganography contains data encryption, then wavelet decomposition and stealthy data embedding. Firstly, secrete info are first encrypted and then embedded with scrambling matrix in to ECG signal. Level vector and scrambling matrix are main parts which are used in the process of embedding. Shared key is used for security purpose. stego ECG signal is send via network to hospital server. The block diagram of sender side ECG steganography is displayed in fig. 2.

1) Encryption

The process of converting plain text to an inexplicable format using a cipher is called encryption. Data Encryption is used to encode the confidential data to avoid any unauthorized access. Before embedding process, data Encryption is done to provide more security.

- ***AES***

XOR Ciphering technique is enormously common in these days. A simple XOR cypher can be easily cracked using frequency analysis. XOR worker is also vulnerable to a known plaintext outbreak. Another famous technique for data encryption is AES encryption. It is one of the most protected and normally utilized encryption algorithms accessible today. The AES algorithm defines a symmetric key algorithm, means the same key is used at both side for encrypting and data decrypting [7].

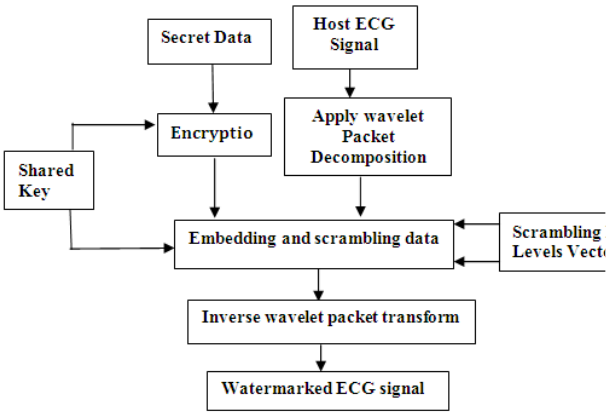

Fig. 2 Block diagram of the sender side ECG steganography.

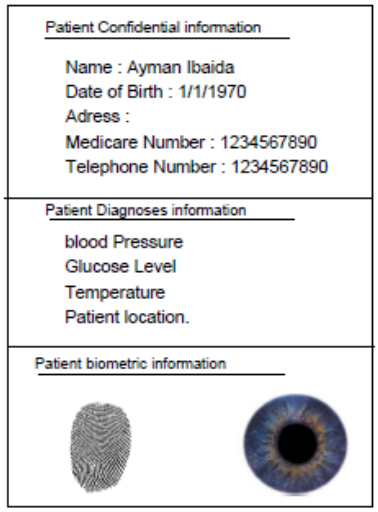

Fig.3 Original data containing of patient info

2) The Embedding Operation

In the offered technique will use a special security implementation to guarantee high data security. In this method a scrambling operation is performed using two parameters. First is, scrambling matrix and second is the shared key, were scrambling matrix is stored in both the transmitter side and the receiver side [1] and shared key is known to the sender side and the receiver side.

$$S=\begin{pmatrix} S_{1,1} & S_{1,2} & \cdots\cdots & S_{1,32} \\ S_{2,1} & S_{2,2} & \cdots\cdots & S_{2,32} \\ . & . & & . \\ . & . & & . \\ S_{128,1} & S_{128,2} & \cdots\cdots & S_{128,32} \end{pmatrix}$$

Were, S is a '128×32' scrambling matrix. S is a number between 1 and 32. While constructing the matrix we make assured that the following conditions are met:

• The same row must not hold duplicate elements

• Rows must not be copied.

C. Receiver Steganography

The receiver side work includes watermark decomposition process, extraction process & decryption process. The received watermarked ECG signal is then extracted with the help of shared key which is known to the authorized persons only.

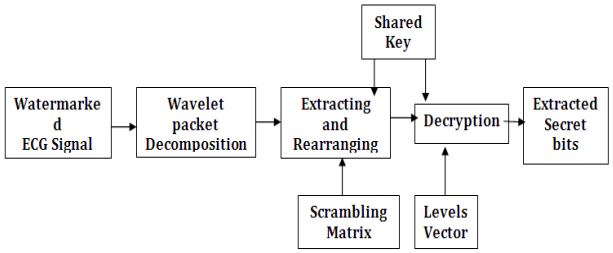

Fig. 4 Block diagram of the receiver side ECG steganography

A. ***Watermarked Extraction Process***

The following information is required to extract the secret bits from the received watermarked ECG signal at the receiver side.

1) The shared(common) key value
2) Scrambling matrix
3) Steganography levels vector

The stages of the mining process can be shown in Fig 4. The first step is decomposing received ECG signal by applying 5-level wavelet packet decomposition which generate the 32 sub-bands signals of that ECG signal. Next, using the scrambling matrix and shared key the extraction operation starts mining the secret bits in the correct order as per the order rows made from the scrambling matrix. Finally, the mined secret bits are decrypted by using the key which is used to encrypt data. The watermark mining process is nearly similar to the watermarking embedding process [1].

IV. RESULT AND DISCUSSION

A. *Diagnosability Measurement of Watermarked ECG Signal*

In this paper, the work done by Amjed S. Al-Fahoum [1] has been implemented. In this model a 5 level wavelet decomposition is applied to the original and watermarked ECG signal. As a result, the original signal will be divided into number of sub-bands denoted by A5, D5, D4, D3, D2 and D1. It is found that band A 5 includes most of the T-wave contribution and some of the P-wave contribution. Therefore, its weight should include the significance of P and T. Moreover, band D5 includes most of the P-wave contribution, part of the T-wave contribution, and a relatively low percentage of the QRS-complex contribution. The weight of D5 should maintain the highest weight contribution of P, T, and QRS. Band D4 also contains most of the QRS-complex contribution, and a little portion of P-wave.

The weight of D4 is higher than A5 but lower than D5. D3 includes some portions of the QRS-complex, and so its weight is lower than QRS weight itself. Bands D2, and D1 are weighted less than any other band as they do not contribute to the spectrum of any of the main features. However, they cannot be excluded where late potentials and delta waves may exist. The researchers used a heuristics weights to mark the contribution of each sub-band.

- Percent Residual Difference (PRD):

After applying 5 level wavelet decomposition a PRD measure of each sub-band is calculated. as shown in Eq. 1

$$\text{WPRDj} = \frac{\sqrt{\sum_{i=1}^{N}(x(n)-x'(n))}}{\sqrt{\sum_{i=1}^{N}(x(n)^2)}} \quad (1)$$

Where,

x(n) is the original coefficient within sub-band j

x'(n) is the coefficient of sub-band j for the stego signal.

Finally, to find the Weighted Wavelet PRD bellow Eq. 2 is used.

$$\text{WWPRD} = \sum_{j=0}^{NL} wj \; WPRDj \quad (2)$$

Where NL is the total number of sub-bands, wj denotes the weight value corresponding to sub-band j and WPRDj represents the calculated wavelet based PRD for sub-band j. The WWPRD measure provides structured error estimation criterion that will focus on diagnostic quality for reconstructed signals rather than random behaviour of error which will be distributed equally between all the samples of the compressed signal. The proposed measure will provide more meaningful results than the PRD measure, since errors due to ECG waves and complexes are weighted differently than isoelectric regions that will not add important information to the reconstructed signal.

- Root Mean Square Error(RMS):

There are some other error measures is literature for comparing original and reconstructed ECG signals, such as the root mean square error (rms):

$$RMS = \sqrt{\frac{\sum_{n=1}^{N}\left(x(n)-x'(n)\right)^2}{N}}$$

- Signal to Noise Ratio(SNR):

Another distortion measure is the signal to noise ratio, which is expressed as

$$SNR = 10log_{10}\left(\frac{\sum_{n=1}^{N}(x(n)-x')^2}{\sum_{n=1}^{N}(x(n)-x'(n))^2}\right)$$

The relation between the SNR and the PRD (2) is SNR = 40 − 20 log10 (PRD) dB or PRD = 10(−SNR20) × 100.

- Peak Signal to Noise Ratio (PSNR) :

It measures the quality of a watermarked signal.

$$PSNR = \frac{MNmax\ \ x(n)^2}{\sum_{n=1}^{N}(x(n)-x'(n))^2}$$

Where, M and N are number of rows and columns in the input signal.

In the implementation, the patient's confidential data such as his/her name, age, gender are encrypted with share key and transmitted along with the ECG signal as cover or host medium to hide the above specified data. Specifically, this scheme hides patient personal data and physiological data in the ECG

B. ***AES Encryption***

The shared key is used to encrypt patient's confidential information such as his/her name, age, gender, glucose level, blood pressure are encrypted. Here, AES encryption is used. In that the confidential information is encrypted with key. Same key is used at receiver side. This encryption technique provides high level security to patient confidential data. In this stage first level security is applied to data.

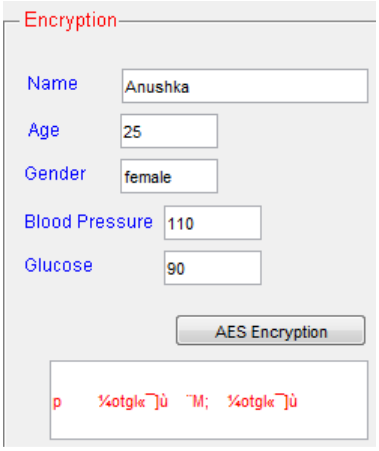

Fig.5 AES Encryption

C. ***Decomposition of ECG signal***

The host ECG lead 1 & lead 2 signals are decomposed in to two part using Haar wavelet transform, Approximation & detailed signal. Were approximation signals are low frequency signals & detailed signals are high frequency signals. ECG signals are related with low frequency signals. After decomposing the ECG signal, the encrypted information is embedded in to decomposed ECG signal.

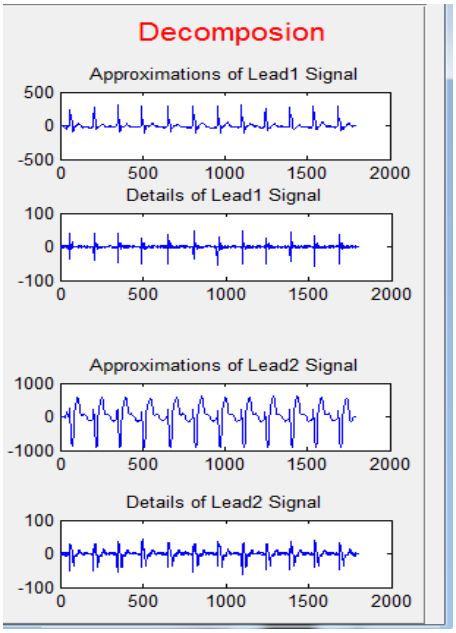

Fig.6 ECG Decomposition

D. ***Stego ECG Signal***

After embedding the inverse haar wavelet is applied to the decomposed signal to get stego ECG signal. Then that stego signal is transmitted over internet to the hospital server for the further operation. Fig. 7 shows the watermarked ECG signal which contains confidential information which is invisible and original ECG signal.

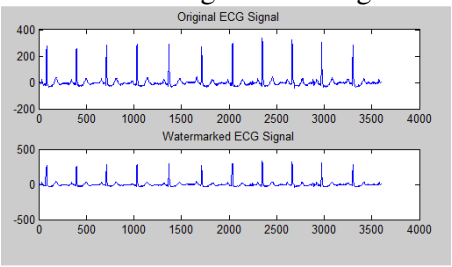

Fig.7 Original and watermarked ECG signal.

E. ***Descrambling Operation***

In the descrambling operation, the confidential information is extracted from stego ECG signal at receiver side. The same security key is used at the receiver side. That key is only known to the authorized doctors. Fig. 8 shows the extracted information.

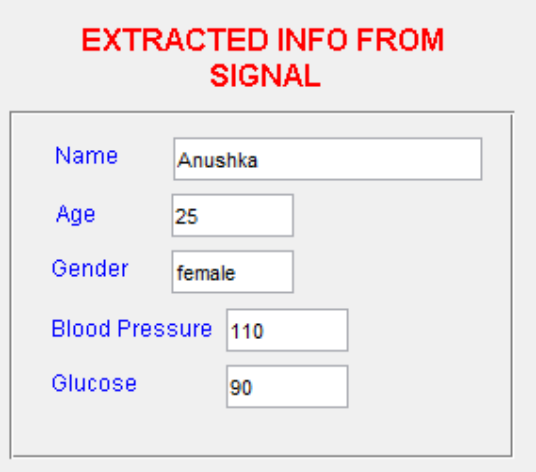

Fig. 8 Extracted Information

F. ***Performance Analysis***

The performance of the proposed technique is measure by using term PSNR, MSE, WPRD and WWPRD. I have taken 10 ECG samples for the performance measure. PSNR value shows the peak signal to noise ratio of original signal and stego signal. WPRD values are wavelet precent residual difference between original signal and stego signal. WWPRD is the weighted wavelet precent residual difference between original and stego ECG signal. From this analysis we can say that the stego ECG signal is approximately same as original ECG signal. Means there is less difference in stego and original ECG signal which is undiscoverable by normal human eye. Table 1 shows the results of performance of the system by using performance measure parameters WPRD, WWPRD, MSE and PSNR values for 10 normal ECG samples.

Table 1 Result for Different Normal ECG Samples.

Sample No.	WPRD	WWPRD	MSE	PSNR (dB)
1	0.1708	0.1531	0.0351	62.351
2	0.1705	0.1535	0.0388	62.521
3	0.1754	0.1578	0.0317	62.012
4	0.1844	0.1660	0.0412	63.124
5	0.1728	0.1555	0.0256	61.857
6	0.1617	0.1455	0.0352	62.352
7	0.1665	0.1499	0.0356	62.353
8	0.1623	0.1464	0.0333	62.125
9	0.1687	0.1519	0.0276	61.958
10	0.1696	0.1565	0.0290	63.121

V. CONCLUSION

In this proposed work, the secrete or confidential data of the patient is hiding inside patient's ECG signal and thus guarantees the patient's confidentiality and privacy using Discrete Wavelet Transform. The proposed algorithm provides secrecy, integrity, and accessibility to confidential information. Three tier of security is providing.

ACKNOWLEDGMENT

I have great pleasure in presenting the paper "AES Encrypted Wavelet Based ECG Steganography". Completing a task is not ever a one-man effort. It is frequently a result of invaluable involvement of a number of individuals in direct or indirect way. I would like to thank Head of Department, Dr. S. L. Lahudkar and Principal,

Dr. D. D. Shah for their support which helped me to achieve the needful.

Finally I wish to thank my friends, colleagues for their constructive comments, suggestions and criticism and all those who have directly or indirectly helped me in carrying out this dissertation work.

REFERENCES

1. *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.*

2. *W. Lee and C. Lee, "A cryptographic key management solution for hipaa privacy/security regulations," IEEE Transactions on Information Technology in Biomedicine,, vol. 12, no. 1, pp. 34–41, 2008.*

3. *Masoud Nosrati, Ronak Karimi and Mehdi Hariri, "An introduction to steganography methods," World Applied Programming, Vol (1), No (3), August 2011. 1999.*

4. *Gordan,Cornelia,ReizRomulus,"ECG Signal processing using wavelets",Unknown*

5. *Daniel Novak, "Processing of ECG signal using Wavelets", THESIS • MAY 2000.*

6. *Ms. Pawar Kshetramala Dilip, 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.*

7. *https://en.wikipedia.org/wiki/Advanced_Encryption_Standard*

8. *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.*

9. *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.*

10. *W. Lee and C. Lee, "A cryptographic key management solution for hipaa privacy/security regulations," IEEE Transactions on Information Technology in Biomedicine,, vol. 12, no. 1, pp. 34–41, 2008.*

11. *H. Wang, D. Peng, W. Wang, H. Sharif, H. Chen, and A. Khoynezhad, "Resource-aware secure ecg healthcare monitoring through body sensor networks," Wireless Communications, IEEE, vol. 17, no. 1, pp. 12–19, 2010.*

12. *Zhicheng Ni, Yun-Qing Shi, Nirwan Ansari, and Wei Su, "Reversible Data Hiding," IEEE Transactions On Circuits And Systems For Video Technology, Vol. 16, No. 3, March 2006.*

13. *Nilanjan Dey, Sayantan Mukhopadhyay, Sheli Sinha Chaudhuri and Achintya Das, "Analysis of P-QRS-T Components Modified by Blind Watermarking Technique Within the Electrocardiogram Signal for Authentication in Wireless Telecardiology Using DWT," I.J. Image, Graphics and Signal Processing, 2012, 7, 33-46 Published Online July 2012 in MECS.*