Steganography of ECG Signals for Hiding of Patient Confidential Data

Nidhi[#1], Dr. Arpinder Singh[*2]

[#]*M.tech Scholar, BCET, Gurdaspur*
**Associate Prof., ECE Department, BCET, Gurdaspur*

Abstract— *Personal Health Record (PHR) refers to the internet-based portals or computer-based applications that records patient confidential information in electronic version. The patient's privacy and security is important in the protection of healthcare privacy. The patients confidential information sent through the public network should be protected and secure. Patient can control who will use his/her confidential health information, such as name, address, telephone number, and Medicare number and who can access data. Monitoring patients at their home can reduce the increasing traffic at hospitals and medical centres. In this paper issues involving digital steganography and its applications in ECG have been discussed. We reviewed the literature on PHRs including design, functionality, implementation, applications, outcomes, and benefits. We implemented the Wavelet based ECG watermarking for Protecting Patient Confidential Information in Point-of-Care Systems.*

Keywords *— PHRs, ECG, Steganography, DWT.*

I. INTRODUCTION

The growth of internet has investigated means of new scientific, entertainment and business opportunities. One of the biggest technological events of the last two decades was the invasion of digital media in everyday life aspects. Digital information/data can be stored efficiently, effectively and with a very high quality however it can be manipulated very easily using softwares. Digital multi-media files offer several advantages over analog multi-media. The quality of digital images, audio and video signals are higher and are easily edited because one can access the exact discrete locations that need to be changed. Copying is simple with no loss of fidelity hence copy of a digital media is identical to the original [1].

The distribution of digital multi-media over internet require authentication due to the possibility of unlimited copying. The easy manipulation of digital information/data constitutes a real threat for information creators. The creator of multi-media files wants to be sure that their work is not used in an improper way (e. g. modified without their permission). For digital data, copyright enforcement and content verification are very difficult tasks. One solution would be to restrict access to the data using some encryption techniques. However, encryption does not provide overall protection. Once the encrypted data are decrypted, they can be freely distributed or manipulated [2].

II. WHY ECG STEGANOGRAPHY

In rural or remote places, people always cannot reach medical health centres as it takes long time to reach. Accordingly, to reduce the medical labour cost, the use of remote healthcare monitoring systems and Point-of-Care (Pock) technologies have become popular. Monitoring patients at their home can drastically reduce the increasing traffic at hospitals and medical centers [3].

The people in rural area may get treatment from doctors transmitting physiological readings of patients to the hospital server or medical practitioners and hence provide treatments accordingly. This exchange involves large amount of patient information such as bio-signals and medical images. It is therefore important that patient confidentiality is protected while data is being transmitted over the public network as well as when they are stored in hospital servers. Hiding the confidential data is termed as steganography. Patient can control his/her confidential information that if anyone can access or control the information like name, age, gender, ID no., address, telephone number. Hiding patient's confidential information and other physiological data in ECG signal is the main goal. Medical images have smaller size whereas the ECG signal has greater size and hence widely used in steganography process [4-5].

The ECG signal of the patients is used to hide information of patient such as temperature, glucose level, blood pressure, location etc., which are collected by using sensors. It is stored on hospital server by transmitted it via public network. The information is then diagnosed by monitoring systems at hospital with the patient privacy is protected against intruders.

III. WAVELET STEGANOGRAPHY

The implemented system provides open access for patient's biomedical ECG signal and prevents unauthorized access to patient confidential

information like temperature, blood pressure, sugar ect. Now the steganography technique will be applied and patient secret information and physiological readings will be embedded inside the ECG host signal [6-7].

The stego ECG signal is sent to the hospital server through the Internet. The quality and size of the stego ECG signal is same as that of original ECG signal, without adding any overhead. The stego ECG signal along with secret hidden information will be stored at hospital server. Any doctor can monitor the stego ECG but only authorized doctors and administrative staff can extract the confidential patient information stored in the stego ECG signal.

The transmitter/sender side of the implemented ECG steganography consists of four stages. The developed model is designed to ensure security of data as well as minimal distortion of the host ECG signal [8-9]. The system uses an authentication stage to prevent the extracting the confidential information.

The four stages of developed system are:

A. Encryption

The developed model encrypts the patient confidential information to prevent the extraction of patient confidential data by unauthorized users who does not have the shared key. For encryption, XOR ciphering technique is used with a shared key. XOR ciphering is selected because of its simplicity.

B. Wavelet Decomposition

Wavelet transform decompose the given signal into coefficients representing frequency components of the signal at a given time. It is a effective and powerful tool to combine time domain with frequency domain in one transform. Discrete wavelet transform (DWT) must be used instead of continuous wavelet transform because in most applications, discrete signals are used.

DWT decomposition can be performed by applying wavelet transform to the signal using band filters. The result of the band filtering operation will be two different signals; one will be related to the high-frequency components and the other related to the low-frequency components of the original signal. If this process is repeated multiple times, then it is called multilevel packet wavelet decomposition.

C. Inverse Wavelet Re-composition

The resultant steganography sub-bands are recomposed using inverse wavelet transform. The result of this operation is the new stego 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 stego ECG signal will be very similar to the original ECG signal.

D. Watermark Extraction Process

To extract the secret bits from the stego ECG signal, the receiver requires the secret key without which the user is not able to retrieve the patient confidential information. The steps of watermark extraction process is the reverse of the embed process.

IV. Results & Discussion

The wavelet based ECG steganography model is developed and implemented in MATLAB. Various ECG signals are used for the experimentation and we evaluated quality measures performance of the developed model. We measure the quality of watermarked images in terms of PSNR (Peak Signal to Noise Ratio) and MSE (Mean Square Error). In ideal case PSNR should be infinite and MSE should be zero. Large value of PSNR and small MSE is desirable to ensure that watermarked image is same as that of original ECG image. The quality measures are calculated using following equations.

$$\mathrm{MS} = \frac{\sum_{\mathrm{M,N}}\left(\mathrm{T(r,c)} - \mathrm{T'(r,c)}\right)^2}{\mathrm{M} * \mathrm{N}}$$

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{\mathrm{R}^2}{\mathrm{MSE}}\right]$$

Where T (r, c) is the original image and *T '(r, c)* is the resultant watermark-image, *r* and *c* are the number of rows and columns in the input images, respectively. *R* is the maximum fluctuation in input image data type or is the maximum intensity value of image. Similarly PRD measure of each sub-band is calculated as

$$WPRD_j = \sqrt{\frac{\sum_{i=1}^{N}(c_i - \tilde{c}_i)^2}{\sum_{i=1}^{N}(c_i^2)}}$$

where c_i is the original coefficient within sub-band j and $\tilde{c}_i$ is the coefficient of sub-band j for the watermarked signal.

We generate text file **msg.*txt*** which contains the patient confidential information to be embedded in ECG images.
The file contain general information of patient like address, phone number, file number, name as well as disease related reports as shown in figure 1.

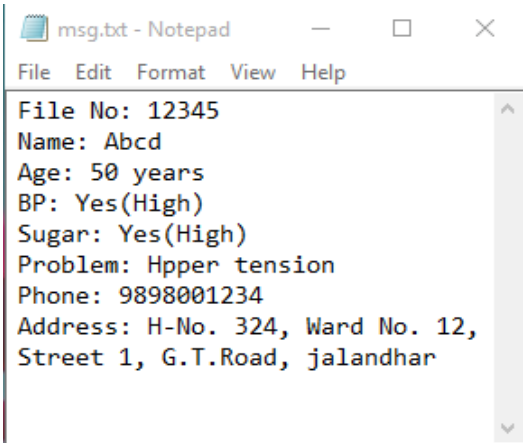

Figure 1: Message text file having patient data

Figure 2 shows the sample of Normal original ECG image whereas figure 3 shows the wavelet based ECG stego image.

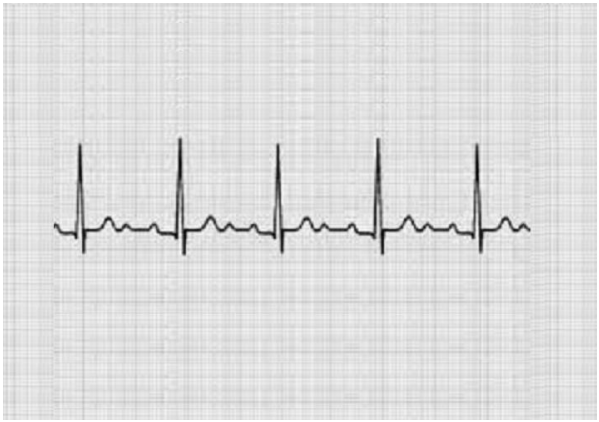

Figure 2: Original ECG image

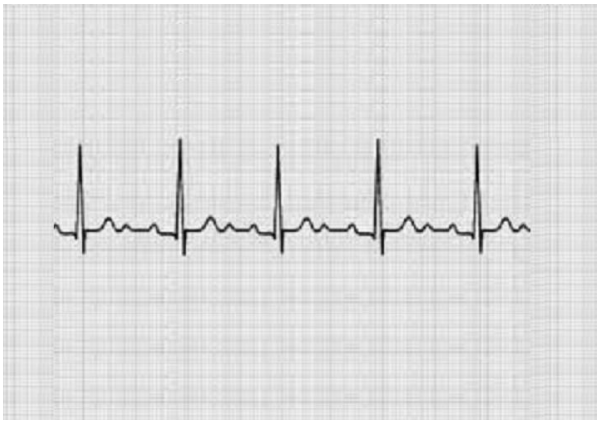

Figure 3: Stego ECG image

The stego ECG image and original ECG image seems to be same however the image contains patient information. Figure 4 and figure 5 shows the histogram of original ECG and Stego ECG image.

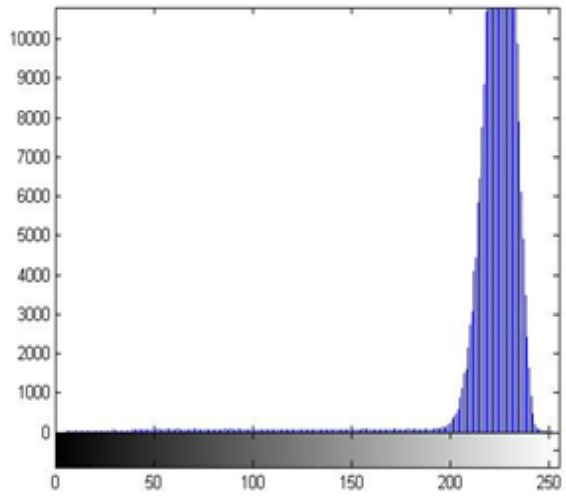

Figure 4: Histogram of Original ECG image

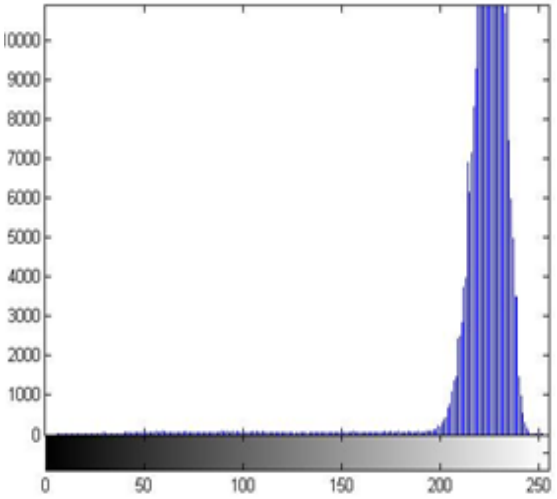

Figure 5: Histogram of Stego ECG image

The figure shown above reveals that the original ECG image is same as that of wavelet based ECG stego image. We take various ECG images and verify the performance in terms of PSD, PSNR and MSE

Table 1 shows the performance results of three ECG images.

Table 1 Various Quality Measures of ECG images

ECG Image	%PSD	PSNR	MSE
1	0.0216	73.5376	0.0029
2	0.0316	70.3573	0.0060
3	0.0278	71.3506	0.0048

V. CONCLUSION

In this paper a wavelet based steganography algorithm is implemented to hide patient confidential information inside ECG signal. This technique will provide a secured communication and confidentiality. A user-defined key is used to encrypt the message for more security to patient confidential information. We tested the diagnoses quality distortion and found that the resultant stego ECG can be used for diagnoses and the hidden data can be totally extracted.

REFERENCES

[1] Win KT, Susilo W, Mu Y. Personal health record systems and their security protection. Jounal of Medical System 2006; vol: 3, pp:309–315.

[2] I. Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Hadjiefthymiades, "Enabling location privacy and medical data encryption in patient telemonitoring systems," IEEE Transactions on Information *Technology in Biomedicine,*, vol. 13, no. 6, pp. 946–954, 2009.

[3] Bliemel M and Hassanein K., "Consumer satisfaction with online health information retrieval: a model and empirical study", e-Service Journal, 2007, vol. 5, pp:53–83.

[4] 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.

[5] 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.

[6] M. Li, S. Yu, Y. Zheng, K. Ren, and W. 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.

[7] Anusha.T, Karthik kumar.B, Thilaka. K, "DWT Based Secured Patient Monitoring System", International Journal of Engineering Trends and Technology (IJETT) – Volume 9 Number 14 - Mar 2014, Page 717.

[8] V.Sankari and K. Nandhini, "Sharing of Patient confidential data using ECG steganography", International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013 pp:2132.

[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.