Protect Patient Confidential Information with ECG Steganography using Wavelet Transform

Neha[1], Mohit Trehan[2]
[1]*M. tech Scholar, GCET, Gurdaspur*
[2]*AP, CSE Department, GCET, Gurdaspur*

Abstract **- Personal Health Record (PHR) is a primary field of health information transmission which allows persons to access and supervise their constant health records. However, if the data of Patient's Personal Health is to be send over network, then there is misnomer of privacy that it easy to modify and misuse the PHR through hacking. The patient's privacy and safety are important in the security of healthcare privacy. ECG Steganography is one of the proposed ways to secure PHR from illegal persons. This paper investigates the study on PHRs covering design, execution, relevance, and benefits. we developed an ECG Steganography system based on Wavelet Transform.**

Index Terms **- PHRs, Steganography, ECG, BSN.**

I.INTRODUCTION

Personal Health Record (PHR) is the network-based system or multimedia applications which records patient private data in electronic form. The accessibility of health information on internet has educated patients about the symptoms, diagnostic tests, diseases, and treatment options [1, 2]. Many individuals today maintain medical records for themselves and their families. However, patient's private data transmit over the unrestricted public network should be secured and shielded. Meanwhile patient can manage who will exploit his/her private medical data, such as name, address, and telephone number. Observing patients at their native place/home may lessen the growing traffic at hospitals and medical care units. The prime purpose is to offer privacy, integrity, and accessibility. However, numerous trials of these PHRs systems have proven that they increment and improve patient and family access to knowledge for self-management of health and wellness issues [3]. Thus, these systems were defined as electronic or paper-based gathering of health or medical information occurring from several sources about a person's health, which are managed, controlled, or shared by that individual or designate. However, prime care physicians have a chief role in advising and supporting patients in education and health self-management [4]. It has the potential to change and possibly to improve patient–provider relationships, enhance patient–physician shared decision making, and enable the healthcare system to evolve toward a more personalized medical model [5]. The chief role aim of steganography is to hide patient's private information and other physiological data in ECG images. These pictures is utilized because the size of ECG is large compared to other medical images. Patients ECG and other physiological data like temperature, blood pressure, glucose reading, position, etc., gathered at their native place/home through Body Sensor Networks (BSNs) will be conveyed and diagnosed by remote patient monitoring systems. Meanwhile, the patient privacy is protected against intruders while data traverse in open network and stored in hospital servers. The aim is to show that both the Host ECG and stego ECG signals can be used for diagnoses and the difference would be undetectable.

II.PHR FUNCTIONALITY & PURPOSE

PHR functionalities can be classified as [6, 7]:

1. Information collection,
2. Information sharing and exchange, and
3. Information self-management.

Functionalities include sending and receiving electronic messages to and from doctors' offices; completing prescription renewal forms, appointments, and referral authorizations; viewing lists of current medications and allergies; and accessing health and practice information. Decision support can also assist patients in managing chronic illnesses, based on

monitoring data. The nature of the patient's illness affects preference for functionalities.

The purposes of PHR are outlines as

- Easy Communication to patient
- Education and lifestyle change
- Health self-management
- Adoption, acceptance, and usability
- Acceptance and satisfaction

III.STEGANOGRAPHY CONCEPT

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 [8].

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 [9, 10].

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.

IV.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 [11, 12]. 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 [13]. 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 are the reverse of the embed process.

V. RESULT & DISCUSSION

In this paper, we implement wavelet-based ECG steganography system for protecting patient private information over the network. Different types of ECG signals are utilized for the experimentation. We evaluate the performance of the developed wavelet-based ECG steganography system and calculate various quality measures. The quality of stego ECG images is measured in terms of PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), Correlation and Percentage Residual Difference (PRD). The various quality measures used in this paper is calculated using following equations.

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

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

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. The embedded text message of the implemented wavelet-based ECG watermarking is shown in figure 1.

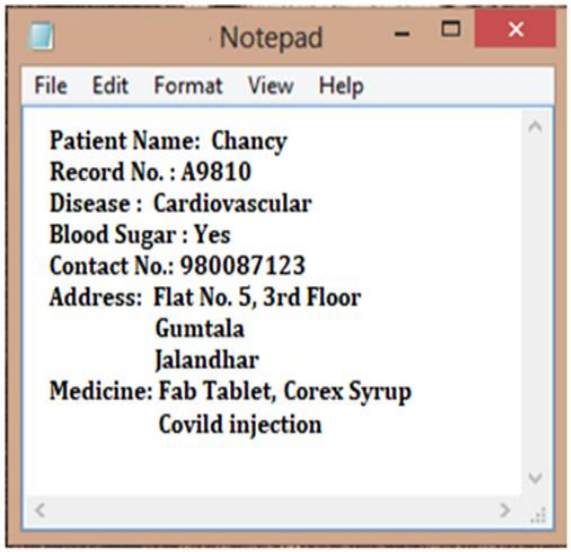

Figure 1: Patient Confidential information

The health record may include basic information of patient such as address, phone number, record number, name as well as disease related reports. Figure 2 shows the sample of Normal original ECG image. We take five normal ECG images of person and verify the average performance of implemented system in terms of PSD, PSNR, MSE, Normalized Cross correlation and Average Difference.

Figure 3 shows the wavelet ECG stego image which is an ECG image with patient confidential information. The wavelet based ECG stego picture shown in figure 3 seems to be same as that of original ECG picture however the picture holds patient information. The implemented ECG stego system hides the patient information efficiently and at the same time preserves the image quality of sample ECG images.

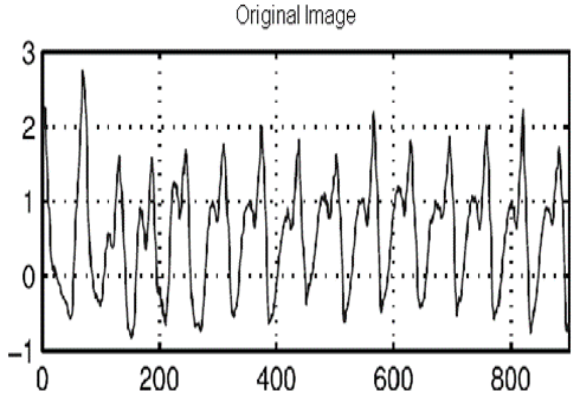

Figure 2: Original Ventricular fibrillation ECG Image

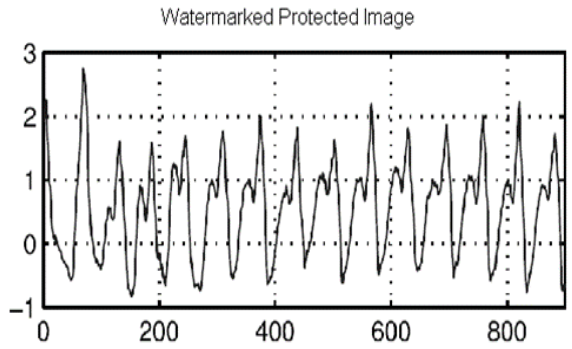

Figure 3: Wavelet based Ventricular fibrillation ECG Stego image

We take five normal ECG images of different person having different quality and embed the patient information shown in figure 1. The various performance metric evaluated for the developed system is shown in table1.

Table 1: Various Quality Measures of Ventricular fibrillation ECG images

Normal ECG Image	% PSD	PSNR	MSE	Normalize Cross-correlation	Average Difference
B1	0.0316	70.3573	0.0060	1.0000	0.0087
B2	0.1921	55.7150	0.1744	0.9996	0.0920
B3	0.0897	61.0966	0.0505	0.9999	0.0365
B4	0.1381	57.6105	0.1127	0.9998	0.0587
B5	0.1871	55.0216	0.2046	0.9995	0.1258

VI.CONCLUSION

This paper portrays the PHR system, their merits, their features and benefits to consumers/patients. We developed and implemented the wavelet-based ECG steganography which conceals the patient private information in ECG pictures. The performance of the developed system is evaluated in terms of numerous quality metrics. The developed system performs efficiently to conceal the information and at the same time preserve image quality.

REFERENCES

[1] Bliemel M, Hassanein K. Consumer satisfaction with online health information retrieval: a model and empirical study. e-Service J 2007; 5:53–83.

[2] Rideout V, Neuman T, Kitchman M, et al. e-Health and the Elderly: How Seniors Use the Internet for Health Information. Menlo Park, CA: Kaiser Family Foundation, 2005.

[3] Taylor H. Two in five adults keep personal or family health records and almost everybody thinks this is a good idea. Health Care News 2004.

[4] Demiris G, Afrin LB, Speedie S, et al. Patient-centered applications: use of information technology to promote disease management and wellness. J Am Med Inform Assoc 2008; 15:8–13.

[5] Kaelber DC, Jha AK, Johnston D, et al. A research agenda for personal health records (PHRs). J Am Med Inform Assoc 2008; 15:729–36.

[6] Earnest MA, Ross SE, Wittevrongel L, et al. Use of a patient-accessible electronic medical record in a practice for congestive heart failure: patient and physician experiences. J Am Med Inform Assoc 2004; 11:410–17.

[7] Wuerdeman L, Volk L, Pizziferri L, et al. How accurate is information that patients contribute to their electronic health record? AMIA 2005 Symposium Proceedings. 2005:834–8.

[8] DeLenardo C. Web-based tools steer patient-focused care. Nurs Manage 2004; 35:60–4.

[9] Halamka JD, Mandl KD, Tang PC. Early experiences with personal health records. J Am Med Inform Assoc2008; 15:1–7.

[10] Tang PC, Ash JS, Bates DW, et al. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. J Am Med Inform Assoc 2006; 13:121–5.

[11] Stolyar A, Lober WB, Drozd DR, et al. Feasibility of data exchange with a patient-centered health record. AMIA 2005 Conference Proceedings; 2005. 2005:1123.

[12] Tang PC, Lee TH. Your doctor's office or the Internet? Two paths to personal health records. N Engl J Med2009; 360:1276–8.

[13] Win KT, Susilo W, Mu Y. Personal health record systems and their security protection. J Med Syst2006; 30:309–15.