Volume 5, Issue 1, January 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Review on Steganography using Medical Signal

Gayatri M. Vengurlekar*
PG Student
Department of E & Tc& S. P. Pune University
Maharashtra, India

P. S. Topannavar
Assistant Professor
Department of E & Tc& S. P. Pune University
Maharashtra, India

Abstract*— Usage of e-health applications is increasing, now a day. The important example of e-health applications is Remote cardiac patients monitoring system. To save patients lives, diagnosing cardiac disease in time is necessary. Therefore, a continuous cardiac monitoring system should be provided in an ideal situation. The health-care providers lack the technology required to achieve this aim. Cloud services can be used to improve the performance of health care providers. There are three main problems which prevents the health care providers from using cloud services. They are privacy, performance and accuracy of the diagnoses. In this paper, to provide strong privacy protection service, tow steganography technique are proposed. Both could achieve promising results in terms of security and distortion measurements. There is difference of 1% in original and resultant watermarked ECG signal. The resultant watermarked ECG signal can be used for diagnoses and only authorised persons having security information can extract the hidden data in the ECG signal.*

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

I. INTRODUCTION

In modern era with increasing number of aging population and a larger portion of that suffering from cardiac diseases it is necessary that remote ECG patient monitoring systems are expected to be widely used as e-health applications. These systems are widely used to provide continuous patient monitoring and to send urgent alerts to specialist. Electrocardiogram (ECG) signals are resulted from electrical activity of heart over time and are collected using electrodes. With the aim of utilizing ECG signals to diagnose most cardiac diseases, development of portable wireless monitoring facilities such as body sensors, has increased significantly.

In typical wireless tele-monitoring system one or more body sensors are used to collect their ECG signals from patient body. Then if any pre-processing is applied if needed and these signals are transmitted to the patient's smart phone. Finally, the collected signals along with patient's private information are transmitted to the medical cloud using internet [52]. Alternatively, patients at hospital can also send their biomedical signal along with their private information to the centralised medical cloud. In this technique many challenges may arise.

1. Patient's biomedical signal with their confidential information requires special mechanism for protection against attackers [1: 10: 2].
2. The Size of the ECG signals is enormous. Therefore for wireless transmission of this large data to the medical cloud, a large bandwidth and considerable power is required.

New security and privacy threats as well as data integration issues are introduced while using Internet as a main communication channel. According to the Health Insurance Portability and Accountability Act (HIPAA), transmission of information through the internet should be protected and secured. HIPAA mandates that while information transmission through the Internet a patient's privacy and confidentiality be protected as follows [7]:

1. **Patient privacy**: It is of very importance that a patient can control who will use his/her confidential health information, such as name, address, contact details, and Medicare number. The security protocol should provide further control on who can access patient's data and who cannot.
2. **Security**: The method should guarantee the security of the information within the communication channels as well as the information stored on the hospital server or on the cloud.

Accordingly, it is very important to implement a security protocol which will have powerful communication and storage security [5].Several researchers have proposed number of security protocols to secure patient confidential information. There are two types of techniques. In first type includes techniques, which are based on encryption and cryptographic algorithms, are used to secure data during the communication and storage. As a result, the final encrypted data will be stored [7: 6: 13: 3]. The drawback of using encryption based techniques is its large computational overhead.
Alternatively, there are many security techniques, which are based on hiding its confidential information inside another insensitive host data without increasing the host data size and huge computational overhead. Such techniques are called steganography techniques. However, steganography techniques alone will not satisfy the conditions stated by HIPAA. Using ECG signal as a host in steganography technique, there are two approaches. First approach is to perform all the

steganography stages in time domain which will result in better performance with lower data hiding capacity. Second approach is to perform the steganography technique on frequency domain which will result in lower performance, with better data hiding capacity. Therefore, here two new security techniques are presented to guarantee secure transmission of patient confidential information along with patient physiological readings from body sensors. The first technique is based on time domain to provide better performance. This technique is based on transforming the ECG signal to a special time domain called (Shift special range transform) to increase the algorithm security. Then it uses LSB embedding to hide the secret data in the transformed special domain ECG. Finally, it returns the resultant ECG signal to its original range. The second technique is based on frequency domain and it is combination of cryptography technique and steganography techniques. Firstly, it uses steganography techniques to hide patient secret information inside patient biomedical signal. Moreover, this technique uses encryption based model to allow only the authorized persons to extract the hidden data. In this technique, the patient ECG signal is used as the host signal that will carry the patient confidential information as well as other readings from body sensors such as temperature, glucose, position, and blood pressure. The ECG signal is used here because of the fact that most of the health-care systems will collect ECG information. Moreover, the size of the ECG signal is greater than the size of other information. Therefore, it will be suitable to be a host for other small size secret information.

In this method body sensor nodes will be used to collect ECG signal, glucose reading, temperature, position and blood pressure, the sensors will collect readings and will send these readings to patient's PDA Device or smart phone via Bluetooth. Then, inside smart phone or PDA device the steganography technique will be applied and patient secret information and physiological readings will be embedded inside the ECG host signal. Finally, the watermarked ECG signal is transmitted to the hospital server or cloud via the Internet. As a result, the real size of the transmitted data is the size of the ECG signal only because the other information are hidden inside the ECG signal without increasing its size and no any overhead is added. At hospital server or cloud, the ECG signal and its hidden information will be stored. Any doctor can see the watermarked ECG signal and only authorized persons can extract the secret information and have access to the confidential patient information as well as otherreadings stored in the host ECG signal. The use of these techniques will slightly affect the quality of ECG signal. However, watermarked ECG signal can still be used for diagnoses purposes.

II. Literature Review

A. A New Reversible Data Hiding Technique

There are number of approaches which are use to secure patient sensitive data [15: 3: 13: 8]. However, one approach [9: 14: 4] proposed is based on using steganography techniques to hide confidential information inside medical images to secure data. The challenging factors of these techniques are how much information can be stored, and to what extent the method is secure. Finally, what will be the resultant distortion on the original medical image or signal is calculated. A new reversible data hiding technique based on wavelet transform is proposed by Kai-Mei Zheng and Xu Qian [4]. It is based on applying B-spline wavelet transform on the original ECG signal to detect QRS complex. After detection of R waves, Haar lifting wavelet transform is applied again on the original ECG signal. Next, the non QRS high frequency wavelet coefficients are selected by comparing and applying index subscript mapping. Then, the selected wavelet coefficients are shifted one bit to the left and the watermark is embedded. At the last, the ECG signal is reconstructed by applying reverse Haar lifting wavelet transform. This method has low capacity since it is shifting single bit. As a result only single bit can be stored for each ECG sample value. Furthermore, the security in this algorithm relies on the algorithm itself. Finally, this algorithm is based on normal ECG signal in which QRS complex can be detected, for abnormal signal in which QRS complex unable to detect, the algorithm will not perform well.

B. A Reversible Blind Watermarking for Medical Images

A reversible blind watermarking for medical images based on wavelet histogram shifting is presented by H. Golpira and H. Danyali [14]. This technique uses medical images such as MRI as a host signal. The histogram of the high frequency sub-bands is determined followed by taking two dimensional wavelet transform of the image. In next step, two thresholds are selected, at the beginning and at the end of the last portion of the histogram. For each threshold a zero point is created by shifting the left histogram part of the first threshold to the left, and shifting the right histogram part of the second threshold to the right. The locations of the thresholds and the zero points are used for inserting the binary watermark data. Performance of this algorithm is good for MRI images but not for ECG host signals. This algorithm has low capacity and no encryption key is involved in its watermarking process.

C. A Digital Watermarking of ECG for Secure Wireless Communication

S.Kauf and O.Farooq [9] proposed new digital watermarking of ECG for secure wireless communication. In this technique, each ECG sample is quantized using 10 bits, and is divided into segments. The size oh the segment is equal to the chirp signal that they use. Thus, for each ECG segment a modulated chirp signal is added. In the modulation process of the chirp signal, patient ID is used. In the next step, the modulated chirp signal is multiplied by a window dependent factor, and then added to the ECG signal. The resulting watermarked signal is 11 bits per sample. Hence with 11 bits for watermarked ECG and 5 bits for the factor and patient ID, the final signal consists of 16 bits per sample. In this algorithm the size of ECG signal is increased from 12 bits/sample to 16 bits/sample. Due to such behaviour overrides completely the concept of using steganography and the main purpose of steganography that does not increase the original size of the host signal.

D. Time Domain Special Range ECG Steganography

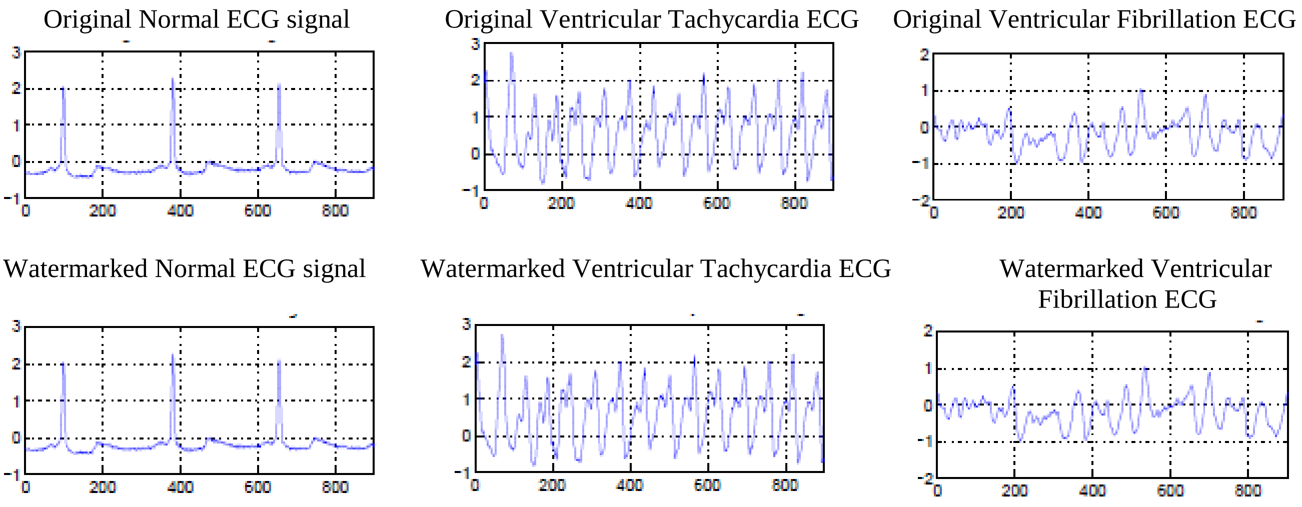
A new steganography technique is proposed by Ayman Ibaida [11] that is able to hide the secret message in any position in the host signal without distorting the original signal. This technique provides high security for the secret message by selecting more secured positions (such as MSB) in the host ECG signal that are unexpected to the attackers. In first step scaling and shifting is applied to ECG signal to avoid the negative values and converting the signal floating point numbers into integers. At the same time, this step represents the fist level of security of the steganography technique by hiding the values of both shifting and scaling factors that are mandatory parameters for extracting the secret information. A number of special values in the ECG signal samples are found to be relevant hosts that can hide the secret bits in the most significant positions with the condition of inverting the values of the right hand bits to the secret bit position. Here for ECG host signal, 32 bits are used to form each ECG sample. In this binary format, there are many special ranges that are relevant to hide the secret bits in all host sample positions. The third step is the actual data hiding process. The basic theme of this process is to hide the secret bits using the shifted value as a host, and then the resultant value would be shifted back to its original level. The final step is to de-scale the signal and shift it back to its original values. The receiver needs to know two parameters, the used range and signal pre-processing parameters to extract the hidden data from the host signal.

E. Frequency Domain Wavelet Based ECG Steganography

A wavelet based ECG steganography is proposed by Ibrahim Khalil and A. Ibaida [12]for protecting patient confidential information in point-of-care system. The first stage of this method is to encrypt the patient confidential information in such a way that prevents unauthorized persons - who do not have the shared key- from accessing patient confidential data. In this stage XOR ciphering technique is used with an ASCII coded shared key, which will play the role of the security key. XOR ciphering can be easily implemented inside a mobile device. Wavelet transform is a process of decomposition which results in coefficients representing frequency components of the signal at a given time. Band filters are used to perform DWT decomposition. It will result in 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 multi-level packet wavelet decomposition. Here 5-level wavelet packet decomposition has been applied to the host signal. Accordingly, 32 sub-bands resulted from this decomposition process. Most of the important features of the ECG signal are related to the low frequency signal. On the other hand, the high frequency signal represents mostly the noise part of the ECG signal. As a result, a small number of the 32 sub-bands will be highly correlated with the important ECG features while the other sub bands will be correlated with the noise. Then for security purpose scrambling operation is performed using shared key which is known to the sender and the receiver and other is scrambling matrix which is stored inside transmitter and the receiver. The next stage is embedding stage which starts with converting the shared key into ASCII code, therefore each character is represented by a number from 1 to 128. For each character code the scrambling sequence fetcher will read the corresponding row from the scrambling matrix. Then in the final stage, the resultant watermarked 32 sub-bands are recomposed using inverse wavelet packet re-composition. The new watermarked ECG signal will be result of this stage which will be similar to original un-watermarked signal. To extract the secret bits from the watermarked ECG signal, the shared key, scrambling matrix and the steganography level vectors are required.

III. DISCUSSION

In Time Domain Special Range ECG Steganography secret bits have been hidden in different positions (8th,16th,24th, and 32nd bits) using four special ranges [11]. To evaluate the proposed steganography technique, the resultant ECG signals are compared with their original signals. The percentage residual difference (PRD) is used for this purpose.Figure 3.1 [11]shows eight ECG segments divided where the first group contains the original normal ECG segment and three resultant host signals when we applied different special ranges and had data hidden in secret bit positions.



Original Normal ECG signal

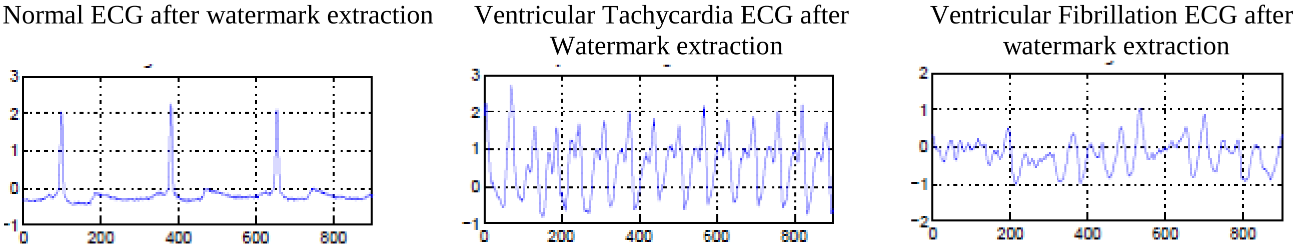
Original Ventricular Tachycardia ECG

Original Ventricular Fibrillation ECG

Watermarked Normal ECG signal

Watermarked Ventricular Tachycardia ECG

Watermarked Ventricular Fibrillation ECG



Normal ECG after watermark extraction

Ventricular Tachycardia ECG after Watermark extraction

Ventricular Fibrillation ECG after watermark extraction

Figure 3.1: ECG signals for normal, VT and VF signal before applying the steganographyoperation and after the steganography operation as well as after extracting the hidden data.

Different types of ECG signal with different diseases such as Ventricular Tachycardia, Ventricular Fibrillation, and Premature Ventricular Contraction, are used as well as normal samples in experimentation. TABLEIclearly shows how the PRD values and WWPRD does not vary widely for different types of ECG signals.

Table I PRD results for different data type and different ECG signals

ECG Type	PRD	WWPRD
Normal	0.0103	0.01
VT	0.0047	0.0052
VF	0.0092	0.0109
PVC	0.012	0.0176

Similar data is used for the frequency domain Wavelet Based ECG Steganography. To evaluate the proposed model, the PRD (percentage residual difference) is used to measure the difference between the original ECG host signal and the resulting watermarked ECG signal as shown in Eq. 3.1.

$$PRD = \sqrt{\frac{\sum_{i=1}^{N}(x_i - y_i)^2}{\sum_{i=1}^{N} {x_i}^2}} (3.1)$$

Where x represents the original ECG signal, and y is the watermarked signal.
To find the Weighted Wavelet PRD Eq. 3.2 is used

$$WWPRD = \sum_{j=0}^{N_L} w_j \, WPRD_J \ (3.2)$$

Where$N_L$is the total number of sub-bands, w_j denotes the weight value corresponding to sub-band $j$and $WPRD_J$ represents the calculated wavelet based PRD for sub-band j.

These measures have been calculated for each sample. Accordingly, to measure distortion caused by the extraction process, PRD and diagnosis PRD have been calculated. Finally to evaluate the reliability of the extracted information, bit error rate has been used as shown in Eq. 3.3

$$BER = \frac{B_{err}}{B_{total}} \times 100\% (3.3)$$

Where BER represents the Bit Error Rate in percentage, B_{err} is the total number of erroneous bits and B_{total} is the total number of bits.

TABLE II shows the results obtained for 8 normal ECG samples [11]. It can be seen that a maximum PRD measured was 0.6%. Secondly, it can be noticed that the difference between the normal PRD and the wavelet based PRD for diagnoses measurement is very small. Accordingly, this proves that the watermarking process does not affect the diagnosability. Finally, this table shows the PRD measured after extracting the watermark. It is obvious from the table that removal of the watermark will have a small impact on the PRD value. As a result, the ECG signal can still be used for diagnosis purposes after removing the watermark.

Table II PRD results for different normal ECG segments

Sample No.	PRD%	WWPRD%	PRD% extracted	WWPRD% extracted
1	0.43446	0.39338	0.57647	0.52692
2	0.59837	0.44557	0.80906	0.62531
3	0.4634	0.6083	0.63565	0.82741
4	0.51913	0.63338	0.70037	0.85416
5	0.41861	0.50547	0.56098	0.68459
6	0.36499	0.42618	0.50238	0.59443
7	0.42648	0.33541	0.57897	0.45032
8	0.44176	0.34352	0.59529	0.46326

IV. CONCLUSION

The methods discussed above are related to the steganography technique utilizing for medical signals. However some are intrusive while the other are non-intrusive methods. A new reversible data hiding technique based on wavelet transform performs well in case of normal ECG signal but in case of abnormal ECG signal it is not possible to use this technique. A reversible blind watermarking for medical images gives better result with MRI images as compared to ECG signal. A digital watermarking of ECG for secure wireless communication overrides the concept of steganography by increasing the size of original signal. Wavelet based ECG concept is the most reliable method, however it provides better security low data distortion and better capacity as compare to time domain special range steganography and the watermarked ECG signal can be used for diagnoses and the hidden data can be completely extracted.

REFERENCES

[1] M. Naghavi, P. Libby, E. Falk, S.W. Casscells, S. Litovsky, J. Rumberger, J. J. Badimon, C. Stefanadis, P. Moreno, G. Pasterkamp, et al. From “Vulnerable plaque to vulnerable patient a call for new definitions and risk assessment strategies: part i.” Circulation, 108 (14):1664–1672, 2003.

[2] M. Nambakhsh, A. Ahmadian, M. Ghavami, R. Dilmaghani, and S. Karimi-Fard. “A novel blind watermarking of ecg signals on medical images using EZW algorithm.” In Engineering in Medicine and Biology Society, 2006. *EMBS’ 06*. 28th Annual International Conference of the *IEEE*, pages 3274–3277, 2006.

[3] 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*, 17(1):12–19, 2010.

[4] 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,* volume 1, 2008.

[5] K. Malasri and L. Wang. “Addressing security in medical sensor networks.” In Proceedings of the 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments, page 12. *ACM*, 2007.

[6] 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,, 13(6):946–954, 2009.

[7] W. Lee and C. Lee. A cryptographic key management solution for hipaa privacy/security regulations. *IEEE* Transactions on Information Technology in Biomedicine,, 12(1):34– 41, 2008.

[8] 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.” Parallel and Distributed Systems, *IEEE* Transactions on, 24(1):131–143, 2013. *ISSN 1045-9219*. doi:10.1109/TPDS.2012.97.

[9] S. Kaur, R. Singhal, O. Farooq, and B. Ahuja. “Digital Watermarking of ECG Data for Secure Wireless Communication.” In 2010 International Conference on Recent Trends in Information, Telecommunication and Computing, pages 140–144. *IEEE*, 2010.

[10] N. Johnson and S. Jajodia. Information hiding: steganography and watermarking: *attacks and countermeasures*, volume 1. Springer, 2001.

[11] Ibaida and I. Khalil. “Wavelet based ECG steganography for protecting patient confidential information in point-of-care systems.”*IEEE* transactions on bio-medical engineering, 2013.

[12] Ibaida, I. Khalil, and F. Sufi. “Cardiac abnormalities detection from compressed ECG in wireless tele-monitoring using principal components analysis (PCA).” In 5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009, pages 207–212. IEEE, 2010.

[13] Hu, M. Jiang, M. Wagner, and D. Dong. “Privacy-preserving tele-cardiology sensor networks: toward a low-cost portable wireless hardware/software design.”*IEEE* Transactions on Information Technology in Biomedicine,, 11(6):619–627, 2007.

[14] 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, pages 31–36. *IEEE*, 2010.

[15] De la Rosa Algarin, S. Demurjian, S. Berhe, and J. Pavlich-Mariscal. “A security framework for xml schemas and documents for healthcare.” In Bioinformatics and Biomedicine Workshops (BIBMW), 2012 *IEEE* International Conference on, pages 782– 789, 2012.