International Journal for Innovative
Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IJIEMR Transactions, online available on 25th June 2020. Link :http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-06

Title: **ENHANCED PRIVATE AND SECURED MEDICAL DATA TRANSMISSION**

Volume 09, Issue 06, Pages: 127-134

Paper Authors

G.HARPITHA, M.AMARANATH REDDY

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

ENHANCED PRIVATE AND SECURED MEDICAL DATA TRANSMISSION

G.HARPITHA[1], M.AMARANATH REDDY[2]
[1]PG Scholar, Dept of ECE, SIR C.V. RAMAN Institute of Technology & Science, AP, India
[2] Assistant Professor, Dept of ECE, SIR C.V. RAMAN Institute of Technology & Science, AP, India

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 centers are used usually around the world in a Point - Of - care (PoC) applications in hospitals around the, huge amount of ECG signal collected by Body Sensor Networks (BSNs) from remote patients at homes will be transmitted such as blood pressure, temperature, glucose level etc along with other physiological readings. If the diagnosed by those remote patient monitoring systems are important that patient confidentiality it is protected while data is being transmitted over the public network as well as when they are stored in hospital servers used in this paper by remote monitoring systems and the wavelet based steganography technique has been introduced which combines encryption and scrambling technique to protect patient confidential data to be allows ECG signal to hide its corresponding patient confidential data and other physiological information thus guaranteeing the integration between ECG and the effectiveness of the proposed techniques for the two distortion measurement metrics have been used: the Wavelet Weighted PRD (WWPRD) and the Percentage Residual Difference (PRD). It is found that the proposed technique provides high security protection for patients data with low (less than 1%) distortion and ECG data remains diagnosable after watermarking and as well as after watermarks are removed from the watermarked data.

I.INTRODUCTION: Hiding the confidential data in to other form of data is call as data steganography. The HIPAA regulations act says that, there should be a protection and security is provided to the patient's confidential information which is sent through the public network. As the patient privacy is important so patient can control his/her confidential health information that if anyone can access or control the information like name, age, gender, ID no., address, telephone number. Monitoring patients at their home can reduce due to increasing rush at hospitals and care centers like medical. Hiding patient's confidential information and other physiological data in ECG signal is the main goal. Provide secrecy, integrity, and accessibility to confidential information. The main branch of cryptography is steganography that involves hiding information in other secondary information.

Hiding the information decrease the chance of the information being detected. Medical images has smaller size were the ECG signal has greater size. Therefore instead of medical image ECG signal is used in steganography process. The ECG signal of the patients is used to hide physiological data of patient like temperature, glucose level, blood pressure, position, etc., which are collected by using Body Sensor Networks (BSNs) at home and stored on hospital server by transmitted via network. Then that data is diagnosed by monitoring systems at hospital. At the same cost that the patient privacy is protected against intruders while data navigate in open network and stored in hospital servers. This technique allows hiding the confidential information of the patient in to ECG signal and thus gives guarantees the patient's privacy and discretion.

The main objective of steganography is to put the undisclosed message in the other coated media so that nobody can see that and both doctor and patient can communicate in secret way. The data security has improved by combining the more number of methods of steganography and the other techniques related to data hiding. The first steganography method is on hiding patient data which is confidential, inside ECG signal of patient which can be called as host signal. Additionally, the proposed method uses model which involves encryption to allow extracting the data which is hidden. That data can be extracted by only the authorized persons like doctors. In this paper, for the host signal, the ECG signal of patient is used and the patient private information and other physiological reading are hiding inside it. The main fact is that the ECG signal which is used here as a host signal because ECG information will collect by many of the healthcare systems. As compare to other host signal, ECG signal has large size thus it can hide more data than hiding data in other host signal. Therefore, for the small size secrete data the ECG signal will be right as a host. The proposed technique fallows the HIPPA, by providing open access for ECG signal and provides security for patient's confidential information from unauthorized access. In this method the ECG signal with temperature, blood pressure and glucose level are collected by using body sensor network. By using Bluetooth the physiological readings collected from sensor are transfer to patient's PDA device. The patient's PDA device contains steganography technique and embedding operation which embed the patient secret information and patient physiological data inside the. ECG signal i.e. host signal.

II.LITERATURE SURVEY: To provide security to patient confidential data, there is no. of methods [4], [1], [5]. However, one approach proposed which is on using steganography. Were, to protect confidential information of the patient it used medical image to stored secret information. How much data can be stored in medical image are the challenging factors of this method and up to which level this method is safe. Kai-meiZheng and XuQian [8] proposed a fresh technique for data hiding which is reversible and depending on wavelet transform. Furthermore, this method dose not used user define key, so in this algorithm the security is depends only on algorithm. At last, this algorithm is not useful for the abnormal ECG signal because in it QRS complex is absent. However this algorithm is depending only on normal ECG signal were QRS complex can be easily find. H. Danyali and H. Golpira [7] proposed a new technique where medical images are used like host signal. So this technique is not useful for ECG signal. Moreover, this algorithm has low capacity. Additionally, the encryption key is not concerned in its watermarking process. In our approach to use ECG signal in data hiding process. To decompose the ECG signal DWT technique is used. Then the patient's confidential information is embedded with share key inside decomposed ECG signal. XOR ciphering method is used with a shared key which is an ASCII coded. Here first security is provided with a shared key which is an ASCII coded. Second security is provided at the time of embedding operation by applying inimitable scrambling matrix. And third security is providing by selection steganography level vector at the time of inverse wavelet transform. So here three tier securities are provide to the patient's confidential information.

III ARCHITECTURE :

The proposed architecture for the system as shown in Figure.1 first collects the patient's ECG signal and other physiological readings using different body sensors. The signals are then sent to the smart phone via Bluetooth on which the secret data of the patient is stored. The secret data is encrypted in the smart phone using some encryption technique. The signals are then transformed into discrete wavelets using Discrete Wavelet Transformation (DWT). The five-level DWT applied on the host signal results into 32 sub-bands. The encrypted data is then embedded into the sub-band's coefficient using LSB substitution.

The 32 steganographed sub-bands are recomposed using inverse wavelet re-composition into a single steganographed ECG signal. The smart phone then sends the signal to the hospital server through Internet. The hospital server extracts the data from the host signal which can then be accessed by authorized personnel. Only the authorized people have the security key to access the hidden data.

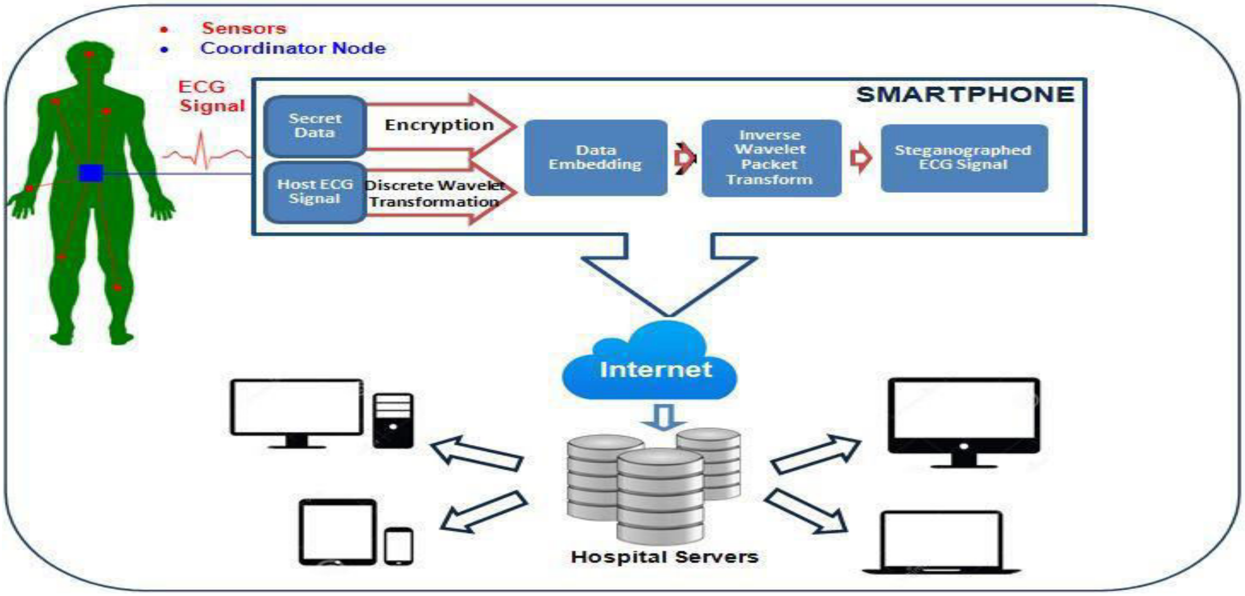

Figure.1: Architecture for ECG steganography and transmission of steganographed ECG signal

IVDIGITAL WATERMARKING SYSTEMS AND MODELS :

There are two main conceptual models of watermarking systems; these models help clarify the actual watermarking systems and the ways they operate first model is based on a view of watermarking as a method of communications like in communications channels, and the other model is based on the geometric views of watermarking methodologies.

A. Communications Channel Based Model of Watermarking

To define the structure of the watermarking systems, communications channel model can be considered due to the fact that watermarking form of communication. Fig.3 illustrates the basic elements of a communications channel model to the encoder creates the symbols from the input message and transmits them across a noisy channel, then at the receiver side the encoder reconstructs the original message from the received noisy transmitted symbols. To ensure the security of the model and the transmission secret keys can be employed at the encoders and decoders to the same generic model can be adopted to illustrate a digital watermarking system. In a digital watermarking model the to-be-embedded watermark can be considered as the input message, the cover media plays the same role as the noisy channel and the detector has the same function as the decoder. The challenge is to design and develop encoders and decoders that lead to correct detection and extraction of the watermark at the receiver, this requirement implies that the watermark and the cover signal are independent of each other. However, the dependence of the embedding algorithms in some methodologies on the cover signal suggests that the encoder should employ side information of the cover signal in the embedding process. Examples of methodologies using side information in the encoder are Cox's spread spectrum watermarking and multi-resolution watermarking. Fig.4. shows the adopted communications channel model used for generic digital watermarking systems.

B. Geometric Model of Watermarking

Watermarking algorithms can be conceptualized in geometric terms besides the communications channel model mentioned earlier. To present a watermarking system geometrically, the cover image is considered to be a point in a high dimensional space, the media space. Within this space different probability distributions and regions of interest can be defined as follows:

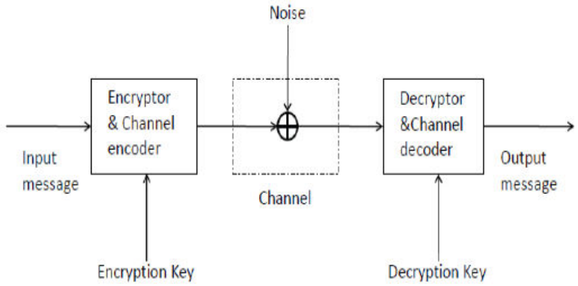

Fig.2.Block diagram of a standard model communications channel with encryption.

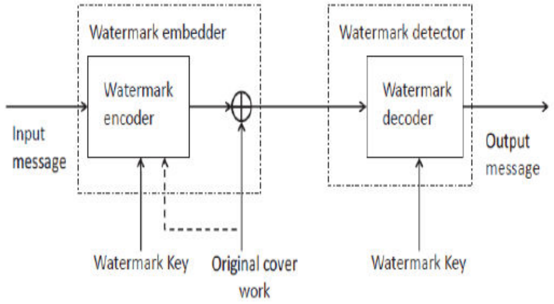

Fig.3. Block diagram of a watermarking system mapped into a communications model.

The distribution of un-watermarked works shows how possible each work is.

The region of acceptable fidelity is a region where all works seem basically the same to a given work. All the signals in this region are considered to be identical to the original signal.The detection region describes the behaviour of the detection algorithm. Successfully watermarked versions of the work are basically the intersection of the acceptable fidelity region and the detection region. The embedding distribution or the embedding region describes the effects of an embedding algorithm.

C. Digital Watermarking Properties

Watermarking systems can be characterized by a number of properties. The importance of each property is relevant to the requirements of the application and the service the watermarking method offers. In this section the most common properties of a digital watermarking scheme are highlighted. There are properties associated with embedding process such as payload, and there are those associated with detection process such as blind or false positive behavior, and robustness. Security and watermark keys are integrated parts that ensure the protection of the watermark and the content.

Effectiveness: The effectiveness of a watermarking system is defined as the probability that the output of the embedded is watermarked, or in other words, the effectiveness is the probability that the embedded mark is detectable immediately after embedding process. Although 100% effectiveness is the definition indicates that a watermarking system might have effectiveness less than 100%. Getting full effectiveness often imposes very high cost with respect to other properties, so in some cases watermarking schemes targeting specific applications might sacrifice some effectiveness to achieve better performance in other characteristics, such as fidelity, security or robustness. For example the watermarking scheme proposed in effective and appropriate for grayscale images are some cases, the effectiveness can be determined analytically, but in most of the schemes this property is estimated empirically by embedding a watermark in a large test set of images. Given sufficiently large test set of images a watermarking scheme targets, such as grayscale or color, leads to a good estimation of effectiveness characteristic of the scheme.

Fidelity: The perceptual similarity between the original signal and the watermarked version of it defines the fidelity of a watermarking system. The fidelity measure depends on the embedding process and the transmission of the marked signal. In the case of a watermarked video content transmitted using NTSC standard, due to relatively low quality of the broadcast technology, channel degradations may let the difference between the original and watermarked signals become imperceptible. But in case of high quality signals such as HDTV and DVD video, it is undesirable to have perceptual distortions; hence much higher fidelity watermark systems are required. There are cases that mildly perceptible watermarks are accepted in exchange for higher robustness or lower cost.

Data Payload (Embedding Capacity): Data payload refers to the number of bits a watermark system embeds within a unit of time or within a unit of cover signal. In photographs, the number of bits embedded into the image is referred to as the data payload and it is usually expressed in bits of information embedded per the measures are number of embedded bits per second and the number of bits per frame or second, respectively. A watermarking scheme that embeds N bits into the cover signal is referred to as an N-bit watermarking system.

Blind or Informed Detection: Applications where the original signal or a part of it is available during watermark detection are referred to informed detection methods (private watermarking systems). This method sometimes substantially improves detector performance as the original version can be subtracted from the marked copy to extract the watermark pattern alone. Blind detection (public watermarking system) refers to applications in which detection must be performed without any access to the original signal, as in copy control application. This property of a watermarking scheme is critical in determining if the method is suitable for a given application.

False Positive Rate: False positive rate refers to the detection probability of a watermark in a signal in which no mark is present, or in other words, this rate is the probability that given a specific watermark and randomly selected host signals, the detector reports the presence of the watermark. As with other properties, the required false positive rate depends on the application the scheme is intended for. In copy control applications, if an un-watermarked content consistently generates false positives, it could cause serious trouble, so in such a case the rate is expected to be infinitesimal.

V. SIMULATION RESULTS

VI. CONCLUSIONS

In this paper a novel steganography algorithm is proposed to hide patient information as well as diagnostics information inside ECG signal. This technique will provide a secured communication and confidentiality in a Point-of-Care system. A 5-level wavelet decomposition is applied. A scrambling matrix is used to find the correct embedding sequence based on the user defined key. Steganography levels (i.e. number of bits to hide in the coefficients of each sub-band) are determined for each sub-band by experimental methods. In this paper we tested the diagnoses quality distortion. It is found that the resultant watermarked ECG can be used for diagnoses and the hidden data can be totally extracted.

VI. REFERENCES

[1] Ayman Ibaida, Ibrahim Khalil, "A Wavelet Based ECG Steganography for Protecting Patient Confidential Information in Point-of-Care Systems", IEEE Transactions on Biomedical Engineering.

[2] Y. Lin, I. Jan, P. Ko, Y. Chen, J. Wong, and G. Jan, "A wireless PDA-based physiological monitoring system for patient transport," IEEE Transactions on information technology in biomedicine, vol. 8, no. 4, pp. 439–447, 2004.

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

[4] A. Ibaida, I. Khalil, and F. Sufi, "Cardiac abnormalities detection from compressed ECG in wireless telemonitoring using principal components analysis (PCA)," in 5th International Conference on Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2009. IEEE, 2010, pp. 207–212.

[5] 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.

[6] 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. ACM, 2007, p. 12.

[7] 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.

[8] 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.

[9] L. Marvel, C. Boncelet, and C. Retter, "Spread spectrum image steganography," IEEE Transactions on Image Processing, vol. 8, no. 8, pp. 1075–1083, 1999.

[10] A. 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, 2012, pp. 782–789.

[11] 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, vol. 24, no. 1, pp. 131–143, 2013.