IOSR Journal of Dental and Medical Sciences (IOSR-JDMS)
e-ISSN: 2279-0853, p-ISSN: 2279-0861.Volume 13, Issue 8 Ver. IV (Aug. 2014), PP 85-94
www.iosrjournals.org

ECG Steganography based privacy protection of medical datas for telemedicine application

[1]Treesa Joseph, [2]Remya U L
[1]Mtech Student,Dept.of CSE, Marian Engineering College, Kazhakuttom,Trivandrum,
[2]Asssistant Professor,Dept.of CSE, Marian Engineering College, Kazhakuttom,Trivandrum.

Abstract: *Over 20 million people worldwide have abnormal electrocardiogram (ECG) signals, i.e., arrhythmias, each year. Most of the cardiac patients are elders.And if they increasingly move to nursing homes, it is a necessary tendency to reduce the medical labor cost by deploying self-organized wireless cardiac-monitoring hardware/ software systems in an area with a radius of hundreds of feet. Such medical information networks could allow the doctors to immediately capture the arrhythmia events of any patient without leaving their offices. In this paper, a wavelet based steganography technique has been introduced which combines encryption and LSB embedding technique to protect patient confidential data.Huge amount of ECG signal collected by Body Sensor Networks (BSNs) from remote patients at homes will be transmitted along with other physiological readings such as blood pressure, temperature, glucose level etc. and diagnosed by those remote patient monitoring systems. An added benefit is the freedom of movement for patients due to the wireless networking technologies. To evaluate the effectiveness of the proposed technique on the ECG signal, distortion measurement metrics, the Percentage Residual Difference (PRD) has been used.*

Keywords: *ECG;Encryption;Steganography;Confidential ;BSN;Embedding;Wavelet;PRD.*

I. Introduction

Using Internet as main communication channel introduces new security and privacy threats as well as data integration issues. Information sent through the Internet should be protected and secured. Accordingly, it is of crucial importance to implement a security protocol which will have powerful communication and storage security [1]. Computer-based emergency healthcare systems are expanding in order to support geographically isolated areas. During the recent past, telemedicine platforms proved significant tools for the improvement of patient treatment in remote areas [2], [6], reducing transport, accommodation, and medical-personnel-related costs [3], and enabling a full time, 24 × 7 patient monitoring [8], [7]. Health monitoring may be delivered not only in a hospital environment but at home as well, through modern homecare telemonitoring systems, providing better possibilities for managing chronic care.

Privacy regulations address the patients' rights to understand and control the use and disclosure of their protected health information [14], [15], which is that part of the health information that reveals an individual's identification, such as name, address, telephone number, medical record number, and so on. Because the content of the protected information is directly interrelated with the patient's privacy, the protection of the health information is actually the protection of the patient's privacy. In contrast, the part of health information that does not involve any identification data is deidentified health information, for example, admission sequence number, charge number, or service sequence number. Protecting the privacy and confidentiality of medical records and patients' data is no longer a choice, but a necessity.

In this model,body sensor nodes will be used to collect ECG signal, glucose reading, temperature, position and blood pressure, the sensors will send their readings to patient's PDA device via Bluetooth. Then,inside the patient's 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 sent to the hospital server via the Internet. As a result, the real size of the transmitted data is the size of the ECG signal only without adding any overhead, because the other information are hidden inside the ECG signal without increasing its size. At hospital server the ECG signal and its hidden information will be stored. Any doctor can see the watermarked ECG signal an d only authorized doctors and certain administrative personnel can extract the secret information and have access to the confidential patient information as well as other readings stored in the host ECG signal.

With the growing number of aging population and a significant portion of that suffering from cardiac diseases, it is conceivable that remote ECG patient monitoring systems are expected to be widely used as Point-of-Care (PoC) applications in hospitals around the world. Therefore, It is utterly 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 used by remote monitoring systems. The proposed steganography technique has been designed in such a way that guarantees minimum acceptable distortion in the ECG signal. Steganography is not a new science. But this aids in protection of medical datas for telemedicine applications.Furthermore, it will provide the highest security that can be achieved. The use of this technique will slightly affect the quality of ECG signal. However, watermarked ECG signal can still be used for diagnoses purposes as it is proven in this paper.

II. Related work

There are many approaches to secure patient sensitive data [9], [11], [10], [13]. However, one approach [12], [5],[4] proposed to secure data is based on using steganography techniques to hide secret information inside medical images.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 re sultant distortion on the original medical image or signal.

Embedding robustness is less in many techniques. Data embedding using Pixel Difference Expansion involves computational overhead. It involves calculating the difference values,partitioning difference values into 4 sets,creating a location map,collecting original LSB values,data embedding by replacement,inverse integer transform. Another technique,Bit Modification is least secure. The security lies on the presumption that no other partiesare aware of this secret message. This method is easy to implement but very susceptible to data loss due to channel noise and re-sampling.

Kai-mei Zheng and Xu Qian [4] proposed a new reversible data hiding technique based on wavelet transform. Their method is based on applying B-spline wavelet transform on the original ECG signal to detect QRS complex. After detecting 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 coefficients are shifted one bit to the left and the watermark is embedded. Finally, the ECG signal is reconstructed by applying reverse haar lifting wavelet transform. Moreover, before they embed the watermark, Arnold transform is applied for watermark scrambling. This method has low capacity since it is shifting one bit. As a result only one bit can be stored for each ECG sample value. Furthermore, the security in this algorithm relies on the algorithm itself, it does not use a user defined key. Finally, this algorithm is based on normal ECG signal in which QRS complex can be detected. However, for abnormal signal in which QRS complex cannot be detected, the algorithm will not perform well.

H.Golpira and H.Danyali [5] proposed a reversible blind watermarking for medical images based on wavelet histogram shifting. In this work medical images such as MRI is used as host signal. A two dimensional wavelet transform is applied to the image. Then, the histogram of the high frequency subbands is determined. Next, two thresholds are selected, the first is in the beginning and the other is in 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. This algorithm performs well for MRI images but not for ECG host signals. Moreover, the capacity of this algorithms is low. Moreover, no encryption key is involved in its watermarking process.

Finally, S.Kauf and O.Farooq [12] proposed new digital watermarking of ECG data for secure wireless communication. In their work, each ECG sample is quantized using 10 bits, and is divided into segments. The segment size is equal to the chirp signal that they use. Therefore, for each ECG segment a modulated chirp signal is added. Patient ID is used in the modulation process of the chirp signal. Next, the modulated chirp signal is multiplied by a window dependent factor, and then added to the

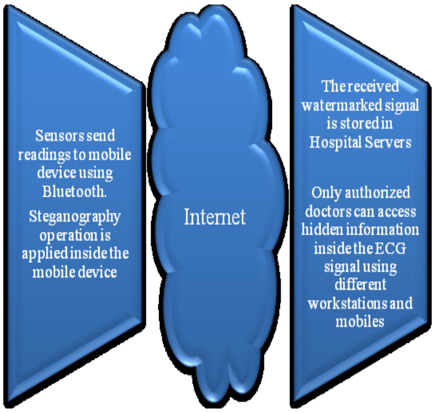

Sensors send readings to mobile device using Bluetooth.
Steganography operation is applied inside the mobile device
Internet
The received watermarked signal is stored in Hospital Servers
Only authorized doctors can access hidden information inside the ECG signal using different workstations and mobiles

Fig .1. ECG steganography scenario in Point-of-Care (PoC) systems where body sensors collect different readings as well as ECG signal and watermarking process implemented inside the patient's mobile device

ECG signal. The resulting watermarked signal is 11 bits per sample. The final signal consists of 16 bits per sample, with 11 bits for watermarked ECG and 5 bits for the factor and patient ID.

III. Methodology

The sender side of the proposed steganography technique consists of four integrated stages.The stages are described in more detail below.The proposed technique is designed to ensure secure information hiding with minimal distortion of the host signal. Moreover, this technique contains an authentication stage to prevent unauthorized users from extracting the hidden information.

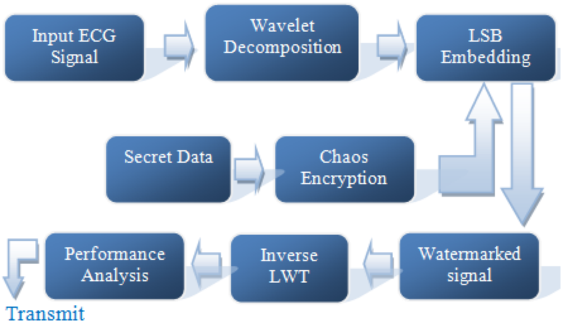


Fig .2. Block Diagram of the sender steganography which includes encryption,wavelet decomposition and secret data embedding.

A. Wavelet Decomposition

Wavelet transform is a process that can decompose the given signal into coefficients representing frequency components of the signal at a given time. Wavelet transform can be definedas shown in Eq 1

$$C(S,P)= \int_{-\infty}^{\infty} f(t)\Psi(S,P)dt \qquad (1)$$

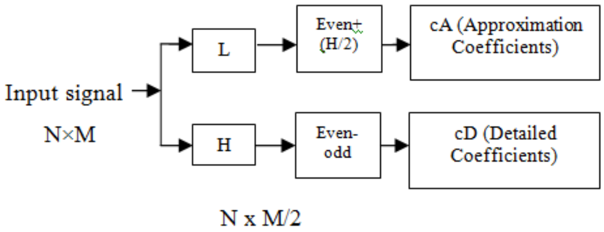
where Ψ represents wavelet function. S and P are positive integers representing transform parameters. C represents the coefficients which is a function of scale and position parameters [15]. Wavelet transform is a powerful tool to combine time domain with frequency domain in one transform. In most applications discrete signals are used.

The Wim Sweldens developed the lifting scheme for the construction of biorthogonal wavelets. The main feature of the lifting scheme is that all constructions are derived in the spatial domain. It does not require complex mathematical calculations that are required in traditional methods. Lifting scheme is simplest and efficient algorithm to calculate wavelet transforms. It does not depend on Fourier transforms. Lifting scheme is used to generate second-generation wavelets, which are not necessarily translation and dilation of one particular function.

It was started as a method to improve a given discrete wavelet transforms to obtain specific properties. Later it became an efficient algorithm to calculate any wavelet transform as a sequence of simple lifting steps. Digital signals are usually a sequence of integer numbers, while wavelet transforms result in floating point numbers. For an efficient reversible implementation, it is of great importance to have a transform algorithm that converts integers to integers. Fortunately, a lifting step can be modified to operate on integers, while preserving the reversibility. Thus, the lifting scheme became a method to implement reversible integer wavelet transforms.

We have used lifting scheme of wavelet transform because lifting scheme is having following advantages over conventional wavelet transform technique.It allows a faster implementation of the wavelet transform. It requires half number of computations as compare to traditional convolution based discrete wavelet transform. This is very attractive for real time low power applications. The lifting scheme allows a fully in-place calculation of the wavelet transform. In other words, no auxiliary memory is needed and the original signal can be replaced with its wavelet transform. Lifting scheme allows us to implement reversible integer wavelet transforms. In conventional scheme it involves floating point operations,which introduces rounding errors due to floating point arithmetic. While in case of lifting scheme perfect reconstruction is possible for loss-less compression. It is easier to store and process integer numbers compared to floating point numbers. Easier to understand and implement.It can be used for irregular sampling .

Wavelets are building blocks that are quickly de-correlate data. To decompose the given signal into coefficients representing frequency components of the signal at a given time the wavelet transform is used. LWT decomposes the signal into different subband coefficients, L and H for



L : Low Pass Filter
H : High Pass Filter
Fig .3. Forward lifting in Lifting Wavelet Transform

Embedding the messages in the approximation and detailed coefficients of subbands.Lifting scheme is a technique to convert DWT coefficients to Integer coefficients without losing information. Lsubband contains the significant part of the spatial domain signal. High-frequency subband contains the detailed with noisy information of signal. These coefficients are selected as reserved space for hiding the text data.3-level packet wavelet decomposition has been applied to host the signal. The secret text data is embedded into the wavelet coefficients of high frequency subbands because it is non sensitive to human visual system.

Forward Lifting in LWT involves column wise processing to get L and H.H = (Ce-Co) and L = (Ce+ [H/2]) where Co and Ce is the odd column and even column wise pixel values.Inverse Integer wavelet transform is formed by Reverse lifting scheme.Procedure is similar to the forward lifting scheme.

In this paper, a 3-level wavelet packet decomposition has been applied to the host signal .Accordingly,15 sub-bands resulted from this decomposition process is shown in the Fig. In each decomposition iteration the original signal is divided into two signals.Moreover,the frequency spectrum is distributed on these two signal. Moreover, the frequency spectrum is distributed on these two signal. Therefore, one of the resulting signals will represent the high frequency component and the other one represents the low frequency component. Most of the important features of the ECG signal are related to the low frequency signal. Therefore, this signal is called the approximation signal (A). On the other hand, the high frequency signal represents mostly the noise part of the ECG signal and is called detail signal (D). 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 components in the original ECG signal [16]. Therefore, in our proposed technique different number of bits will be changed in each wavelet coefficient (usually called steganography level) based on its sub-band. As a result, a different steganography level will be selected for each band in such a way that guarantees the minimal distortion of the important features for the host ECG signal.

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 multi-level packet wavelet decomposition.

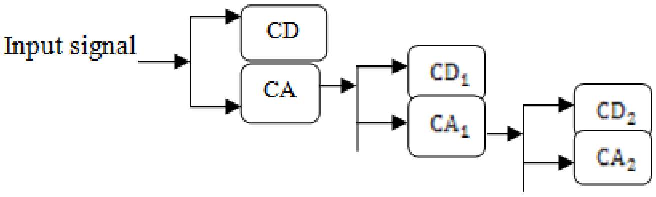


Fig .4. 3-level lifting wavelet transforms to obtain the detailed coefficients

B. Encryption

Encryption is the most powerful and common approach to protect information confidentiality. Used to encrypt the patient confidential information in such a way that prevents unauthorized persons. This method is one of the advanced encryption standard to encrypt the privacy data for secure transmission.It encrypts the original text data's with encryption key value generated from chaotic sequence with threshold function by bitxor operation. Here logistic map is used for generation of chaotic map sequence.It is very useful to transmit the secret data through unsecure channel securely which prevents data hacking. Details are converted to ASCII codes and then encryption is applied. XOR ciphering technique provides security.XOR cipher is a type of additive cipher,an encryption algorithm that operates according to the principles:

$A \oplus 0 = A$
$A \oplus A = 0$

$(A \oplus B) \oplus C = A \oplus B \oplus C)$
$(B \oplus A) \oplus A = B \oplus 0 = B$

Where ⊕ denotes the exclusive disjunction(XOR) operations

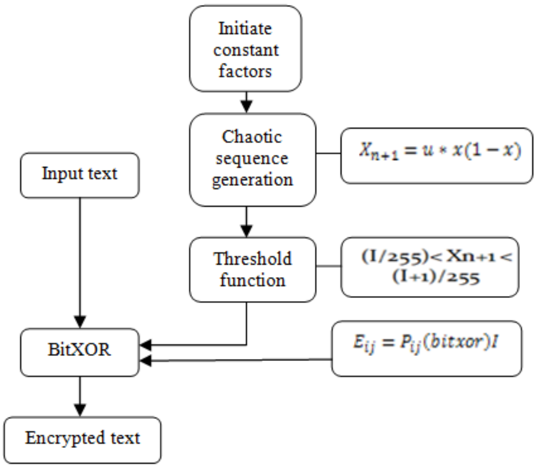

Initiate constant factors
Chaotic sequence generation
$X_{n+1} = u * x(1-x)$
Input text
Threshold function
$(I/255) < X_{n+1} < (I+1)/255$
BitXOR
$E_{ij} = P_{ij}(bitxor)I$
Encrypted text

Fig .5. Block Diagram showing the detailed construction of the chaotic encryption operation..

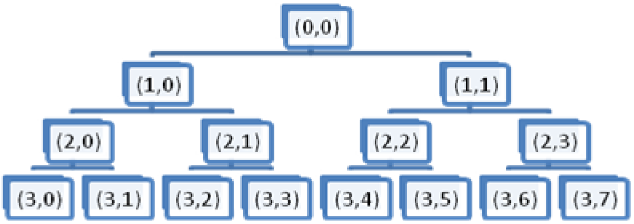


Fig .6. 3-level wavelet decomposition tree showing 15 sub-bands of ECG host signal and the secret data will be hidden inside the coefficients of the sub-bands.

C. LSB Embedding

Encrypted data has to be embedded onto the ECG signal. Encrypted data is hidden onto the ECG signal via LSB embedding.

The embedding algorithm

```
cip  : the cipher text
r      : number of rows of det matrix
c      : number of columns of det matrix
len   : length of the cipher text
CH1&CH2 : 2 successive detailed coefficients
a threshold 240 is taken
det     : detailed coefficients
det2    :embedded coefficients
embed(CH1,CH2,txt)
        CH1←bitand(CH1,240)
        CH2←bitand(CH2,240)
        if bitand(txt,128)= =128
          CH1←bitor(CH1,8)
        end
         if bitand(txt,64)= =64
          CH1←bitor(CH1,4)
        end
        if bitand(txt,32)= =32
          CH1←bitor(CH1,2)
        end
        if bitand(txt,16)= =16
          CH1←bitor(CH1,1)
        end
        if bitand(txt,8)= =8
          CH2←bitor(CH2,8)
        end
        if bitand(txt,4)= =4
          CH2←bitor(CH2,4)
        end
        if bitand(txt,2)= =2
          CH2←bitor(CH2,2)
        end
        if bitand(txt,1)= =1
          CH2←bitor(CH2,1)
        end
end
j ←1
for i=1 to len do
      CH1←det[j]:detailedcoefficientbefore                embedding
      CH2←det[j+1] :successive detailed coefficient before  embedding
      txt ←cip(i)
      call embed(CH1,CH2,txt)
      det(j) ←CH1     :coefficient after embedding
      det(j+1) ←CH2 :coefficient after embedding
      increment j
end
det2 ←[rD,rD1,rD2]
Rs3 ←wavelet recomposition(det2)
```

Initially, binary values of 2 successive detailed coefficients are taken. Least significant 4 bits of the coefficients are cleared. Most significant 4 bits of text data are embedded into lower 4 bits of 1st coefficient. Least significant 4 bits of the text data are embedded into the lower 4 bits of 2nd coefficient.Hence,embedding is achieved.

D. Inverse wavelet re-composition and extraction process

The inverse wavelet process will convert the signal to the time domain instead of combined time and frequency domain.Therefore,the newly reconstructed watermarked ECG signal will be very similar to the original unwatermarked ECG signal.In this stage,the resultant watermarked 15 sub-bands are recomposed using inverse wavelet packet re-composition. The result of this operation is the new watermarked ECG signal.

The first step is to apply 3-level wavelet packet decomposition to generate the 15-sub-band signals.Next,the extraction starts by extracting the secret bits in the correct order from the LSB.Finally,the extracted bits are decrypted.The extraction process is almost similar to the embedding process except that instead of changing the bits of the selected coefficients,it is required to read values of the bits in the selected coefficients,and then resetting them to zero.

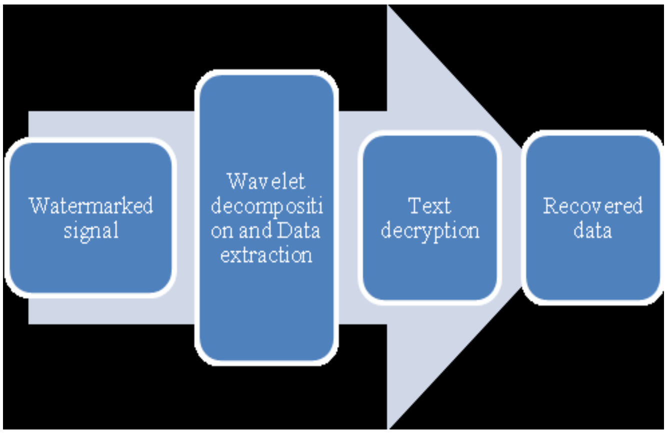


Fig .7. Block Diagram of the receiver which includes wavelet decomposition,extraction,decryption

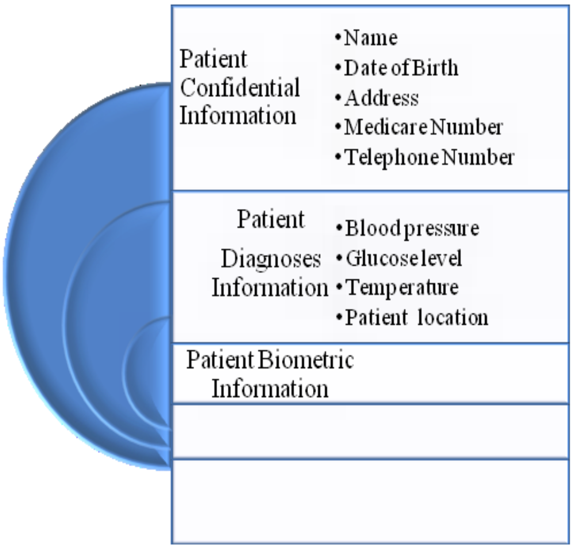


Fig .8. Original data consisting of patient information and sensor readings as well as patient biometric information.

IV. Evaluation

In this section ,we evaluate the performance of the method. In this paper, three different types of ECG signals are used for experimentation. A testbed of 12 ECG samples is used for experimentation. The set of samples consist of 4 normal (NSR) ECG samples, 4 Ventricular fibrillation ECG samples and 4 Ventricular Tachycardia ECG samples. Each sample is 10 seconds long with 250 Hz sampling frequency. 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 11.

$$\mathrm{PRD} = \sqrt{\frac{\sum_{i=0}^{N}(x_i - y_i)^2}{\sum_{i=0}^{N} x^2}} \qquad (2)$$

Where x represents the original ECG signal, and y is the watermarked signal.

Finally to evaluate the reliability of the extracted information, bit error rate has been used as shown in Eq 12.

$$\mathrm{BER} = \frac{B_{err}}{B_{total}} \times 100\% \qquad (3)$$

Where BER represents the Bit Error Rate in percentage, Berr is the total number of erroneous bits and Btotal is the total number of bits.

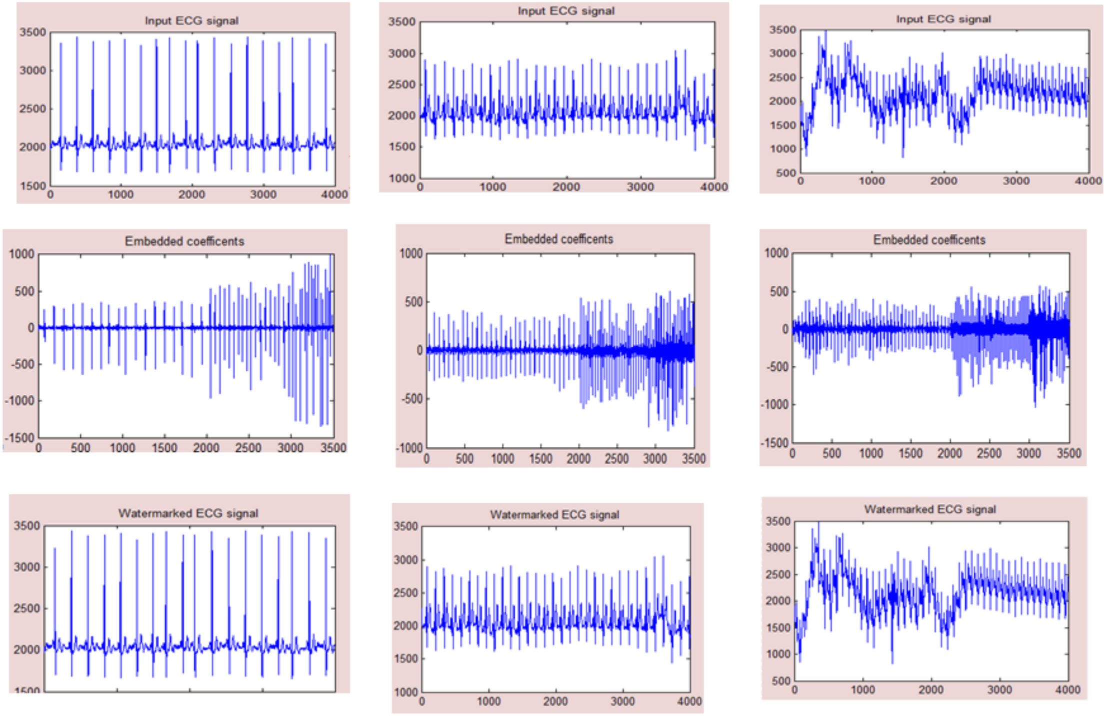


Fig .9. ECG signals for normal, VT and VF signal before applying the steganography operation and after the steganography operation as well as after extracting the hidden data.

V. Experiments And Results

Fig.9 shows 3 ECG signal types,and the resultant watermarked signals before and after watermark extraction process.

To validate diagnosability of the digitally processed ECGs, two specialist doctors were consulted. 12 ECG Segments for both normal and abnormal cases were shown to them before and after watermarking, and also after removal of watermarks. They were asked the following questions:

- How similar is the original and the watermarked ECG?
- Can the watermarked ECG be used for diagnoses?

Both the specialist doctors admitted that the similarity is so high that the difference is undetectable and the both the watermarked and un-watermarked signals can be used for diagnoses.

Tables show the results obtained for 14 ECG samples. It can be seen from the table that a maximum of PRD for minimum data measured was 0.2% and maximum of PRD for maximum data measured was 0.5%. 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 diagnoses purposes after removing the watermark.

TABLE I PRD RESULTS FOR DIFFERENT NORMAL ECG SEGMENTS

Sample No	Percentage Residual Difference	
	PRD% for minimum data	*PRD% for maximum data*
1	0.142213	0.344168
2	0.142661	0.342233
3	0.190538	0.390863
4	0.243995	0.345898

TABLE II PRD RESULTS FOR VENTRICULAR FABRILLATION

Sample No	Percentage Residual Difference	
	PRD% for minimum data	*PRD% for maximum data*
1	0.124462	0.38448
2	0.16381	0.40912
3	0.19697	0.43247
4	0.19213	0.37474

VI. Conclusion

In this paper,a novel steganography algorithm is proposed to hide patient information as well as diagnostics information inside ECG signal. The system is designed to provide security measurements against malicious attacks and stealing of patient information. This technique will provide privacy protection of medical datas for telemedicine applications.The proposed technique has been designed in such a way that guarantees minimum acceptable distortion in the ECG signal.A 3-level wavelet decomposition is applied. 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.

References

[1] 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.

[2] J. C. Lin, “Applying telecommunication technology to health care delivery,” IEEE Eng. Med. Biol. Mag., vol. 18, no. 4, pp. 28–31, Jul./Aug. 1999.

[3] D. Hailey, R. Roine, and A. Ohinmaa, “Systematic review of evidence for the benefits of telemedicine,” J. Telemed. Telecare, vol. 8, pp. 1–7, 2002.

[4] K. Zheng and X. Qian, “Reversible Data Hiding forElectrocardiogram Signal Based on Wavelet Transforms,” in International Conference on Computational Intelligence and Security, 2008. CIS’08, vol. 1, 2008.

[5] 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.

[6] I. Maglogiannis, “Design and implementation of a calibrated store and forward imaging system for teledermatology,” J. Med. Syst., vol. 28, no.5, pp. 455–467, 2004.

[7] A. Kollmann, D. Hayn, J. Garcia, B. Rotman, P. Kastner, and G. Schreier, “Telemedicine framework for manufacturer independent remote pacemaker follow-up,” in Proc. Comput. Cardiol., 2005, pp. 49–52.

[8] V. Traver, E. Monton, J. L. Bayo, J. M. Garcia, J. Hernandez, and S. Guillen, “Multiagent home telecare platform for patients with cardiac diseases,” in Proc. Comput. Cardiol., 2003, pp. 117–120.

[9] 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.

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

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

[13] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, “Scalable and secure sharing of personal health records in cloud computing using attributebased encryption,” Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 1, pp. 131–143, 2013.

[14] Standards for privacy of individually identifiable health information,” Fed. Regist., vol. 67, pp. 53181–53273, 2002.

[15] G.M. Stevens, “A brief summary of the medical privacy rule,” CRS Rep. Congr. 2003.

[16] I.S. Jacobs and C.P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G.T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271-350.

[17] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740-741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982.

[18] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

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

[24] D. Stinson, Cryptography: theory and practice. CRC press, 2006.

[25] A. Poularikas, Transforms and Applications Handbook. CRC, 2009.

[26] A. Al-Fahoum, “Quality assessment of ECG compression techniques using a wavelet-based diagnostic measure,” IEEE Transactions on Information Technology in Biomedicine, vol. 10, no. 1, 2006.