ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

StegoImage Based Protection of Medical Datas

L.Keerthana
Assistant Professor
Dept. of Electronics and Communication Engineering
Bharathiyar Institute of Engineering For Women
keerthuloganathan@gmail.com

Abstract— **The project proposes the enhancement of protection system for secret data communication through encrypted data concealment in ECG signals. The proposed encryption technique used to encrypt the confidential data into unreadable form and not only enhances the safety of secret carrier information by making the information inaccessible to any intruder having a random method. After data encryption, the data hider will conceal the secret data into the ECG signal coefficients. Although encryption achieves certain security effects, they make the secret messages unreadable and unnatural or meaningless. This system is still enhanced with encrypt messages using chaos crypto system. This is the reason a new security approach called reversible data hiding arises. It is the art of hiding the existence of data in another transmission medium to achieve secret communication. It does not replace cryptography but rather boosts the security using its obscurity features. Here the discrete wavelet transformation is used to decompose an ECG signal to different frequency subbands. The data hiding technique uses the LSB replacement algorithm for concealing the secret message bits into the high frequency coefficients. In the data extraction module, the secret data will be extracted by using relevant key for choosing the relevant data to extract the data. By using the decryption keys, extracted text data will be decrypted from encryption to get the original information. Finally the performance of this proposal in encryption and data hiding will be analyzed based on image and data recovery.**

Index Terms—**ECG, Steganography, Encryption, Wavelet, Watermarking.**

I. INTRODUCTION

The identification of objects in an image and this process would probably start with image processing techniques such as noise removal, followed by (low-level) feature extraction to locate lines, regions and possibly areas with certain textures.

The clever bit is to interpret collections of these shapes as single objects, e.g. cars on a road, boxes on a conveyor belt or cancerous cells on a microscope slide. One reason this is an AI problem is that an object can appear very different when viewed from different angles or under different lighting. Another problem is deciding what features belong to what object and which are background or shadows etc. The human visual system performs these tasks mostly unconsciously but a computer requires skilful programming and lots of processing power to approach human performance. Manipulation of data in the form of an image through several possible techniques. An image is usually interpreted as a two-dimensional array of brightness values, and is most familiarly represented by such patterns as those of a photographic print, slide, television screen, or movie screen. An image can be processed optically or digitally with a computer.

To digitally process an image, it is first necessary to reduce the image to a series of numbers that can be manipulated by the computer. Each number representing the brightness value of the image at a particular location is called a picture element, or pixel. A typical digitized image may have 512 × 512 or roughly 250,000 pixels, although much larger images are becoming common. Once the image has been digitized, there are three basic operations that can be performed on it in the computer. For a point operation, a pixel value in the output image depends on a single pixel value in the input image. For local operations, several neighbouring pixels in the input image determine the value of an output image pixel. In a global operation, all of the input image pixels contribute to an output image pixel value.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

II. RELATED WORK

There are many approaches to secure patient sensitive data. However, one approach 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 resultant distortion on the original medical image or signal. Kai-mei Zheng and Xu Qian 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.

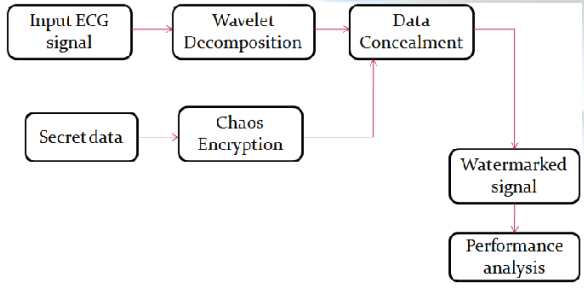


Fig.1. Block diagram for embedding process.

III. METHODOLOGY

The sender side of the proposed steganography technique consists of four integrated stages. 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.

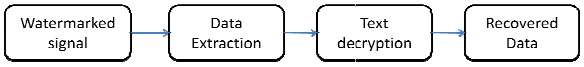


Fig. 2 Block diagram for extraction process.

Stage 1:Choas crypto system

This method is one of the advanced encryption standard to encrypt the image for secure transmission.It encrypts the original image pixel values 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 image through unsecure channel securely which prevents data hacking as shown in Fig 3.

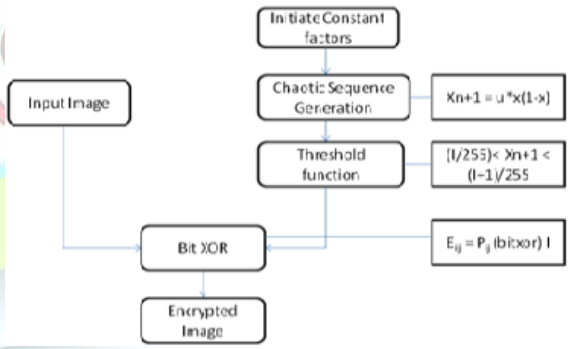


Fig. 3 Block diagram for process flow of choas encryption.

Stage 2:Wavelet decomposition

Lifting wavelet transform

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Basically we use Wavelet Transform (WT) to analyze non-stationary signals, i.e., signals whose frequency response varies in time, as Fourier Transform (FT) is not suitable for such signals.
To overcome the limitation of FT, Short Time Fourier Transform (STFT) was proposed. There is only a minor difference between STFT and FT. In STFT, the signal is divided into small segments, where these segments (portions) of the signal can be assumed to be stationary. For this purpose, a window function "w" is chosen. The width of this window in time must be equal to the segment of the signal where it is still be considered stationary. By STFT, one can get time-frequency response of a signal simultaneously, which can't be obtained by FT. The short time Fourier transform for a real continuous signal. Christo Ananth et al. [6] proposed a work, in this work, a framework of feature distribution scheme is proposed for object matching. In this approach, information is distributed in such a way that each individual node maintains only a small amount of information about the objects seen by the network. Nevertheless, this amount is sufficient to efficiently route queries through the network without any degradation of the matching performance. Digital image processing approaches have been investigated to reconstruct a high resolution image from aliased low resolution images. The accurate registrations between low resolution images are very important to the reconstruction of a high resolution image. The proposed feature distribution scheme results in far lower network traffic load. To achieve the maximum performance as with the full distribution of feature vectors, a set of requirements regarding abstraction, storage space, similarity metric and convergence has been proposed to implement this work in C++ and QT.

The wavelet transform involves projecting a signal onto a complete set of translated and dilated versions of a mother wavelet $\Psi(t)$. The strict definition of a mother wavelet will be dealt with later so that the form of the wavelet transform can be examined first. For now, assume the loose requirement that $\Psi(t)$ has compact temporal and spectral support (limited by the uncertainty principle of course), upon which set of basis functions can be defined.

The basis set of wavelets is generated from the mother or basic wavelet is defined as:

$$\Psi_{a,b}(t)= \frac{1}{\sqrt{a}}\psi\left(\frac{t-b}{a}\right) ;$$

$a, b \in \Re$ and $a>0$ -------- (1)

The variable 'a' (inverse of frequency) reflects the scale (width) of a particular basis function such that its large value gives low frequencies and small valuegives high frequencies. The variable 'b' specifies its translation along x-axis in time. The term $1/\sqrt{a}$ is used for normalization.

Forward Lifting in IWT

Column wise processing to get H and L

H = (Co-Ce) and L = (Ce+ [*H/2]*)

Where Co and Ce is the odd column and even column wise pixel values

Reverse Lifting scheme in IWT

Inverse Integer wavelet transform is formed by Reverse lifting scheme. Procedure is similar to the forward lifting scheme.

Stage 3: Adaptive LSB Embedding

An ideal steganographic technique embeds message information into a carrier image with virtually imperceptible modification of the image. Adaptive steganography comes closer to this ideal since it exploits the natural variations in the pixel intensities of a cover image to hide the secret message. The objective of steganography is a method of embedding an additional information into the digital contents, that is undetectable to listeners. We are investigating its embedding, detecting, and coding techniques. The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels. As the application domain of embedding data in digital

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

multimedia sources becomes broaden, several terms are used by various groups of researchers, including steganography, digital watermarking, and data hiding. This paper introduces a new, principled approach to detecting least significant bit (LSB) steganography in digital signals such as images and audio. It is shown that the length of hidden messages embedded in the least significant bits of signal samples can be estimated with relatively high precision. The new stegano approach is based on some statistical measures of sample pairs that are highly sensitive to LSB embedding operations. The resulting detection algorithm is simple and fast. To evaluate the robustness of the proposed stegano approach, bounds on estimation errors are developed. Furthermore, the vulnerability of the new approach to possible attacks is also assessed, and counter measures are suggested. A detailed algorithm is presented along with results of its application on some sample images.

Least Significant Bit Insertion

A detailed coefficients obtained from wavelet domain are used here for concealment process and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first bit selected coefficient and the second bit of message is embedded into the second bit location and so on. The resultant watermarked signal which holds the secret message with original form and difference between the input signal and the watermarked signal is not visually perceptible. The quality of the signal, however degrades with the increase in number of LSBs. This hiding process will introduce the error between input and output signal and it is determined by mean square error and Peak signal to noise ratio determines the signal quality.

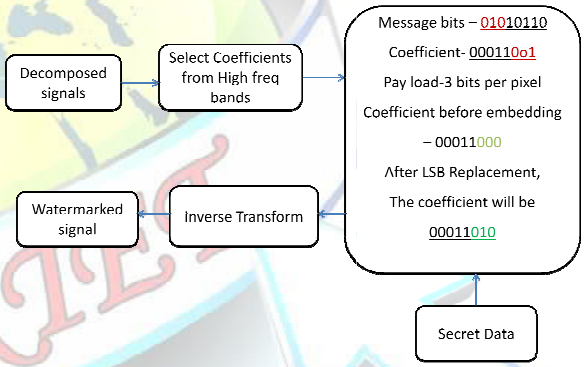


Fig. 4 Block diagram for the algorithm flow of least significant bit insertion.

The idea behind the LSB algorithm is to insert the bits of the hidden message into the least significant bits of the pixels.

Stage 4: Inverse wavelet re-composition

In this stage, the resultant watermarked 32 sub-bands are recomposed using inverse wavelet packet re-composition. The result of this operation is the new watermarked ECG signal. The inverse wavelet process will convert the signal to the time domain instead of combined time and frequency domain.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

Therefore, the newly reconstructed watermarked ECG signal will be very similar to the original unwatermarked ECG signal. The algorithm starts by initializing the required variables. Next, the coefficient matrix will be shifted and scaled to ensure that all coefficients values are integers. Then, the algorithm will select a node out of 32 nodes in each row of the coefficient matrix. The selection process is based on the value read from the scrambling matrix and the key. The algorithm will be repeated until the end of the coefficient matrix is reached. Finally, the coefficient matrix will be shifted again and re-scaled to return its original range and inverse wavelet transform is applied to produce the watermarked ECG signal.

Stage 5: Watermark extraction process

To extract the secret bits from the watermarked ECG signal, the following information is required at the receiver side.

1) The shared key value
2) Scrambling matrix
3) Steganography levels vector

The first step is to apply 5-level wavelet packet decomposition to generate the 32 sub-bands signals. Next, using the shared key and scrambling matrix the extraction operation starts extracting the secret bits in the correct order according to the sequence rows fetched from the scrambling matrix. Finally, the extracted secret bits are decrypted using the same shared key. The watermark extraction process is almost similar to the watermarking embedding process except that instead of changing the bits of the selected node, it is required to read values of the bits in the selected nodes, and then resetting them to zero.

IV. SECURITY ANALYSIS

The security of the proposed algorithm is mainly based on the idea of having several parameters shared between the transmitter and the receiver entities. Any change in any parameter will lead to extraction of wrong data. Accordingly, The receiver and transmitter should agree on the following information:

1) The scrambling matrix
2) The encryption key (ASCII text string) i.e shared secret.
3) steganography levels vector

As a result, even if the key is stolen the attacker will require to know the scrambling matrix as well as the steganography levels vector. The scrambling matrix is stored inside the transmitter/receiver pair and it will not be transmitted under any circumstance. For example, each patient could have his own device from his medical service provider and the matrix is burnt on this device. Therefore, for each pair of transmitter and receiver, it must be a unique scrambling matrix.

On the other hand, the sequence of rows fetched from the scrambling matrix is totally related to the user defined key. As a result, the longer the key is, the stronger the steganographic technique will be. To guarantee the maximum security the length of the key used (Lkey) should satisfy the following condition stated

$$Lkey = Max[(B/180), M] \quad \text{-----(2)}$$

Where B is the size of the embedded data in bits. and M represents the minimum key size. Accordingly, Table I shows the probabilities to break the proposed technique using different key lengths and the minimum data size that can be hidden to achieve the maximum security for each key length.

The amount of data that can be stored inside the ECG host signal using the proposed model totally depends on the steganography levels vector. In our proposed model and for ECG with 10 seconds length and sampling rate of 360 a 2531 bytes (2.4KB) of data can be embedded inside ECG host signal.

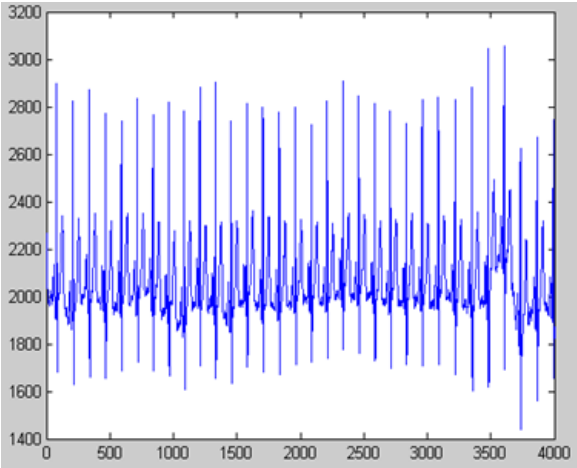
V. EXPERIMENTS AND RESULTS

To verify the proposed method, it is tested on medical signals. 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. Results have been obtained by using the same scrambling matrix. To generalize our results we

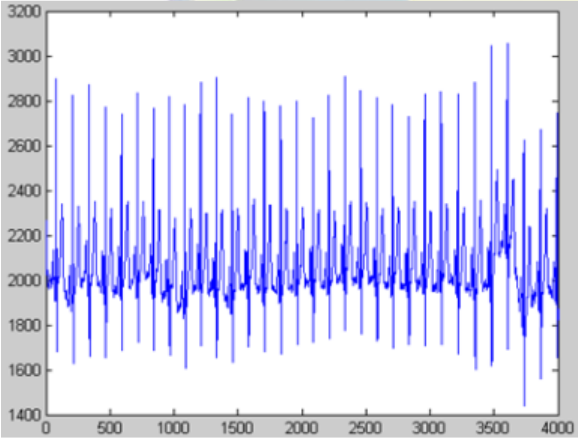
ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

performed the same experiments and calculated the average PRD values for different cases of scrambling matrices.

Input signal



Watermarked signal



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.

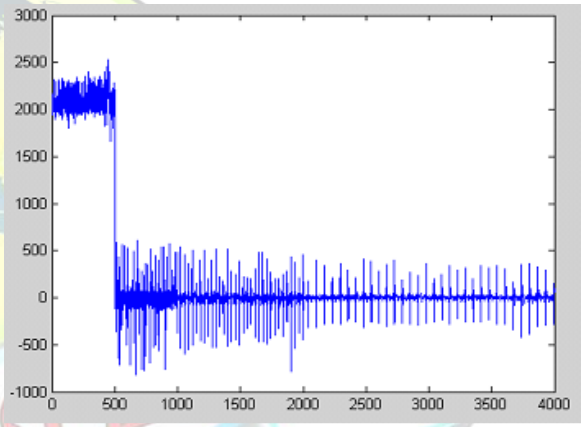
$$PRD = sqrt(sum((x - y).^2)/sum(x)) \quad ----(3)$$

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 is used.

$$BER = (Berr/Btotal) \times 100\% \quad -----(4)$$

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.

Multilevel Wavelet Decomposition



It is obvious 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. This encouraging result clearly demonstrates that the watermarked ECG signals can be used for diagnoses. ECG signal types, and the resultant watermarked signals before and after watermark extraction process. Previous results have been obtained by using the same scrambling matrix.

VI. CONCLUSION

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 wavelet decomposition is applied. A scrambling matrix is used to find the correct

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 2, March 2016

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. It is found that the resultant watermarked ECG can be used for diagnoses and the hidden data can be totally extracted.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[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*. ACM, 2007, p. 12.

[6] Christo Ananth, R.Nikitha, C.K.Sankavi, H.Mehnaz, N.Rajalakshmi, "High Resolution Image Reconstruction with Smart Camera Network", International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Issue 4,July 2015, pp:1-5

[7] 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.

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

[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] 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.

[11] 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.

[12] 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.

[13] 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*, vol. 1, 2008.

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

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

[16] 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.