Curvelet-based ECG steganography for protection of patient data

[1]Ms.Vishakha M. Patil, [2]Prof. Mrs. M. V. Patil
[1]Mtech Student, [2]Prof of BVUCOEP
[1,2]Electronics Department, Bharati Vidyapeeth Deemed University College of Engineering, Pune, India

***Abstract*—The Steganography is to hiding secret information in different texts. Now a day's various hiding techniques such as Image, Video, and Audio and ECG steganography are developed. This paper has concise review of various steganography techniques. The comparison of different techniques has been done on the basis of Peak Signal to Noise Ratio (PSNR), mean square error (MSC), bit error rate (BER), Percentage Residual Difference (PRD), Kullback-Leibler (KL), TICK TIME, etc.**

***Index Terms*— Electrocardiogram (ECG), Wavelet, steganography, Watermarking, Cryptography, Contourlet, SLT etc.**

I. INTRODUCTION

Steganography: The Johannes Trithemius has developed steganographia in 1499.Stegnography is the hiding of a secret information in image, audio and video etc. This secret information is extracted by using different techniques. Fig 1 shows the basic process of steganography.

ECG steganography: The patient data has embedded in the ECG signals called as ECG steganography. The number of ECG signals has collected from patient body. The secret data is embedding in that ECG signal and that embedding signal is transmitted to medical cloud through internet. The extraction of secret data without loss and inability is the major challenge to steganography by using ECG signal.

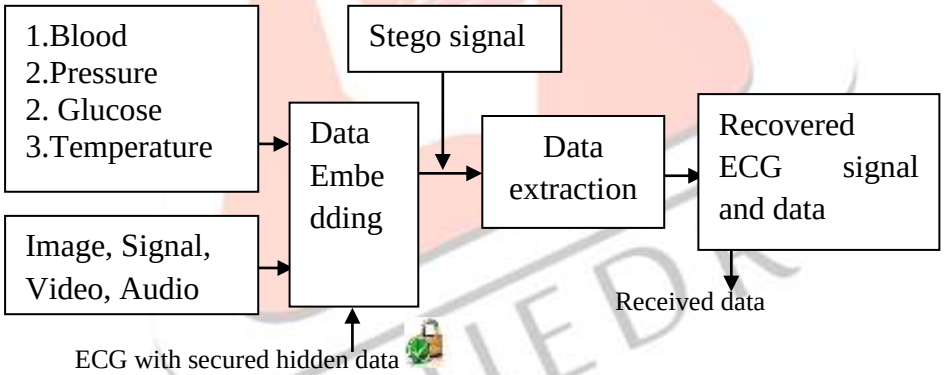


Fig 1: Basic process of steganography.

Received data:(Patient Confidential information Name: X.Y.Z, Date of Birth: 15/6/1994, Address: Pune, Medicare Number: 9890124814, Telephone Number: 1234567 ,Patient Diagnoses information 1. Blood Pressure.2. Temperature. 3. Glucose Level. 4.Patient biometric information).

In steganography the decomposion of cover signal into various frequency bands that can be achieved by discrete wavelet transform (DWT). Coefficients are evaluated by any transform and hiding secret information in those coefficients is called as watermarking. The Least Significant Bit (LSB) and quantization techniques are used in watermarking technique. The inverse of this transform is used to modify the results. Therefore, this technique does not representing curved edges because of limitations. The new curvelet transform is providing solution on that limitation.

The Data embedded using Pixel Difference Expansion, Bit Modification Technique and RSA encryption algorithm have major drawbacks of low data hiding capacity and more distortion due to hiding process. It may degrade the signal quality. These problems are covered by using curvelet based ECG steganography. Sometimes there is problem occur in extraction of patient data and original signal. Therefore the imperceptibility of the watermark and extraction calculates the performance of any steganography method. This evaluates the performance of curvelet based ECG steganography.

The time domain is first technique to provide lower data hiding capacity with improved performance. For increasing the algorithm safety this technology is depends upon transforming the ECG signal to a special time domain. Then LSB embedding is applied for hiding the secret message in transformed special domain ECG. Lastly, the embedded ECG signal is extracted to its original form. The frequency domain is second technique to provide improved data hiding capacity with lower performance. Cryptography and steganography techniques are combined in frequency domain technique. Firstly, steganography techniques are

used for hiding the patient secret information inside patient biomedical signal such as ECG signal. The patient ECG signal is taken as the host signal in this technique. That host signal will store or hide the patient information such as glucose, temperature, blood pressure and position. Always remember other information size is smaller than the ECG signal size.

II. LITERATURE REVIEW

In the past few years, various ECG steganography techniques have been proposed. The numbers of techniques are reviewed below.

Kozat et al. [1] presented an embedding and retrieving private metadata in electrocardiogram signal. In this technique, the patient data is replaced with the least significant bits of DWT coefficients of ECG signal.

Chen et al. [2] have generalized an idea of Watermarking. For data copyright and biological protection this technique is frequently used. They apply watermarking technique by using quantization on ECG for protection of secret data. The quantization based watermarking method is implemented by using three transform domains such as DCT, DWT and DFT. While the watermarks embed technology is not invertible, the very small change occurred between the amplitude and PQRST complex of ECG signal. Therefore the watermarked information can get together the necessities of physiological diagnostics

Edward et al. [3] have concluded that the DWT and DCT provide improved performance than DFT. The performance of this method is calculated by using PSNR, PRD and KL parameter. The BER is zero when size of the patient data is bigger but deteriorates the extracted signal. It is concluding that the patient information was increased 1.5 times then signal deterioration at 10 percent. Therefore the projected technique can be applicable for good steganography.

Candès .E [4] have proposed a new techniques by using two transforms, such as curvelet transform and the ridgelet transform. The wavelet based reconstruction exhibit lower perceptual quality than curvelet reconstruction, offer visually sharper images and advanced excellence improvement of edges and of faint-linear and curvi-linear feature. Obtainable assumptions for ridgelet and curvelet transforms advise that wavelet transform is not better for reconstruction of image.

Engin et al. [5] have compares the performance of DWT based ECG steganography with Daubechies 2 (db2) and biorthogonal wavelet functions where db2 performs better than biorthogonal wavelet. They recognized that the information was embedded in high frequency band. The result of that technique was better in performance than the other frequency bands.

To provide security to patient confidential data, there is no. of methods [6-8] the steganography technique proposed in these papers. Were, to protect confidential information of the patient it used medical image to stored secret information. The medical image can store how much data this is the challenging factors of this technique and up to which level this method is safe.

There are two techniques. The first technique is based on encryption and second technique is based on cryptographic algorithms. During the communication and storage these techniques is used to secure information. Since an outcome, the last encrypted message will be stored [9-12].

Rahul Mane1, Manish Sharma2 [13] have proposed a Contourlet transform (CT) and wavelet transform (WT) techniques of images steganography. These two techniques are used to compare the quality of embedded image. High performance steganograph extraction is meet when Embedding encrypted steganograph to high frequency sub-bands. They found that the levels of decomposition of steganographed image are rises then quality of extraction of message and original image is increased, also protect data from attackers. Contourlet transform provide multi-scale and multi-resolution expansion for images with smooth contour and rich in directional information. The directional filter bank is used in contourlet transform and gives shift invariant directional multi resolution. The improved enhancement result is achieved by SVD and contourlet transform.

Dhiah et al. [14] have proposed steganography technique and calculate some parameter such as PRD. In this method normal and abnormal ECG signals have PRD of customized watermarked ECG segment were extremely small. In PDA device the very simple mathematical equations is used for implementation. The secure key and signal pre processing parameter is known to receiver. Because of this the receiver will easily extract embedded data.

The Personal information security of a patient ECG is offered by ECG steganography through LSB embedding algorithm in transform domain using SLT described by Priti B. Patil1 and Prof .N. C. Patil [15] for diagnosability measurement, the embedded ECG has been evaluated using the metric MSE. LSB embedding gives less distortion in embedded ECG signal result shows that the improved similarity and diagnosis measurement of embedded ECG is possible in ECG steganography using slantlet transform.

III. METHODS OF ECG STEGANOGHRAPHY

The ECG steganography have the different methods for embedding data in ECG signal such as given below

3.1Watermarking: A watermarking of images by using wavelet histogram shifting proposed by H. Golpira and H. Danyali [16]. In this technique the host signal is medical images such as MRI. The two dimensional wavelet transform of the image is used to determine high frequency sub band histogram. In next step, 2thresholds are chosen, at the end of the last portion of the histogram and at the beginning. In this algorithm MRI images Performance is good but ECG host signals performance is not good. This algorithm has no encryption key and low capacity is involved in its watermarking process.

For protection of wireless communication S. Kauf and O. Farooq [17] have generalized an idea of digital watermarking technique of ECG signal. In this technique, each ECG sample is divided into segments and quantized using 10 bits. Due to such behavior override completely the concept of using stegnography. The original size of the host signal is does not raise this is the main purpose of stegnography.

3.2 Wavelet decomposition: Kaimei Zheng and Xu Qian. [18] Have generalized an idea of stegnography by using wavelet transform. The data hiding technique which is reversible and depending on wavelet transform. Also, this method does 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 signals were QRS complex be able to easily find.

3.3 Time domain steganography: Ayman Ibaida [19] have proposed ECG steganography by using wavelet transform and calculate security by using MSE parameter. The time domain steganography method is remove loss occurred in secrete information of patient in the host ECG signal. This secrete data is not hacked by attackers. In first step the negative values and integers which are meet by signal floating point numbers is avoided by applying the scaling and shifting. The wavelet decomposition has five levels which are applied here. The right embedding sequence depends on user secrete key and this key is find by using scrambling matrix. By using experimental methods the Steganography are determined for each sub bands. The diagnoses quality distortion is tested in this paper. They establish that the resulting watermarked ECG signal is able to use for diagnoses and all data is extracted completely.

3.4 Curvelet: Curvelet transform is to remove the limitations or drawbacks of wavelet transform and watermarking techniques. The curvelet transform uses multi scale frequency and time local portion also make use of the direction of features. Hence the curvelet transform is very efficient technique. The curvelet transform is divided into two types such as wrapping based fast Curvelet Transform and spaced Fast Fourier Transform. Ramu .P [20] have generalized an idea which is ECG steganography by using curvelet transform, a new threshold selection algorithm and adaptive selection of watermark location. The result of the watermark is calculated by using parameters such as PSNR, PRD and KL Also BER is used to calculate ability to extraction of patient. The results validate for watermarking coefficients around zero are ideal and this reduce deterioration and also reduces loss occurs in the data extraction.BER is zero when size of patient data is increased but deteriorates the cover signal. Therefore the proposed technique is reliable steganography. The table 1 shows the summary of steganography techniques.

IV. Parameter Evaluation

Curvelet algorithm for ECG steganography is evaluated by parameters such as PSNR, BER, PRD and KL.

4.1 Peak Signal to Noise Ratio: PSNR is the ratio of maximum value of the extracted ECG signal to the mean squared deviation of original and embedding ECG signal. The quality is improved when value of PSNR is higher.

$$PSNR = 20log10 = \frac{\max[xc]}{\sqrt{\frac{1}{N}\text{Nn=1}[xc-xw]^2}} \quad (1)$$

4.2 Percentage Residual Difference: PRD is the dissimilarity of the normal, abnormal ECG signal and embedding ECG signal. If this dissimilarity is increases linearly at that time PRD increases linearly.

$$PRD\% = \sqrt{\frac{\sum_{i=1}^{N}(Xc-Xw)^2}{\sum_{i=1}^{N}(Xc)^2}} \times 100 \quad (2)$$

4.3 Bit error rate: It is the ratio between the number of bits extracted at receiver and the total number of bits. This measures the information loss. Increase in data loss at that time BER increases.

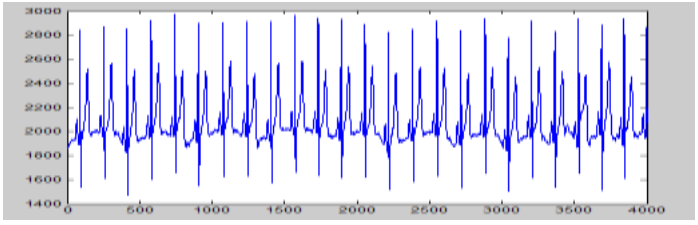
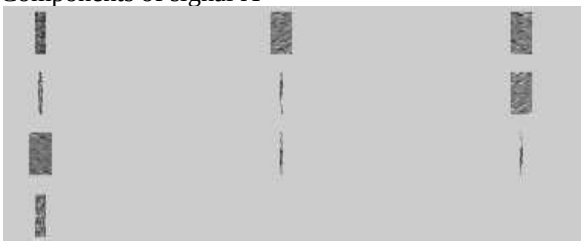
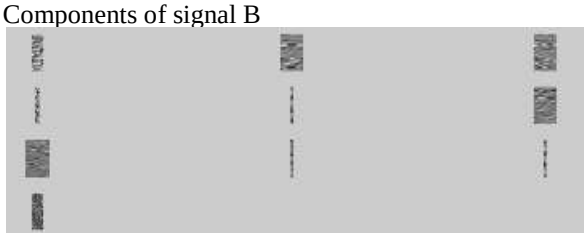
$$\text{BER} = \frac{\text{No of Bits extracted}}{\text{Total no of Bits}} \times 100 \quad (3)$$

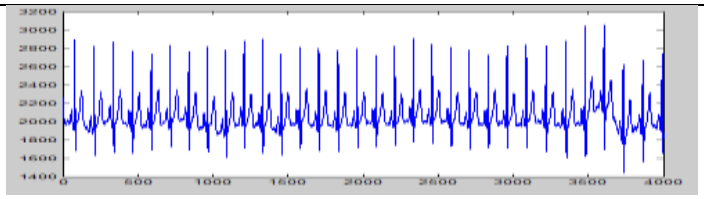
4.4 Kullback-Leibler: this measure the distance between the watermarked signals and the histograms of the cover signal.

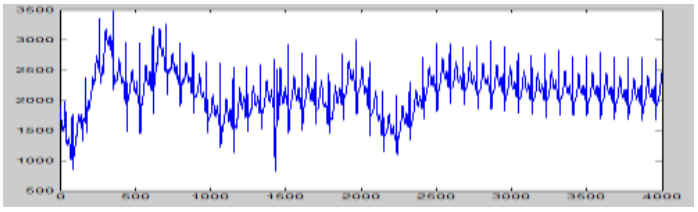
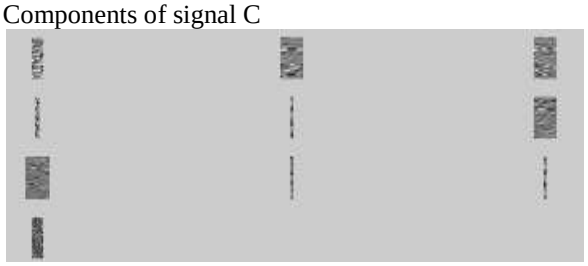
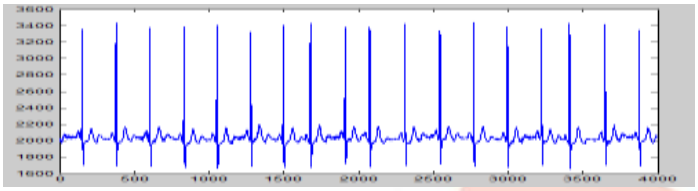
V. Mini Result

The ECG signal is taken from patient body then apply curvelet transform on that signal. The below table 1 shows the mini result of our technique.

Table 1: Components of ECG signal

ECG A 	Components of signal A 
ECGB	Components of signal B 



ECGC	Components of signal C
	
ECG D	Components of signal D
	

VI. Conclusion

From the literature review, it is clear that the curvelet based ECG steganography is good approach for protection of data. This review has introduced a variety of steganography technique for ECG signal in time domain as well as frequency domain. It reviews the applications of ECG stenography in detail. The various encryption methods, but LSB based technique is power full technique as it gives data rate of hiding. Frequency domain watermarking technique using DWT gives more robustness against signal processing attacks as compare to the time domain methods. This DWT based method provide higher bit rate. Using this literature review, the further research can be carried out to improve the robustness of transform based techniques against synchronous attacks.

VII. Acknowledgment

I am greatly pleased to proof: M V Patil who guided me through my project curvelet based ECG steganography for protection of data.

REFERENCES

[1] S. S. Kozat, M. Vlachos, C. Lucchese, H. Van Herle, and P. S. Yu, "Embedding and retrieving private metadata in electrocardiograms," J.Med. Syst., vol. 33, no. 4, pp. 241–259, 2009.
[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] S. Edward Jero, P. Ramu, and S. Ramakrishnan, "Discrete Wavelet Transform and Singular Value Decomposition Based ECG Steganography for Secured Patient Information Transmission," J.Med. Syst., vol. 38, 2014.
[4] Candès .E, Demanet L, Donoho .D, and Ying .L, "Fast discrete curvelet transforms," Multi scale Model Simul5, pp. 861–899, 2006, doi: 10.1137/05064182x.
[5] M. Engin, O. Çidam, and E. Z. Engin, "Wavelet transformation based watermarking technique for human Electrocardiogram (ECG)," J.Med. Syst., vol. 29, no. 6, pp. 589–594, 2005.
[6] 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.
[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] 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.

[9] Maglogiannis, L. Kazatzopoulos, K. Delakouridis, and S. Hadjiefthymiades, "Enabling location privacy and medical data encryption in patient tele-monitoring systems," IEEE Transactions on Information Technology in Biomedicine, vol.13, no.6 pp.946–954, 2009.
[10] 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.
[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] 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,, vol.11, no.6, pp.619–627, 2007.
[13] Rahul Mane1, Manish Sharma2, "Adaptive contourlet transform and wavelet transform based image stegnography using SVD on ECG signal," ISSN: 2320-8163, vol 3, no 3, pp. 294-297, (May-June 2015).
[14] AymanIbaida, Ibrahim Khalil and Dhiah Al-Shammary, "Embedding Patients Confidential Data in ECG Signal for HealthCare Information Systems," 32nd Annual International Conference of the IEEE EMBS Buenos Aires, Argentina, August 31 - September 4, 2010.
[15] Priti B. Patil1 and Prof. N. C. Patil, "SLT based ECG Signal Steganography for Telemedicine Application," vol 03, no.06,June-2016.
[16] 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), pp 31–36, 2010.
[17] 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, pp.140-144, 2010.
[18] K. Zheng and X. Qian, "Reversible Data Hiding for Electrocardiogram Signal Based on Wavelet Transforms," In international conference on computational intelligence and security, vol.1, 2008.
[19] Ibaida .A and Khalil. I, "Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems," IEEE Trans. Biomed. Eng. vol. 60, no.12, pp. 3322–3330, doi: 10.1109/ tbme.2013.2264539.
[20] Jero, Edward., Ramu, Palaniappan., Ramakrishnan, S. :ECG steganography using curvelet transforms, Biomedical Signal Processing and Control 22. doi: 10.1049/el.2015.3218, pp. 161–169.


IJEDR