IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 11, November 2015.
www.ijiset.com
ISSN 2348 – 7968

ECG Steganography based Privacy Protection of Medical Data Utilizing Chaos Encryption.

Gayatri M. Vengurlekar [1] S. K. Bhatia[2]

[1] Department of E & Tc & S. P. Pune University, India,
[2] Department of E & Tc & S. P. Pune University, India

Abstract

In this paper the enhancement of protection system for secret data communication through encrypted data concealment in ECG signals is proposed. The proposed encryption technique encrypts the confidential data in to unreadable format 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 secret data is concealed into the ECG signal coefficients. Although encryption achieves certain security effects, they make the secret messages unreadable and 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 sub-bands. 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.

Keywords: Intruder, physiological readings, Steganography data extraction, Wavelet Decomposition

1. Introduction

Here, a security technique with ECG is proposed to guarantee secure transmission of patient confidential information combined with patient physiological readings from body sensors. This technique is based on using steganography techniques to hide patient confidential information inside biomedical signal. Moreover, the proposed technique uses encryption based model to allow only the authorized persons to extract the hidden data.

In this paper, the ECG signal is used as the host signal that will carry the patient secret information as well as other readings from other sensors such as temperature, glucose, position, and blood pressure.
The Electrocardiogram (ECG) signal is used here due to the fact that most of the healthcare systems will collect ECG information. Moreover, the size of the ECG signal is large compared to the size of other information. 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 and 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. The proposed steganography technique has been designed in such a way that guarantees minimum acceptable distortion in the ECG signal, Furthermore, it will provide the highest security that can be achieved. The use of this technique will slightly affect the quality of ECG signal.

2. Literature Review

Over years several works have been introduced for the Steganography using biomedical signal. H. Golpira and H. Danyali [4] proposed a reversible blind watermarking for medical images based on wavelet histogram shifting. In this work medical image such as MRI is used as host signal. Kai-mei Zheng and Xu Qian [5] 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.

There are several researches present on Steganography in the literature. All the methods in literature are with some drawbacks such as low capacity, security issues. Due to that we go for the proposed method that is ECG steganography based privacy protection of medical data for telemedicine application using chaos encryption. In this Patient's details are encrypted using chaos encryption and then encrypted data is embedded in to ECG signal using LSB technique.

ISSN 2348 – 7968

3. Methodology

The proposed encryption process used to encrypt the personal information into unreadable form and no longer accessible enhances the safety of secret message by making the information inaccessible to any intruder having a random system. After information encryption, the information hider will conceal the secret information into the ECG signal coefficients. While encryption completes distinctive safety effects, they create the key messages in unreadable and unnatural or meaningless form. The proposed system has five Stages: 1) Encryption 2) Wavelet Decomposition 3) The Embedding Operation 4) Inverse Wavelet recomposition 5) Watermark Extraction Process In the literature survey many algorithms were developed for Steganography. But they have drawbacks such as low capacity, security issues.

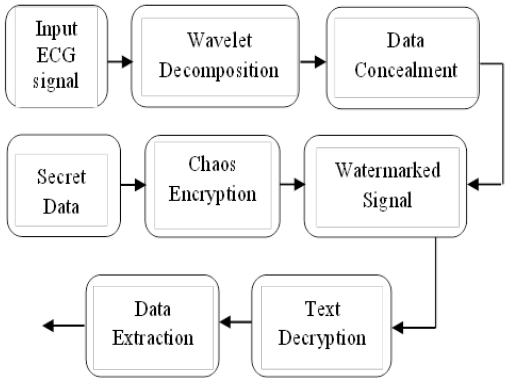

Fig. 1 Process to perform stegnography using Chaos Encryption

3.1 Encryption

Patient information contains Patient name, Age, Medicare no., medical readings corresponding to Glucose level, cholesterol etc. The aim of this stage is to encrypt the patient confidential information in such a way that prevents unauthorized persons who does not have the shared key from accessing patient confidential data. In this stage chaos encryption technique is used which will play the role of the security key. Chaos encryption is selected because of its simplicity. As a result, this ciphering can be easily implemented inside a mobile device.

The broad chaos encryption method is the simplest technique to encrypt data or message by chaotic equation. This method can facilitate to discover some essential information and establish the crucial stage of security. Chaos encryption technique encrypts the original text data with encryption key value generated from chaotic sequence with threshold function by bit XOR operation. Chaotic sequence is generated by using following Eq.

$$f(x) = \mu * x\,(1-x) \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (3.1)$$

Where, $x \in (0, 1)$ and $3.569 < \mu < 4.0$ initial value x_0 and μ can be adapted as a system key [7].

3.2 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. In most applications discrete signals are used. Therefore, Discrete Wavelet Transform (DWT) must be used instead of continuous wavelet transform. DWT 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.

3.3 The embedding operation

At this stage the proposed technique will use a special security implementation to ensure high data security. 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.

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

3.4 Inverse Wavelet re-composition

In this final stage, the resultant watermarked 32 sub-bands are recomposed using inverse wavelet packet recomposition.

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. Therefore, the newly reconstructed watermarked ECG signal will be very similar to the original unwatermarked ECG signal.

ISSN 2348 – 7968

3.5 Watermark Extraction Process

The Watermark Extraction process is as shown in following fig. For this stage newly reconstructed watermarked ECG signal obtained from previous stage is used as input. Data is extracted from this newly reconstructed watermarked ECG signal. After extracting data , it is cecrypted using Chaos Decryption.

4. Results

In this work, a steganography algorithm using Chaos Encryption and LSB embedding technique is utilized to hide patient's information inside ECG signal using MATLAB software. Here results obtained by using XOR cyphering method for patient's information encryption and by using Chaos encryption method for patient's information encryption are compared. Here host signal that is ECG signal is taken as input signal to hide the patient's confidential data. Proposed method is tested over 25 ECG signal samples [32] for experimentation. Each ECG signal have frequency range of 0.01 – 100 Hz and its amplitude range is 0.05 – 3 mV. To evaluate the proposed model, the PRD (Percentage Residual Difference), RMSE (Root Mean Square Error), PSNR (Peak Signal to Noise Ratio) and CC (Correlation Coefficient) is used. Experimental results tested over 25 ECG signal samples are presented in following tables.

4.1 Percentage Residual Difference

The PRD is frequently employed distortion measure that quantifies the error between the original ECG host signal and the resulting watermarked ECG signal PRD is calculated by using following Eq.

$$PRD = \sqrt{\frac{\sum_{i=1}^{N}(x_i - y_i)^2}{\sum_{i=1}^{N} x_i^2}} \quad \text{..... (5.1)}$$

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

4.2 Root Mean Square Error

The root-mean-square error (RMSE) or root-mean-square deviation (RMSD) or is a frequently used measure of the differences between values predicted by a model or an estimator and the values actually observed. The RMSE represents the sample standard deviation of the differences between predicted values and observed values. These individual differences are called residuals when the calculations are performed over the data sample that was used for estimation, and are called prediction errors when computed out-of-sample.

Here RMSE is used to calculate error between the original ECG signal and the resulting newly constructed watermarked ECG signal. RMSE is calculated by using following Eq.

$$RMSE = \sqrt{\frac{1}{n}\sum_{j=1}^{n}(x_j - y_j)^2} \quad \text{..... (4.2)}$$

Where *x* represents the input signal and *y* is the watermarked signal. '*n*' represents length of the text.

4.3 Peak Signal to Noise Ratio

PSNR is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale.

PSNR shows the peak signal to noise ratio of watermarked signal. It is used to determine quality of the watermarked signal. PSNR can be calculated using following Eq.

$$PSNR = 10 log_{10} \frac{x^2}{RMSE} \quad \text{..... (4.3)}$$

Where *x* represents input ECG signal.

4.4Correlation Coefficient

The correlation coefficient is usually given the symbol *r* and it ranges from -1 to +1. A correlation coefficient quite close to 0, but either positive or negative implies little or no relationship between the two variables .Here CC indicates similarity between the original ECG input signal and the resulting newly constructed watermarked ECG signal.

$$CC = \frac{n\sum x_i y_i - \sum x_i y_i}{\sqrt{n\sum x_i^2 - \sum x_i^2 \times \sqrt{n\sum y_i^2 - \sum y_i^2}}} \quad \text{..... (4.4)}$$

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

Here Table I and Table II shows Results obtained by using XOR cyphering method for patient's information encryption and results obtained by using Chaos encryption method for patient's information encryption respectively without addition of white noise to watermarked signal.

ISSN 2348 – 7968

Table I Results obtained by using XOR cyphering method for patient's information encryption

ECG Signal Sample	PRD	WWPRD	RMSE	PSNR(dB)	CC
1	3.8226	0.4104	1.9416	44.1620	0.9993
2	3.8629	0.4277	1.8714	43.0789	0.9992
3	3.1802	0.3732	1.8398	42.2131	0.9995
4	2.8325	0.3340	1.8580	42.8387	0.9996
5	3.4518	0.3838	1.9525	42.8502	0.9994
6	2.4887	0.3274	1.9143	44.5501	0.9993
7	2.2191	0.3795	1.9431	46.2727	0.9997
8	3.7245	0.4046	1.9176	41.2004	0.9993
9	3.0079	0.4361	1.9401	43.6894	0.9995
10	2.1167	0.2432	1.9393	46.2204	0.9998
11	1.9590	0.2416	2.0520	46.8974	0.9998
12	4.1439	0.3334	1.9081	43.7615	0.9991
13	2.4721	0.3151	1.8820	42.1639	0.9994
14	1.8510	0.2438	2.0317	44.9148	0.9998
15	1.9008	0.2140	1.8403	48.1828	0.9998

Table II Results obtained by using Chaos encryption method for patient's information encryption.

ECG Signal Sample	PRD	WWPRD	RMSE	PSNR(dB)	CC
1	2.0992	0.1275	1.0663	46.7650	0.9998
2	2.1539	0.1270	1.0435	45.6159	0.9998
3	1.4999	0.0864	0.9839	45.5998	0.9999
4	1.4249	0.0807	1.0057	49.1932	0.9999
5	1.0173	0.0520	1.0660	49.7435	0.9999
6	1.2433	0.0799	0.9466	45.1487	0.9999
7	1.0931	0.0868	0.9571	49.3481	0.9999
8	2.2394	0.1157	1.0467	43.0886	0.9997
9	1.5677	0.1098	0.9112	46.5194	0.9999
10	1.1380	0.0751	1.0423	48.7009	0.9999
11	1.3939	0.1051	1.0722	50.0675	0.9998
12	2.2347	0.1004	1.0290	46.4435	0.9998
13	1.2433	0.0799	0.9466	45.1487	0.9999
14	0.9368	0.0523	1.0283	47.8724	0.9999
15	1.0777	0.0530	1.0434	50.6472	0.9999

ISSN 2348 – 7968

5. Conclusion

The project presented the privacy data protection of patients through Stego analysis approach for telemedicine application. Here the cover medium was chosen as an ECG signal and this system was concentrated on preserving signal quality during text message concealment. Chaos crypto system was utilized to encrypt the text before hiding into the signal. The simulated results was generated the watermarked signal with least error which measured through percentage residual difference. This protection system will be enhanced to utilize these techniques for two dimensional signals for secret data communication.

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 tele cardiology sensor networks: toward a low-cost portable wireless hardware/ software code sign," *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] 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.
[5] 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.
[6] 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.
[7] H Xiping, Zhu Qingsheng. Chaos-based algorithm for Encryption in Wavelet Domain [J], Computer Applications, 2007, 27(8): 1895-1900.
[8] Miss. Gayatri M. Vengurlekar and Dr. S. L. Lahudkar "Encryption of Patient's Details using Chaos Encryption", International Journal of Computer Informatics & Technological Engineering, Volume 2, Issue 6, June 2015.

Miss .Gayatri Manohar Vengurlekar, received her B.E degree from Mumbai University, in 2013. This author is persuing M.E degree in Signal Processing in Pune University