International Journal of Scientific & Technical Development
(A Peer-Reviewed Bi-Annual Journal) ISSN: 2348-4047

Medical Data Security and ECG Steganography: Issues and Challenges

Butta Singh, Himali Sarangal and Manjit Singh
Guru Nanak Dev University, Regional Campus, Jalandhar
Corresponding Author Email ID: bsl.khana@gmail.com

Abstract

It becomes utmost important that the patient confidentiality is ensured while medical data is being sent over the public networks as well as when it is stored in the healthcare repository used by a remote monitoring system. ECG monitoring facilitates in providing accelerated health status of the concerned patient to the healthcare centre in case of the hostile cardiac behaviour. Transmission of this compressed ECG via a communication channel introduces various security and privacy issues [5]. To counteract with these concerns, there is a need for implementation of efficient security protocols. To this effect, several algorithms have been developed in the past two to three decades. The patient's confidential data hiding through watermarking and the ECG encryption techniques are the emerging biometric security mechanisms. This paper attempts to explore the state of the are approaches developed for ECG encryption and steganography.

Keywords: ECG; Steganography; Encryption; Medical Data

Introduction

In the modern era, cardiovascular diseases had emerged as one of the essential causes of mortality in both urban and rural areas [1], [2]. ECG monitoring facilitates in providing accelerated health status of the concerned patient to the healthcare centre in case of the hostile cardiac behaviour [4]. Cardiac monitoring using ECG signal is the best representative of heart's electrical functionality and had proven to be useful in the diagnosis of most of the heart diseases. Transmission of this compressed ECG via a communication channel introduces various security and privacy issues [3]. To counteract with these concerns, there is a need for implementation of efficient security protocols. To this effect, several algorithms have been developed in the past two to three decades [4].

It becomes utmost important that the patient confidentiality is ensured while data is being sent over the public networks as well as when it is stored in the healthcare repository used by a remote monitoring systems [5]. The information sent over the public network or the internet should be highly protected and secured [5], [6]. The techniques used for data ciphering are based on encryption and cryptographic algorithms. After, the process of encryption healthcare centre receives the encrypted ECG data which can be de-encrypted using either the symmetric or asymmetric keys which ensures the higher end-to-end security, when applied to e-health monitoring system [7].

To simultaneously protect the biometric credentials of the patient and to ensure reliable diagnosis of ECG, hybrid approaches that incorporates both the confidential patient data hiding as well as encryption continue to advance in literature. The confidential patient data includes information like Patient Reference ID, Name, Sex, Age, Case History, Temperature, Blood Pressure, Concern Doctor, Prescription etc.

2. ECG DATA SECURITY TECHNIQUES

The patient's confidential data hiding through watermarking and the ECG encryption techniques are the emerging biometric security mechanisms. The ECG encapsulates the sensitive information about the cardiovascular state of patient's ECG. Transmitting it without encryption makes it vulnerable to spoof attack and also is against the HIPAA regulations. So to prevent the imposters from capturing the ECG segments and gaining the unauthorized access to the secured facilities, the segments needed to be efficiently encrypted.

Ayman and Ibrahim [5] proposed a wavelet-based steganography technique which combines encryption and scrambling technique to defend confidential patient data. The proposed method allows ECG signal to hide its corresponding patient private data and other physiological information thus guaranteeing the integration between ECG and the rest.

Lu et al. [8] presented an effective scheme to protect patients personal privacy for a medical information system. In the scheme, personal data was encrypted before being stored in the database of the server of a medical information system, so that even if server information was disclosed, data be difficult to be decrypted and interpreted. Han et al. [39] proposed the use of multi scroll chaos to encrypt the ECG packets. The encryption was achieved by XORing the ECG packet with the chaos key generated from chaos generator server. The devised approach proved to be 18 times faster than permutation based ECG encoding, 25 times faster than wavelet-based ECG and 31 times faster than noise based ECG data ciphering technique.

Khalil et al. [9] devised a specialized permutation based ECG encryption technique. The permutation key is only known to the authorized personnel, who can decrypt the ECG from encrypted ECG. The original ECG can be transformed into fully encoded ECG (in the form of scrambled ASCII letters). When combined with existing encryption schemes, the strength can be further raised thus providing unmatched protection against spoof attacks.

Sufi et al. [10] proposed an efficient ECG obfuscation method which involved detection of P, QRS complex and T wave feature from ECG and then replacing them with their noisy versions. The advantage of the proposed approach over existing encryption method was that the corrupted ECG appears as regular ECG though it is encrypted ECG. The limitation of using this method was that the overall ECG data size increased by 0.9% by the addition of the key for decryption.

Zhou et al. [11] used quantization-based digital watermark encryption technology on the ECG to protect patient rights and information. The patient's confidential data, e.g., name, age, and ID, etc. are collected and treated as a watermark for medical data. They concluded that after testing with ten selected data sets from the MIT-BIH arrhythmia database, the difference between the watermarked ECG and the original one is very small and negligible for physiological diagnostics.

Murillo-Escobar et al. [12] proposed a symmetric encryption algorithm based on logistic map with double chaotic layer encryption in diffusion process and just one round of confusion-diffusion for the confidentiality and privacy of clinical information such as ECG, Electroencephalograms (EEG), and Blood Pressure (BP) for applications in telemedicine. The achieved information entropy is 7.96 for 8-bit quantization.

Raeiatibanadkooki et al. [13] designed a mechanism for encrypting the ECG signal. The sequence of steps followed for preprocessing were the removal of the baseline noise, peak detection, and determination of heart rate. Huffman coding with chaos accomplishes the ECG signal encryption.

A steganography approach based on Discrete Wavelet Transform (DWT) and SVD was developed by Jero et al. [14]. DWT was used to decompose the signal and SVD was employed to embed the secret information into the signal. Experimenting with 76,800 ECG samples from MIT-BIH arrhythmia database with secret data size equal to 350 bytes, the reported values of Peak Signal to Noise Ratio (PSNR), PRD, and Kulback-Leibler Divergence (KL-Div) were equal to 69.13, 0.0687, and 6.84×10-5. The designed method resulted in an overall signal degradation of 0.6%. The approach is very sensitive to the selection of mother wavelet and provides low embedding rate. Another Transformed-domain quantization based scheme for ECG steganography was proposed in [11]. 4096 ECG samples from MIT-BIH arrhythmia database has been selected for experimentation. The achieved amplitude similarity, Relative Root Mean Square Error (rRMSE), and amplitude Root Mean Square Error (RMS) were equal to 99.96, 0.153, and 22.847 for ECG record 103 for a secret data size of 32 bits. Later in the year 2015, authors in [14] explored fast discrete curvelet transform with adaptive thresholding for ECG Steganography. After experimenting on 128 trains of ECG from MIT-BIH Normal Sinus Rhythm (NSR), the obtained values were 43.44, 0.0132, and 0.1448 for the PSNR, PRD, and KL Distance at the payload equal to 502 bytes. Every 1.5 times increase in the patient confidential data, the ECG signal deterioration increases by 10 %. Same research group proposed a Continuous Ant Colony Optimization (CACO) algorithm based ECG steganography scheme using DWT and SVD [48]. The PSNR, PRD, and KL-Div values for a secret data size of 21 Kb were 34.46, 0.06, and 2.04 for Normal Sinus Rhythm (NSR) dataset. The parameter selection for the CACO was computationally expensive while extending the proposed method to other signals. Yang and Wang [49] validated their lossy and the reversible ECG steganography technique on MIT-BIH arrhythmia database. Investigations on Lead II ECG signals resulted in average values of SNR, and mean absolute error equal to 56.34, and 0.90 at a payload equal to 7500 bits.

3. PERFORMANCE EVALUATION METRICS

The performance evaluation metrics are broadly divided into the categories of ECG compression, encryption, and the transmission. The brief description is given as under:

3.1 ECG Data Compression

The performance evaluation metrics for ECG compression include CR, PRD, Percentage Root Mean Square Difference with Base Removed (PRD1024), Percentage Root Mean Square Difference Normalized (PRDN), RMS Error, SNR, Quality Scores (QS, QS1024, QSN), Wavelet-based Weighted Percentage Root Mean Square Difference (WWPRD) and Wavelet Energy Based Diagnostic Distortion (WEDD).

3.2 ECG Data Security

The performance evaluation analysis for ECG stenography includes reconstructed ECG security and sensitivity analysis, Bit Error Rate for Secret data (BERs), Embedding Score (ES). Evaluation analysis for ECG encryption includes Histogram analysis, Entropy analysis, Correlation analysis.

3.3 ECG Transmission

The performance evaluation analysis for processed ECG transmission and reception includes Channel Signal to Noise Ratio: SNRc and Bit Error Rate due to Channel and receiver: BERc.

4. CONCLUSION

Most of the approaches mentioned above lack a suitable trade-off between the attributes of higher secret data security, reversibility of secret data, lower degradation of stego-ECG signal and higher Embedding Capacity (EC). Increasing EC often leads to higher degradation of stego-ECG signal. ECG steganography causes irreversible degradation to stego-ECG as compared to the cover ECG signal. Many approaches have been devised for ECG data encryption, yet the previously reported works did not focus on the issues of simultaneously processing the patient confidential data in ciphered version and ECG signal in the encrypted version.

REFERENCES

[1] M. Nichols, N. Townsend, P. Scarborough, and M. Rayner, “Cardiovascular disease in Europe: Epidemiological update,” Eur. Heart J., vol. 35, no. 42, pp. 3028–3034, 2014.

[2] S. Gupta, R. Gudapati, K. Gaurav, and M. Bhise, “Emerging risk factors for cardiovascular diseases: Indian context,” Indian J. Endocrinol. Metab., vol. 17, no. 5, pp. 806–814, 2013.

[3] S. S. Mahmoud, Q. Fang, Z. M. Hussain, and I. Cosic, “A blind equalization algorithm for biological signals transmission,” Digit. Signal Process. A Rev. J., vol. 22, no. 1, pp. 114–123, 2012.

[4] A. Ibaida, D. Al-Shammary, and I. Khalil, “Cloud enabled fractal based ECG compression in wireless body sensor networks,” Futur. Gener. Comput. Syst., vol. 35, pp. 91–101, 2014.

[5] A. Ibaida and I. Khalil, “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, 2013.

[6] W. B. Lee and C. D. Lee, “A cryptographic key management solution for HIPAA privacy/security regulations,” IEEE Trans. Inf. Technol. Biomed., vol. 12, no. 1, pp. 34–41, 2008.

[7] S. K. Chen, T. Kao, C. T. Chan, C. N. Huang, C. Y. Chiang, C. Y. Lai, T. H. Tung, and P. C. Wang, “A reliable transmission protocol for zigbee-based wireless patient monitoring,” IEEE Trans. Inf. Technol. Biomed., vol. 16, no. 1, pp. 6–16, 2012.

[8] C. Lu, Z. Wu, M. Liu, W. Chen, and J. Guo, “A patient privacy protection scheme for medical information system,” J. Med. Syst., vol. 37, no. 6, 2013.

[9] F. Sufi and I. Khalil, “Enforcing secured ECG transmission for realtime telemonitoring : A joint encoding , compression , encryption mechanism,” Secur. Comm. Networks, vol. 1, no. 5, pp. 389–405, 2008.

[10] F. Sufi and I. Khalil, “A new feature detection mechanism and its application in secured ECG transmission with noise masking,” J. Med. Syst., vol. 33, no. 2, pp. 121–132, 2009.

[11] S.-T. T. Chen, Y.-J. J. Guo, H.-N. N. Huang, W.-M. M. Kung, K.-K. K. Tseng, and S.-Y. Y. Tu, “Hiding patients confidential datainthe ECG signal viaa transform-domain quantization scheme,” J. Med. Syst., vol. 38, no. 6, p. 54, 2014.

[12] M. A. Murillo-Escobar, L. Cardoza-Avendaño, R. M. López-Gutiérrez, and C. Cruz-Hernández, “A double chaotic layer encryption algorithm for clinical signals in telemedicine,” J. Med. Syst., vol. 41, no. 4, pp. 1–17, 2017.

[13] M. Raeiatibanadkooki, S. R. ahati Quchani, M. M. KhalilZade, and K. Bahaadinbeigy, “Compression and encryption of ECG signal using wavelet and chaotically huffman code in telemedicine application,” J. Med. Syst., vol. 40, no. 3, p. 73, 2016.