REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 23, No. 3 (2022)
http://www.veterinaria.org
Article Received: July 2022; Revised: August 2022; Accepted: September 2022

An Integrated Approach for ECG Compression and Encryption in E-healthcare Systems

Neetika Soni[1]*, Vinit Grewal[2]

[1*,2]Department of Engineering and Technology, Guru Nanak Dev University, Regional Campus, Jalandhar, 144007, India. *neetikabhalla@gmail.com

ABSTRACT
The recent developments in tele-healthcare services has raised the concern over the management and security of biomedical data during its transmission and storage. This paper proposes an integrated approach of signal compression and encryption to resolve these issues. Signal compression is done using Adaptive Fourier Decomposition (AFD) technique that decompose the Electrocardiogram (ECG) signal in terms of adaptively selected Basis functions instead of fixed Basis functions used in other decomposition techniques. Further chaotic maps are employed to encrypt the AFD coefficients. The performance of the integrated approach is evaluated in terms of distortion parameters such as PRD, PSNR and SNR while Compression Ratio (CR) and Quality score are used to measure compression efficiency. The results show that the proposed technique is efficient as compared to the state of the art techniques.

Keywords: ECG Compression, Encryption, Adaptive Fourier Transform (AFD), Combined Chaotic Map CCM), Compression Ratio (CR), Quality Score(QS)

Introduction

The conventional healthcare systems has been upgraded to new remote e-healthcare systems where the well experienced doctors provide remote healthcare solutions to the patients without their physical interface. However, in case of continuous monitoring of remote patients, there needs to send a long term recordings to doctors which generates huge data that imposes a burden on the transmission channel and storage devices. Moreover communicating patients' information on public channels or storing it at hospital servers can be a threat to its security. To resolve these issues signal processing techniques such as compression and encryption have been proposed in this work. Electrocardiogram (ECG) which is considered as a primary signal for assessing cardiac functions, detecting other health ailments [1, 2] and a pre-requisite during surgeries [3] is marked as a prime signal in the e-healthcare paradigm. Therefore, in this work signal processing techniques are implemented on ECG signals.

Literature Review

Various significant approaches have been reported in literature that perform ECG compression in time domain, transform domain, or performed compression using feature extraction techniques. [4-9]. The time domain techniques are lossless and recover the complete signal correctly but they have very low compression ratio. The transform based techniques and feature detection approaches are lossy techniques where there is distortion in the recovered signal. But the compression ratio is significantly high. ECG encryption techniques are also reported in literature [10,11] to avoid any illicit access by eavesdroppers during transmission. These techniques addressed the issues of compression and encryption separately. This paper proposes a joint approach that will acknowledge the issues of huge data size and data security jointly.

Methods

In this work, two methods have been used to implement ECG compression and encryption. To compress ECG signal, Adaptive Fourier Decomposition (AFD) approach is used that decomposes the ECG signal into AFD coefficients. These AFD coefficients possess successively increasing non-negative analytic instantaneous frequencies [12,13]. AFD adaptively select the Basis functions from

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 23, No. 3 (2022)
http://www.veterinaria.org
Article Received: July 2022; Revised: August 2022; Accepted: September 2022

the rational orthogonal system, e.g. Takenaka-Malmaquist (TM) system in accordance with the input using Maximal Projection Principle (MPP) thus making it capable to reconstruct the high fidelity signal with few coefficients only.

Second method is the Random Sequence Generator to perform encryption. The random Sequence generator generate random sequences that are random like chaos yet deterministic. These sequences are highly sensitive to their initial conditions and control parameters. Amongst various existing mathematical functions that are capable to produce these random sequences, in this work 1D Combined Chaotic Map (CCM) [14,15] is used that exhibits random behaviour over wide range of initial and control parameters are employed.

Methodology

In this work, a novel integrated approach is proposed which is capable of performing two signal processing techniques; ECG compression and encryption. These techniques are essential for successful implementation of e-healthcare services. The proposed technique employs AFD to compress the ECG signal where ECG is initially divided into non-overlapping blocks of size L. AFD is then applied on the non-overlapping ECG blocks of fixed length (L) and the AFD coefficients (Mi) and their Basis functions (Ri) obtained from each block are stacked vertically to form 2-dimensional (2D) matrices (M) and (R) respectively. The Basis functions and AFD coefficients are then encrypted, encoded and transmitted over the communication channel as shown in Figure 1. The number of decomposition levels or iterations performed to decompose the ECG signal determines the quality of the reconstructed signal and compression efficiency of the signal.

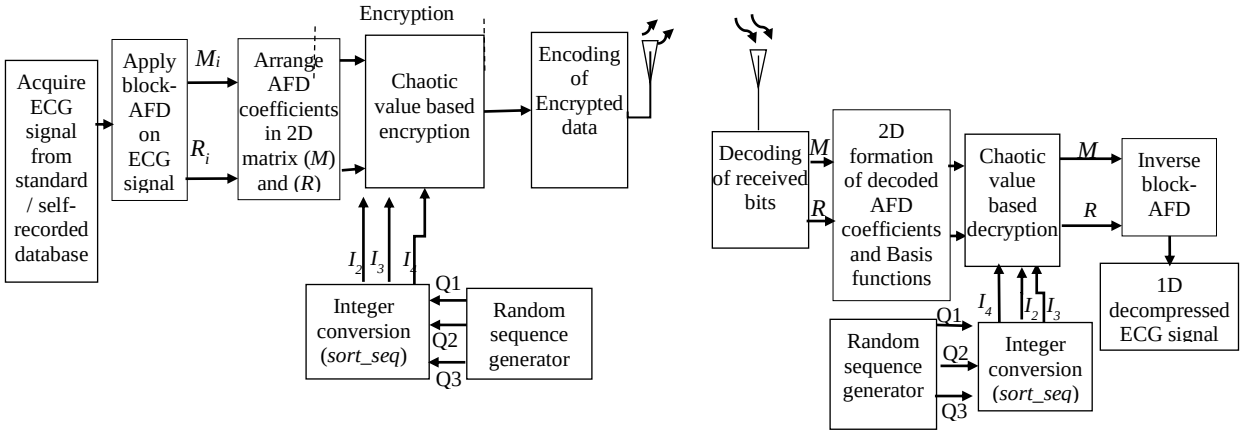

Figure 1. (a)ECG Compression and Encryption (b) ECG Decryption and Decompression

Compression Process

To perform AFD, the real-valued ECG samples (S) in each block are initially projected into Hardy's space ($H^2(\mathbb{D})$) via Hilbert transform. A dictionary of evaluators{eai}'s is generated and then according to modified TM system and the greedy algorithm with MPP principle, ECG is decomposed into AFD coefficients (R) and their basis functions (M) each of length N, where N is the number of decomposition levels. AFD adaptively selects the basis functions from the rational orthogonal system, e.g. Takenaka-Malmaquist (TM) system in accordance with the input signal thus making it capable to reconstruct the high fidelity signal with few coefficients only.

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 23, No. 3 (2022)
http://www.veterinaria.org
Article Received: July 2022; Revised: August 2022; Accepted: September 2022

Encryption Process

Further encryption is performed on R and M using chaotic sequences. Three set of chaotic sequences are generated using CCM. For encryption, these sequences are sorted in ascending order and their index values are used to swap the R and M coefficients. The signal reconstructed with the modified coefficients is completely distorted. This exhibits the encryption properties of the proposed technique as the recipient needs the correct key to decrypt the AFD coefficients for decompression.

Encoding Stage

The encrypted coefficients, *R* and *M* are the complex numbers which are required to be encoded into a binary format for transmission [16]. For this purpose, an adaptive bit length encoding technique is used that not only encodes the encrypted coefficients but performs purely lossless compression as well [17].

Results

The major focus of the signal processing techniques while implementing on medical data, is to preserve their diagnostic features. As discussed earlier, the proposed technique performs compression and encryption and these operations are crucial to securely communicate patients' medical information in remote-healthcare systems. It is essential to study the impact of these techniques on the ECG signal for the correct diagnosis. Figure 2 displays the comparison between the original and the reconstructed ECG along with the amount of error occurred in first 4000 samples of record 100, 117 and 119 of MIT-BIH arrhythmia database [18] with N=50.

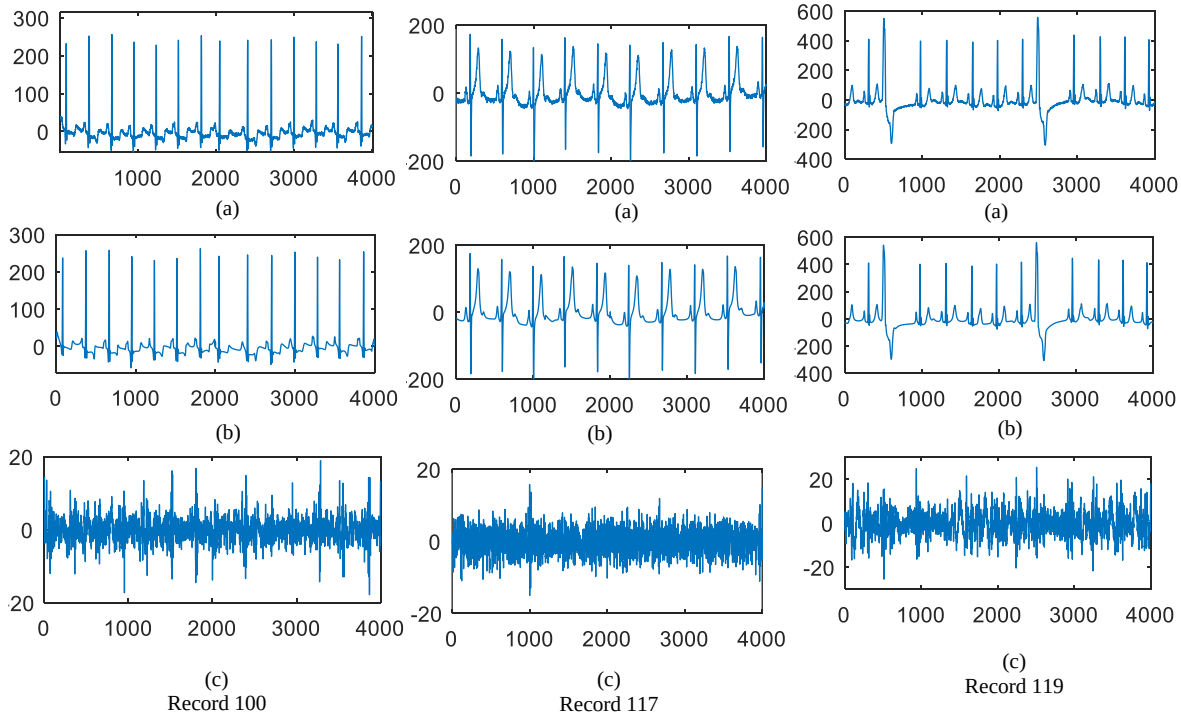

Figure 2. (a) Original ECG signal (b) Decompressed ECG signal (c) error signal when measured on first 4000 samples of records 100, 117 and 119 of MIT-BIH arrhythmia database for N=50

The visual inspection of both the original and decompressed signals validates the resemblance between the two signals with minor error. Although for short signals, the distortion can be evaluated

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 23, No. 3 (2022)
http://www.veterinaria.org
Article Received: July 2022; Revised: August 2022; Accepted: September 2022

through visual inspection by experts but for long duration signals, the distortion is measured in terms of distortion measurement parameters such as Percentage Root Mean square Difference (PRD), Signal to Noise Ratio (SNR) and Peak Signal to Noise Ratio (PSNR) [15]. The process specific parameters such as compression ratio (CR) and quality score (QS) are used to measure compression.

Significance of number of decomposition levels (N)

The choice of the number of decomposition levels (N) in AFD has direct influence on the performance of the proposed algorithm. As discussed earlier, the number of AFD coefficients into which ECG signal is decomposed apparently decides the quality of the reconstructed signal i.e higher the value of N, better is the quality of the reconstructed signal. Figure 3 demonstrates the comparison between the original signal and the reconstructed signal for various values of N. It is observed from the figure that for higher values of N the decompressed ECG is comparable to the original ECG.

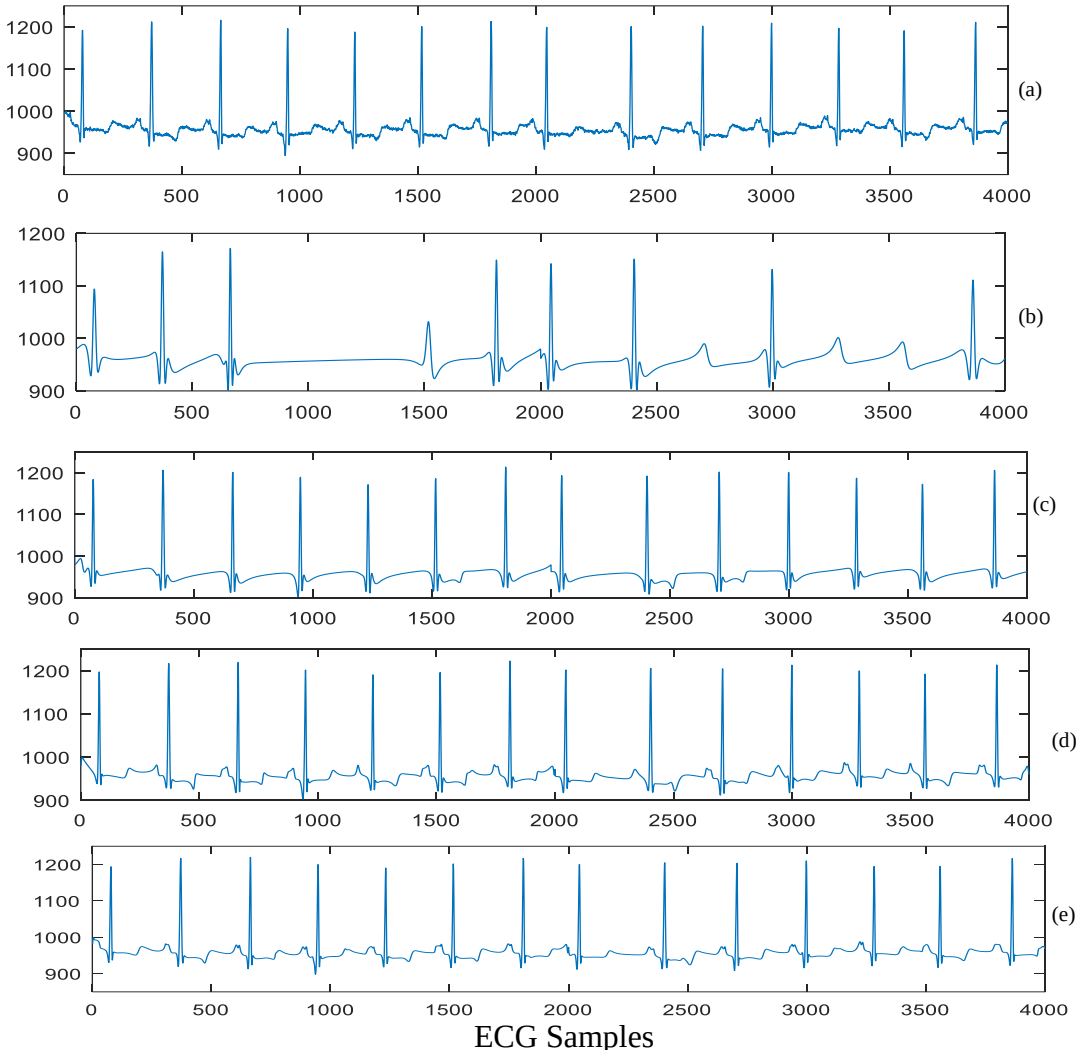

Figure 3 Demonstration of the difference between a) original ECG and decompressed ECG for b) N=10 c) N=30 d) N=50 and e) N=70

REDVET - Revista electrónica de Veterinaria - ISSN 1695-7504
Vol 23, No. 3 (2022)
http://www.veterinaria.org
Article Received: July 2022; Revised: August 2022; Accepted: September 2022

Compression Analysis

In lossy compression techniques, there is always a trade-off between CR and the reconstruction quality. In contrast to the existing transform domain techniques with the fixed basis, AFD capably reconstructs the signal with limited decomposition coefficients by adaptively choosing the input dependent basis function. The impact of number of decomposition level N on CR, PRD, QS, SNR and PSNR when measured on record 100 of MIT-BIH arrhythmia database with N vary from 30 to 100 is displayed in Table 1.

Table 1 The impact of N on the performance metrics measured on Record 100 of MIT-BIH arrhythmia database of 2 mins

N	CR	PRD	QS	SNR	PSNR
30	15.88536	0.184842	98.97348	15.28148	31.48109
40	12.57536	0.129801	96.88169	17.73442	36.73302
50	10.07818	0.090981	123.4253	21.27404	37.47366
60	8.585541	0.076212	126.3419	22.84974	39.04936
70	7.502148	0.066732	127.1479	24.04873	40.24834
80	6.675476	0.060767	124.2373	24.8638	41.06341
90	6.025092	0.056188	121.5355	25.55089	41.75051
100	5.507332	0.052866	118.0373	26.07561	42.27523

Limitations and Future Studies

The compression technique proposed in this work is highly efficient as compared to state of the art techniques but implementation of AFD on long duration ECG signals increase the computational cost. This can be improved if the approach to evaluate the AFD Coefficients and Basis Functions be improved by using some optimization techniques.

References

[1] Berkaya, S.K., Uysal, A.K., Gunal, E.S., et al.: 'A survey on ECG analysis', Biomedical Signal Processing and Control, 2018, 43, pp. 216–235
[2] Seera, M., Lim, C.P., Liew, W.S.,et al.: 'Classification of electrocardiogram and auscultatory blood pressure signals using machine learning models', Expert Systems with Applications, 2015, 42, (7), pp. 3643–3652
[3] Algeria-Barrero, E., Algeria-Ezquerra, E.: 'When to perform pre-operative ECG', E-journal of Cardiology Practice, 2008, 7, (13)
[4] Pandey, A., Saini, B.S., Singh, B., et al.: 'A 2D electrocardiogram data compression method using a sample entropy-based complexity sorting approach,' Computers and Electrical Engineering, 2016, 56, pp. 36-45
[5] Mukhopadhyay, S.K., Mitra, S., Mitra, M.: 'ECG signal compression using ASCII character encoding and transmission via SMS', Biomedical Signal Processing and Control, 2013, 8, (4), pp. 354–363
[6] Ma, J.L., Zhang, T.T., Dong, M.'A novel ECG data compression method using adaptive Fourier decomposition with security guarantee in e-health applications', IEEE Journal of Biomedical and Health Informatics, 2015, 19, (3), pp. 986-994

[7] Jha, C.K., Kolekar, M.H.: 'Electrocardiogram data compression using DCT based discrete orthogonal stockwell transform', Biomedical Signal Processing and Control, 2018, 46, pp. 174-181
[8] Chandra, S., Sharma, A., Singh, G.K.: 'Computationally efficient cosine modulated filter bank design for ECG signal compression', IRBM, 2020, 41, (1), pp. 2-17
[9] Feli, M., Abdali-Mohammad, F.: '12 lead electrocardiography signals compression by a new genetic programming based mathematical modeling algorithm', Biomedical Signal Processing and Control, 2019, 54, 101596, pp. 1-11
[10] Mathivanan, P., Ganesh, A.B., Venkatesan, R.: 'QR code–based ECG signal encryption/decryption algorithm', Cryptologia, 2019, 43, (3), pp. 233-253
[11] Zhai, X., Ali, A.A.S., Amira, A., Bensaali, F.: 'ECG encryption and identification based security solution on the Zynq SoC for connected health systems', Journal of Parallel and Distributed Computing, 2017, 106, pp. 143–152
[12] Qian, T., Zhang, L., Li, Z.: 'Algorithm of adaptive Fourier decomposition', IEEE Transactions on Signal Processing, 2011, 59, (12), pp. 5899-5906
[13] Qian, T., Li, H., Stessin, M.: 'Comparison of adaptive mono-component decompositions', Nonlinear Analysis: Real World Applications, 2013, 14, (2), pp. 1055-1074
[14] Soni, N., Saini, I., Singh, B.: 'A morphologically robust chaotic map based approach to embed patient's confidential data securely in non-QRS regions of ECG signal', Australasian Physical & Engineering Sciences in Medicine, 2019, 42, (1), pp. 111-135
[15] Hua, Z., Zhou, Y., Pun, C.M., et al.: '2D sine logistic modulation map for image encryption', Information Sciences, 2015, 297, pp. 80-94
[16] Rajaraman, V.: 'IEEE standard for floating point numbers', Resonance, 2016, 21, (Laszlo, A., & Castro, K. (1995). Technology and values: Interactive learning environments for future generations. *Educational Technology, 35*(2), 7-13.
[17] AFD and chaotic map-based integrated approach for ECG compression, steganography and encryption in E-healthcare paradigm, IET Signal Processing, vol. 15, Issue 5, pp. 337 - 351, 2021
[18] www.physionet.org/cgi-bin/atm/ATM