ECG Waveform Encryption Using Shifted FFT and DWT

Khattab M Ali Alheeti[1], Abdullah Mohammed Awad [2], Muzhir Shaban Al-Ani [3]

[1]Department of Computer Networking Systems, College of Computer Sciences and Information Technology, University of Anbar, Iraq, Email: co.khattab.alheeti@uoanbar.edu.iq

[2]Department of Information System, College of Computer Sciences and Information Technology, University of Anbar, Iraq, Email: am_awad2@yahoo.com

[3]Department of Information Technology, College of Science and Technology, University of Human Development, Sulaymaniyah, KRG, Iraq, Email: muzhir.al-ani@uhd.edu.iq

Abstract

Recently, millions of medical information passed different media to reach their destination without any error. The introduction of advanced media including communications, wireless networks, mobile networks and Internet offer wide range of e-health application. Electrocardiogram (ECG) waveform is an important issue in e-health in which it recognizes the heart activities and it gives an efficient indication about the patient. The most important issue of ECG waveform is to transmit and receive this waveform with an efficient way. This means ECG waveform must reach its destination secure and accurate. The implemented approach introduces an efficient way for compression and encryption of ECG waveform. This approach based on both discrete wavelet transforms (DWT) and shifted fast Fourier transform (FFT). The obtained results indicated that there is 100% of similarity between transmitted and received signal in addition there is a compression ratio of ¼ when applying second level DWT.

Keywords: ECG Waveform; Signal Encryption; Signal Decryption; Discrete Wavelet Transform.

Introduction:

The great trend the world is witnessing today is about Internet of Things (IoT) [1]. This, in turn, focuses on the tremendous development of the communications and mobile media, information technology, sensors and Internet [2]. These great technological developments led to a major revolution in e-healthcare or e-health [3]. E-health have wide range of applications which provides an important assistance of medical support [4]. E-health is an emerging field of hybridizing of medical informatics, public health and business, health services and information provided by the networking, Internet and related technologies [5]. E of e-health not only stands for electronic but it extending to many aspects such as efficiency, enhancement, evidence, empowerment, encouragement, … etc. Another aspect in this subject is telemedicine or online health which indicated the use of electronic media in exchange of medical information from one position to another in order to improve a personal health.

Electrocardiogram (ECG) waveform is an important part of e-health to recognize diagnose the heart disease [6]. The main aspect of e-health is to achieve all required information anytime and anywhere. The information passed from source to destination via Internet or any other communications media. ECG waveform required to reach the destination with high quality and secure form. So, an encryption / decryption approach is proposed to ensure the ECG waveform reach the destination in a secured and compressed form.

ECG Waveform:

Now a days, there are wide use of healthcare via new technologies. One of the important aspects of healthcare is the introduction of electronic environment to support healthcare. E-healthcare concern with the using of electronic media in transmitting and receiving medical information. Security and privacy are the most important aspects in e-healthcare, in addition, to receive that information in time and in a good condition. Healthcare information including many medical measurements of the individual. ECG waveform is the medical signal that will be concerned in this work [7]. ECG Detecting the activities of the heart that can identify many heart disorders. The main parts of ECG signal are shown in figure 1. ECG signal including three important durations [8]:

- P-wave on the ECG signal: represents the depolarization wave and it is about 80-100 *ms*.
- Complex QRS of the ECG signal: represents ventricular depolarization and it is 60-100 *ms*.
- T-wave of the ECG signal: represents ventricular repolarization and its duration 20-40 *ms*.

978-1-7281-3021-7/19/$31.00 ©2019 IEEE
DOI 10.1109/DeSE.2019.00071

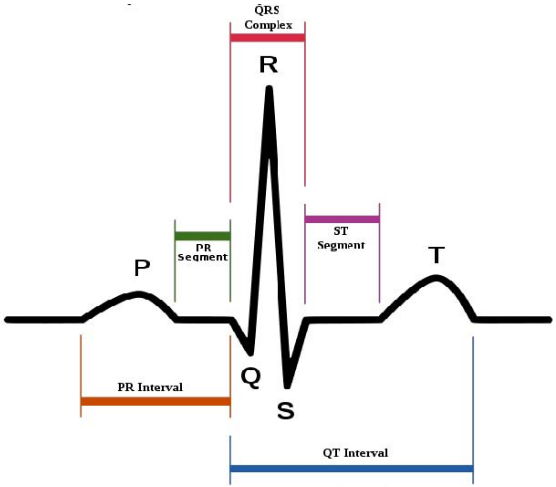


Fig.1 ECG signal [9].

Discrete Wavelet Transform:

Many techniques are used to extract features and the most important technique id discrete wavelet transform (DWT). DWT have many families such as Haar, Daubechies, Biorthogonal, Coiflets, Symlets, Morlet, Mexican Hat, Meyer … etc. Each of these families have more subgroups and DWT can be applied for one dimension, two dimensions and more dimensions. This work deals with one dimensional discrete wavelet transform, so the decomposition of one-dimensional DWT is performed by the combination of low pass filter and high pass filter of the original signal to generate the low band and high band of the first level DWT as shown in figure 2. In addition to down samples by 2 for both bands in order to get the half of the coefficients in both bands. On the other hand, to get the second level DWT, applying both low pass filter and high pass filter on the low band, so this generates ¼ if the original signal size.

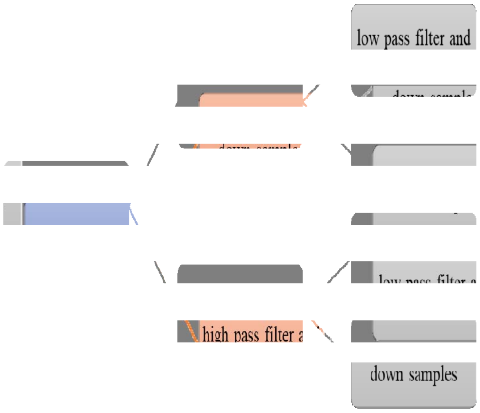


Fig.2 DWT structure

Literature Review:-

Many works are published dealing with the encryption of ECG waveform and this section will consider some of the updated works.

Ching-Kun Chen et al. (2012) improved an efficient data encryption for high security of the transmission of information. This work presented a unique ECG features used for cryptography. In addition, this work improved the chaos theory to develop an encryption algorithm in order to generate the initial chaotic keys. The proposed encryption system used a handy portable device to collect the ECG signals. The obtained results indicated that an efficient key generator is implemented for data encryption. This work demonstrated that the application of this approach for text and image encryption leading to secure issue of communications.

Óscar J. Rubio et al. (2013) implemented an efficient security extension approach after analyzing the characteristics and the measures of other medical protocols. This work is securely stored the ECG files and ensure an appropriate access to the users for different goals: experimental test, consultation and clinical teaching. Access privileges supported by cryptographic are scaled using role-based profiles (encryption, certificates and signatures). These factors are organized into metadata to generate a new section to expand the proposed protocol. The application is designed to implement this method that has been thoroughly tested. This work demonstrated the ability to authenticate users and protect the integrity of the file and the confidentiality of used data. This work is compatible with all versions of ECG and can be easily integrated with e-health platforms [10].

L. F. Carvalho et al. (2014) explained that the digital signature of the network segment using flow analysis as a network management mechanism. This approach introduced three methods for different groups: firstly, the statistical method applied principal component analysis, secondly, the metaheuristic ant colony optimization and thirdly, the prediction method applied Holt-Winters. These methods organized the traffic into two different levels. The first level is the network infrastructure, which covers the entire network including non-health related data that comes from different sectors of eHealth environment. The second level is the creation of profiles in the traffic used to monitor the behavior of the patients. Then, an anomaly detection approach is proposed, capable of recognizing unusual events which may affect the proper services provided by the network [11].

M. Wcislik et al. (2015) demonstrated the monitoring system applied on wireless healthcare. This work explained a prototype medical system that includes a wireless device of healthcare monitoring and advanced mobile base station. The work is implemented a system to monitor the conditions of the human body. They explained the current market conditions for healthcare and available devices. Then they tested the issues related to population in Europe and their impact on the healthcare market. This work showed a review of the wireless communication systems that are available in the Europe market. This work also presented the information that can help to develop low-power portable devices [12].

J. Chukwunonyerem et al. (2016) examined the security of transmission energy for biosensors in a wireless body area sensor network. It has been observed that the existing security solutions in this field use static authentication keys, which are not secure and consume a lot of power. A safety system based on electrocardiogram (ECG) biometry was developed using the index of peak location and the interval between pulses of the heart rate. The method of fast Fourier transform has been applied for the processing of ECG data sets individually selected diabetic patients and the method of differential equation was applied to extract the characteristic of ECG. The power model specification was applied to evaluate the power consumption performance between the nodes. The obtained results indicated that different various characteristics were extracted from the ECG data sets and generated unpredictable authentication keys. The evaluation of the power consumption performance of the node showed a 25% reduction in energy consumption for successful transmission from node to node. The developed approach was provided a secure communication between nodes with an energy efficiency of 25% in the power consumption of transmission between nodes [13].

Xiaojun Zhai et al. (2017) proposed a set of security solutions that can be implemented in a connected health environment, including the advanced encryption standard method and the identification system for ECG. Effective implementation of the system was made for the proposed algorithms of the prototype board. The results of the hardware implementation indicated that the proposed advanced encryption standard and ECG system met the requirements of real time and formed the existing FPGA systems in several key performance metrics. The implemented systems need 10.7 ms to process the ECG sample in which used only 30% of available hardware resources with 107 mW energy consumption [14].

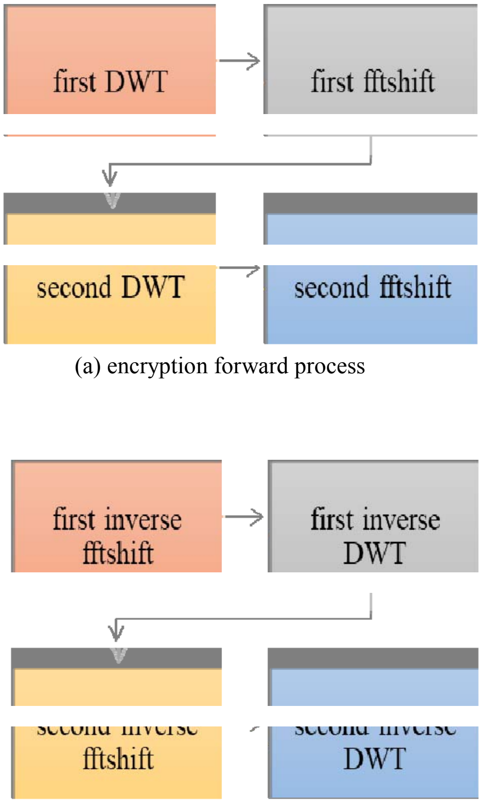
Implemented Encryption / Decryption Approach:-

Due to the advanced of e-health, huge number of medical signals and images are circulated via different types of media every minute. Transmitting and receiving of ECG signal must reach the destination with a high accuracy and high security. The implemented approach is divided into two parts: encryption part which is situated at the transmitting side (patient) and decryption part which is situated at the receiving side (doctor). Normally at the transmitting side after applying preprocessing, then the signal is resized into an adequate length. Then applying four main steps:

- First DWT: applying first level DWT to get compressed low band signal.
- First fftshift: applying first type fast Fourier transform with shifted positions to get the first encrypted model.
- Second DWT:applying second level DWT on the shifted low band to get the second compressed low band signal.
- Second fftshift: applying second type fast Fourier transform with shifted positions to get the second encrypted model.

These four steps ensure both compression and encryption which are very important aspects in e-health. Normally at the receiving side after applying preprocessing, then the signal is resized into an adequate length and removing the unwanted noise as possible. Then applying four main steps figure 3b:

- First inverse fftshift: applying first typeinverse fftshifton the received signal to get unshifted signal.
- First inverse DWT: applying first levelinverse DWT to get the first uncompressed signal.
- Second inverse fftshift:applying second type inverse fftshifton the shifted uncompressed signal to get the decrypted signal.
- Second inverse DWT: applying second levelDWT to get the second decompressed signal with is the same as the original signal.



(a) encryption forward process

(b) decryption inverse process

Fig. 3 Proposed encryption / decryption approach

Results and Discussions:-

The proposed approach including many steps including preprocessing and resizing to avoid the crowded of samples via the overall signal. The overall tested signal contains of 149856 samples. The resizing process divided the original signal into parts and each part contains of 100 samples. Figures 4,5 and 6 demonstrate the division parts of the original signal such as first four parts, second four parts and third four parts respectively.

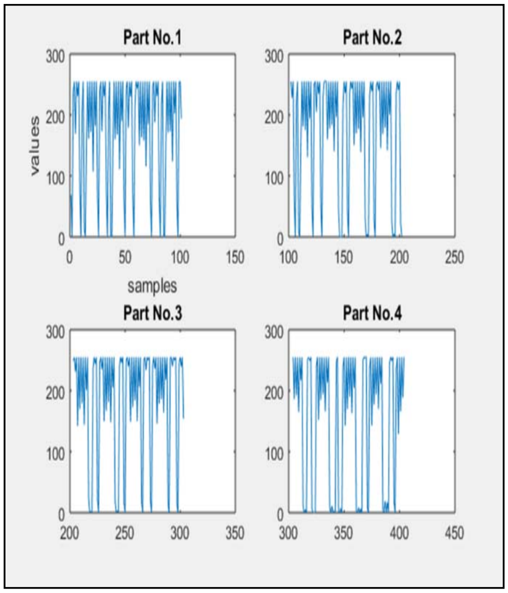


Fig.4 first four parts of the signal

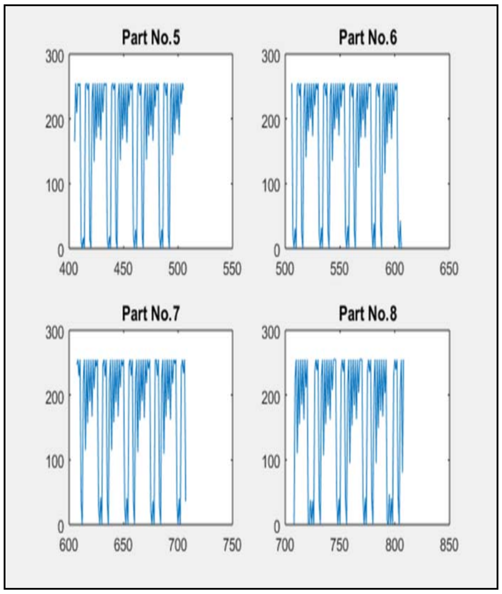


Fig.5 second four parts of the signal

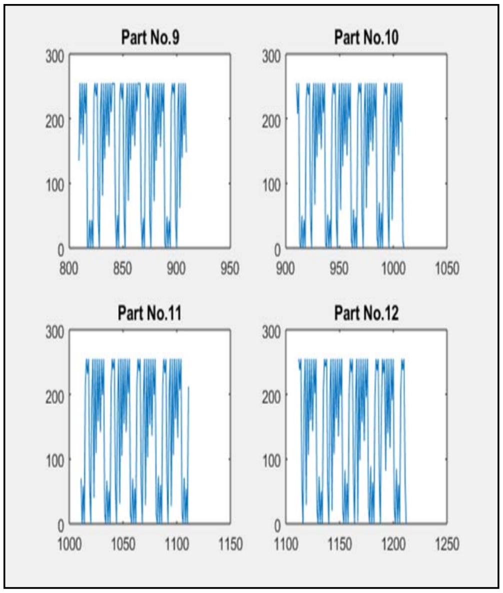


Fig.6 third four parts of the signal

It is impossible to demonstrate all parts of the processing of the overall signal. So, this section will explain the processing applied on the first part of the signal. To understand the obtained results, it is better to explain the procedure steps of the proposed encryption/decryption approach. This approach is divided into two parts: encryption part and decryption part. Firstly, the encryption part including of four steps.

The original signal is divided into many sections and each section contains of 100 samples as shown in figure 7. The first step is applying first level DWT in which it generates 50 samples of the compressed signal that represents the extracted features. The second step is applying the first shift fft which represents the exchange of data positions according to the identify values. The third step is applying second level DWT in which it generates 25 samples of the compressed signal that represents the extracted features. The fourth step is applying the second shift fft which represents the exchange of data positions according to the identify values. This step generates the encrypted compressed signal in which can be transmitted via the communications media.

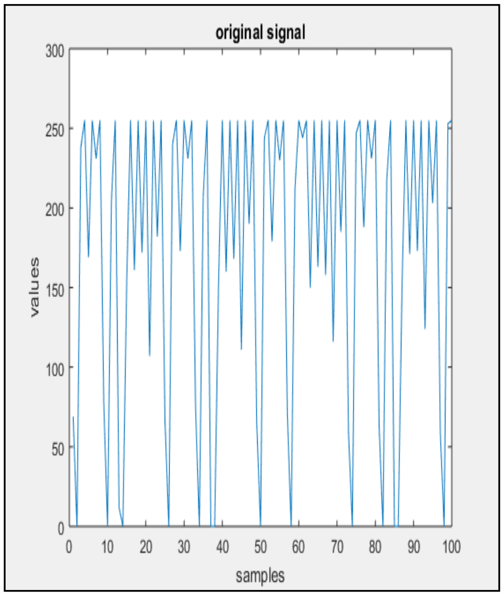


Fig. 7 original signal

Secondly, the decryption part including of four steps. The received signal at the destination side (doctor) contains of 25 samples as shown in figure 12.

- The first step is applying inverse first shift fft to regenerate the signal with right order.
- The second step applying first level inverse DWT in which it generates 50 samples that represents the decompressed signal.
- The third step is applying the second inverse shift fft which represents the second exchange of data positions to achieve the signal with the right order.
- The fourth step is applying second level inverse DWT in which it generates 100 samples of the signal in which it is similar to the original signal.

Conclusion:-

The advanced of medical technologies leading to big growth of doctor supports. Recently, the applications of E-health are extended widely. E-health deals with the accessing of required information anytime and anywhere via any communications media. ECG waveform is an important issue of e-health. Encryption / decryption approach are applied in this work to transmit the ECG waveform from source to destination via communication media. This approach is implemented via applying two levels of DWT and shift FFT respectively. the original ECG waveform is divided many parts and each part contains of 100 samples. The obtained results indicated that the transmitted ECG waveform is received at the destination side with 100 % of similarity.

It concluded from obtained results that the aqueous extract of M. oleifera contains lower protein contents and only one band of C-H stretching compared with aqueous-NaCl extract but showed best absorbent activity towards metal ions. The data mentioned recommended using Moringa seeds in waste water treatment system that can be used to control pollution cause by batteries manufacturing plants which have hazard effect on human health and other living organisms as well particularly in developing countries considering the fact that Moringa plant non-toxic, ecofriendly and low coast natural coagulant.

References:-

[1] Al-Ani M. S., Flying with Internet of Things via Global Structure, IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE), Volume 12, Issue 3 Ver. IV (May – June 2017), PP 36-42.

[2] Al-Ani M S., and Khattab M. A. Alheeti, Intelligent Internet of Things for Energy Conservation Based on Routing Protocol, 2017 IEEE, 2017 International Conference on Current Research in Computer Science and Information Technology (ICCIT), Slemani – Iraq.

[3] Jebadurai J., Peter J. D., Super-resolution of retinal images using multi-kernel SVR for IoT healthcare applications, Future Generation Computer Systems, Volume 83, June 2018, Pages 338-346.

[4] Verma P., Sandeep K. S., Cloud-centric IoT based disease diagnosis healthcare framework, Journal of Parallel and Distributed Computing, Volume 116, June 2018, Pages 27-38.

[5] Wu J., Hao-Yun K. Vallabh S., The integration effort and E-health compatibility effect and the mediating role of E-health synergy on hospital performance, International Journal of Information Management, Volume 36, Issue 6, Part B, December 2016, Pages 1288-1300.

[6] Papa A. Papa, Monika M., Paola P., Manlio Del G., E-health and wellbeing monitoring using smart healthcare devices: An empirical investigation, Technological Forecasting and Social Change, In press, corrected proof, Available online 17 March 2018.

[7] Mshali H., Tayeb L., Damien M., Adaptive monitoring system for e-health smart homes, Pervasive and Mobile Computing, Volume 43, January 2018, Pages 1-19.

[8] Sardi L. S., Ali I., José Luis F. A., A systematic review of gamification in e-Health, Journal of Biomedical Informatics, Volume 71, July 2017, Pages 31-48.

[9] Bates D. W., Kathrin M. C., Adam W., Aziz S., Chapter 20: The Future of Medical Informatics, Key Advances in Clinical Informatics, 2017, Pages 293-300.

[10] Nisbet R., John E., Gary M., Chapter 14: Medical Informatics, Handbook of Statistical Analysis and Data Mining Applications, 2009, Pages 313-319.

[11] Robbins Ti. David, S. N. Lim Choi Keung, Theodoros N. Arvanitis, E-health for active ageing; A systematic review, Maturitas, Volume 114, August 2018, Pages 34-40.

[12] Pirlo R. D., Giuseppe, Éric A., Céline R. Masaki N., Personal digital bodyguards for e-security, e-learning and e-health: A prospective survey, Pattern Recognition, Volume 81, September 2018, Pages 633-659.

[13] Wen C. L., Chapter 8: Telemedicine, eHealth and Remote Care Systems, Global Health Informatics, 2017, Pages 168-194.

[14] Walton K. M., Karen, Peter W., Maree F., Eleanor B. A framework for eHealth readiness of dietitians, International Journal of Medical Informatics, Volume 115, July 2018, Pages 43-52.