Multimedia Tools and Applications (2021) 80:10679–10703
https://doi.org/10.1007/s11042-020-09369-5

Encryption of ECG signals for telemedicine applications

Abeer D. Algarni [1] · Naglaa F. Soliman [1,2] · Hanaa A. Abdallah [1,2] · Fathi E. Abd El-Samie [1,3]

Received: 27 January 2019 / Revised: 15 June 2020 / Accepted: 16 July 2020 /
Published online: 27 November 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract
Multimedia security has been extensively used in content protection, image authentication, data hiding and signal encryption. Similarly, transmission of biomedical data or information remotely for healthcare applications should be secure. One of the important medical signals that need to be transmitted to healthcare centers is the Electrocardiogram (ECG) signal. This paper is concerned mainly with ECG signal encryption for security applications. The paper presents three cryptosystems for ECG signal encryption based on the fusion of ECG signals with other masking signals that are rich in activities such as speech signals. The common thread between these cryptosystems is the operation on sample values of the ECG signal rather than adopting encoding and decoding schemes, and this saves much time and is more immune to both noise and hacking scenarios. The proposed cryptosystems are compared to the encryption technique that uses 1-D logistic map. The performances of the proposed cryptosystems are evaluated through simulation experiments in terms of histogram, structural similarity index, Signal-to-Noise Ratio (SNR), log-likelihood ratio, spectral distortion and correlation coefficient. It is clear from the experiments that the utilization of more levels of encryption increases the security.

Keywords ECG signals -fusion - encryption - chaotic systems - random projection- salting- logistic map

✉ Abeer D. Algarni
adalqarni@pnu.edu.sa

Naglaa F. Soliman
nagla_soliman@yahoo.com

Hanaa A. Abdallah
dr.hanaaabdalaziz@gmail.com

Fathi E. Abd El-Samie
fathi_sayed@yahoo.com

Extended author information available on the last page of the article

1 Introduction

The ECG signal is a registration of the electrical activities of the heart. It can be used as a tool for diagnosis of cardiac diseases. It reflects the state of the heart. The heart is composed of the myocardium muscle, which contracts in a rhythmic way, and then pushes the blood circulation along the body. The propagation wave of electric current goes in the whole heart, and this causes the myocardial shrinking before each normal heart beat. The electric current spread is not random. It is well coordinated. Hence, this makes a strong and coordinated systole. The produced signal is the ECG signal. The main factors that affect the ECG signal include the shortage of oxygen in myocardium and the macroscopic disorders in the geometry of the heart [6, 32].

The different circulation action potentials in the heart cause a current flow, which leads to an electrical field that can be examined, in a weak form, at the body surface, through voltage measurement to get the ECG signal. Hence, the ECG signal is a graphical measurement of the electrical activities produced by the heart. This signal shows the rhythm of the heart, the quality of the electrical conduction, the state of chambers, and the blood supply in a heart attack (myocardial infarction). It is typically in the level of ±2 mv, and it needs a registration bandwidth of 0.05 to 150 Hz. An ECG recording of a normal person is illustrated in Fig.1 [32].

The ECG signal comprises waves, segments, and intervals. The waves are known as P, QRS, T and U. The P wave is the result of the action potential that causes depolarization of the atrial myocardium. The PR interval starts at the beginning of the P wave and ends at the start of the Q wave. It defines the period in conduction across the atria to the ventricles. Normal recording for PR interval takes 120 ms to 200 ms. The PR segment starts with the point at

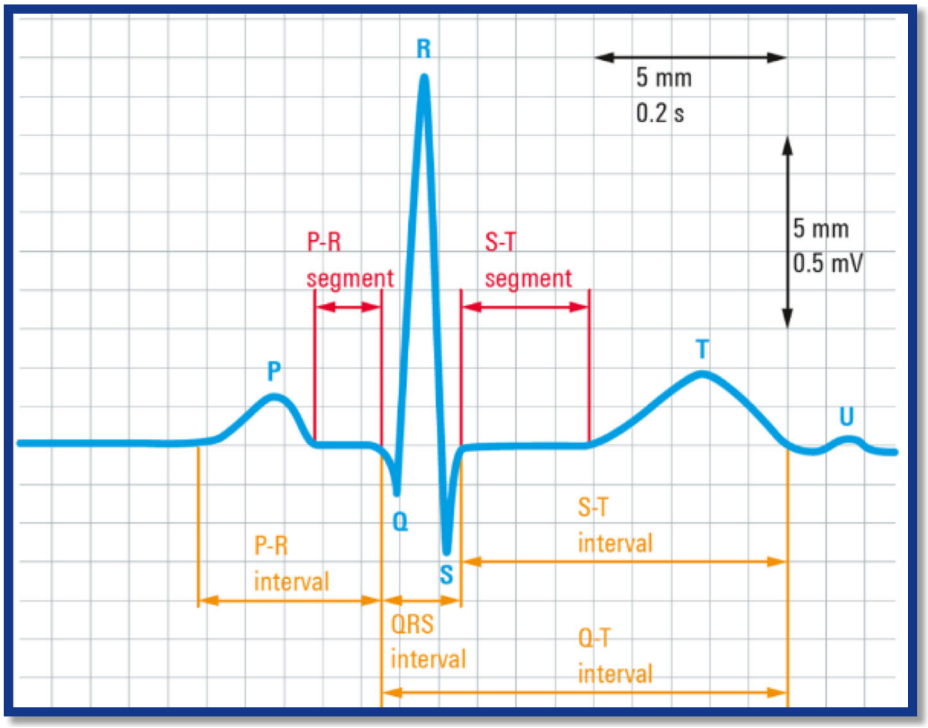


Fig. 1 An ECG signal for a normal person [32]

which the P wave finishes, and this segment ends at the beginning of the Q wave. It defines the period of conduction from the atria-ventricular node, down the collection of its end through the collection branches to muscle.

The QRS complex is composed of three individual waves, and it results from ventricular depolarization and determines the onset of the ventricular contraction. The QRS complex agrees with the duration of ventricular contraction or depolarization. The atrial depolarization signal is sunk by a bigger ventricular signal. It results from ventricular depolarization across the Bundle Branches and Parkinje (BBP) fiber. The QRS complex is a larger signal, which causes elimination that happens when the waves of depolarization in the left move opposite to the directions of the right parts. If any side of the heart does not work well, there may be an increase in the size of the QRS complex. The QRS can be recorded from the start of its first wave to the arrival of the last wave to the base. Normal measurements for QRS take 60 ms to 100 ms.

The T wave represents re-polarization of the ventricles and precedes the ventricular relaxation. The T wave is caused by the re-polarization of the ventricles and has a longer time than that of the QRS complex, because the ventricular re-polarization is slower than depolarization. For normal recordings, the T wave has a deviation of about 0.5 mv. The period of the T wave normally takes 200 msec or less. Segments are periods between waves. Intervals are periods including waves and segments. The circulation of the sinoatrial (SA) node movement potential through the atria results in contraction of the atria, producing the P wave. The measurable attributes of the P wave are 50–100 μV for amplitude and 100 msec for duration.

It can be noticed from Fig. 1 that the ECG is not strictly a periodic signal. It has some differences in period and amplitude levels of beats. Each region has different frequency components. The QRS has high-frequency oscillations. The T region has lower frequencies, and the P and U regions have very low frequencies. The signal contains noise components due to various sources, and therefore the noise should be suppressed during processing of ECG signals. The Fourier Transform (FT) and the Short-Time Fourier Transform (STFT) are not appropriate for representation of ECG signals. The first provides only frequency information and the time information is lost. However, the second describes both time and frequency information, but it resolves all frequencies, equally. On the other hand, the wavelet transform is efficient to analyze the ECG signals as it provides good time resolution and poor frequency resolution at high frequencies and good frequency resolution and poor time resolution at low frequencies. It is considered as a useful tool, when the signal at hand has high-frequency components for a short duration and low-frequency components for a long duration as in ECG signals.

The ECG signals need to be analyzed for automated diagnosis of heart state and diseases. This task requires the transmission of the ECG signals from the measurement system to the processing unit for further processing and information extraction for healthcare applications. The ECG signals need to be secure during the transmission process. That is why ECG signal encryption is important. Moreover, ECG signals can be used as biometrics for the access of healthcare systems. With the wide spread of attacks on healthcare systems, the trend of cancelable biometrics has evolved. Encrypted biometrics can be used in healthcare systems rather than the original ones, which may be subject to hacking attempts. The cancelable versions of ECG signals can be generated through ECG signal encryption. For these two reasons, the issue of ECG signal encryption is considered in this paper. Different frameworks are presented in this paper for ECG signal encryption. The strength of these frameworks is also studied.

This paper is organized as follows. Section 2 introduces the related work to ECG signal encryption. The proposed ECG cryptosystems are presented in section 3. Simulation results and discussion are given in section 4. Finally, the concluding remarks are presented in section 5.

2 Related work

Recently, the mobile health has been provided with a new technology that is represented with Wireless Body Sensor Networks (WBSNs) [11]. The most important requirement of transmission over a WBSN is the security. The ECG signal encryption is essential for secure communication to keep confidentiality, data integrity, access control, authentication and non-repudiation for transmitted ECG signals [4, 30]. It provides a way to protect sensitive information in the ECG signals by transforming the signals into unintelligible and permuted versions. Only, the authorized receiver can be able to access this information by recovering the original signals. Moreover, telemedicine has been used with Body Area Networks (BANs) for protection of the important information of patients. The BANs do not use classical encryption algorithms due to the hacking attempts, and therefore there is a need for complex algorithms for encryption [1]. Smartphone applications and cloud computing have been widely used in telemedicine as they can deal with a large amount of data [2, 17].

In [5], a web-service-oriented design for heart monitoring of patients has been presented. This design is responsible for the recording and analysis of graphical signals of patients to allow reliable identification of abnormal activities. In emergency cases, it communicates the patient information with a foreign station for help.

The Advanced Encryption Standard (AES) is one the most popular public-key encryption algorithms that have been widely used for data as well as image encryption. It has been extended to ECG encryption by Hameed et al. [12]. It is well-known that the efficiency and computational cost of the AES encryption depends mainly on the mode of operation. Four different modes of operation can be used for the implementation of the AES: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feed-Back, and Output Feed-Back (OFB). The simplest mode is the ECB mode as it is based on the segmentation of the signal to be encrypted into separate blocks and the encryption of each block as a single unit that is different from the preceding and succeeding units.

As the ECB is a simple mode of operation, similar blocks will yield similar cipher blocks. This property makes the utilization of the ECB mode for ECG signal encryption a trivial task, because the ECG signal has a repetitive behavior. The other modes comprise some sort of dependence between blocks in the form of feed-forward or feed-back. They yield better results with ECG signals. The major shortcoming of them is the inability to tolerate any noise effect on the encrypted ECG signals. Any sort of noise may be sputtered in the decrypted signals leading to a very large degree of degradation.

The utilization of the other modes of operation with the AES to encrypt ECG signals is assumed to be acceptable only in a noise-free scenario, which is an unrealistic scenario. Another major problem is the computational cost required for implementation of the AES that comprises Sub-Bytes, Shift-Rows, Mix-Columns, and Add-Round-Key operations in the encryption and their inverses in the decryption. These tasks are very time-consuming. Reported computational costs ranging from 10 min to 20 min are presented in Hameed et al. [12] for the encryption of a single ECG signal, which makes the AES infeasible to protect ECG signals transmitted over healthcare networks. There is a bad need to develop time-efficient as well as noise-tolerant ECG encryption algorithms for healthcare applications.

The idea of lock-up tables has been widely used in the signal and image processing fields for applications such as compression and encryption. In the algorithms that adopt lock-up tables, a substitution process is performed for signal values or vectors. For example, in the vector quantization algorithms, a vector of several values is replaced by a single statistical attribute.

In other algorithms, the signal samples are converted into binary codes, which are replaced by other binary codes of different lengths according to a mapping process. This concept has been extended to the encryption of ECG signals. Mathivanan et al. [29] developed an ECG signal encryption scheme that depends on the conversion of ECG samples to binary equivalents for the decimal values. The binary strings are mapped to equivalent strings called Quick Response (QR) codes, and then remapped to other decimal values. The obtained decimal values are used instead of the original ones. This process is assumed to work properly in a noise-free environment. In the presence of noise, the coding operation is majorly disturbed. In addition, the processes of coding and decoding have large computational complexity.

Bai et el. suggested an encryption algorithm that is suitable for BANs by extracting the initial key of encryption from the vital signs using a shift register [1]. The key can be generated dynamically by a simple hardware with low-power consumption. In [18], the authors provided a lightweight ECG-monitoring device for clinical and non-clinical environments within a telemedicine system to allow remote and continuous surveillance of patients. This device can acquire, store and/or transmit ECG signals to computer-based platforms, or specially-configured Access Points (APs) with Intranet/Internet capabilities to reach remote monitoring stations. The acquired data could be stored in a storage device.

The secure communication that provides confidentiality, privacy, efficiency and accuracy characteristics depends on effective cryptography [1, 2, 4, 17, 18]. Muhammad et el. [22] investigated the security aspects and processes elaborated in the design and implementation of most broadly-used symmetric encryption algorithms. They estimated and compared the performance of different parameters of the encryption algorithms such as encryption and decryption times, throughput, key size, Avalanche effect, memory size, correlation and entropy to select the appropriate encryption algorithm for each application.

The ECG signals can also be used as biometrics. Biometrics can be used for authentication due to uniqueness. ECG signals can be encrypted and used for authentication purposes in electronic Health (e-Health) systems used to transmit medical data on networks. The encryption keys and algorithms can be changed to generate cancelable biometric versions of the ECG signals. Unfortunately, most of the existing cryptography algorithms are not appropriate for biometric applications due to the non-stationary nature of the ECG signals [37]. Mario Merone and Paolo Soda [20] presented a comparison study between the existing systematic encryption algorithms for ECG signals that can be used for biometric applications.

A low-latency approach has been presented in [34] for generating secure ECG features based on cryptographic keys to be used for biometric applications. These ECG features are unique and random in nature. This approach guarantees low latency due to short-time key initiation. In [35], Moosavi, and Nigussie concentrated on the development and investigation of secure and efficient ECG-based cryptographic key generation techniques. They proposed two different techniques for biometric applications.

A double-layer approach for encryption based on one-dimensional logistic map for different types of clinical signals including ECG, Electroencephalogram (EEG), and Blood Pressure (BP) signals was presented in [23]. The most important property of that approach is the small encryption/ decryption time of less than 0.2 s for a signal of 10 s length. Therefore, it can be used for real-time telemedicine and verification applications.

Recently, the watermarking techniques have been utilized for hiding data [15, 31]. They have been used for hiding data in plain biomedical signals and images. A reversible watermarking technique for ECG signals based on wavelet transform has been presented in

[16]. This technique depends on the application of the wavelet transform on the original ECG signals to distinguish the QRS complex through watermark verification. Sankari and Nandhini [36] developed a steganography technique for ECG signals based on the DWT to protect the patients' confidential data, and thus assure the patients' privacy and confidentiality. A watermarking technique for medical images based on histogram shifting in the wavelet transform domain has been presented in [10]. In this technique, the host data is a Magnetic Resonance (MR) medical image and the watermark data is embedded into the high-frequency sub-bands of the transformed image.

Raeiatibanadkooki et al. proposed a technique to compress ECG signals without losing the important medical information, and then encrypt the data to make it secure from unauthorized users [30]. They used mobile processors to apply their technique. They start by removing different types of noise from the ECG signal, and then compressing the signal using 3-level wavelet transform with a thresholding strategy. After that, they compress the ECG signal using Huffman coding with chaos concepts. They achieved a compression rate of 97.72% in order to send the signal all over the world with TCP/IP protocol.

The authors of [38] proposed a technique to compress ECG signals using contrast coding. This technique is appropriate for telemedicine applications. The fundamental pre-requisite of telemedicine, i.e., security, has been accomplished by having ECG information packed in the validated header design. The bandwidth limitations or channel limit imperatives can be overwhelmed by increasing the number of packets in a unit time.

Wang et al. presented a deep learning algorithm for compression of ECG signals depending on a spindle convolutional auto-encoder [40]. This auto-encoder compresses the signal by decreasing its dimensionality, while keeping its quality level. It contains two sections; encoder and decoder, with multiple functional layers. A high ratio of compression of about 106.45 has been achieved. This ensures that the spindle convolutional auto-encoder is a good candidate for transmission of medical data.

Bhalerao et al. presented a multi-purpose algorithm for data hiding in ECG signals [3]. A hashing algorithm is applied on the ECG signals for watermark embedding to hide the patients' data, and deep learning is adopted for data prediction. The authors investigated the robustness of ownership watermarks and the tampering effect localization, and proved a good performance.

Chaotic maps have also been used in multiple works for data encryption as they have an efficient randomization property [24, 25]. The authors of [25] suggested embedding the important data of patients in their ECG signals. The signals are then ciphered by a Fused Coupled Chaotic Map (FCCM) scheme. Four different initial conditions have been investigated by changing the control parameters.

Most of the recently published work for securing ECG signals adopt algorithms that depend on binary data. In addition, they need decimal-to-binary conversion and encryption in the binary domain. Hence, they are very sensitive to noise if binary data is disturbed. So, they need a noise-free environment. The other algorithms that work on the sample level may be hacked easily due to the repetitive nature of the ECG signals. So, there is a need for ECG signal encryption algorithms that are tolerant to noise. This can be achieved on the sample level, but with algorithms that can mask patterns even if they are repetitive. This paper is mainly concerned with the encryption of ECG signals in a noise-tolerant framework on the sample level. It presents three cryptosystems for this purpose. They are compared to the encryption technique that adopts the 1-D logistic map. The performances of the proposed cryptosystems are evaluated in the simulation experiments in terms of histogram, Signal-to-Noise Ratio

(*SNR*), correlation coefficient, Log-Likelihood Ratio (*LLR*), Spectral Distortion (*SD*) and Structural Similarity Index (*SSIM*). We implement multiple layers of encryption to allow working on the sample level, while hiding the repetitive patterns of ECG signals. The proposed cryptosystems produce more permutations and diffusions to achieve uniform histogram distributions of the encrypted signals, which increases the security.

3 The proposed ECG cryptosystems with auxiliary tools

In the proposed cryptosystems, the encryption process is applied on patients' or individuals' data before transmission over the wireless network. At the receiver side, the data can be extracted using a secret key and a decryption technique for further analysis of the patients' states or used directly in encrypted format for authentication in cancelable biometric applications.

In this section, three cryptosystems are proposed to ensure better security of ECG signals. The output sequences of these cryptosystems have good randomness, low correlation with original signals and non-predictability. The first and second cryptosystems depend on the fusion of the wavelet coefficients of the 1-D ECG signal with those of a random signal. The fusion depends on random projection or salting.

A chaos-based encryption scheme is developed in the third cryptosystem to generate the encrypted ECG signals. It is highly sensitive to the initial conditions. Therefore, if different initial conditions are used, the system will run in different orbits, which are difficult to be analyzed and calculated. The third implemented cryptosystem has three phases of encryption to keep confidentiality and privacy. These phases are fusion, substitution and chaotic permutation. The fusion is implemented with 2-D DWT. The ECG signal is masked with a speech signal that has no silent periods to hide the ECG repetitive pattern. The security of this proposed cryptosystem depends mostly on the initial conditions of the chaotic system, which are the key factors of the randomization process. Therefore, the two layers of encryption increase the security of communication over wireless networks.

3.1 Random projection in the DWT domain

The proposed algorithm for ECG signal encryption based on random projection in the DWT domain is illustrated in Fig. 4. A single-level DWT decomposes the signal into approximation and details. The approximation represents the low-frequency constituent, while the details are the high-frequency constituents. The DWT is applied on the ECG signal to decompose it into two sub-signals of half its length. One sub-signal is the running average or trend (A_1); and the other is the running difference or fluctuation (D_1). The random projection is applied through multiplication of both components with the same or different random matrices to encrypt the wavelet coefficients. The random projection is widely used for generating cancelable biometric templates [27, 28]. Random projection is the process of projecting the original signal or feature vector on a random space. It can be implemented through multiplication with a random matrix. If we have a vector $\mathbf{X}$ of the ECG signal or one of its components in the wavelet domain, we can multiply it by a random matrix $\mathbf{A}$ to generate a random vector $\mathbf{Y}$,

$$\mathbf{Y}_{k\times 1} = \mathbf{A}_{k\times d} \cdot \mathbf{X}_{d\times 1} \tag{1}$$

With this multiplication process, the input vector is transformed to a random vector. At the receiver, the inverse random projection, and then the Inverse DWT (IDWT) are applied to reconstruct the ECG signal to be used for further analysis. On the other hand, if the ECG signal is to be used for authentication, it can be correlated with the templates stored in the database. Another implementation is also possible. The DWT can be replaced with Discrete Cosine Transform (DCT) as illustrated in Fig. 2. The DCT coefficients are encrypted using the random projection as illustrated in Fig. 3.

3.2 Salting in the DWT domain

In this scenario, the fusion process is performed by salting as illustrated in Fig. 4. Salting is implemented by the addition of a random sequence either to the ECG signal or its wavelet coefficients. The salting technique is well known for cancelable biometric applications [27]. It depends on the type of the random sequence, whether Gaussian or uniform. The noise power affects the performance of the salting-based cryptosystem. In this cryptosystem, a random pattern is mixed with the DWT coefficients of the original ECG pattern. At the receiver, a simple subtraction operation is performed to extract the original ECG signal for further analysis. There is no need to extract the original ECG pattern in cancelable biometric applications. This cryptosystem can be implemented using the DCT instead of the DWT.

3.3 The cryptosystem based on three phases

In this cryptosystem, 2-D wavelet fusion is used to merge the ECG signal with a speech signal without silent periods to get rid of the problem of ECG low-activity periods. To fulfill the requirements for fusion, a pre-processing step is applied on both the ECG and speech signals. Firstly, in the pre-processing step, each of the ECG and speech signals is divided into non-overlapping frames and reshaped to 2-D matrices. The 2-D DWT is then performed on both of them.

The proposed cryptosystem is composed of three phases to keep confidentiality and privacy, which are fusion, substitution and chaotic permutation as shown in Fig. 5. The first phase is the DWT fusion with the averaging fusion rule as shown in Fig. 8. The averaging fusion rule is selected because it makes the decryption of the ECG signal simple. The second phase provides the substitution through either DCT or DST. Finally, the third phase is chaotic encryption to present confusion to the signal.

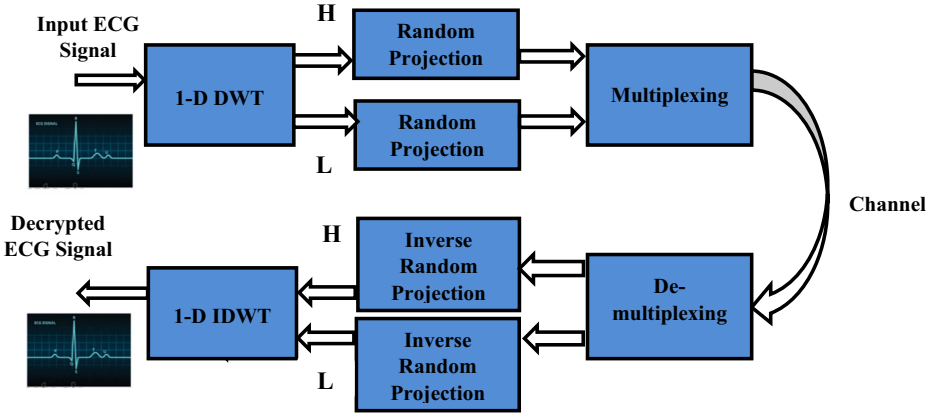


Fig. 2 Schematic diagram of the proposed ECG signal cryptosystem based on random projection in the DWT domain

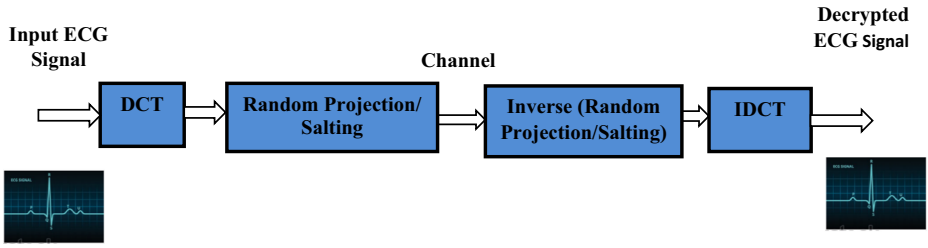


Fig. 3 Schematic diagram of the proposed ECG signal cryptosystem based on random projection in the DCT domain

3.4 The discrete wavelet transform and the fusion process

The DWT is utilized in the proposed cryptosystems for the fusion process. It is one of the most popular transforms used in signal processing. It is a type of time-frequency analysis. The basic idea of the DWT is the decomposition of the signal into lowpass and highpass components using digital filters of lowpass and highpass nature, respectively [8, 13]. Decimation by 2 is adopted after each filtering process to keep the signal size after the decomposition. Perfect reconstruction property of the input signal is maintained through the IDWT. Figure 6 illustrates the DWT decomposition and reconstruction filter bank. We assume that the filters H_o, and H_1 are used for wavelet decomposition, and G_o, and G_1 are used for wavelet reconstruction. From Fig. 6, it is clear that $Y(z)$ is given by:

$$\begin{aligned} Y(z) &= \frac{1}{2}(X_o(z) + X_o(-z))G_o(z) + \frac{1}{2}(X_1(z) + X_1(-z))G_1(z) \\ &= \frac{1}{2}X(z)(H_o(z)G_o(z) + H_1(z)G_1(z)) + \frac{1}{2}X(-z)(H_o(-z)G_o(z) + H_1(-z)G_1(z)) \end{aligned} \tag{2}$$

To allow perfect reconstruction,

$$(H_o(-z)G_o(z) + H_1(-z)G_1(z)) = 0 \tag{3}$$

This can be achieved if

$$H_1(z) = z^{-k}G_o(-z) \tag{4}$$

and

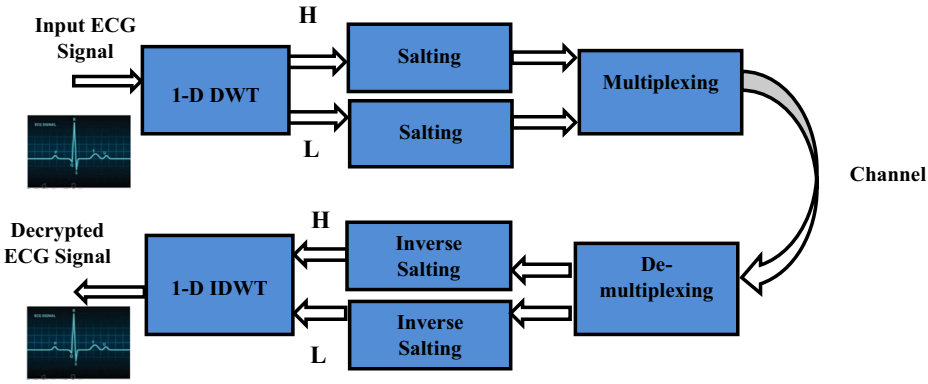


Fig. 4 Schematic diagram of the proposed ECG signal cryptosystem based on salting in the DWT domain

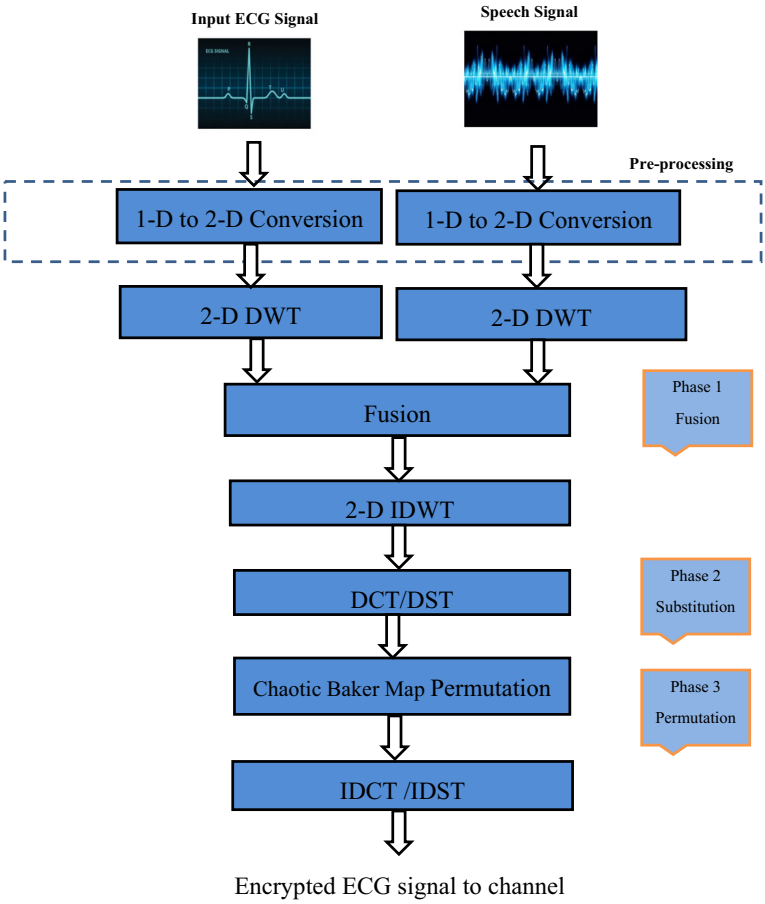


Fig. 5 Cryptosystem based on three phases of encryption

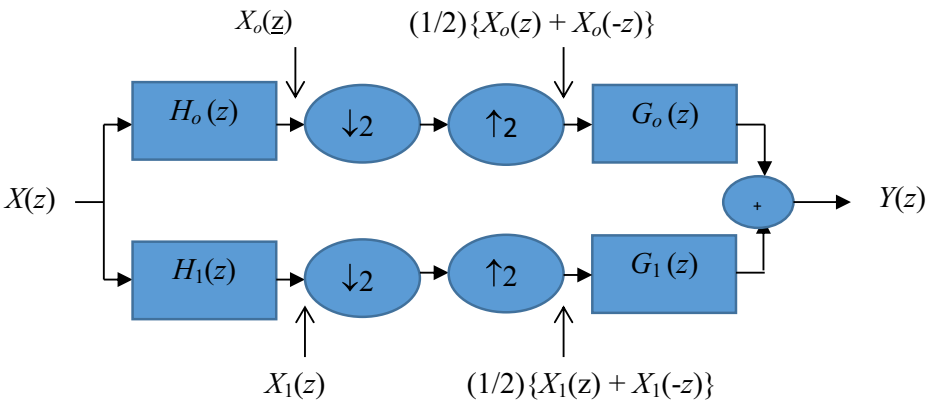


Fig. 6 The two-band decomposition-reconstruction wavelet filter bank

$$G_1(z) = z^k H_o(-z) \tag{5}$$

where $k = \pm 1$.
The other perfect reconstruction condition is:

$$H_o(z)G_o(z) + H_1(z)G_1(z) = 2 \tag{6}$$

Hence, we can conclude that

$$H_o(z)G_o(z) + H_1(z)G_1(z) = P(z) + P(-z) = 2 \tag{7}$$

The polynomial $P(z)$ must satisfy the zero-phase condition and take the shape:

$$P(z) = \ldots\ldots + p_5 z^5 + p_3 z^3 + p_1 z + 1 + p_1 z^{-1} + p_3 z^{-3} + p_5 z^{-5} + \ldots\ldots. \tag{8}$$

The wavelet adopted in this paper is the Haar wavelet, for which,

$$P(z) = \frac{1}{2}\left(z + 2 + z^{-1}\right) = \frac{1}{2}(z+1)\left(1 + z^{-1}\right) = G_o(z)H_o(z) \tag{9}$$

Hence,

$$H_o(z) = \frac{1}{2}\left(1 + z^{-1}\right) \tag{10}$$

$$G_o(z) = (z+1) \tag{11}$$

$$G_1(z) = zH_o(-z) = \frac{1}{2}z\left(1 - z^{-1}\right) = \frac{1}{2}(z - 1) \tag{12}$$

$$H_1(z) = z^{-1}G_o(-z) = z^{-1}(-z+1) = \left(z^{-1} - 1\right) \tag{13}$$

The wavelet fusion process is illustrated in Fig. 7. It depends on the average fusion rule in the proposed cryptosystems.

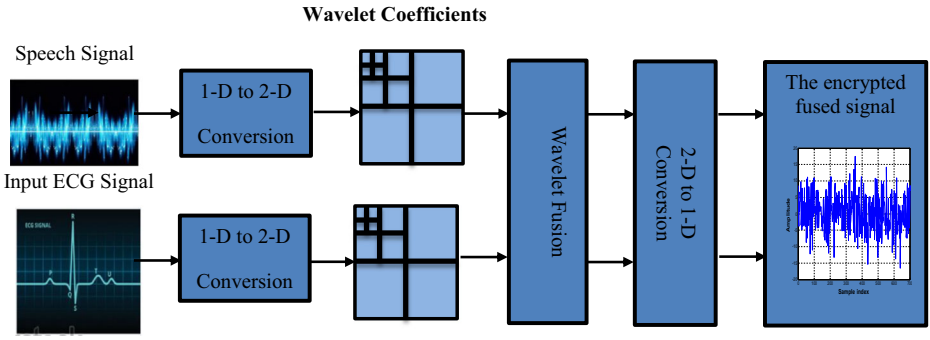


Fig. 7 The 2-D wavelet fusion process

3.5 Chaotic Baker map

The Baker map is another tool that is used in the proposed cryptosystems. It is a 2-D chaotic map, which transfers each element in a square matrix into a new position [39, 42, 44]. The objective of using this type of maps is to randomize the elements of the square matrix in a nonlinear manner in a framework that is sensitive to the initial conditions. The high sensitivity to initial conditions is a required property in cryptosystems that need to achieve confusion and diffusion. We can summarize the two main properties of chaotic Baker map as follows:

1. Its output has excellent randomness, non-predictability and low correlation with the input.
2. It has a strong dependence on input parameters, and starting points or initial values [33].

There are two types of Baker map: generalized Baker map, and discretized Baker map [6]. The discretized map shown in Fig. 8, which is more appropriate to work on blocks of data. It adopts a mapping formula to transfer elements from place to place. The discretized map is represented by $B(r,s)$, with the values $u_1, u_2, \ldots\ldots,$ and u_k selected, so that each integer u_i divides Z, and $Z_i = u_1 + \ldots\ldots + u_i$. The mapping process for an element in the square matrix at the position (r,s), with $0 \le s \le Z$ and $Z_i \le r \le Z_i + u_i$, is performed as presented in Eq.(14):

$$B(r,s) = \left(\frac{Z}{u_i}(r - Z_i) + s mod\left[\frac{Z}{u_i}\right], \frac{u_i}{Z}\left(s - s mod\left(\frac{Z}{u_i}\right)\right) + Z_i\right) \tag{14}$$

where mod means modulo division.
The following assumptions are set:

a. The matrix is of dimensions $Z \times Z$, and it is divided into k vertical slices with height Z and width u_i.
b. Each slice contains u_i boxes, and each box has Z elements.
c. Each slice is formulated as a row as illustrated in Fig.(8) with $Z = 8$, $u_1 = 2$, $u_2 = 4$, and $u_3 = 2$.

3.6 Logistic map

One of the classical chaotic maps is the logistic map, which can be used for key generation for an encryption algorithm. It is used in this paper for the comparison purpose. The 1-D logistic map is represented as follows:

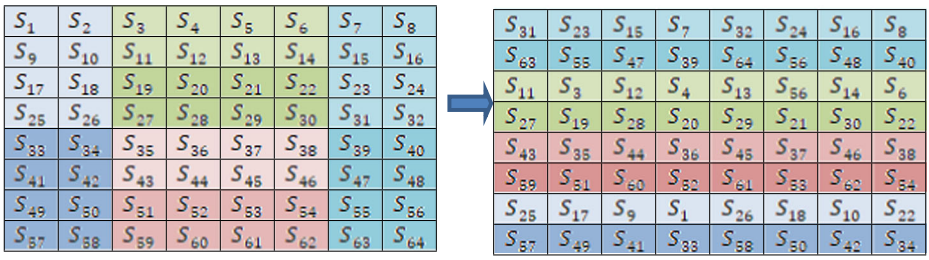


Fig. 8 Chaotic Baker map

$$x_{m+1} = h\, x_m(1-x_m) \tag{15}$$

where the range of x_m is from 0 to 1, and h is a constant having values up to 4. The behavior of the logistic map is controlled by the value of h. For the encryption purpose, h is selected to be 3.57 as the iterations become completely chaotic. A modified 2-D logistic map has been established for encryption due to the limitations of the 1-D logistic map. It is defined as follows [41]:

$$x_{m+1} = h(3y_m + 1)x_m(1-x_m) \tag{16}$$

$$y_{m+1} = h(3x_{m+1} + 1)y_m(1-y_m) \tag{17}$$

4 Simulation results and discussions

For performance evaluation of the proposed cryptosystems, simulation tests are introduced. All proposed cryptosystems are implemented with MATLAB (R2017a). To verify the effectiveness of these cryptosystems, the logistic map encryption is applied for encryption of the original ECG signals as it is popular in many related works. ECG signals from MIT-BIH arrhythmia database [21] have been used. The duration of each signal in the database is about 30 min and the sampling frequency is 360 Hz. The MIT-BIH arrhythmia database contains nearby 48 ECG signals. Different metrics and perspectives have been considered in the performance evaluation process.

4.1 Histogram

Histogram is used to measure the robustness against statistical attacks. For an efficient cryptosystem, the encrypted signals should have uniform distributions that are reflected in their histograms. An example of a plain ECG signal and its histogram are shown in Fig. 9 (a and b).

Histograms of the encrypted and decrypted signals are estimated for quality assessment of the encryption and decryption processes. A comparison between different cryptosystems is illustrated in Table 1. It is worth noting that the histograms of the encrypted signals with the proposed cryptosystem based on three phases are uniform, which means robustness to statistical attacks.

4.2 Structural similarity index (SSIM)

The *SSIM* is utilized to check the similarity between the plain signal and the encrypted one. It gives better evaluation than that with the Mean Square Error (*MSE*). It is calculated with Eq.18 [43].

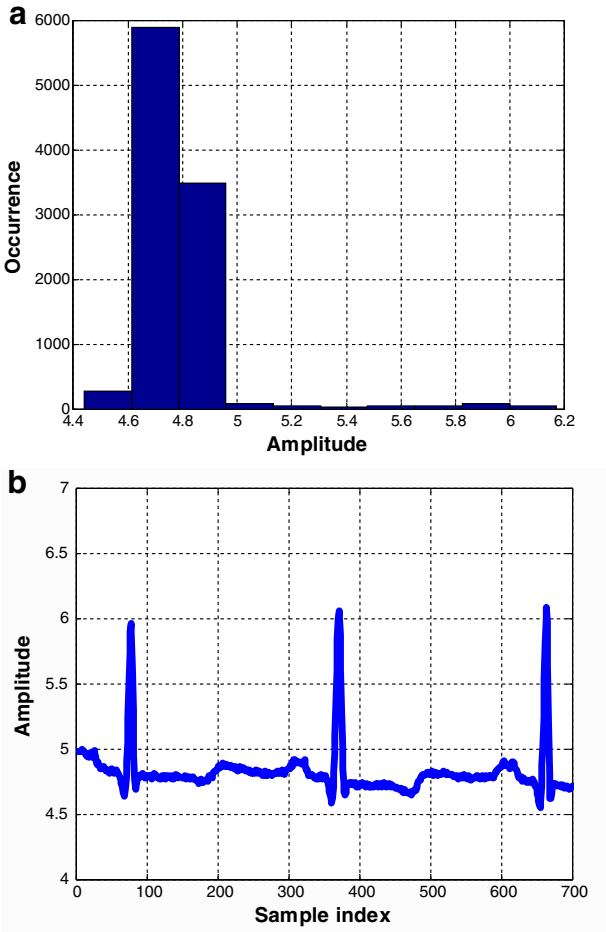


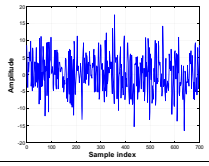
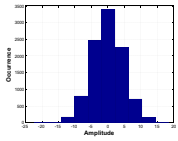
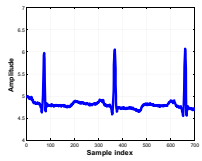
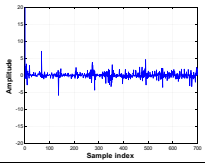
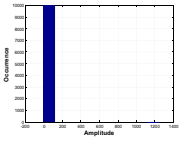
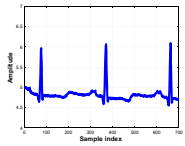
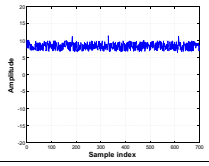
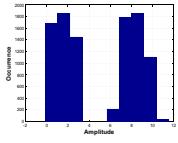
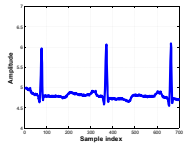
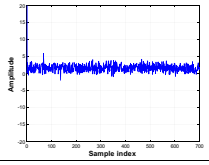
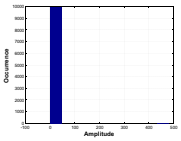
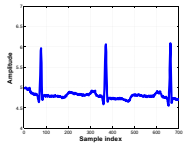
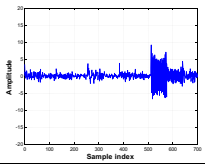
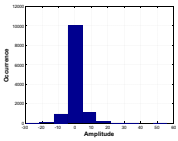
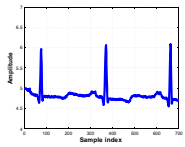
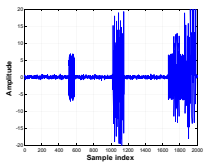
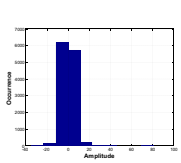
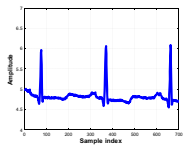
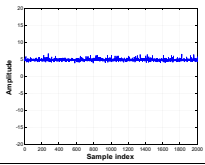
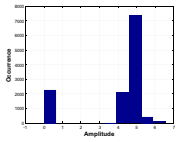
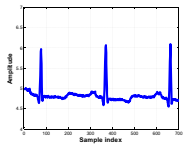
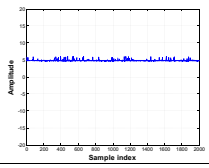
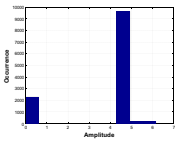
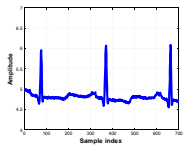
Fig. 9 **a** Plain ECG signal **b** Histogram of the plain signal

$$SSIM = \frac{\left(2\mu_x\,\mu_y + S_1\right)\left(2\delta_{xy} + S_2\right)}{\left(\mu_x^2 + \mu_y^2 + S_1\right) + \left(\delta_x^2 + \delta_y^2 + S_2\right)} \tag{18}$$

where μ_x and μ_y are the mean values of the signals x and y, respectively, δ_x^2 , and δ_y^2 are the variances of the signals x and y, respectively, δ_{xy} is the cross-covariance between the two signals x and y, S_1 and S_2 are small values [43], and the value of *SSIM* is less than 1.

A comparison between the SSIM values for the proposed cryptosystems and the logistic map encryption is illustrated in Fig. 10. It is well known that the *SSIM* value is equal to one, when the two signals are identical, but it is approximately zero, when they are different. It is clear from Fig. 10 that the random projection in the DWT domain has the best value of *SSIM* of 0.001. The cryptosystem based on three phases achieves an *SSIM* value of 0.2.

Table 1 Comparison of encrypted and decrypted signals for the proposed cryptosystems

Encryption Method	**Encrypted signal**	**Histogram of encrypted signal**	**Decrypted signal**
Random projection based on DWT			
Random projection based on DCT			
Salting based on DWT			
Salting based on DCT.			
Cryptosystem based on three phases in DST domain			
Cryptosystem based on three phases in DCT domain			
Cryptosystem based on three phases in spatial domain			
Encryption using logistic map			

4.3 Statistical metrics

The performance of ECG cryptosystems can be investigated using quality metrics such as *SNR*, SNR_{seg}, *LLR*, and *SD*. All these metrics can be estimated between the original and encrypted ECG signals. The lower the *SNR* and SNR_{seg} are, the better the encryption quality. In addition, the higher the *LLR* and *SD* are, the better the encryption quality.

The *LLR* is an objective metric that depends on the distance between the two vectors of Linear Prediction Coefficients (LPCs) calculated from the plain and encrypted signals [19, 26]. It can be estimated mathematically by the Eq.19:

$$LLR = \left| log \left[\frac{\overline{\mathbf{a}}_x \, \overline{\mathbf{R}}_x \, \overline{\mathbf{a}}_x^T}{\overline{\mathbf{a}}_y \, \overline{\mathbf{R}}_y \overline{\mathbf{a}}_y^T} \right] \right| \tag{19}$$

where the LPC coefficients for the original ECG signal are represented with $\overline{\mathbf{a}}_x$ and those of the encrypted ECG signal are represented with $\overline{\mathbf{a}}_y$. The values of $\overline{\mathbf{R}}_x$ and $\overline{\mathbf{R}}_y$ are the auto-correlation matrices for the original and encrypted ECG signals, respectively.
The *SNR* is defined as [19];

$$SNR = 10 \, log_{10} \, \frac{\sum_{n=1}^{N} x^2(n)}{\sum_{n=1}^{N} (x(n) - y(n))^2} \tag{20}$$

where $x(n)$ is the plain ECG signal, $y(n)$ is the encrypted signal, and n is the time index.

A comparison between the proposed cryptosystems from the *SNR* perspective is illustrated in Fig. 11. It is clear that the cryptosystem based on random projection and the cryptosystem based on three phases in DCT/DST domain provide the highest levels of security, when

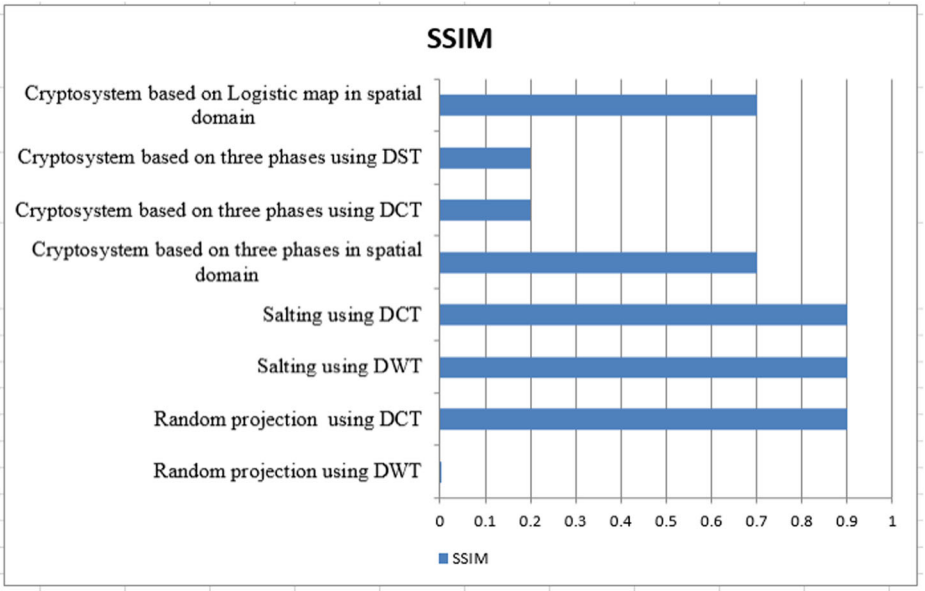


Fig. 10 *SSIM* comparison between the proposed cryptosystems

compared to the other proposed cryptosystems, because they achieve the lowest *SNR* values of −46 dB and − 2.5 dB, respectively.

The average *SNR* can be calculated over short frames of the signal. This metric is well known as the SNR_{seg}. It can be estimated from with Eq. 21:

$$SNR_{seg} = \frac{10}{M} \sum_{m=0}^{M-1} log_{10} \sum_{i=Nm}^{Nm+N-1} \left(\frac{x(i)}{x(i)-y(i)} \right)^2 \tag{21}$$

where N represents the length of the frame that can be chosen between 15 and 20 ms, and M is the total number of frames in the ECG signal.

Figure 12 reports the *LLR* values of the proposed cryptosystems compared with that of the logistic map encryption. The proposed cryptosystem based on three phases provides the highest level of security, because it achieves the highest *LLR* value, when compared with the other cryptosystems.

The Spectral Distortion (SD) shows how far is the encrypted signal spectrum from the original signal spectrum [19, 25, 26, 28]. It is estimated in the frequency domain as:

$$SD = \frac{1}{M} \sum_{m=0}^{M-1} \sum_{i=Nm}^{Nm+N-1} \left| V_s(i) - V_y(i) \right| \tag{22}$$

where $V_s(i)$ and $V_y(i)$ are the spectra of the original and encrypted ECG signals, respectively.

A comparison from the *SD* perspective between the proposed cryptosystems is illustrated in Fig. 13. It is clear that the *SD* of the random projection in the DWT domain is the best, because it reflects the highest spectral distortion.

The correlation is estimated between the original and encrypted ECG signals to estimate the performance of a cryptosystem as follows:

$$r_{xy} = \frac{c_v(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{23}$$

where $c_v(x,y)$ is the covariance between the original signal x and the encrypted one y. $D(x)$ and $D(y)$ are the variances of these signals [7].

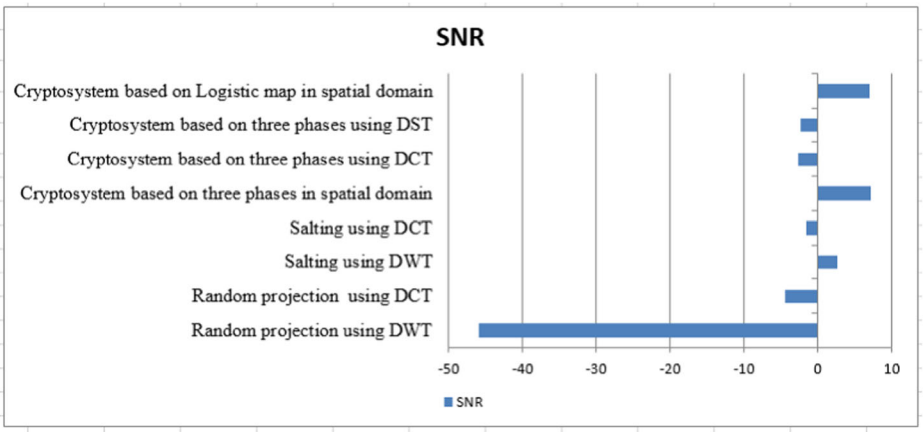


Fig. 11 Comparison in *SNR* (dB) between the proposed cryptosystems

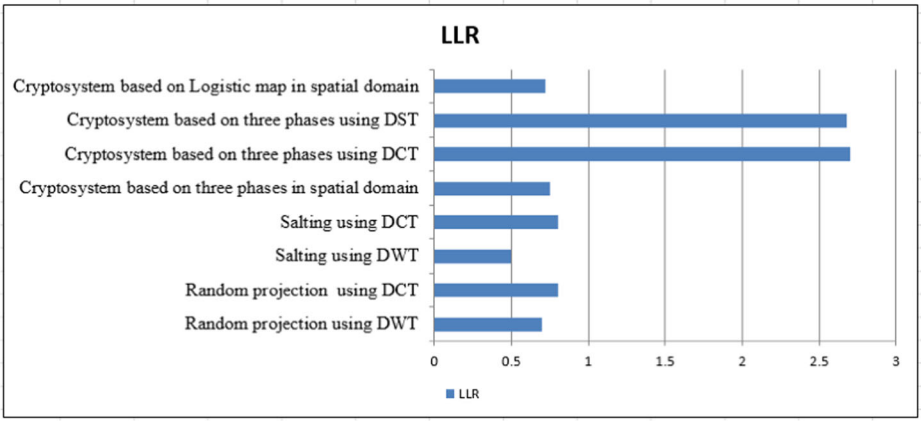


Fig. 12 Comparison between *LLR* values of the proposed cryptosystems

Comparisons in *SNR*, r_{xy}, *SSIM*, *SD*, SNR_{seg} and *LLR* between plain and encrypted ECG signals are illustrated in Table 2. Similar comparisons are performed between plain and decrypted signals as shown in Table 3. The objective of these comparisons is to investigate the performance of the encryption and decryption processes.

It can be noticed from Table 2 that the proposed cryptosystems achieve high levels of security as the correlation values are close to zero. On the other hand, the logistic map records a correlation value of 0.48. Moreover, the decrypted ECG signals have good quality as the correlation values between the original and decrypted ECG signals equal 1 as shown in Table. 3. It is clear from Table 2 that the *SNR* values are significantly low due to the large difference between the original and encrypted signals. The results show correlation values close to zero, small values of *SNR*, small

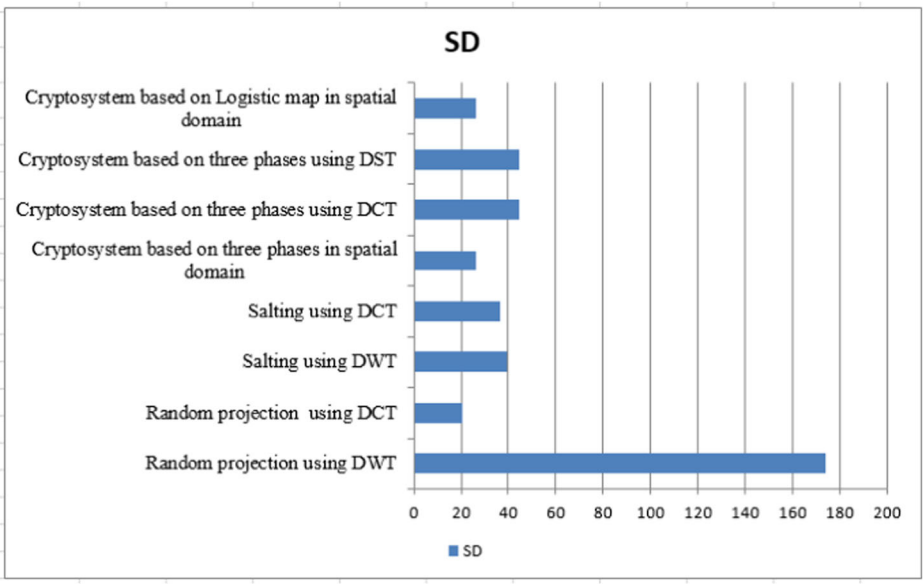


Fig. 13 Comparison between *SD* values of the proposed cryptosystems

Table 2 Evaluation metrics for the comparison between plain and encrypted signals

Encryption							
Encryption Method	Algorithm	*SNR*	r_{xy}	*LLR*	*SD*	SNR_{seg}	*SSIM*
Fusion	Random projection using DWT	−46	0.003	0.7	174	−47	0.001
	Random projection using DCT	−4.5	0.01	0.8	20.5	−16.8	0.9
	Salting using DWT	2.7	0.06	0.5	39.6	2.7	0.9
	Salting using DCT	−1.6	0.01	0.8	36.7	−14.2	0.9
Cryptosystem based on three phases	In spatial domain	7.1	0.48	0.75	26.5	7.1	0.702
	In transform domain using DCT	−2.69	0.002	2.7	44.7	−2.6	0.2
	In transform domain using DST	−2.4	0.018	2.68	44.49	−2.39	0.2
Logistic map	In spatial domain	7.0159	0.4757	0.72	26.49	7.02	0.7

values of *SSIM*, large values of *LLR*, and large values of *SD*. All these findings ensure that the proposed ECG cryptosystems have good performance.

4.4 Attacks on encrypted signals

The encrypted signals can be subjected to noise attacks, when transmitted over a communication channel. The effect of noise attacks on the proposed cryptosystems is presented in this section. Here, salt and pepper (impulsive) noise is applied with a percentage of 1.9 on the encrypted signals. Table 4 shows the effect of noise on the decrypted signals. It is clear that the noise affects the decryption process, and there is data loss in the recovered signals. The effect of cropping 40% of the encrypted signals is studied, and the results are shown in Table 5. It is clear that the effect of cropping is less than the effect of salt and pepper noise. It is noticed from Tables 4 and 5 that the cryptosystem based on three phases records the best results, which means robustness to noise attacks.

Table 3 Evaluation metrics for the comparison between plain and decrypted signals

Decryption							
Encryption Method	Algorithm	*SNR*	r_{xy}	*LLR*	*SD*	SNR_{seg}	*SSIM*
Fusion	Random projection using DWT	222.8	1	0	0	222.7	1
	Random projection using DCT	310	1	0	0	310	1
	Salting using DWT	314	1	0	0	314	1
	Salting using DCT	313	1	0	0	313	1
Cryptosystem based on three phases	In spatial domain	304	1	0	0	304	1
	In transform domain using DCT	304	1	0	0	304	1
	In transform domain using DST	302	1	0	0	302	1
Logistic	In spatial domain	500	1	0	0	500	1

Table 4 Evaluation metrics for the comparison between plain and decrypted signals in the presence of salt and pepper (impulsive) noise attack

Decryption after adding salt and pepper noise 1.9%							
Encryption Method	Algorithm	*SNR*	r_{xy}	*LLR*	*SD*	SNR_{seg}	*SSIM*
Fusion	Random projection using DWT	−0.013	0.015	0.87	15.7	−0.013	0.98
	Random projection using DCT	0.0019	0.27	0.52	15.6	0.0009	0.98
	Salting using DWT	−0.003	−0.87	1.21	32.82	−0.87	0.93
	Salting using DCT	−0.215	0.038	0.36	32.97	−0.29	0.92
Cryptosystem based on three phases	In spatial domain	1.49	0.85	0.66	18.59	1.49	0.99
	In transform domain using DCT	0.49	0.29	0.74	17.96	0.49	0.99
	In transform domain using DST	−15.69	0.26	1.9	18.41	−15.73	0.98
Logistic	In spatial domain	2.008	0.96	0.37	19.2	2.008	0.99

5 Conclusions

The paper presented different cryptosystems for generating secure ECG signals that can be used for telemedicine applications. The first one is based on applying random projection on DWT coefficients of the ECG signals. The second one is implemented using a salting algorithm. The third one is a cryptosystem based on three phases: fusion, substitution and chaotic permutation. It depends on fusing the original ECG signal with a speech signal to compensate for the long periods of ECG signals with low activities. The 2-D chaotic Baker map is applied after the fusion of the two signals to achieve permutation. The utilization of more than one level of processing for encryption increases the level of security. The fusion and chaotic encryption have been applied and tested in the spatial and transform domains. The proposed cryptosystems have been compared with the chaotic logistic map, which is common for ECG cryptosystems. The proposed cryptosystems have high security levels. The simulation results ensured that the proposed cryptosystem based on three phases has the best performance with robustness to attacks. In the future work, deep learning will be used for feature extraction from ECG signals for diagnosis and authentication applications.

Table 5 Evaluation metrics for the comparison between plain and decrypted signals in the presence of cropping attack

Decryption after cropping by 40%							
Encryption Method	Algorithm	*SNR*	r_{xy}	*LLR*	*SD*	SNR_{seg}	*SSIM*
Fusion	Random projection Using DWT	26.21	0.58	0.30	15.23	26.19	1
	Random projection Using DCT	63.14	0.99	0.004	0.38	63.15	1
	Salting Using DWT	12.39	0.15	0.66	28.54	12.39	0.99
	Salting Using DCT	12.38	0.149	0.236	32.97	4.41	0.98
Cryptosystem based on three phases	In spatial domain	7.63	0.69	0.208	15.06	7.64	0.99
	In transform domain using DCT	7.54	0.68	0.093	14.37	7.54	0.99
	In transform domain using DST	6.70	0.68	0.092	14.56	6.7	1
Logistic	In spatial domain	7.656	0.69	0.119	15.02	7.65	0.99

Acknowledgments This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program.

References

1. Tong Bai, Jinzhao Lin, Guoquan Li, Huiqian Wang, Peng Ran, Zhangyong Li,Dan Li, Yu Pang, Wei Wu, and Gwanggil Jeon,(2018). A lightweight method of data encryption in BANs using electrocardiogram signal. In future generation computer systems. March 2019 92:800-811. DOI: https://doi.org/10.1016/j.future.2018.01.031, database: science direct.
2. Baig MM, GholamHosseini H, Moqeem AA, Mirza F, Lindén M (2019) Clinical decision support systems in hospital care using ubiquitous devices: current issues and challenges. Health informatics journal 25(3): 1091–1104. https://doi.org/10.1177/1460458217740722
3. Siddharth Bhalerao, Irshad Ahmad Ansari, Anil Kumar, Deepak Kumar Jain, (2019). A reversible and multipurpose ECG data hiding technique for telemedicine applications", *Pattern Recognition Letters* , Jul2019, Vol. 125, p463–473, 11p; DOI: https://doi.org/10.1016/j.patrec..06.004, Database: Applied Science & Technology Source
4. Chai, Xiuli, Gan, Zhihua, Chen, Yiran, Zhang, Yushu. (2016). A visually secure image encryption scheme based on compressive sensing Signal Processing 134. https://doi.org/10.1016/j.sigpro.2016.11.016.
5. Claudio DC, Meduri A, Morello R (2010) A Smart ECG Measurement System Based on Web-Service-Oriented Architecture for Telemedicine Applications. Instrumentation and Measurement, IEEE Transactions on 59:2530–2538. https://doi.org/10.1109/TIM.2010.2057652
6. Clifford, Gari D., Francisco Azuaje, And Patrick McSharry.)2006(. Advanced methods and tools for ECG data analysis. Boston: Artech House http://www.books24x7.com/marc.asp.
7. H Ding, C Xie, and L Zeng,)2016(". The Correlation Between Signal Distance and Consonant Pronunciation in Mandarin Words", Chinese Spoken Language Processing (ISCSLP), 2016 10th International Symposium Conference: IEEE Xplore.
8. El-Hoseny HM, El Kareh ZZ, Mohamed WA et al (2019) An optimal wavelet-based multi-modality medical image fusion approach based on modified central force optimization and histogram matching. Multimed Tools Appl 78:26373–26397. https://doi.org/10.1007/s11042-019-7552-1
9. Fridrich J (1998) Symmetric ciphers based on two-dimensional chaotic maps. International Journal of Bifurcation and Chaos 8(6):1259–1284
10. Golpîra H, Danyali H (2010) Reversible blind watermarking for medical images based on wavelet histogram shifting. IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2009:31–36. https://doi.org/10.1109/ISSPIT.2009.5407489
11. Guang Z, Carmen P, Yuan-Ting Z (2011) Analysis of Using Interpulse Intervals to Generate 128-Bit Biometric Random Binary Sequences for Securing Wireless Body Sensor Networks. IEEE transactions on information technology in biomedicine : a publication of the IEEE Engineering in Medicine and Biology Society 16:176–182. https://doi.org/10.1109/TITB.2011.2173946
12. Hameed M, Nurulfajar AM, Attiah M (2019) Comparative study of several operation modes of AES algorithm for encryption ECG biomedical signal. International Journal of Electrical and Computer Engineering 9:4850–4859. https://doi.org/10.11591/ijece.v9i6.pp4850-4859
13. Hashad, Fatma, Zahran, O., El-Rabaie, El-Sayed, Elashry, Ibrahim, Abd El-Samie, Fathi. (2019). Fusion-based encryption scheme for cancelable fingerprint recognition Multimedia Tools and Applications 78. https://doi.org/10.1007/s11042-019-7580-x
14. Pei Huang, Borui Li, Linke Guo, Zhanpeng Jin, Yu Chen, (2016) "A robust and reusable ecg-based authentication and data encryption scheme for ehealth systems "2016 IEEE Global Communications Conference, Pages: 1–6,.
15. Jagadish N, Rajendra AU, Kumar M (2009) Efficient Storage and Transmission of Digital Fundus Images with Patient Information Using Reversible Watermarking Technique and Error Control Codes. Journal of medical systems 33:163–171. https://doi.org/10.1007/s10916-008-9176-2.
16. Zheng Kai-mei, Qian Xu. (2008). Reversible data hiding for electrocardiogram signal based on wavelet transforms. 295–299. https://doi.org/10.1109/CIS.2008.71.
17. Lila R, Abdusalam S, Masoud T, Amirhossein G, Arshad B (2019) Healthcare big data processing mechanisms: The role of cloud computing. International Journal of Information Management 49:271–289. https://doi.org/10.1016/j.ijinfomgt.2019.05.017.
18. Lucani, Daniel, Cataldo, Giancarlos, Cruz, Julio, Villegas, Guillermo, Wong, Sara. (2006). A portable ECG monitoring device with Bluetooth and Holter capabilities for telemedicine applications. Conference proceedings : ... Annual International Conference of the IEEE Engineering in Medicine and Biology Society.

IEEE Engineering in Medicine and Biology Society. Conference. 1. 5244–7. https://doi.org/10.1109/IEMBS.2006.260798
19. Manjunath G., Anand Gargeshwari. (2002). Speech encryption using circulant transformations. Proceedings - 2002 IEEE International Conference on Multimedia and Expo, ICME 2002. 1. 553–556 vol.1. https://doi.org/10.1109/ICME.2002.1035841.
20. Merone, Mario & Soda, Paolo, Sansone, Mario, Sansone, Carlo. (2016). ECG databases for biometric systems: a systematic review. Expert Syst Appl 67. https://doi.org/10.1016/j.eswa.2016.09.030.
21. Moody, GB, Mark, RG (2001). The impact of the MIT-BIH arrhythmia database. IEEE engineering in medicine and biology magazine: the quarterly magazine of the engineering in Medicine & Biology Society. 20. 45-50. https://doi.org/10.1109/51.932724.
22. Muhammad M, Sapiee J, Abdulkadir D, Zahraddeen P, Nur S, Mustafa MD (2017) A Survey on the Cryptographic Encryption Algorithms. International Journal of Advanced Computer Science and Applications 8:333–344
23. Murillo-Escobar, Miguel, Cardoza-Avendaño, L., Lopez-Gutierrez, Rosa, Cruz-Hernández, C.. (2017). A double chaotic layer encryption algorithm for clinical signals in telemedicine. J Med Syst 41. https://doi.org/10.1007/s10916-017-0698-3.
24. Pak, Chanil, Huang, Lilian. (2017). A new color image encryption using combination of the 1D chaotic map. Signal Process 138. https://doi.org/10.1016/j.sigpro.2017.03.011.
25. Anukul Pandey , Butta Singh, Barjinder Singh Saini, Neetu Sood (2019). A novel fused coupled chaotic map based confidential data embedding-then-encryption of electrocardiogram signal " In Biocybernetics and Biomedical Engineering. April–June 2019 39(2):282–300 Language: English. DOI: https://doi.org/10.1016/j.bbe.2018.11.012, Database: ScienceDirect
26. Pascal S, Jozue F (1996) Speech enhancement based on a priori signal to noise estimation. ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings 2(2):629–632. https://doi.org/10.1109/ICASSP.1996.543199.
27. Patel V, Ratha N, Chellappa R (2015) Cancelable biometrics: a review. Signal processing magazine. IEEE. 32:54–65. https://doi.org/10.1109/MSP.2015.2434151
28. Pillai, Jaishanker, Patel, Vishal, Chellappa, Rama, Ratha, Nalini. (2011). Secure and robust Iris recognition using random projections and sparse representations. IEEE Trans Pattern Anal Mach Intell 33. https://doi.org/10.1109/TPAMI.2011.34.
29. Ponnambalam, Mathivanan & Ganesh, A. & Rv, Venkatesan. (2019). QR code–based ECG signal encryption/decryption algorithm. Cryptologia. https://doi.org/10.1080/01611194.2018.1549122.
30. Raeiatibanadkooki Mahsa, Quchani Saeed, Khalilzadeh Mohammad Mahdi, Bahaadinbeigy Kambiz. (2016). Compression and encryption of ECG signal using wavelet and chaotically Huffman code in telemedicine application. J Med Syst 40. https://doi.org/10.1007/s10916-016-0433-5.
31. Rajendra AU, Udipi N, Choo L (2004) Simultaneous storage of patient information with medical images in the frequency domain. Computer Methods and Programs in Biomedicine 76:13–19. https://doi.org/10.1016/j.cmpb.2004.02.009.
32. RajendraAcharya U, Suri JS, Spaan JAE, Krishnan SM (2007) Advances in cardiac signal processing. Springer-Verlag, Berlin Heidelberg
33. Saad SA, Hato E (2014) A speech encryption based on chaotic maps. Int J Comput Appl 93:19–28
34. Rahimi Moosavi Sanaz, Nigussie Ethiopia, Levorato Marco, Virtanen Seppo, Isoaho Jouni. (2017). Low-latency Approach for Secure ECG Feature Based Cryptographic Key Generation. IEEE Access. PP. 1–1. https://doi.org/10.1109/ACCESS.2017.2766523.
35. Rahimi Moosavi Sanaz, Nigussie Ethiopia, Virtanen Seppo, Isoaho Jouni. (2017). Cryptographic key generation using ECG signal https://doi.org/10.1109/CCNC.2017.7983280.
36. Sankari, V, Nandhini, K. (2015). Steganography technique to secure patient confidential information using ECG signal. 2014 international conference on information communication and embedded systems, ICICES 2014. https://doi.org/10.1109/ICICES.2014.7033925.
37. Shih-Chin F, Hsiao-Lung C (2009) Human identification by quantifying similarity and dissimilarity in electrocardiogram phase space. Pattern Recognition 42:1824–1831. https://doi.org/10.1016/j.patcog.2008.11.020.
38. Vinod K, Suresh S, Giri V (2006) Direct data compression of ECG signal for telemedicine. Int. J. Systems Science. 37:45–63. https://doi.org/10.1080/00319100500412337.
39. Wang, Xiong & Chen, Guanrong. (2012). Constructing a chaotic system with any number of equilibria. Nonlinear Dynamics 71. https://doi.org/10.1007/s11071-012-0669-7.
40. Fei Wang , Qiming Ma, Wenhan Liu, Sheng Chang, Hao Wang, Jin He, Qijun Huang (2019). A novel ECG signal compression method using spindle convolutional auto-encoder" In Computer Methods and Programs in Biomedicine journal, July 2019 175:139–150. DOI: https://doi.org/10.1016/j.cmpb.2019.03.019, Database: ScienceDirect

41. Yue W, Gelan Y, Huixia J, Joseph N (2012) Image encryption using the two-dimensional logistic chaotic map. Journal of Electronic Imaging 21:3014. https://doi.org/10.1117/1.JEI.21.1.013014
42. Zhang Y, Wenying W, Moting S, Ming L (2014) Cryptanalyzing a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system. Optik - International Journal for Light and Electron Optics 125:1562–1564. https://doi.org/10.1016/j.ijleo.2013.09.018
43. Zhou W, Alan B, Hamid S, Eero S (2004) Image Quality Assessment: From Error Visibility to Structural Similarity. Image Processing, IEEE Transactions on 13:600–612. https://doi.org/10.1109/TIP.2003.819861.
44. Zhou Y, Long B, Chen C (2014) A new 1D chaotic system for image encryption. Signal Processing 97: 172–182. https://doi.org/10.1109/ICSSE.2012.6257151

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Abeer D. Algarni received the B.Sc.(Hons.) in Computer Science from King Saud University,Riyadh, Saudi Arabia in 2007. She received the M.Sc., and Ph.D. degrees from the School of Engineering and Computer Sciences, Durham University, United Kingdom in 2010 and 2015, respectively. She worked as an assistant professor at the College of Computer and Information Sciences at Princess Nourah Bent Abdulrahman University since 2008 up to now. Her current research interests include networking and communication systems, digital image processing, digital communications and cyber security.

Naglaa F. Soliman received the B.Sc., M.Sc., and Ph.D. degrees from the Faculty of Engineering, Zagazig University, Egypt in 1999, 2004, and 2011, respectively. She worked at the Department of Information Technology, College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, KSA since 2015 up to now. She has been a Teaching Staff Member with the Department of Electronics and Communications Engineering, Faculty of Engineering, Zagazig University, Egypt. Her current research interests include digital image processing, information security, multimedia communications, medical image processing, optical signal processing, big data processing, and cloud computing.

Hanaa A. Abdallah received the BSc. MSc., and PhD degrees from the Faculty of Engineering, Zagazig University, Egypt. She is a Lecturer at the Department of Electronics and Communications Engineering, Faculty of Engineering, Zagazig University. She is currently working with the College of Computer and Information Sciences, Princess Nourah Bint Abdulrahman University, Riyadh, Saudi Arabia. Her areas of interest are image enhancement, image compression, data hiding, steganography, and watermarking.

Fathi E. Abd El-Samie received the B.Sc. (Honors), M.Sc., and Ph.D. from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 1998, 2001, and 2005, respectively. He joined the teaching staff of the Department of Electronics and Electrical Communications, Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2005. He has received the most cited paper award from Digital Signal Processing journal in 2008. His current research areas of interest include image enhancement, image restoration, image interpolation, super-resolution reconstruction of images, data hiding, multimedia communications, medical image processing, optical signal processing, and digital communications.

Affiliations

Abeer D. Algarni [1] • Naglaa F. Soliman [1,2] • Hanaa A. Abdallah [1,2] • Fathi E. Abd El-Samie [1,3]

[1] Department of Information Technology, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh 84428, Saudi Arabia

[2] Department of Electronics and Communications, Faculty of Engineering, Zagazig University, Zagazig, Egypt

[3] Department of Electronics and Electrical Communications Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt