A New Approach for Securing Medical Images and Patient's Information by Using A hybrid System

Jamal N. Bani Salameh

Department of Computer Engineering, Faculty of Engineering, Mutah University
Mutah, Karak, P.O. Box: 7, Zip Code: (61710), Jordan

Summary

Today a huge number of medical images and patient's information are transferred between different entities who are geographically apart to be reviewed and evaluated. Any illegal modification in this information during transmission may lead to wrong assumptions and wrong diagnosis. Therefore, the security of medical images and patient's information has always been a concern. In this research, we developed a hybrid security system that combines cryptography and steganography techniques to provide a secure distribution for both the medical images and patient's information over un-secured channel. For cryptography we used our encryption algorithm MJEA (for Modified Jamal Encryption Algorithm); it is a symmetric (64-bit) block encryption algorithm with (120-bit) key. For steganography we used a very simple algorithm that hides the patient's information within the medical image by using bit-by-bit Xoring. The proposed system deals with the medical image and patient's information as shares, the first share represents the medical image after it will be encrypted by using MJEA and the second share represents all patient's information embedded in the medical image and encrypted by using MJEA. For more security, before transmitting the two shares we mixed them together by using a scrambling algorithm. We adopted different simulation metrics for evaluating the performance of the proposed system such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and the histogram distribution analysis. All experimental results proved the strength of the proposed system, and the receiver was able to recover back the original medical image and the patient's information that was sent by the sender without any loss.

Key words:

Medical image, Patient's information, Data hiding, Telemedicine, Cryptography, Steganography.

1. Introduction

The field of Telemedicine involves exchanging medical images and patient's information from one location to another via different forms of electronic telecommunications, it has many applications such as: Tele-consulting, Tele-radiology, Tele-diagnosis, Tele-surgery, and others. Those benefits are associated with various types of risks during sharing the medical information across the vulnerable public networks [1]. Medical information, such as Electronic Patient Records (EPRs) and Electronic Health Records (EHRs) which may include: clinical examinations, diagnosis explanations and other findings, is often closely related to patients' privacies need to be protected in order to prevent malicious tampering [2].

In the growing field of telemedicine, the size of medical information being exchanged over the Internet are extremely increasing and these information are vulnerable to variety types of security attacks. Therefore; securing medical images and patient's information has gained important attention in recent years to protect them from unauthorized accessing or interception. The transferred medical information should be reached accurately to the other party without any change; otherwise; this can lead to false diagnosis causing adverse effects to the normal medical condition. The importance of a secured exchange of medical images encourage international healthcare organizations to publish special standards that deal with medical data security issues. One such standard is the Digital Imaging and Communications in Medicine (DICOM) standard [3]. DICOM provides guidelines and mechanisms to healthcare professionals and entities to achieve three telemedicine security services: confidentiality, authenticity and integrity [4]. Confidentiality ensures that only the authorized individuals or systems have the right to access the exchanged information. Authenticity allows verification of the origin and owner of the exchanged information, and integrity ensures that the exchanged information has not been modified or tampered with. The confidentiality service is necessary to prevent illegal access to the transmitted images, whereas the integrity and authenticity are needed to verify ownership and detect tampering of the received images [5].

There are a lot of techniques that were used to ensure security for telemedicine applications; these techniques are cryptography, steganography and digital watermarking. Cryptography convert the medical information to unreadable form except to those who are authorized to achieve confidentiality and to provide authenticity. Steganography hide the existence of medical information in another object so it can maintain the integrity of the information. Digital watermarking is the process that hides watermark data into a multimedia object such that the watermark can be detected or extracted from the object to

Manuscript received April 5, 2019
Manuscript revised April 20, 2019

prove its ownership or validate its integrity [5]. Various encryption algorithms have been proposed in literature in order to ensure security for telemedicine applications [6-8]. Numerous numbers of digital watermarking schemes have been proposed to embed information into medical images for the protection of private information and the authentication of medical images, however, this technique has the disadvantage of not providing confidentiality to the watermarked multimedia objects [9-12]. There are a lot of steganography algorithms in the literature that are used to protect medical information [13-14].

Combining cryptography with steganography together can make a strong security system for securing medical information in order to maintain its confidentiality and integrity. There have been lots of work in the literature that combine steganography with cryptography for more security [15-20]. Reversible data hiding schemes in encrypted images are proposed in [21-22]. The image is encrypted with a stream cipher, and then information is embedded into the encrypted images by modifying a small proportion of those encrypted data. In [23], medical images are firstly divided into blocks; then, three LSB planes substitution is utilized in the regions of noninterest (RONI) in medical images for hiding the additional data. In [24], a reversible data hiding scheme in encrypted images by reserving room before encryption is proposed. The self-embedding of LSB planes guarantees the reversibility of LSB substitution embedding. In [25], additional information is firstly coded with a quantization index modulation (QIM) method; then this coded information is encrypted with RC4 algorithm; finally, the encrypted coded information is embedded into medical image with LSB substitution method. In [26], the authors proposed an encryption frame of medical image with watermark based on hyper chaotic system. Medical information is embedded into the regions of interest (ROI) in medical images with a high capacity difference-histogram based reversible data-hiding scheme, then the watermarked medical images are encrypted with hyper chaotic systems. The authors of [27] applied a reversible data hiding algorithm on encrypted medical images. They used AES algorithm to encrypt the medical image first, and then they used bit-substitution based method for hiding data in the encrypted domain. Algorithm [28] proposed reversible watermarking techniques and applied it on various medical image modalities. The proposed algorithm is region-based, and the RSA algorithm was used to provide secured transmission. In [29] a hybrid watermarking/ encryption algorithm was proposed. The algorithm combines quantization index modulation (QIM) and the AES algorithm. In [30] a randomized cryptographic fusion watermarking system was proposed. The system operates by encrypting the patient information then embedding the encrypted data in the medical image by bitwise operation.

We can summarize the previous works as follows: Some techniques used cryptography algorithms alone to secure medical information: all medical images and/or patient’s information should be encrypted before transmission to the other party. Some techniques used steganography algorithms a lone to secure medical information: embed the patient’s information in the medical image and send them to the other party. Some techniques used digital watermarking a lone to secure medical information: the patient’s information (the watermark) is inserted into the medical image (visible or invisible) and send them to the other party. Some techniques used a hybrid system by combing encryption and watermarking together to protect medical information.

Other hybrid systems were combined by using cryptography and steganography together to protect medical information; but the question is; which one comes first? Steganography or encryption. Some techniques used the encryption first for the medical image then use steganography second to embed the patient’s information in the encrypted image. Since the entropy of the encrypted image is maximal, the embedding step is considered like noise, is not possible by using standard data hiding algorithms. Reversible data hiding algorithms should be applied on encrypted images by wishing to remove the embedded data before the image decryption. Furthermore, some techniques used the encryption algorithm first to encrypt the patient’s information then use steganography second to embed the encrypted patient’s information in the medical image. Obviously combining steganography and cryptography together can give a strong security system to secure the medical information.

In this paper, we proposed a new approach for securing both medical images and patient’s information during transmission over an open access network (i.e. Internet) by using a hybrid system combined of cryptography and steganography. The cryptography technique adopted in this research was our encryption algorithm: Modified Jamal Encryption Algorithm (MJEA). MJEA is a novel symmetric block encryption algorithm; it has a 64-bit block size, 8-rounds and 120-bit key. Former evaluation experiments show the capability of MJEA for securing both plain texts and digital images [31-32]. For steganography we used a very simple algorithm that hides the patient’s information within the medical image by using bit-by-bit Xoring operation.

The rest of the paper is organized as follows: Section 2 gives a detailed description of the design process of the proposed technique. Section 3 shows experimental results and discusses the efficiency of the proposed mechanism. Finally, section 4 provides some concluding remarks and future work.

2. Description of the Proposed System

In this section, we are going to give a detailed description of the design process to define the proposed technique precisely. Figure 1 shows a block diagram for the proposed system at the transmitter side. As we see in this figure, we have three inputs for this system and two outputs. The inputs are: the medical image (Med_Img), the patient's information (Pat_Info) and the encryption key (K =120-bit). The outputs are: the encrypted image (Enc_Img) and the encrypted steganography image (Enc_Steg_Img); those outputs represent the two shares that will be transmitted to the other party. The proposed system works as follows: Firstly, we used the hexadecimal representation algorithm to convert the (Med_Img) and (Pat_Info) into 8-bit binary representation and store the result in arrays called (MI) and (PI). After that we used the encryption algorithm MJEA by the help of K (120-bit) to encrypt (MI) and store the result in array called (Enc_MI) which represents the encrypted form of the medical image. Note that the medical image will play the role as a cover media in this system and it will be used to hide the other secret which is the patient's information; to do that we used the embedding algorithm to do bit-by-bit XORing between (MI) and (PI) and store the result in an array called (SI) which represents the steganography image. As a double security, we encrypted the result (SI) by using MJEA and the help of (120-bit) key to get (Enc_SI) which represents an encrypted form of the steganography image. As a third level of security in this system, we used the scrambling algorithm to mix both arrays { Enc_MI & Enc_SI} in order to scramble them before transmission and the outputs for this level are: {Enc_Img & Enc_Steg_Img}; those outputs represent the two shares that will be sent to the anticipated recipient.

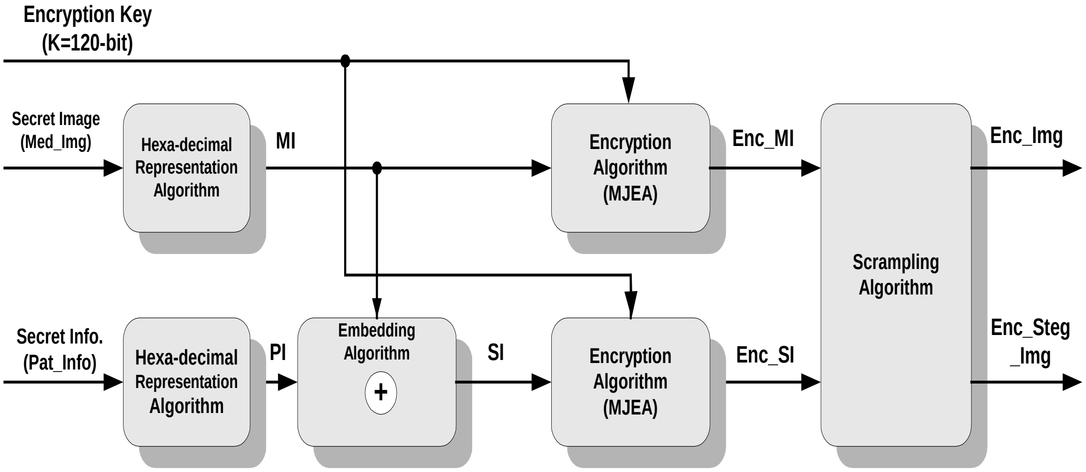


Fig. 1 A block diagram for the proposed system at the sender side

From the previous description about the proposed system at the transmitter side; we can note the following points:

If the attacker intercepted one of the two shares; he still needs the other one in order to start the process of recovering the original information. Furthermore, If he got the two shares and he was able to separate them; he still needs to break down the encryption algorithm; which is not an easy job; in order to recover back the original medical image. If the attacker was able to decrypt the (Enc_Img) and recovered the original medical image; still it is meaningless to him because it has no information about the case and about the patient; it is just an image; that is the reason why we did not embed the patient's information in the first share. Note that, the patient's information that was included in the second share passed through three levels of security; so it is secured against most known types of attacks. The size of the patient's information that will be embedded in the cover medium should not exceed the size of the medical image.

Figure 2 shows a block diagram for the proposed system at the receiver side. As we see in this figure, we have three inputs for this system and two outputs. The inputs are: the encrypted image (Enc_Img), the encrypted steganography image (Enc_Steg_Img) and the encryption key (K =120-bit). The outputs are: The medical image (Med_Img) and the patient's information (Pat_Info) that was sent by the transmitter. This system works as follows: The first step; we need to rearrange the received shares (Enc_Img and Enc_Steg_Img) in arrays with 8-columns and S/8 rows; where S represents the number of pixels for the medical image. Then we used the Scrambling Algorithm to separate both arrays to get the original ones (Enc_MI and Enc_SI). After that, we used the decryption algorithm (MJEA) by the help of K (120-bit) to decrypt

(Enc_MI) and (Enc_SI) to get the original arrays that represents the medical image and the steganography image (MI, SI). Furthermore; we used the extracting algorithm to do bit-by-bit XORing between MI and SI to get back the original PI. The last step we used the hexadecimal representation algorithm in the reverse direction to reconstruct the (Med_Img) by reshaping the array (MI) and to reconstruct the (Pat_Info) by reshaping the array (PI). The proposed system was able to recover back the original: {Med_Img & Pat_Info} that was sent by the sender.

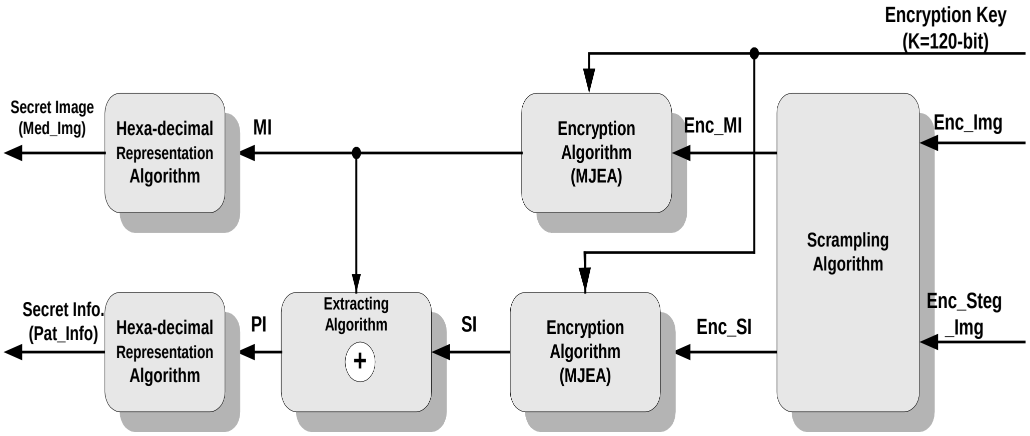


Fig. 2 A block diagram for the proposed system at the receiver side

As seen in Figures (1 & 2), the proposed system has four algorithms: the hexadecimal representation algorithm, the embedding / extracting algorithm, the encryption / decryption algorithm and the scrambling algorithm. In the following sections, we will give a detailed description about each one of them.

2.1 Hexadecimal Representation Algorithm

The main use of this algorithm at the transmitter side is to convert the medical image and patient's information into 8-bit binary representation (known that each pixel of the medical image needs 8-bit of storage). At the receiver side this algorithm works in the reverse direction to reconstruct the (Med_Img) by reshaping the array (MI) and to reconstruct the (Pat_Info) by reshaping the array (PI.) Note that each row in all arrays used in the proposed system {MI, PI and SI) should store 64-bit this is necessary to match the requirement of the encryption algorithm (MJEA) that will be used in the proposed system which is (64-bit) block encryption algorithm.

2.2 The Embedding/ Extracting Algorithm

The main use of this algorithm is to embed the secret information (patient's information) into the cover image (medical image) at the sender side and to extract those information from the cover image at the receiver side. The inputs for the embedding process comes from the previous step (MI and PI). Those inputs are arrays with 8-columns and S/8 rows; which represents the hexadecimal representation of the medical image and the patient's information. This process could be done simply by using the idea of bit-by-bit Xoring between MI and PI to get the steganography image. This output stored in an array (SI) with 8-columns and S/8 rows. The reason for choosing this simple algorithm because SI will be secured by two more levels of security: first, it will be encrypted by using the encryption algorithm MJEA then it will be scrambled by the scrambling algorithm; we will talk about those steps in sections 2.3 and 2.4. The extracting process is done at the receiver side and it is used to extract the secret information (i.e. patient's information) from the cover image (medical image). This process will be done by applying the inverse bit-by-bit Xoring that was done at the sender side. The inputs for this process are: (MI and SI) that comes out of the decryption algorithm; the output for this process was the array (PI) that represents the original patient's information that was sent by the sender. This output will be transferred to the hexadecimal representation algorithm to be used in the reverse direction to reconstruct the (Pat_Info) by reshaping the array (PI). This process was able to recover back the original secret information (Pat_Info) that was sent by the sender.

2.3 Encryption / Decryption Algorithm

In this research we used our encryption algorithm (MJEA) for image encryption / decryption. MJEA is a novel symmetric-key block ciphering algorithm, it has a 64-bit block size, 8-rounds and 120-bit key. MJEA divides the plain text message or the secret image into (64-bit) blocks then it encrypts each block separately. All operations in MJEA are XORed on 8-bit words. The 64-bit block of the plain text (Pt) goes in one end of the algorithm, and then the algorithm runs to produce the 64-bit of ciphered text (Ct) at the end. Each (Pt) block is converted into a (Ct) block in 8-roundes under the control of (120-bit) encryption key. The decryption process in MJEA is different from the encryption process in that the S-boxes must be used in the reverse order, as well as the inverse linear transformation and reverse order of the sub-keys.

Decryption for MJEA is relatively straightforward beginning with the ciphered text as input which is divided into (64-bit) blocks, then each block is decrypted separately. The (64-bit) block of the Ct goes in one end of the algorithm, and then the algorithm runs to produce the (64-bit) of Pt at the end. Each Ct block is converted into a Pt block in 8-roundes under the control of the same (120-bit) encryption key that was used in the sender side. The design of the algorithm is easy to implement and its performance results is good according to the avalanche effect. MJEA has been analyzed considerably as plain text encryption algorithm through a series of simulation tests. The algorithm thoroughly scrambling the plaintext with the key and it achieved a good Avalanche Effect when it is tested separately; on average more than 50% of the bits were changed when we changed a bit in the plaintext, key or the ciphertext. A comparison has been conducted between MJEA and different encryption algorithms and the simulation results clearly showed the superiority of MJEA over the other encryption algorithms in terms of Avalanche Effect [31]. Also MJEA has been analyzed considerably as image encryption algorithm. Experimental results showed the possibility of applying MJEA to encrypt digital images. The algorithm was able to achieve high embedding capacity and high quality of encoded image. It was able to replace and transform of all pixels in the original-image, and on the other side there was no loss of the image quality after performing the decryption process [32].

We applied MJEA at the sender side to encrypt the medical image and the steganography image to get the (Enc_Img & Enc_SI). At the receiver side we applied MJEA to decrypt the (Enc_Img & Enc_SI) to get back the original medical image that was sent by the sender and the steganography image (SI) that hides the patient's information.

2.4 The Scrambling Algorithm

As a third level of security in the proposed system, we used the scrambling algorithm at the transmitter side to mix both arrays { Enc_MI & Enc_SI} in order to scramble them before transmission and the outputs for this algorithm are: {Enc_Img & Enc_Steg_Img}; those outputs represent the two shares that will be sent to the other party. Note that, if any attacker intercepted one of the two shares; he/she still needs the other one in order to start the process of recovering the original information. If the attacker got the two shares; he needs to know how to separate them in order to continue the process for recovering medical information. This algorithm will be used at the receiver side to separate the received shares (Enc_Img, Enc_Steg_Img) out of each other to get the original arrays (Enc_MI, Enc_SI) that represents the encrypted form of the array (MI) and the encrypted form of the array (SI) that will be sent to the decryption process. This algorithm is described in details step-by-step as follows:

```
Scrambling Algorithm at the sender side:
Inputs: Enc_MI and Enc_SI: that are received from the encryption algorithm
Outputs: Enc_Img, Enc_Steg_Img: that represent the two shares that will be sent to the receiver
Assume that:
• Enc_MI = X, Enc_SI = Y, Enc_Img = X′, Enc_Steg_Img = Y′
• S: represents the number of pixels for the medical image
  (known that each pixel needs 1-byte of storage).
• X, Y, X′and Y′: are arrays with 8-columns and S/8 rows, this
  means that each row will store 64-bit.
• Each array has (S/8) rows and each row stores a (64-bit) block
  of data
In this algorithm we will mix (X&Y) to generate (X′ & Y′)
• Assign the odd number of elements of X[1 … S/8] & Y[1 …
  S/8] to generate X′ [1 … S/8]
• Assign the even number of elements of X[1 … S/8] & Y[1 …
  S/8] to generate Y′ [1 … S/8]
1. X′ [1 .. S/8] = {X′[1], X′[2], X′[3], X′[4],… , X′[S/8-1], X′
   [S/8] }
         = {X [1], Y [1], X [3], Y [3], ……, X [S/8-1], Y[S/8-1] }
2. Ý [1 S/8] = {Y′ [1],Y′ [2],Y′ [3],Y′ [4], .., Y′ [S/8-1], Y′
   [S/8] }
          = {X [2], Y[2], X[4], Y[4], , X[S/8], Y[S/8] }
3.   X′ [1 … S/8] = Enc_Img, Y′ [1 … S/8] =
     Enc_Steg_Img

Scrambling Algorithm at the receiver side:
Inputs: Enc_Img, Enc_Steg_Img: that are received from the transmitter side
Outputs: Enc_MI and Enc_SI: that will be passed to the decryption algorithm
In this algorithm we will separate (X′ & Y′) to generate (X & Y) :
•   Assign the odd number of elements of X′[1 … S/8] & Y′[1
    … S/8] to generate X [1 … S/8]
•   Assign the even number of elements of X′[1 … S/8] & Y′[1 …
    S/8] to generate Y[1 … S/8]
1.  X [1 … S/8] = {X [1], X [2], X [3], …, X [S/8-1], X [S/8] }
          = {X′ [1], Y′ [1], X′ [3], Y′ [3], ……, X′ [S/8-1], Y′
```

In the next section; the performance of the proposed technique will be evaluated by considering several experimental tests under different metrics.

3. Experimental Results and Analysis

The performance evaluating process that was done in this research involves several experimental tests to check the invisibility and the robustness properties of the proposed technique; those tests will include the following:

- Visual testing to show how the proposed system works.
- Statistical test which include the PSNR (Peak Signal to Noise Ratio) to measure the quality of the image and the MSE (Mean Square Error) to measure the distortion in the image.
- Histogram analysis test: we calculated the histogram for each one of the medical images at the four phases of the proposed system then we did our analysis by comparing them together to check if the proposed technique is secure against histogram analysis attack.
- The Entropy test: used to measure the uncertainty association with random variable.
- The correlation coefficient test which is used to display the relationship between two neighboring pixels.

To check the robustness of the proposed system according to all tests that will be conducted in this section; we calculated and analyzed each metric for each one of the medical images at the four phases of the proposed system:

- The original medical image (Org_Img)
- The (Steg_Img), that represent the medical image mixed with the patient's information
- The encrypted medical image (Enc_Img)
- The encrypted steganography image (Enc_Steg_Img)

For conducting those experimental tests; we used MatLab because it supports image processing by using a group of orders under the Image Processing Tool Box.

For evaluation purposes, we selected three grey-scale medical images to be applied on the proposed technique: {EyeIris, Chest and Hand}; each image has (512 X 512) pixels; known that each pixel needs 1-byte of storage; that means each image needs 262144-byte of storage. We choose (59022 byte of data) that represents patient's information to be embedded in each one of the medical images which forms (22.5%) of the total size of each one of the cover images. We chose the following encryption key randomly to be used by MJEA algorithm for the encryption/decryption process in all experimental tests (given in hexa-decimal notation):

K (120-bit)= 1 1 2 2 3 3 4 4 5 5 6 6 7 7 8 8 0 0 9 9 7 7 5 5 3 3 1 1 2 2

3.1 Visual Testing for the Proposed Method

In this section we did a series of experiments to show the effectiveness and the correctness of the proposed technique: We need to proof that the sender is able to send both the medical image and the patient's information securely to the other party; also; we need to ensure that the receiver is able to recover back the exact original medical information that was sent by the sender without any loss.

For this test, we applied all selected medical images on the proposed technique. Figures (3-5) show all results for this experiment for the (EyeIris, Chest and Hand) images at the sender side: Figures (3-5).a show the medical images (Org_Img) that should be sent securely to the other party, Figures (3-5).b show images that represents the secret patient's information (Pat_Info) that should be sent securely to the other party, Figures (3-5).c show the medical images after they were encrypted by using MJEA and the help of the encryption key (Enc_Img), Figures (3-5).d show the (Steg_Img) that hides the patient's information and Figures (3-5).e show the (Enc_Steg_Img). Note that: {Figures (3-5).c & Figures (3-5).e} forms the two shares that will be sent to the receiver side. Both figures in this bundle are encrypted by using MJEA and the help of (120-bit) key; there is no risk sending them over unsecured channel because they are protected against man-in-the-middle attack.

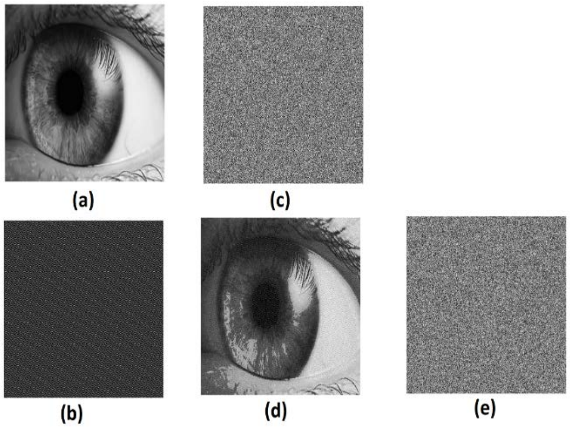


Fig. 3 Testing the EyeIris image at the sender side

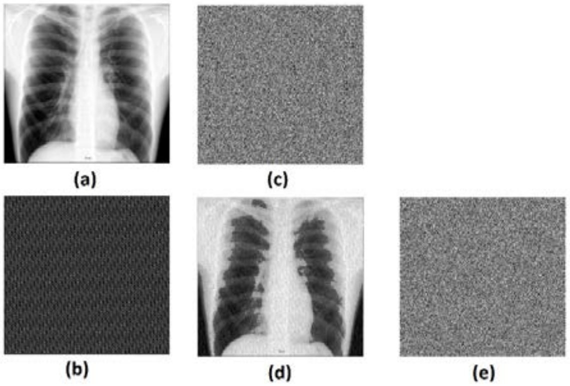


Fig. 4 Testing the Chest image at the sender side

Fig. 5 Testing the Hand image at the sender side

Assuming that the bundle that was sent by the sender is received correctly and securely and the receiver use the same encryption / decryption key that was used at the sender side. Figures (6-8) show all results for this experiment at the receiver side: Figures ((6-8).a and (6-8).b) show the bundle that was received from the sender, the first part of this bundle represents the (Enc_Steg_Img) and the second part represents the (Enc_Img). After we separate those parts and decrypt them by using MJEA and the help of (K=120-bit) we got the original medical images that are shown in Figures (6-8).c and the (Steg_Img) which are shown in Figures (6-8).d. The last step in this process is to extract the original secret information out of the (Steg_Img); this can be done by Xoring Figures (6-8).c and (6-8).d together and all results are shown in Figures (6-8).e which represents original patient’s information that was sent by the sender. Note that the recovered medical images and patients’ information that are shown in Figures ((6-8).c and (6-8).e) are exactly the same as the original ones that are shown in Figures ((3-5).a and (3-5).b) that were sent by the sender. Figures (6-8).e looks intact with Figures (3-5).a and the recovered patient’s information are exactly the same as the one that was sent by the sender. This means that the proposed system at the receiver side was able to recover back the original medical images and patient’s information that were sent by the sender without any loss.

As a final note on this test; it is obvious that nobody can notice by human visual system that the two shares which will be sent to the other side contain the secret medical image and secret patient’s information. There is no risk sending them over unsecured channel because they are protected against man-in-the-middle attack. At the receiver side: In all experiments; we noticed that the recovered medical images looks intact with the original ones that were sent by the sender, and the recovered patient’s information are exactly the same as the one that was sent by the sender. We can conclude that the proposed system works probably according to this test.

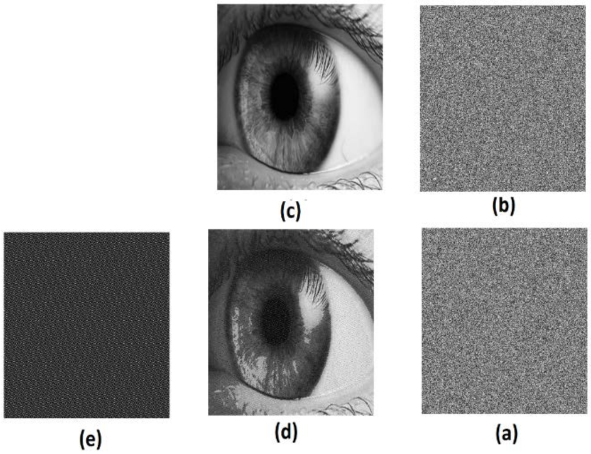


Fig. 6 Testing the EyeIris image at the receiver side

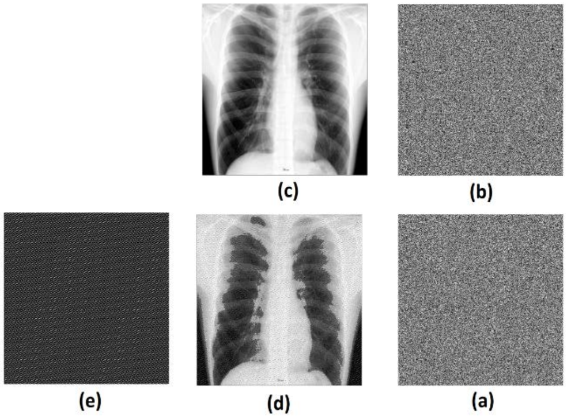


Fig. 7 Testing the Chest image at the receiver side

Fig. 8 Testing the Hand image at the receiver side

3.1 Histogram Analysis Test

A good image encryption scheme should always generate a cipher image of uniform histogram for any original images because the quality of images could be visually noticed by applying the histogram analysis. To check the robustness of the proposed system according to the histogram test; we calculated and analyzed the histogram for each one of the medical images at the four phases of the proposed system. For this test, we applied all selected medical images on the proposed technique. Figures (9-11) show the histogram analysis for the (EyeIris, Chest and Hand) images at the sender and receiver side. As we see in this image Figures (9-11).a represent histograms for the (Org_Img), Figures (9-11).b represent histogram for the (Enc_Img), Figures (9-11).c represent the histograms for the (Steg_Img), and Figures (9-11) .d represent the histograms for the (Enc_Steg_Img). Note that: {Figures (9-11).b and Figures (9-11).d} represent the two shares that will be transmitted by the sender over unsecured channel toward the receiver side. It is clear that those figures are close to the flat shape. They are fairly uniform and significantly different from the respective histograms shown if Figures (9-11).a and Figures (9-11).c. They does not contain any statistical resemblance to the original image and hence does not provide any clue to employ any statistical attack on the proposed system. The histogram uniformity in the results ensures the success of the proposed system in achieving the required randomness. Also, it is hard for the stegoanalysist to notice that there is an embedded data in Figures (9-11).d by analyzing and comparing it with Figures (9-11).c because it is totally different.

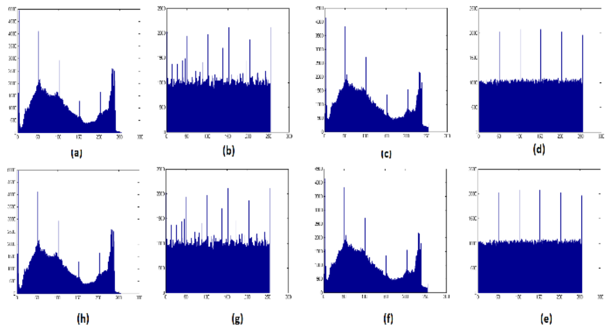


Fig. 9 The histogram of EyeIris image at the sender and receiver side

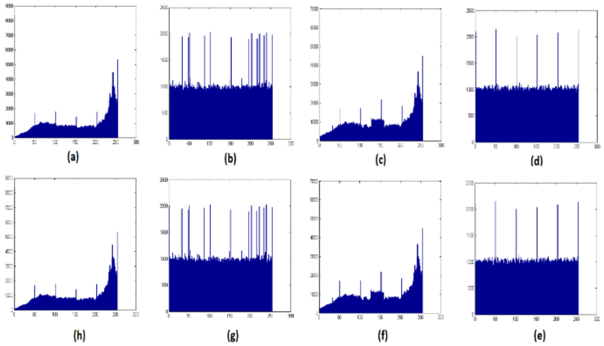


Fig. 10 The histogram of Chest image at the sender and receiver side

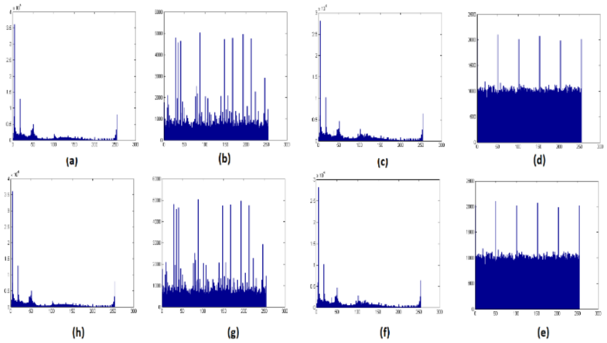


Fig. 11 The histogram of Hand image at the sender and receiver side

Assuming that the other party received correctly the same bundle that was sent by the sender: Figures (9-11).e represent the histograms for the received (Enc_Steg_Img), Figures (9-11).g represent the histograms for the received (Enc_Img), Figures (9-11).f represent the histograms for the decrypted (Steg_Img) and Figures (9-11).h represent the histograms for the decrypted medical images. Note that histograms of the recovered medical images that are shown in Figures (9-11).h looks intact with histograms of the original medical images at the sender side that are shown in Figures (9-11).a; this means that the proposed system at the receiver side was able to recover back the original medical image that was sent by the sender without any loss.

Histogram measurements further confirm the robustness level of the proposed technique; this means that the proposed technique is secured against histogram analysis attack and the known-plaintext attack.

3.2 Correlation Coefficient Analysis

Correlation test measures the relationship among various adjacent image pixels and this is considered as another evaluator metric to examine the robustness of the proposed system. If correlation between two pixels is nearly 1, the image Pixels is highly correlated but if it is nearly 0, the image pixels are highly uncorrelated; we need to get smaller values of the correlation coefficient, the lower values of correlation are better. The correlation coefficient between various pairs of different medical images have been analyzed and calculated by using equation 1 [5]:

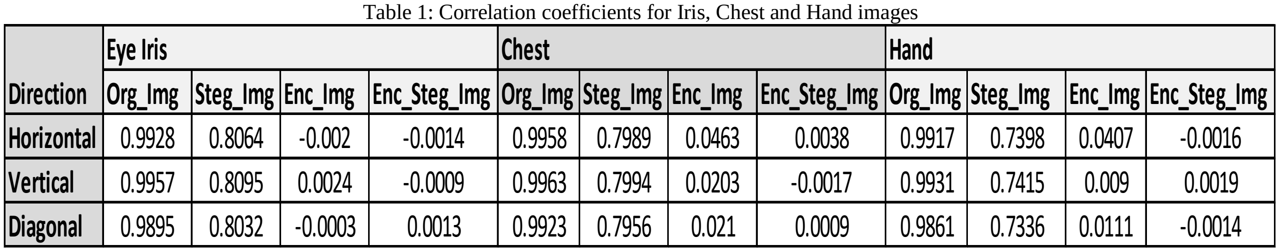
$$r_{xy} = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{(\sum_{i=1}^{N}(x_i - E(x))^2)}\sqrt{(\sum_{i=1}^{N}(y_i - E(y))^2)}} \quad (1)$$

Where:
x_i and y_i are gray level values of two adjacent pixels of the tested image, N is the number of pairs (x_i , y_i), E(x) is the mean of x_i : $E(x) = \frac{1}{N}\sum_{I=0}^{N} x_i$ and E(y) is the mean of y_i : $E(y) = \frac{1}{N}\sum_{I=0}^{N} y_i$

To check the robustness of the proposed system according to the correlation test; we calculated the correlation between various pairs for each medical image at the four phases of the proposed system. Table 1 shows the correlation of: {two horizontal adjacent pixels, two vertical adjacent pixels and two diagonal adjacent pixels} for the {Org_Img, Steg_Img, Enc_Img and Enc_Steg_Img }. Before start analyzing the results in this test; we will divide the tested images into two groups: the first group represents the plain images (not encrypted) which includes {Org_Img, Steg_Img} and the second group represents the encrypted images which includes {Enc_Img, Enc_Steg_Img} that will be sent to the other party.

As we can see from results for all medical images shown in Table 1; the correlation values for group 2 are close to zero while it is close to one in the first group which indicates a good performance for the proposed system that is because of the powerful permutation technique that was used in our encryption algorithm (MJEA) which based on reducing correlation between neighborhood pixels.

Table 1: Correlation coefficients for Iris, Chest and Hand images



Direction	Eye Iris				Chest				Hand			
	Org_Img	Steg_Img	Enc_Img	Enc_Steg_Img	Org_Img	Steg_Img	Enc_Img	Enc_Steg_Img	Org_Img	Steg_Img	Enc_Img	Enc_Steg_Img
Horizontal	0.9928	0.8064	-0.002	-0.0014	0.9958	0.7989	0.0463	0.0038	0.9917	0.7398	0.0407	-0.0016
Vertical	0.9957	0.8095	0.0024	-0.0009	0.9963	0.7994	0.0203	-0.0017	0.9931	0.7415	0.009	0.0019
Diagonal	0.9895	0.8032	-0.0003	0.0013	0.9923	0.7956	0.021	0.0009	0.9861	0.7336	0.0111	-0.0014

3.3 Image Entropy

Entropy measures the uncertainty association with random variable. Block Based Image Encryption techniques decreases the mutual information among encrypted image variables (i.e. high contrast) and thus increases the entropy value; a ciphered image encrypted by using such techniques should not provide any information about the original image. When evaluating the entropy for a truly random source that emits symbols with equal probability, it is calculated to be equals to (He= 8). Actually, a practical information source rarely generates random messages, in general its entropy value is smaller than the ideal one. However, when we have a secure cryptosystem; the entropy of the encrypted images should be nearly close to 8; if the output of such a cipher emits symbols with entropy less than that, there exists certain degree of predictability, which threatens its security. The information entropy is computed according to Equation 2 [7].

$$H_e = -\sum_{K=0}^{G-1} P(K).\log_2(P(K)) \quad (2)$$

Where: G represents the Gray value of an input image (0-255), and P(k) represents the probability of the occurrence of symbol (k)

To check the robustness of the proposed system according to the entropy test; we calculated the entropy for each medical image at the four phases of the proposed system. Table 2 shows the entropy of the {Org_Img, Steg_Img, Enc_Img and Enc_Steg_Img} for all tested medical images.

As we can see in Table 2; the information entropy obtained in all medical images for the {Enc_Img and Enc_Steg_Img} are very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the proposed system is secure against entropy attack. Also, we can see that using steganography technique followed by encryption by using MJEA resulted in higher entropy compared to using encryption alone.

The entropy values for the two shares that will be sent to the other party are very close to 8 which ensures a good performance for the proposed system according to this test.

Table 2: Entropy for different medical images at the four phases of the proposed system

Img Entropy	Org_Img	Steg_Img	Enc_Img	Enc_Steg_Img
Eye-Iris	7.7152	7.8053	7.9913	7.9993
Chest	7.8894	7.7903	7.9837	7.9991
Hand	8.8319	7.1795	7.7833	7.9985

3.4 PSNR and MSE Comparison Test

PSNR (Peak Signal to Noise Ratio) is a measure of the quality of the image and it is measured by comparing the (Cov-Img) with the (Steg-Img). And it is calculated by using Equation 3. Higher PSNR value indicates better quality of image (i.e. lower distortion which decrease the possibility of visual attach by human eyes) [1].

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAXi}^2}{\mathrm{MSE}}\right) \tag{3}$$

Where MAX_i is the maximum value of the samples and it equal 255 for a monochrome image have 8 bits per pixel
MSE (Mean Square Error) which defines as the square of error between the (Cov-Img) and the (Steg-Img) and it is calculated by using Equation 4. Higher value of MSE means more image distortion.

$$\mathrm{MSE} = \frac{1}{M*N}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}(C(i,j) - S(i,j))^2 \tag{4}$$

Where: M*N is the image size, C(i,j) is intensity of the pixel at the Cov-Img and S(i,j) is the intensity of the pixel at the Steg-Img.
To conduct this test, we embedded (59022 byte of data) that represents: {patient's information, medical image report, description about the case, etc…) in each one of the selected medical images then we calculated the PSNR and MSE values for all {Steg_Img, Enc_Img and Enc_Stego_Img} produced by the proposed technique.
Table 3 shows the MSE and the PSNR results for this test. As seen from the results shown in this table; the MSE values for the encrypted images goes up compared to the steganography images and the PSNR values for the encrypted images goes down compared to the steganography images; so the performance of the proposed system shows a good behavior under the PSNR and MSE tests. This result ensures the strength of the proposed system that was able to add more image distortion; which makes it difficult for anyone to notice by human eyes that there is exist a hidden data in the encrypted images that will be sent to the other party.

Table 3: PSNR and MSE results

Images	MSE	PSNR
[EyeIris_Img, Steg_Img]	912.297	18.5294
[EyeIris_Img, Enc_Img]	1.04E+04	7.98E+00
[EyeIris _Img,Enc_Steg_Img]	1.08E+04	7.89E+00
[Chest_Img, Steg_Img]	1.15E+03	1.75E+01
[Chest_Img, Enc_Img]	1.24E+04	7.20E+00
[Chest_Img,Enc_Steg_Img]	1.28E+04	7.07E+00
[Hand_Img, Steg_Img]	1.35E+03	1.88E+01
[Hand_Img, Enc_Img]	1.32E+04	8.92E+00
[Hand_Img,Enc_Steg_Img]	1.40E+04	8.88E+00

All experimental results proved the capability of the proposed system in providing a secure distribution of medical images and patient's information between entities while transmission over unsecure channel. At the receiver side, the proposed system was able to recover back the original medical image and the patient's information that was sent by the sender without any loss.

4. Conclusions and Future Work

The main contribution of this research is developing a new security system that combine cryptography and steganography techniques to provide a secure distribution for both the medical images and patient's information to the other party over un-secure channel to protect it against attackers.
From the simulation results that was done in this research; we can conclude the following points: Based on the visual testing result: the two shares looks scrambled because the proposed system was able to add more image distortion to them; which makes it difficult for anyone to notice by human eyes that there exists a hidden data in those images. There is no risk sending them over unsecured channel because they are protected against man-in-the-middle attack. The correlation values for those shares are very close to zero which indicates a good performance for the proposed system that is because of the powerful permutation technique that was used in our encryption algorithm (MJEA) which based on reducing correlation between neighborhood pixels. The information entropy for those shares are very close to the theoretical value of 8. This means that information leakage in the encryption process is negligible and the proposed system is secured against entropy attack. The MSE values for the two shares goes up and the PSNR values goes down compared to the steganography images. So, the performance of the proposed system shows a good behavior under the PSNR and MSE tests. The histogram uniformity in the results ensures the robustness level of the proposed technique; this means that our system is secured against histogram analysis attack and the known-plaintext attack. Using steganography technique followed by encryption resulted in a lower correlation and higher entropy compared to using encryption alone. The receiver was able to recover back all medical images and patients' information and they looks exactly the same as the original ones that were sent by the sender without any loss.
Some further work that could be done to improve the performance of the proposed system: Use the proposed algorithm with the transform domain embedding technique which will improve the robustness of the algorithm. Try to use the losses compression image format such as JPEG. Try to use 32-bit color medical images. More thorough testing and analysis to get better performance

References

[1] M. Barni, F. Bartolini, "Data Hiding for Fighting Piracy", IEEE Signal Processing Magazine, Vol. 21, No. 2, pp. 28–39, 2004.

[2] V. Fotopoulos, M. Stavrinou, and A. Skodras, "Medical Image Authentication and Self-Correction Through an Adaptive Reversible Watermarking Technique", in Proceedings of the 8th IEEE International Conference on BioInformatics and BioEngineering (BIBE'08), pp. 1–5, 2008.

[3] O. Pianykh, Digital Imaging and Communications in Medicine (DICOM), Springer-Verlag, 2012.

[4] L. Kobayashi, S. Furuie, and P. Barreto, "Providing Integrity and Authenticity in DICOM Images: A novel Approach", IEEE Transactions on Information Technology in Biomedicine, Vol. 13, Issue. 4, pp. 582-589, 2009.

[5] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 2013.

[6] G. Alvarez, S. Li, and L. Hemandez, "Analysis of Security Problems in A medical Image Encryption System", Computers in Biology and Medicine, Vol. 37, No. 3, pp. 424-427, 2007.

[7] A. Mahmood, R. Dony, "Segmentation Based Encryption Method for Medical Images", in Proceedings of the 6th International Conference on Internet Technology and Secured Transactions, December 2011.

[8] F. Taleb, "A New Chaos Based Image Encryption Scheme Using Chaotic Logistic Maps", in Proceedings of the Multimedia Computing and Systems 2014 International Conference (ICMCS), pp. 1222-1228, 2014.

[9] C. Cruz, R. Reyes, J. Mendoza, M. Nakano, and H. Perez, "A Novel Verification Scheme for Watermarking Based Image Content Authentication Systems", Telecommunications and Radio Engineering, Vol. 67, No. 19, pp. 1777-1790, 2008.

[10] A. Giakoumaki, S. Pavlopoulos, and D. Koutsouris, "Multiple Image Watermarking Applied to Health Information Management", IEEE Transactions on Information Technology in Biomedicine, Vol. 10, No. 4, pp. 722-732, 2006.

[11] D. Nilanjan, P. Moumita , D. Achintya, "A Session Based Blind Watermarking Technique Within the NROI of Retinal Fundus Images for Authentication Using DWT, Spread Spectrum and Harris Corner Detection", International Journal of Modern Engineering Research, Vol. 2, Issue. 3, pp. 749-757, 2010.

[12] M. Soliman, A. Hassanien, N. Ghali, and H. Onsi, "An Adaptive Watermarking Approach for Medical Imaging Using Swarm Intelligent", International Journal of Smart Home, Vol. 6, No. 1, pp. 37-49, 2012.

[13] M. E. Whitman, H. J. Mattord, Principles of Information Security, Fourth Edition, Course Technology, 2012.

[14] P. Hall, Modern Cryptography: Theory and Practice, Hewlett-Packard Company, 2003.

[15] K. Joshi, R. Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", in Proceedings of the Third International Conference on Image Information, pp. 86-90, 2015.

[16] Y. Renaer, Z. Zhiwei, T. Shun, D. Shilei, "Image Steganography Combined with DES Encryption Pre-processing", in Proceedings of the Sixth International Conference on Measuring Technology and Mechatronics Automation, pp. 323-326, 2014.

[17] S. Ushll, G. Kumal, K. Boopathybagan, "A Secure Triple Level Encryption Method Using Cryptography and Steganography", in Proceedings of the International Conference on Computer Science And Network Technology, pp. 1017-1020, 2011.

[18] G. S. Charan, N. Kumar, B. Karthikeyan, V. Yanathan and K. Lakshmi, "A Novel LSB Based Image Steganography with Multi-Level Encryption", International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19-20 March 2015.

[19] S. Laskar, K. Hemachandran, "High Capacity Data Hiding Using LSB Steganography and Encryption", International Journal of Database Management Systems, Vol. 4, No. 6, pp. 57-62, 2012.

[20] W. Al-qwider, J. Bani Salameh, "A Novel Technique for Securing Data Communication Systems by Using Cryptography and Steganography", Jordanian Journal of Computers and Information Technology (JJCIT), Vol. 3, No. 2, pp. 110-130, 2017.

[21] X. Zhang, "Reversible data hiding in encrypted image", IEEE Signal Processing Letters, Vol. 18, No. 4, pp. 255–258, 2011.

[22] W. Hong, T. Chen, and H. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match", IEEE Signal Processing Letters, Vol. 19, No. 4, 2011, pp. 199–202, 2012.

[23] A. Lavanya and V. Natarajan, "Watermarking Patient Data in Encrypted Medical Images", in Proceedings of the Sadhana-Academy in Engineering Sciences, Vol. 37, pp. 723–729, 2012.

[24] X. Zhang, "Separable Reversible Data Hiding in Encrypted Image", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, pp. 826–832, 2012.

[25] D. Bouslimi, G. Coatrieux, M. Cozic, and C. Roux, "A Joint Encryption /Watermarking System for Verifying the Reliability of Medical Images", IEEE Transactions on Information Technology in Biomedicine, Vol. 16, pp. 891–899, 2012.

[26] S. Zhang, G. Tiegang, and L. Gao, "A Novel Encryption Frame for Medical Image with Watermark Based on Hyperchaotic System", Mathematical Problems in Engineering, Vol. 11, 2014.

[27] W. Puech, "An Efficient Hybrid Method for Safe Transfer of Medical Images", in Proceedings of the 2nd International Conference: E-Medical Systems, PP. 29-31, 2008.

[28] A. Umamageswari, U. Ferni, and G. Suresh, "A Survey on Security in Medical Image Communication", International Journal of Computer Applications, Vol. 30, No.3, 2011.

[29] D. Bouslimi, and G. Coatrieux, "A joint Watermarking/ Encryption Algorithm for Verifying Medical Image Integrity and Authenticity in Both Encrypted and Spatial Domains", in Proceedings of the 33th Annual International Conference of the IEEE- EMBS, Massachusetts USA, 2011.

[30] P. Viswanathan and P. Krishna, "Randomized Cryptographic Fusion Watermarking Medical Image with Reversible Property", International Journal of Computer Information Systems, Vol. 2, 2011.

[31] J. Bani Salameh, "A New Symmetric-Key Block Ciphering Algorithm", Middle-East Journal of Scientific Research (MEJSR), Vol. 12, No. 5, pp. 662-673, 2012.
[32] J. Bani Salameh, "An Investigation of the Use of MJEA in Image Encryption", WSEAS Transactions on Computers, Vol. 15, pp. 12-23, 2016.

Dr. Jamal N. Bani Salameh was born in Irbed, Jordan. He received the B.C degree in Electrical Engineering from Mutah University, Jordan, in 1988, M.S. and Ph.D. degrees in Computer Engineering from New Mexico State University, U.S.A, in 2000 and 2005. Dr. Bani Salameh became Associate Professor at the Department of Computer Engineering of Mutah University in 2013 and has published widely in international journals. Now, he works as Vice Dean of Faculty of Engineering at Mutah University. His research interests are in the fields of wireless computer networks, multicast routing, network security and cryptography. Dr. Bani Salameh held a number of administrative positions including Chairman of the IT Department, SUR College for Applied Sciences, Oman, Sept. 2010 – Aug. 2011, Chairman of the Computer Engineering Department, Mutah University, Jordan, Sept. 2015 – Sept. 2016.