IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON INFORMATION SECURITY SOLUTIONS FOR TELEMEDICINE APPLICATIONS

Received February 20, 2018, accepted March 17, 2018, date of publication March 21, 2018, date of current version May 2, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2817615

Secure Medical Data Transmission Model for IoT-Based Healthcare Systems

MOHAMED ELHOSENY[1], GUSTAVO RAMÍREZ-GONZÁLEZ[2], OSAMA M. ABU-ELNASR[3], SHIHAB A. SHAWKAT[4], ARUNKUMAR N[5], AND AHMED FAROUK[1]

[1]Faculty of Computers and Information, Mansoura University, Mansoura 35516, Egypt
[2]Department of Telematics, University of Cauca, Popayán 190001, Colombia
[3]Computer Science Department, College of Computes and Information, Mansoura University, Mansoura 35516, Egypt
[4]Directorate of Education, Salah Al-Din, Iraq
[5]School of Electrical and Electronics Engineering, SASTRA University, Thanjavur 613401, India

Corresponding author: Mohamed Elhoseny (mohamed_elhoseny@mans.edu.eg)

ABSTRACT Due to the significant advancement of the Internet of Things (IoT) in the healthcare sector, the security, and the integrity of the medical data became big challenges for healthcare services applications. This paper proposes a hybrid security model for securing the diagnostic text data in medical images. The proposed model is developed through integrating either 2-D discrete wavelet transform 1 level (2D-DWT-1L) or 2-D discrete wavelet transform 2 level (2D-DWT-2L) steganography technique with a proposed hybrid encryption scheme. The proposed hybrid encryption schema is built using a combination of Advanced Encryption Standard, and Rivest, Shamir, and Adleman algorithms. The proposed model starts by encrypting the secret data; then it hides the result in a cover image using 2D-DWT-1L or 2D-DWT-2L. Both color and gray-scale images are used as cover images to conceal different text sizes. The performance of the proposed system was evaluated based on six statistical parameters; the peak signal-to-noise ratio (PSNR), mean square error (MSE), bit error rate (BER), structural similarity (SSIM), structural content (SC), and correlation. The PSNR values were relatively varied from 50.59 to 57.44 in case of color images and from 50.52 to 56.09 with the gray scale images. The MSE values varied from 0.12 to 0.57 for the color images and from 0.14 to 0.57 for the gray scale images. The BER values were zero for both images, while SSIM, SC, and correlation values were ones for both images. Compared with the state-of-the-art methods, the proposed model proved its ability to hide the confidential patient's data into a transmitted cover image with high imperceptibility, capacity, and minimal deterioration in the received stego-image.

INDEX TERMS Cryptography, DWT-1level, DWT-2level, encryption, healthcare services, Internet of Things, medical images, steganography.

I. INTRODUCTION

IoT creates an integrated communication environment of interconnected devices and platforms by engaging both virtual and physical world together [1]. With the advent of remote digital healthcare based IoT systems, the transmission of medical data becomes a daily routine. Therefore, it is necessary to develop an efficient model to ensure the security and integrity of the patient's diagnostic data transmitted and received from IoT environment [2]–[8]. This goal is carried out using steganography techniques and system encryption algorithms together to hide digital information in an image [9]–[16].

Cryptography is another term for data encryption [17]. Encryption cryptography is the process of encoding messages in a way that hackers cannot read it, but that can be authorized personnel. The two main algorithms used for data encryption in this work are the Advanced Encryption Standard (AES) and the Rivest-Shamir-Adleman (RSA) algorithm [18]. AES is a symmetric cipher where the same key is used on both sides [19]. It has a fixed message block size of 128 bits of text (plain or cipher), and keys of length 128,192, or 256 bits. When longer messages are sent, they are divided into 128-bit blocks. Apparently, longer keys make the cipher more difficult to break, but also enforce a longer encrypt and decrypt process. On the contrary, the RSA is a public key algorithm, which widely used in business and personal communication sectors [20]. It has the advantage of having a variable key size ranging from (2-2048) bits.

The primary research in hiding data started with steganography, which refers to the science and art of hiding

information within an image. The benefit of steganography is that it can be utilized to transmit classified messages without the fact of the transmission being detected. The DWT has a tremendous spatial localization, frequency spread, and multi-resolution characteristics, which are matching with the theory of forms in the human visual system. This paper implements both 1-level and 2-level of DWT steganography techniques that operate on the frequency domain. It split up the image into high and low iteration parts. The high iteration part contains edge information, whereas the low iteration part is frequently divided into high and low iteration parts [21].

The purpose of the steganography is not only preventing others from knowing the hidden information, but also removing the suspicion in having hidden information. The message is a confidential document to be transmitted and camouflaged in the carrier so that it becomes difficult to detect. There are two main aspects in any steganography system, which are steganography capacity and imperceptibility. However, these two properties are confusing with each other because it is tough to increase capacity while maintaining the steganography imperceptibility of a steganography system. Furthermore, there are still limited methods of concealing information for use with data transfer communication protocols, which can be unconventional but their future is promising.

This paper aims to improve the security of medical data transmission based on the integration between a steganography technique and a hybrid encryption scheme to get a highly secured healthcare system.

This paper is organized into five sections including this section. Section 2 illustrates the related works; Section 3 explains the proposed model and their algorithms; Section 4 provides the experimental results and their discussions, and Section 5 summarizes the main conclusions.

II. RELATED WORKS

Shehab *et al.* [2], surveyed a comprehensive study on security issues in IoT networks. Various security requirements such as authentication, integrity, confidentiality were discussed. A comparative study of different types of attacks, their behavior, and their threat level that categorized into low-level, medium-level, high-level, and extremely high-level attacks and suggested possible solutions to encounter these attacks were provided.

Bairagi *et al.* [3], proposed three color image steganography approaches for protecting information in an IoT infrastructure. The first and third approaches use three (red, green, and blue) channels, while the second approach uses two (green and blue) channels for carrying information. Dynamic positioning techniques have been used for hiding information in the deeper layer of the image channels with the help a shared secret key.

Anwar *et al.* [4], developed a technique to secure any type of images especially medical images. They aimed to maintain the integrity of electronic medical information, ensuring availability of that information, and authentication of that information to ensure that authorized people only can access the information. First, the AES encryption technique was applied on the first part. The ear print also embedded in this work, where seven values were extracted as feature vector from the ear image. The proposed technique improved the security of medical images through sending them via the internet and secured these images from being accessed via any unauthorized person.

Abdelaziz *et al.* [5], surveyed the analysis of the security vulnerabilities and the risk factors detected in mobile medical apps. According to risk factor standards, these apps can be categorized into remote monitoring, diagnostic support, treatment support, medical information, education and awareness, and communication and training for healthcare workers. Eight security vulnerabilities and ten risks factors detected by the World Health Organization (OWASP) mobile security project in 2014 have been analyzed.

Razzaq *et al.* [9], proposed a fused security approach based on encryption, steganography, and watermarking techniques. It decomposed into three stages; (1) encrypting the cover image using XOR operation, (2) embedding process done using least significant bits (LSBs) for generating the stego-image, then (3) watermarking the stego-image in both spatial and frequency domains. Experimental results proved that proposed method was very much efficient and secured.

Jain *et al.* [11], proposed a new technique for transferring the patient's medical information into the medical cover image by hiding the data using decision tree concept. The coding is done in the form of different blocks that evenly distributed. In concealment, secret code blocks are assigned to the cover image to insert the data by the mapping mechanism based on breadth-first search. RSA algorithm was used to encipher the data before embeddings.

Yehia *et al.* [12], surveyed various healthcare applications based on wireless medical sensor network (WMSN) that can be implemented in IoT environment. Also, discussed the security techniques that used for handling the security issues of healthcare systems especially hybrid security techniques.

Zaw and Phyo [13], presented an algorithm based on dividing the original image to the group of blocks, where these blocks are arranged in the form of turns using a transformation algorithm. After that, the transformed image is encryption using the Blowfish algorithm. It was found that the correlation decreases and the entropy increase by increasing the number of blocks through using smaller block sizes.

Sreekutty and Baiju [21], proposed a medical integrity verification system to improve the security of medical image. The proposed system mainly decomposed into two stages: 1) the protection and 2) the verification. Through the protection stage, the binary form of the secret data is embedded in the high-frequency part (HH) within the cover image using 2D Haar DWT frequency domain technique. Through the verification stage, the extraction algorithm is applied to retrieve the original cover image and secret data.

Bashir *et al.* [22], proposed an image encryption technique based on the integration of shifted image blocks and the

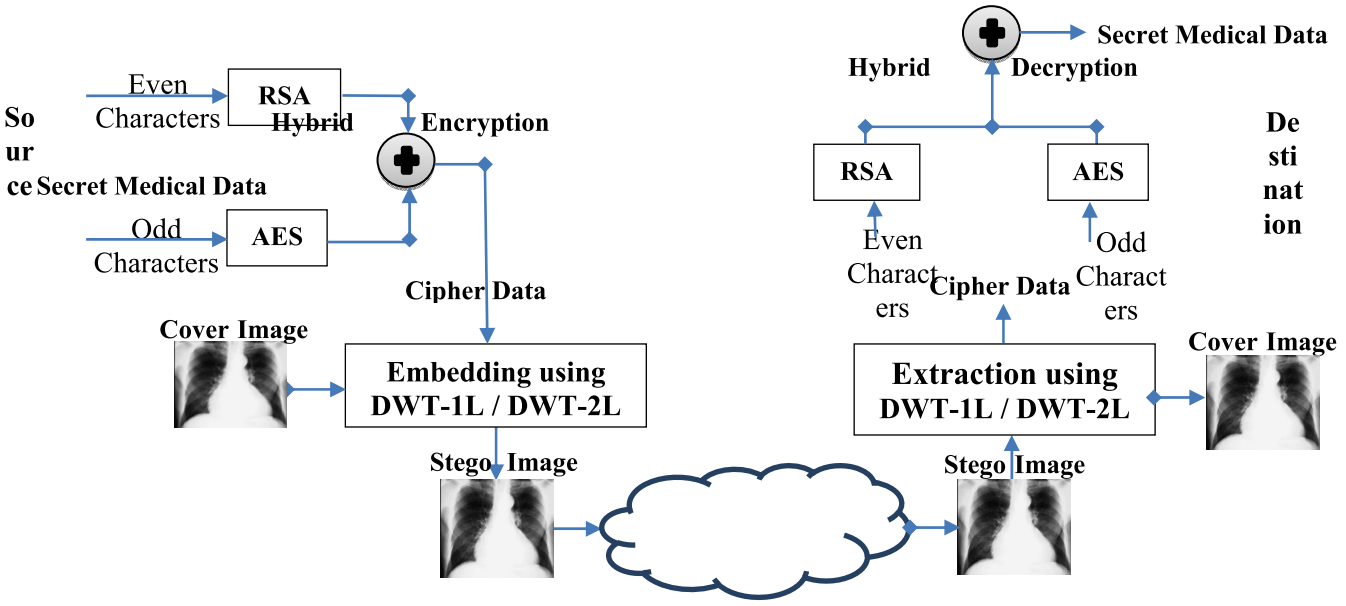

FIGURE 1. The proposed framework for securing the medical data transmission.

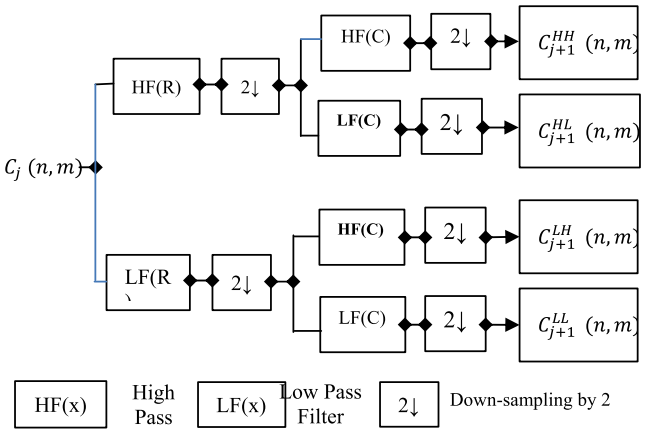

FIGURE 2. The decomposition process of DWT-2L.

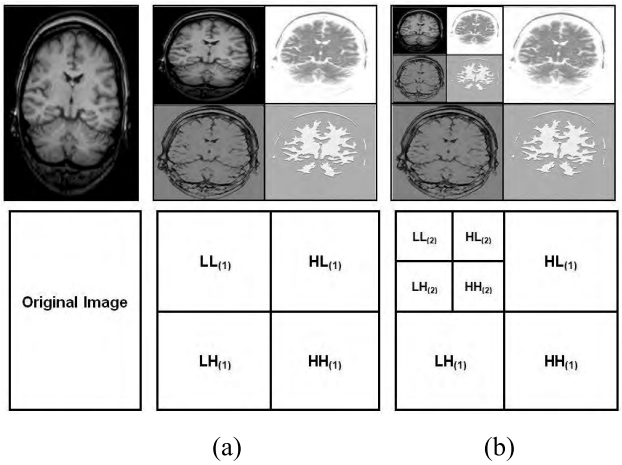

FIGURE 3. DWT decomposition of an image. (a) DWT-1L. (b) DWT-2L.

basic AES. The shifted algorithm technique is used to divide the image into blocks. Each block consists of many pixels, and these blocks are shuffled by utilizing a shift technique that moves the rows and columns of the original image in such a way to produce a shifted image. This shifted image is then used as an input image to the AES algorithm to encrypt the pixels of the shifted image.

Muhammad *et al.* [23], presented an efficient, secure method for RGB images based on gray level modification (GLM) and multi-level encryption (MLE). The secret key and the secret data are encrypted using MLE algorithm before mapping it to the gray-levels of the cover image. Then, a transposition function is applied to the cover image before data hiding. The usage of transpose, secret key, MLE, and GLM adds four different levels of security to the proposed algorithm, making it very difficult for a malicious user to extract the original secret information.

Yin *et al.* [24], proposed an image steganography approach based on Inverted LSB (ILSB) technique for securing the transmitted face images from the IP camera as the IoT device to the home server in the LAN network. The local home server serves as a processing power node for the encryption of the stego images before transmitting them to the cloud and other devices for further processing.

Seyyedi *et al.* [25], proposed a secure steganography method based on encrypting the confidential information using the symmetric RC4 encryption method and embedding it within the cover image based on the partitioning approach with minimal degrading of the quality. The cover image is partitioned into a predefined 8×8 blocks. Each block is manipulated using Integer Lifting Wavelet Transform (ILWT) method, then TSO (Tree Scan Order) is applied

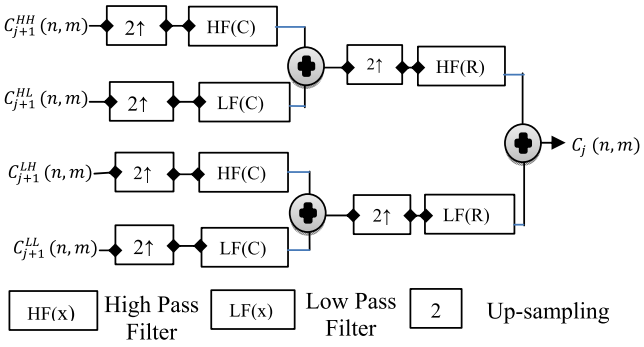

FIGURE 4. The synthesis process of 2D-DWT-2L.

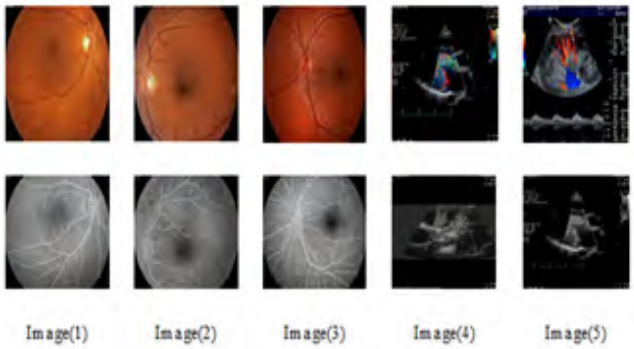

FIGURE 5. Color and gray format of the dataset.

to each manipulated block to identify proper location of confidential information.

Khalil [26], proposed a method that studies the medical image quality degradation when hiding data in the frequency domain. The secret plaintext was encrypted using RC4 encryption before the embedding process. The Discrete Fourier Transform (DFT) was applied to transfer the cover image into the frequency domain by decomposing it into its sinusoidal (sine and cosine) fundamental components in different frequencies. The results indicated that the quality of the image is exceptionally degraded when embedding data close to the low-frequency bands (DC) and this effect decreases in the upper-frequency bands.

Abdel-Nabi and Al-Haj [27], proposed a crypto-watermarking approach based on AES standard encryption algorithm and reversible watermarking data hiding technique to secure medical images. The results proved that the proposed approach achieves both the authenticity and integrity of the images either in the spatial domain or the encrypted domain or both domains.

Li *et al.* [28], proposed a secret image sharing scheme compatible with an IoT- cloud framework for embedding the secret image shares. The proposed scheme composed of two modules; shadow images generation module for generating the secret shares based on the Shamir's polynomial, and sharing key formulation module for embedding the secret image shares into the cover image based on a 24-ary notational system.

TABLE 1. Results of PSNR and MSE values using 2D-DWT-1L and 2D-DWT-2L for color images.

Image	Text Size (byte)	PSNR		MSE	
		DWT-2L	DWT-1L	DWT-2L	DWT-1L
Image(1)	15	56.60	56.13	0.14	0.16
	30	53.48	52.44	0.29	0.37
	45	51.65	50.49	0.44	0.58
	55	51.91	49.73	0.41	0.69
	100	52.46	46.80	0.37	1.36
	128	50.70	46.05	0.55	1.61
	256	51.66	43.04	0.44	3.22
Image(2)	15	56.60	56.13	0.14	0.16
	30	53.48	52.44	0.29	0.37
	45	51.62	50.49	0.45	0.58
	55	51.88	49.73	0.42	0.69
	100	52.45	46.80	0.37	1.36
	128	50.65	46.07	0.56	1.60
	256	51.60	43.06	0.45	3.21
Image(3)	15	56.24	56.00	0.15	0.16
	30	53.42	52.30	0.29	0.38
	45	51.56	50.40	0.45	0.59
	55	51.82	49.64	0.43	0.70
	100	52.40	46.79	0.37	1.36
	128	50.59	46.02	0.57	1.62
	256	51.49	43.00	0.46	3.25
Image(4)	15	56.39	54.88	0.15	0.21
	30	54.25	51.86	0.24	0.42
	45	52.42	50.14	0.37	0.63
	55	52.37	49.33	0.38	0.76
	100	53.78	46.82	0.27	1.35
	128	51.79	45.85	0.48	1.69
	256	51.27	42.77	0.43	3.43
Image(5)	15	57.44	55.15	0.12	0.17
	30	56.42	52.41	0.29	0.21
	45	53.66	52.19	0.37	0.47
	55	51.69	50.63	0.38	2.95
	100	51.88	52.92	0.30	1.01
	128	52.66	50.86	0.49	2.69
	256	50.58	48.82	0.41	3.14

Sajjad *et al.* [29], proposed a domain-specific mobile-cloud assisted framework for outsourcing the medical stego-images to cloud for selective encryption. The visual saliency detection model has been used for detecting the region of interest (ROI) from the transmitted image. The directed-edge steganography method has been used for embedding the detected ROI in the cover image and producing the stego image which sent to cloud for selective encryption.

Parah *et al.* [30], proposed a secure high capacity scheme capable of securing an electronic patient record (EPR) concealed in medical color images for an IoT based healthcare system. Two address vectors namely MAV (Main Address Vector) and CAV (Complementary Address Vector) have been generated as pseudorandom addresses to address the pixel locations for further embedding. It utilizes LSB method for concealing EPR using two/three RGB bit planes.

III. THE PROPOSED MODEL

This paper proposes a healthcare security model for securing a medical data transmission in IoT environments. The proposed model composes of four continuous processes:

(1) The confidential patient's data is encrypted using a proposed hybrid encryption scheme that is developed from both AES and RSA encryption algorithms. (2) The encrypted data is being concealed in a cover image using either 2D-DWT-1L or 2D-DWT-2L and produces a stego-image. (3) The embedded data is extracted. (4) The extracted data is decrypted to retrieve the original data. Fig. 1 shows the general framework of our proposed model for securing the medical data transmission at both the source's and the destination's sides.

A. DATA ENCRYPTION SCHEME

The proposed model implements the cryptographic scheme. The cryptographic scheme $\hat{C} = \{f\eta, f\eta^{-1}, C, S, T\}$ is composed of encryption and decryption processes. Throughout the encryption process, the plain text T is divided into odd part T_{odd} and even parts T_{even}. The AES is used to encrypt T_{odd} using a secret public key s. The RSA is used to encrypt T_{even} using a secret public key m. The private key x that used in the decryption process at the receiver side is encrypted using AES algorithm and sent to the receiver in an encrypted form to increase the security level. The encryption process can be mathematically modeled as given in the following equations below.

$$C = \{'E_{AES}, 'E_{RSA}, T_{odd}, T_{even}, \dot{T}_{odd}, \dot{T}_{even}, s, m, x\} \quad (1)$$

$$\dot{T}_{odd} = \{'E_{AES}(T_{odd}, s)\} \quad (2)$$

$$\dot{T}_{even} = \{'E_{RSA}(T_{even}, m)\} \quad (3)$$

$$\dot{X} = \{'E_{AES}(x, s)\} \quad (4)$$

The algorithm used in the encryption procedure is described below.

Algorithm 1 Hybrid (AES & RSA) Algorithm

Inputs: secret plain Stext message.
Output: main_cipher message, key s
Begin
1. Divide plain msg into two parts (Odd_Msg, Even_Msg)
2. Generate new AES key s
3. EncOdd = AES-128 (Odd_Msg, s)
4. Generate new RSA key (public = m) and (private = x)
5. EncEven = RSA (Even_Msg, m)
6. Build FullEncTxt by inserting both EncOdd and EncEven in their indices
7. EncKey = AES-128 (x, s)
8. Compress FullEncMsg by convert to hashs
9. Compress EncKey by convert to hashs
10. Define message empty main_cipher = ""
11. main_cipher = Concatenate (FullEncMsg, EncKey)
12. Return main_cipher and s

End

B. EMBEDDING PROCEDURE

In this process, A Haar-DWT was implemented. Throughout Haar-DWT, 2D-DWT-2L can be formulated as a consecutive transformation using low-pass and high-pass filters along the rows of the image; then the result decomposed along the columns of the image [21]. Fig. 2 elucidates this process.

Fig. 2 illustrates the elemental decomposition process for $C_j(n, m)$ image of a size $N \times M$ in four decomposed sub-band images which are referred to a high-high (HH), a high-low (HL), a low-high (LH), and a low-low (LL) frequency bands. Fig. 3 shows the effect of the decomposition process on the image.

The proposed model implements the steganographic scheme. The steganographic scheme $\hat{S} = \{f\eta, f\eta^{-1}, C, S, T\}$ is composed of embedding and extraction processes. The embedding process takes a cover image C and a secret text message T as input and generates a stego-image S. While the extraction process inversely extracts the embedded message. It can be mathematically modeled as given in the following equations below.

$$\hat{S} = \{f\eta, f\eta^{-1}, C, S, T\} \quad (5)$$

$$S = \{f\eta(C, T)\} \quad (6)$$

$$T = \left\{f\eta^{-1}(S)\right\} \quad (7)$$

Throughout the embedding process, the secret text is transformed into an ASCII format and then divided into even and odd values. The odd values are concealed in vertical coefficients mentioned by LH2. The even values are concealed in diagonal coefficients specified by HH2. The algorithm that is used in the embedding procedure by evolved 2D-DWT-2L is described below.

Algorithm 2 Embedding 2D-DWT-2L Algorithm

Inputs: cover image, a secret message (main_cipher and s).
Output: stego image.
Begin
1. Convert the secret message in ASCII Code as asciiMsg
2. Divide asciiMsg to odd and even
3. Scan the image row by row as img
4. Compute the 2D wavelet for the first level by harr filter that generates (LL1), (HL1), (LH1), and (HH1)
5. Compute the 2D wavelet for the second level by harr filter that generates (LL2), (HL2), (LH2), and (HH2)
6. Loop
   - 6.1 Hide odd values in vertical coefficient, set LH2(x,y) = odd values
   - 6.2 Hide even values in vertical coefficient, set HH2(x,y) = even values
7. End Loop
8. Return Stego image

End

C. EXTRACTION PROCEDURE

After incorporating the text into the cover image, the 2D-DWT-2L technique is carried to extract the secret message and retrieve the cover image. The extraction algorithm is described in Algorithm 3.

Algorithm 3 Extraction algorithm

Inputs: stego image
Output: Retrieved secret message and original cover image
Begin
1. Scan the stego image row by row
2. Compute the 2D wavelet for the first level by harr filter
3. Compute the 2D wavelet for the second level by harr filter
4. Prepare msg = ""
5. Loop
   - 5.1 Extract the text embedded in vertical coefficient, set odd values =LH2(x,y)
   - 5.2 Extract the text embedded in vertical coefficient, set even values = HH2(x,y)
6. End Loop
7. msg = Append (odd values, even values)
8. Compute idwt2 for the constructed approximation that generates the original image
9. Return msg as a retrieved secret message and original cover image

Once the secret text message has been extracted, the cover image is synthesized from the reconstructed approximation by calling the idwt2 for the second level and then for the first level [21]. Figure 4 elucidates the basic DWT synthesis process.

D. DATA ENCRYPTION SCHEME

Decryption refers to the process of converting the encrypted data back to the user in a well-known format; which is the reverse of the encryption process. The same key used by the sender has to be used over the cipher-text throughout the encryption process. The decryption process can be mathematically expressed as given in the following equations below.

$$\hat{C} = \{'\mathrm{E}_{AES}^{-1}, '\mathrm{E}_{RSA}^{-1}, T_{odd}, T_{even}, \dot{\mathrm{T}}_{odd}, \dot{\mathrm{T}}_{even}, s, x \quad (8)$$

$$x = \left\{'\mathrm{E}_{AES}\left(\dot{\mathrm{X}}, \mathrm{s}\right)\right\} \quad (9)$$

$$T_{even} = \{'\mathrm{E}_{RSA}^{-1}((\dot{\mathrm{T}}_{even}, x)\} \quad (10)$$

$$T_{odd} = \{'\mathrm{E}_{AES}^{-1}\left(\dot{\mathrm{X}}_{odd}, s\right) \quad (11)$$

The proposed decryption algorithm is described in Algorithm 4.

IV. EXPERIMENTAL RESULTS AND EVALUATION

A. SIMULATION ENVIRONMENT

The implementation of our proposed model was carried out using the MATLAB R2015a software running on a personal computer with a 2.27 GHz Intel (R) Core (TM) I3 CPU, 8 GB RAM and Windows 7 as the operating system.

The calculation of specific statistical metrics determines the quality of the proposed security model. These metrics calculate the ratio between the original image and the stego image. The obtained results were evaluated based on six statistical parameters; the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Bit Error Rate (BER), Structural Similarity (SSIM), Structural Content (SC), and Correlation.

Algorithm 4 Hybrid Decryption (AES & RSA) Algorithm

Inputs: main_cipher (secret) message, key
Output: secret (plain, text) message.
Begin
1. Divide main_cipher into two parts; HashedTxt and HashedKey
2. FullEncMsg = Decompress (HashedTxt)
3. EncKey = Decompress (HashedKey)
4. x = Decrypt_AES-128 (EncKey, s)
5. EncOdd = Split (FullEncMsg, odd)
6. EncEven = Split (FullEncMsg, even)
7. Odd_Msg = Decrypt_ AES-128 (EncOdd, s)
8. Even_Msg = Decrypt_ RSA (EncEven, x)
9. Define main_plain message
10. Loop on All Char
    - 10.1 If odd Insert odd characters into odd indices within main_plain message
    - 10.2 Else Insert even characters into even indices within main_plain message
11. End of Loop
12. Return main_plain (text) message

End

TABLE 2. Results of PSNR and MSE values using 2D-DWT-1L and 2D-DWT-2L for gray scale images.

Image	Text Size (byte)	PSNR		MSE	
		DWT-2L	DWT-1L	DWT-2L	DWT-1L
Image(1)	15	56.04	55.43	0.16	0.18
	30	53.43	51.96	0.29	0.41
	45	51.59	50.17	0.45	0.62
	55	51.81	49.46	0.42	0.73
	100	52.44	46.71	0.37	1.38
	128	50.60	46.05	0.56	1.61
	256	51.49	43.14	0.46	3.15
Image(2)	15	56.05	55.43	0.16	0.18
	30	53.43	51.96	0.29	0.41
	45	51.58	50.17	0.45	0.62
	55	51.79	49.46	0.43	0.73
	100	52.46	46.68	0.36	1.39
	128	50.57	45.97	0.56	1.64
	256	51.42	43.06	0.46	3.21
Image(3)	15	56.00	55.25	0.16	0.19
	30	53.42	51.87	0.29	0.42
	45	51.60	50.11	0.44	0.63
	55	51.77	49.37	0.43	0.75
	100	52.50	46.68	0.35	1.39
	128	50.52	46.04	0.57	1.61
	256	51.34	43.10	0.47	3.17
Image(4)	15	56.39	53.85	0.14	0.26
	30	54.01	51.30	0.24	0.48
	45	53.87	49.76	0.37	0.68
	55	52.42	49.03	0.37	0.81
	100	53.78	46.69	0.27	1.39
	128	51.27	45.78	0.48	1.71
	256	51.13	42.70	0.42	3.49
Image(5)	15	56.09	53.76	0.15	0.27
	30	53.56	51.26	0.27	0.48
	45	52.35	49.74	0.43	0.68
	55	52.33	48.87	0.42	0.84
	100	53.23	47.80	0.35	1.07
	128	51.17	47.68	0.56	1.10
	256	51.94	44.86	0.46	2.11

TABLE 3. Results of the six statistical parameters obtained from performing the (2D-DWT-2L) with hybrid (AES and RSA) scheme on color images with different text sizes.

Image	Text Size (byte)	PSNR	MSE	BER	SSIM	SC	Correlation
Image(1)	15	56.60	0.14	0	1	1	1
	30	53.48	0.29	0	1	1	1
	45	51.65	0.44	0	1	1	1
	55	51.91	0.41	0	1	1	1
	100	52.46	0.37	0	1	1	1
	128	50.70	0.55	0	1	1	1
	256	51.66	0.44	0	1	1	1
Image(2)	15	56.60	0.14	0	1	1	1
	30	53.48	0.29	0	1	1	1
	45	51.62	0.45	0	1	1	1
	55	51.88	0.42	0	1	1	1
	100	52.45	0.37	0	1	1	1
	128	50.65	0.56	0	1	1	1
	256	51.60	0.45	0	1	1	1
Image(3)	15	56.24	0.15	0	1	1	1
	30	53.42	0.29	0	1	1	1
	45	51.56	0.45	0	1	1	1
	55	51.82	0.43	0	1	1	1
	100	52.40	0.37	0	1	1	1
	128	50.59	0.57	0	1	1	1
	256	51.49	0.46	0	1	1	1
Image(4)	15	56.39	0.15	0	1	1	1
	30	54.25	0.24	0	1	1	1
	45	52.42	0.37	0	1	1	1
	55	52.37	0.38	0	1	1	1
	100	53.78	0.27	0	1	1	1
	128	51.79	0.48	0	1	1	1
	256	51.27	0.43	0	1	1	1
Image(5)	15	57.44	0.12	0	1	1	1
	30	56.42	0.29	0	1	1	1
	45	53.66	0.37	0	1	1	1
	55	51.69	0.38	0	1	1	1
	100	51.88	0.30	0	1	1	1
	128	52.66	0.49	0	1	1	1
	256	50.58	0.41	0	1	1	1

TABLE 4. Results of the six statistical parameters obtained from performing the (2D-DWT-2L) with hybrid (AES and RSA) scheme on gray images with different text sizes.

Image	Text Size (byte)	PSNR	MSE	BER	SSIM	SC	Correlation
Image(1)	15	56.04	0.16	0	1	1	1
	30	53.43	0.29	0	1	1	1
	45	51.59	0.45	0	1	1	1
	55	51.81	0.42	0	1	1	1
	100	52.44	0.37	0	1	1	1
	128	50.60	0.56	0	1	1	1
	256	51.49	0.46	0	1	1	1
Image(2)	15	56.05	0.16	0	1	1	1
	30	53.43	0.29	0	1	1	1
	45	51.58	0.45	0	1	1	1
	55	51.79	0.43	0	1	1	1
	100	52.46	0.36	0	1	1	1
	128	50.57	0.56	0	1	1	1
	256	51.42	0.46	0	1	1	1
Image(3)	15	56.00	0.16	0	1	1	1
	30	53.42	0.29	0	1	1	1
	45	51.60	0.44	0	1	1	1
	55	51.77	0.43	0	1	1	1
	100	52.50	0.35	0	1	1	1
	128	50.52	0.57	0	1	1	1
	256	51.34	0.47	0	1	1	1
Image(4)	15	56.39	0.14	0	1	1	1
	30	54.01	0.24	0	1	1	1
	45	53.87	0.37	0	1	1	1
	55	52.42	0.37	0	1	1	1
	100	53.78	0.27	0	1	1	1
	128	51.27	0.48	0	1	1	1
	256	51.13	0.42	0	1	1	1
Image(5)	15	56.09	0.15	0	1	1	1
	30	53.56	0.27	0	1	1	1
	45	52.35	0.43	0	1	1	1
	55	52.33	0.42	0	1	1	1
	100	53.23	0.35	0	1	1	1
	128	51.17	0.56	0	1	1	1
	256	51.94	0.46	0	1	1	1

PSNR calculates the imperceptibility of the stego-image [31]. The higher the value of PSNR of stego image reveals a higher quality of stego image or a higher imperceptibility of hidden message. The PSNR is calculated according to the following equation:

$$\mathrm{PSNR} = 10\log_{10}\left[\frac{\mathrm{I}^2}{\mathrm{MSE}}\right] \tag{12}$$

where I represent the maximum possible value of the pixel in the image (e.g., for a gray-scale image the maximum value is 255) and MSE is the mean square error.

MSE calculates the magnitude of average error between the original image and stego-image [32]. The MSE is computed as depicted below:

$$\mathrm{MSE} = \frac{1}{[\mathrm{R}\times\mathrm{C}]^2}\sum_{i=0}^{n}\sum_{\mathrm{j}=1}^{\mathrm{m}}(\mathrm{X_{ij}}-\mathrm{Y_{ij}})^2 \tag{13}$$

where, R and C are the numbers of rows and columns in the cover image, X_{ij}, is the intensity of X_{ij} the pixel in the cover image, and Y_{ij} is the intensity of Y_{ij} the pixel in stego image.

BER calculates the probability that a bit will be incorrectly received due to noise [33]. It is the number of bits received in error divided by the total number of bits transferred. The BER is calculated using the following equation:

$$\mathrm{BER} = \mathrm{Errors/Total\ Number\ of\ Bits} \tag{14}$$

SSIM measures the structural similarity between two images [34]. Its value ranges between -1 and 1. When two images are nearly identical, their SSIM is close to 1. The following formula is used to compute the SSIM between two sequences seq_1 and seq_2 at a given pixel P:

$$\mathrm{SSIM} = \frac{2*\mathrm{mu_1\,(p)\,mu_2\,(p)} + \mathrm{c_1}}{\mathrm{mu_1\,(p)^2{+}mu_2\,(p)^2{+}\,c_1}} \times \frac{2*\mathrm{cov\,(p)} + \mathrm{c_2}}{\mathrm{s_1\,(p)^2{+}s_2\,(p)^2{+}\,c_2}} \tag{15}$$

where, $mu_1(P)$ and $mu_2(P)$ are the mean value of seq_1, and seq_2 computed over a small XY window located around P. While, $s_1(P)$ and $s_2(P)$ are the standard deviations of seq1, and seq2 computed over the same window. And cov(P) is the covariance between seq_1 and seq_2 which are computed over the same window. $C_1 = (K1*L)^2$ is a regularization constant, $C2 = (K2*L)^2$ is a regularization constant, K1 and K2 are

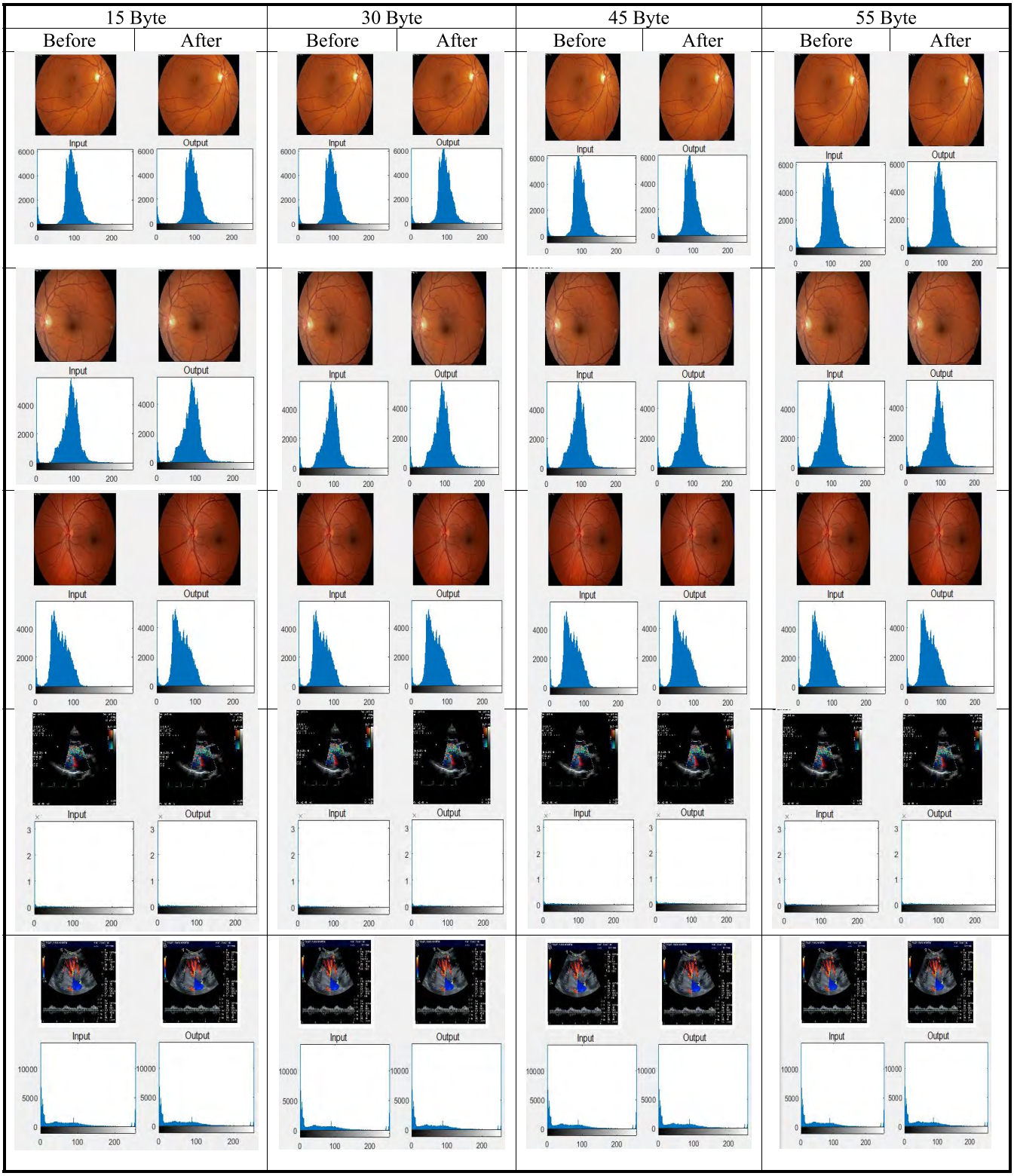

FIGURE 6. Histogram of the cover image before and after applying the proposed model on color images with different text sizes (15, 30, 45 and 55 bytes).

regularization parameters (must be >0), and L is a dynamic range of the pixel values.

SC is a correlation-based measure, where it also measures the similarity between two images [35]. It is calculated according to the following equation:

$$SC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} (y\,(i, j))^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} (x\,(i, j))^2} \tag{16}$$

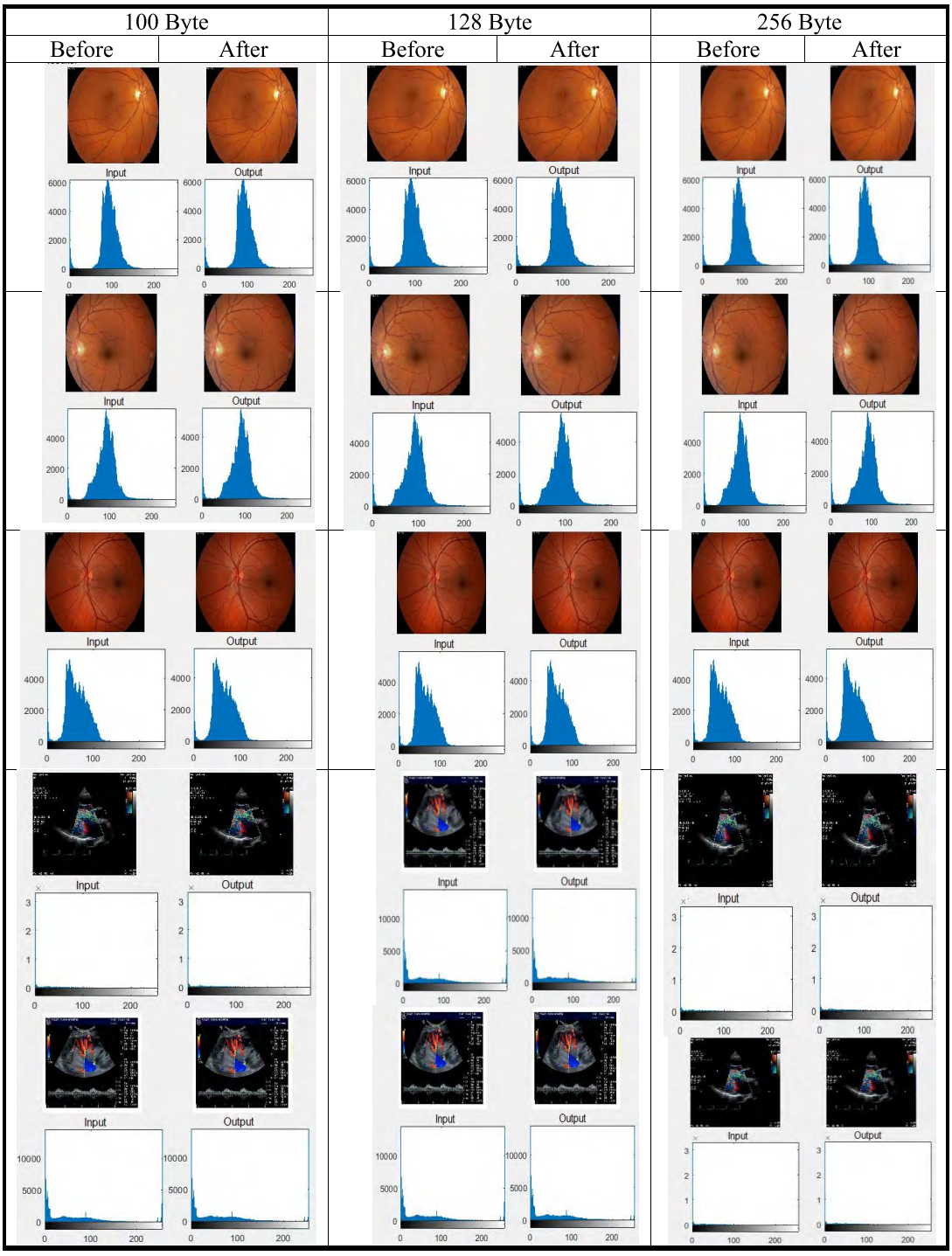

FIGURE 7. Histogram of the cover image before and after applying the proposed model on color images with different text sizes (100, 128 and 256 bytes).

where, x(i, j) represents the original image and y(i, j) represents the distorted image.

Correlation determines how much two signals or vectors are similar or different in phase and magnitude when two sets of data are strongly linked together [36]. It reaches its maximum when the two signals are similar. It is calculated by using the following equation:

$$\text{Correlation} = \frac{n\sum xy - \left(\sum x\right)\left(\sum y\right)}{\sqrt{n\left(\sum x^2\right) - \left(\sum x\right)^2}\sqrt{n\left(\sum y^2\right) - \left(\sum y\right)^2}} \quad (17)$$

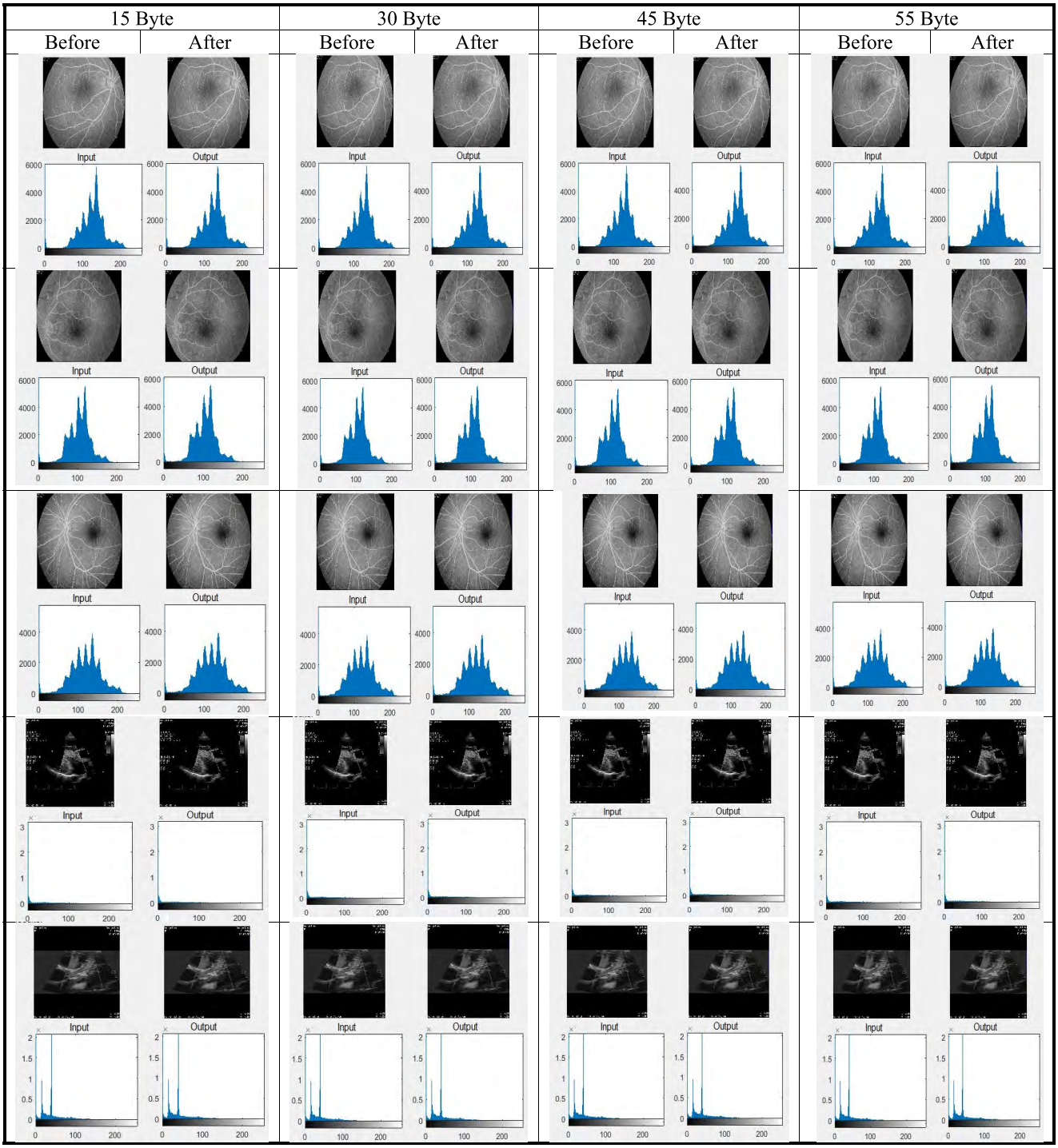

FIGURE 8. Histogram of the cover image before and after applying the proposed model on gray-scale images with different text sizes (15, 30, 45 and 55 bytes).

where n is the number of pairs of data, X is the input image, and Y is the stego image.

B. SECURITY ANALYSIS

In this study, the comparisons were conducted between the original medical cover image and the stego-image. The proposed model was tested using different messages with different lengths and hiding them in both color and gry scale images. The hidden message was analyzed before being transmitted and after being received by the expected recipient. That is to guarantee less distortion occurs within to the original cover file after concealing the secret text. Our model was applied to both datasets; DME eyes dataset [37] that represent the first three images, and DICOM dataset [38] that represent

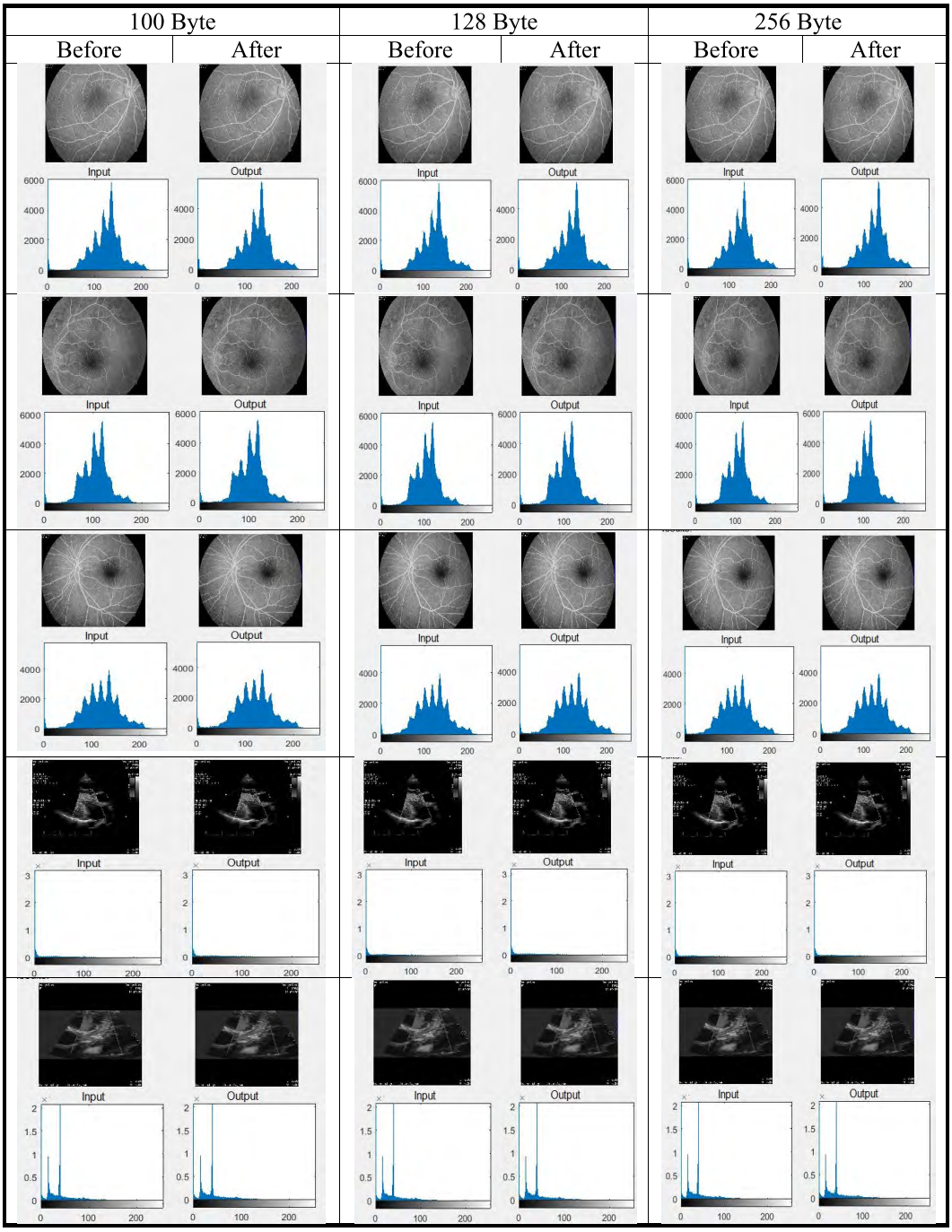

FIGURE 9. Histogram of the cover image before and after applying the proposed model on gray-scale images with different text sizes (100, 128 and 256 bytes).

the last two images. Fig. 5 shows the color and gray versions of these dataset.

In this model, the text is encrypted by using the evolved hybrid encryption scheme that was previously explained. Then it is being embedded using either 2D-DWT-1L or 2D-DWT-2L stenography techniques. It was found that DWT-2L gives better PSNR and MSE results compared with DWT-1L in case of both color and gray scale images as illustrated in table 1 and table 2 respectively. The PSNR values were relatively reached to 57.44 and 56.39 in case of DWT-2L for color images and gray-scale images respectively. While the PSNR values were relatively reached to 56.13 and 55.43 in case of DWT-1L for color images and gray-scale images, respectively. The MSE values using DWT-2L varied from 0.12 to 0.57 for the color images and from 0.14 to 0.57 for the gray images. While the MSE

TABLE 5. Comparing the performance of our proposed model with Anwar et al. approach

MODEL	PSNR	MSE
Anwar et al. [4]	56.76	0.1338
Proposed Model	57.02	0.1288

values by using DWT-1L were ranged from 0.16 to 3.43 for the color images; and from 0.18 to 3.49 for the gray scale images.

There was no variation between the studied images in the BER, where its values were zero for both images. The SSIM, SC, and Correlation were almost equal to one with all of the studied color and gray images as illustrated in table 3 and table 4 respectively. Figures (6, 7, 8 and 9) show the histograms of the cover image before and after applying the proposed model on both color and gray scale images sequentially with different text sizes.

C. COMPARING THE RESULTS AGAINST ANOTHER APPROACH

The performance of our model was compared with another technique developed by Anwar *et al.* [4] on 256×256 pixel medical color image using 18-byte text size. Table 5 shows the obtained PSNR and MSE values from applying our model as compared with those resulted by [4]. The results obtained after applying the models on 256∗256 color medical images with text size 18 bytes. It was found that our proposed model had a higher PSNR value and a smaller MSE value that reveals the higher performance of our proposed model.

V. CONCLUSION

A secure patient's diagnostic data transmission model using both color and gray-scale images as a cover carrier for healthcare based IoT environment has been proposed. The proposed model engaged either 2D-DWT-1L or 2D-DWT-2L steganography and hybrid blending AES and RSA cryptographic techniques. The experimental results were evaluated on both color and gray-scale images with different text sizes. The performance was assessed based on the six statistical parameters (PSNR, MSE, BER, SSIM, SC, and correlation). Compared to the state-of-the-art methods, the proposed model proved its ability to hide the confidential patient's data into a transmitted cover image with high imperceptibility, capacity, and minimal deterioration in the received stego-image.

REFERENCES

[1] A. Darwish, A. E. Hassanien, M. Elhoseny, A. K. Sangaiah, and K. Muhammad, "The impact of the hybrid platform of Internet of Things and cloud computing on healthcare systems: Opportunities, challenges, and open problems," *J. Ambient Intell. Humanized Comput.*, to be published, doi: https://doi.org/10.1007/s12652-017-0659-1

[2] A. Shehab *et al.*, "Secure and robust fragile watermarking scheme for medical images," *IEEE Access*, vol. 6, pp. 10269–10278, 2018, doi: 10.1109/ACCESS.2018.2799240.

[3] A. K. Bairagi, R. Khondoker, and R. Islam, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," *Inf. Secur. J., Global Perspect.*, vol. 25, nos. 4–6, pp. 197–212, 2016.

[4] A. S. Anwar, K. K. A. Ghany, and H. El Mahdy, "Improving the security of images transmission," *Int. J. Bio-Med. Inform. e-Health*, vol. 3, no. 4, pp. 7–13, 2015.

[5] A. Abdelaziz, M. Elhoseny, A. S. Salama, and A. M. Riad, "A machine learning model for improving healthcare services on cloud computing environment," *Measurement*, vol. 119, pp. 117–128, Apr. 2018. [Online]. Available: https://doi.org/10.1016/j.measurement.2018.01.022

[6] M. Paschou, E. Sakkopoulos, E. Sourla, and A. Tsakalidis, "Health Internet of Things: Metrics and methods for efficient data transfer," *Simul. Model. Pract. Theory*, vol. 34, pp. 186–199, May 2013.

[7] M. Sajjad *et al.*, "Raspberry Pi assisted face recognition framework for enhanced law-enforcement services in smart cities," *Future Generat. Comput. Syst.*, to be published, doi: https://doi.org/10.1016/j.future.2017.11.013

[8] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[9] M. A. Razzaq, R. A. Shaikh, M. A. Baig, and A. A. Memon, "Digital image security: Fusion of encryption, steganography and watermarking," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 5, pp. 224–228, 2017.

[10] N. Dey and V. Santhi, *Intelligent Techniques in Signal Processing for Multimedia Security*. New York, NY, USA: Springer, 2017, doi: 10.1007/978-3-319-44790-2.

[11] M. Jain, R. C. Choudhary, and A. Kumar, "Secure medical image steganography with RSA cryptography using decision tree," in *Proc. 2nd Int. Conf. Contemp. Comput. Inform. (IC3I)*, Dec. 2016, pp. 291–295.

[12] L. Yehia, A. Khedr, and A. Darwish, "Hybrid security techniques for Internet of Things healthcare applications," *Adv. Internet Things*, vol. 5, pp. 21–25, Jul. 2015.

[13] Z. M. Zaw and S. W. Phyo, "Security enhancement system based on the integration of cryptography and steganography," *Int. J. Comput.*, vol. 19, no. 1, pp. 26–39, 2015.

[14] R. K. Gupta and P. Singh, "A new way to design and implementation of hybrid crypto system for security of the information in public network," *Int. J. Emerg. Technol. Adv. Eng.*, vol. 3, no. 8, pp. 108–115, 2013.

[15] S. A. Laskar and K. Hemachandran, "High capacity data hiding using LSB steganography and encryption," *Int. J. Database Manage. Syst.*, vol. 4, no. 6, p. 57, 2012.

[16] L. Yu, Z. Wang, and W. Wang, "The application of hybrid encryption algorithm in software security," in *Proc. 4th Int. Conf. Comput. Intell. Commun. Netw. (CICN)*, Nov. 2012, pp. 762–765.

[17] S. F. Mare, M. Vladutiu, and L. Prodan, "Secret data communication system using steganography, AES and RSA," in *Proc. IEEE 17th Int. Symp. Design Technol. Electron. Packag. (SIITME)*, Oct. 2011, pp. 339–344.

[18] A. K. Mandal, C. Parakash, and A. Tiwari, "Performance evaluation of cryptographic algorithms: DES and AES," in *Proc. IEEE Students' Conf. Elect., Electron. Comput. Sci. (SCEECS)*, Mar. 2012, pp. 1–5.

[19] S. F. Mjolsnes, Ed., *A Multidisciplinary Introduction to Information Security*. Boca Raton, FL, USA: CRC Press, 2011.

[20] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.

[21] M. S. Sreekutty and P. S. Baiju, "Security enhancement in image steganography for medical integrity verification system," in *Proc. Int. Conf. Circuit, Power Comput. Technol. (ICCPCT)*, Apr. 2017, pp. 1–5.

[22] A. Bashir, A. S. B. Hasan, and H. Almangush, "A new image encryption approach using the integration of a shifting technique and the AES algorithm," *Int. J. Comput. Appl.*, vol. 42, no. 9, pp. 38–45, 2012.

[23] K. Muhammad, J. Ahmad, H. Farman, Z. Jan, M. Sajjad, and S. W. Baik, "A secure method for color image steganography using gray-level modification and multi-level encryption," *TIIS*, vol. 9, no. 5, pp. 1938–1962, 2015.

[24] J. H. J. Yin, G. M. Fen, F. Mughal, and V. Iranmanesh, "Internet of Things: Securing data using image steganography," in *Proc. 3rd Int. Conf. Artif. Intell., Modelling Simulation (AIMS)*, Dec. 2015, pp. 310–314.

[25] S. A. Seyyedi, V. Sadau, and N. Ivanov, "A secure steganography method based on integer lifting wavelet transform," *IJ Netw. Secur.*, vol. 18, no. 1, pp. 124–132, 2016.

[26] M. I. Khalil, "Medical image steganography: Study of medical image quality degradation when embedding data in the frequency domain," *Int. J. Comput. Netw. Inf. Secur.*, vol. 9, no. 2, p. 22, 2017.

[27] H. Abdel-Nabi and A. Al-Haj, "Efficient joint encryption and data hiding algorithm for medical images security," in *Proc. 8th Int. Conf. Inf. Commun. Syst. (ICICS)*, Apr. 2017, pp. 147–152.
[28] L. Li, M. S. Hossain, A. A. A. El-Latif, and M. F. Alhamid, "Distortion less secret image sharing scheme for Internet of Things system," in *Cluster Computing*. New York, NY, USA: Springer, 2017, pp. 1–15, doi: https://doi.org/10.1007/s10586-017-1345-y
[29] M. Sajjad *et al.*, "Mobile-cloud assisted framework for selective encryption of medical images with steganography for resource-constrained devices," *Multimedia Tools Appl.*, vol. 76, no. 3, pp. 3519–3536, 2017.
[30] S. A. Parah, J. A. Sheikh, F. Ahad, and G. M. Bhat, "High capacity and secure electronic patient record (EPR) embedding in color images for IoT driven healthcare systems," in *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*. Cham, Switzerland: Springer, 2018, pp. 409–437.
[31] N. F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *Computer*, vol. 31, no. 2, pp. 26–34, Feb. 1998.
[32] F. A. Jassim. (2013). "A novel steganography algorithm for hiding text in image using five modulus method." [Online]. Available: https://arxiv.org/abs/1307.0642
[33] Wikipedia Contributors. *Mean Absolute Error*. Accessed: Mar. 1, 2018. [Online]. Available: https://en.wikipedia.org/wiki/Mean_absolute_error
[34] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," *IEEE Trans. Image Process.*, vol. 13, no. 4, pp. 600–612, Apr. 2004.
[35] C. S. Varnan, A. Jagan, J. Kaur, D. Jyoti, and D. S. Rao, "Image quality assessment techniques in spatial domain," *Int. J. Comput. Sci. Technol.*, vol. 2, no. 3, pp. 177–184, 2011.
[36] E. A. Silva, K. Panetta, and S. S. Agaian, "Quantifying image similarity using measure of enhancement by entropy," *Proc. SPIE, Mobile Multimedia/Image Process. Military Secur. Appl.*, vol. 6579, pp. 65790U-1–65790U-12, Jan. 2007.
[37] H. Rabbani, M. J. Allingham, P. S. Mettu, S. W. Cousins, and S. Farsiu, "Fully automatic segmentation of fluorescein leakage in subjects with diabetic macular edema," *Investigative Ophthalmol. Vis. Sci.*, vol. 56, no. 3, pp. 1482–1492, 2015.
[38] F. J. McEvoy and E. Svalastoga, "Security of patient and study data associated with DICOM images when transferred using compact disc media," *J. Digit. Imag.*, vol. 22, no. 1, pp. 65–70, 2009.

MOHAMED ELHOSENY received the Ph.D. degree in computer and information sciences from Mansoura University, Egypt (in a scientific research channel with the Department of Computer Science and Engineering, University of North Texas, USA). He is currently an Assistant Professor with the Faculty of Computers and Information, Mansoura University. He has authored/co-authored over 65 International Journal articles, Conference Proceedings, Book Chapters, and two Springer brief book. His research interests include network security, cryptography, machine learning techniques, Internet of Things, and quantum computing. He is a TPC Member or Reviewer in over 30 International Conferences and Workshops. Furthermore, he has been reviewing papers for over 20 International Journals. His Ph.D. thesis was awarded the best Ph.D. thesis prize (2016) at Mansoura University.

GUSTAVO RAMÍREZ-GONZÁLEZ is currently a Professor with the Department of Telematics Engineering, Universidad del Cauca, Colombia. His research interests include image processing, secure communication, and machine learning. He has published several research papers in reputed journals. He served as a Guest Editor for several special issues at many journals, such as *Computers and Electrical Engineering* and *Cluster Computing*.

OSAMA M. ABU-ELNASR received the M.S. degree in computer vision and the Ph.D. degree in empowering software testing process for improving software quality from Mansoura University in 2009 and 2014, respectively.

Since 2014, he has been a Lecturer with the Computer Science Department, College of Computers and Information, Mansoura University. His research interests include information security, IoT, machine learning, and software quality management.

SHIHAB A. SHAWKAT received the B.Sc. degree in computer Science from the University of Tikrit in 2009 and the M.Sc. degree in computer science from Mansoura University in 2017.

He is currently an Assistant Teacher with the Directorate of Education in Salah Al-Din, Ministry of Education, Iraq. His research interest lies in image processing and computer security and media digital files like steganography and cryptography.

ARUNKUMAR N received the B.E., M.E., and Ph.D. degrees in electronics and communication engineering with specialization in biomedical engineering. He has a strong academic teaching and research experience of more than 10 years in SASTRA University, India. His research interest areas include image processing, biomedical engineering, and information security.

AHMED FAROUK received the M.S. and Ph.D. degrees from Mansoura University in 2009 and 2015, respectively. He is especially well known for seminal contributions to theories of quantum mechanics, communication and cryptography. He has published 50 papers in reputed and high impact journals like *Nature Scientific Reports*, *Physical Review A*, and 14 book chapters. His research interests include quantum communication, quantum cryptography, quantum machine learning and quantum information processing. He has worked for various conferences at different levels from reviewer to Organizer-Chairman. His continuous support for reviewing process lead to award 29 Certificates of appreciation for generous support and for invaluable efforts in the reviewing process. He received the Best Researcher for 2015 and 2016 by the Al-Zahra College for Women, Oman.