



# Confidentiality considerations: multimedia signals transmission over different wireless channels utilized efficient secured model

Sabry S. Nassar<sup>1</sup> · Mohsen A. M. El-Bendary<sup>2</sup>

Received: 27 August 2020 / Revised: 17 August 2021 / Accepted: 14 January 2022 /

Published online: 24 March 2022

© The Author(s) 2022

## Abstract

The confidentiality of highly-sensitive multimedia signals is considered in this paper, it can be enhanced by efficient secured model utilizing several-layer security algorithms. The hybrid data hiding and cryptographic techniques are merged for constructing secured model. The Least Significant Bit (LSB) data hiding steganography is utilized with a 2-D Logistic-based map (Model-I) and second Model-II involves data hiding merging within chaotic-Baker-based image encryption security techniques. Performance analyzing and comparison have been presented utilizing various images for examining the applicability of the different proposed image security scenarios for securing wireless image transmission over noise-free, and noisy channels. Moreover, the proposed algorithms are applied for transmission over Orthogonal Frequency-Division Multiplexing (OFDM) channels, and their performance is evaluated under different conditions of fading environments with utilizing the powerful error control schemes in the case of SUI-3 model channel and randomizing the packet based on the encryption tools. An equalizer is used to mitigate the impact of composite fading. A multi-layer security model using Discrete Wavelet Transform (DWT) steganography with chaotic Baker encryption is proposed to protect highly-sensitive text based data records. The results reveal that it can be used efficiently for protecting highly-sensitive text message and records (text-based data). The timing analysis and comparative study are considered with respect to the previous related works.

**Keywords** Confidentiality · Security techniques · Wireless channels · OFDM · Discrete transforms · Randomized error control technique

---

✉ Mohsen A. M. El-Bendary  
engmohsen2004@yahoo.com

Sabry S. Nassar  
sabry2000@yahoo.com

<sup>1</sup> Nuclear Research Center, Atomic Energy Authority of Egypt, Cairo, Egypt

<sup>2</sup> Department of Electronics Technology, Faculty of Technology and Education, Helwan University, Helwan, Egypt

## 1 Introduction

Multimedia signals security is interested research point due to the wide spreading of multimedia signals exchanges over the open environments and over the various wireless communications systems. Also, with raising the threats and attacks, developing the security technique became essential for providing immune and secured wireless link for multimedia signals transmission to achieve the confidentiality. The various existing security techniques focus on the data protection and data contents integrity verification. The forged image detection algorithms are method for detecting the tampering and unauthorized manipulation attacks, these algorithm are called data contents integrity verification tools [16, 18]. Encryption techniques are efficient method for preventing the attacks from accessing the secret multimedia files, it achieves the confidentiality [9].

Data Confidentiality means achieving high protection for sensitive and secret information from any unauthorized accessing. Cryptographic techniques and data hiding are common and utilized widely to achieve data confidentiality. Also, for providing high level security there is the hybrid techniques. This technique is built based on combining the cryptographic technique and data hiding tools for securing highly-sensitive data [10, 21, 33].

In this paper, cryptography is accompanied and merged with data hiding steganography technique for constructing hybrid security techniques that can strengthen the level of security and achieve highly confidential data for transmission process or storing. The presented models in this paper are evaluated and tested over the various wireless communications channels which are Rayleigh fading, Additive White Gaussian Noise (AWGN) communications channels and OFDM system over various wireless communications channel conditions. Additional security is performed on the transmitted packets level, where the randomizing tool based on the encryption techniques is executed on packet-by-packet [, 7, 30].

The error performance of the whole proposed models is considered through utilizing different error control schemes. Utilizing the error control schemes enhances the extracted images quality and reduces the bad conditions effects of images transmission on the various proposed secured models performance. The various experiments are executed for measuring the behavior of the proposed models over the different channels conditions. The results of the executed experiments present cleared evidence the superior performance of the presented models for enhancing the confidentiality of the multimedia signal over the various transmission scenarios. The suitability and applicability of the proposed model on the text message security is investigated in our research work using different data transform techniques [14, 27, 36].

This research paper in the following has been organized:- section 2 presents the related works overview. The models of multimedia signals confidentiality enhancing are presented in section 3. The models description and its contents have been discussed in section 4. In section 5, The various computer simulation experiments are presented in section 5. OFDM system based evaluation experiments are presented in section 6. In section 7, text confidentiality based on the proposed models is presented. The comparative study has been presented in section 8. Section 9 introduces the final conclusions.

## 2 Related works overview

The recent published research works have been presented in this section with merged comparative study with our proposed secured models has been discussed this research paper.

In general, the cryptography techniques are considered efficient tools for providing the multimedia confidentiality and securing the confidential data. Also, the combined multi-cryptographic techniques under the known hybrid cryptosystems are utilized widely for achieving the security requirements of the multimedia signals [42]. In the following the various security techniques which are proposed for providing the security requirements for the multimedia signals transmission are discussed.

In [3], the RGB image security using the cryptographic process for securing its wireless transmission. This process is proposed utilizing the Pseudo Random Number Generator (PRNG) and involving two cascaded process of encryption for enhancing the RGB images transmission security. The merged between various security techniques is proposed in [22], authors in this paper used multi-chaotic maps and cryptography techniques for encrypting the transmitted speech signals. The cubic map is employed for segmenting the speech signal to four parts, also, for raising the robustness of the proposed security technique against the various attacks series of 1-D chaotic maps are utilized. The blowfish algorithm with the secret key have been used to protect parameters of these maps.

The security of exchange medial information and medical information is considered in several research works such as in [1, 8]. In [8], transmission securing of the Electrocardiogram (ECG) utilizing efficient encryption tools is presented, the authors in this research paper used the common 1-D chaotic maps for securing the ECG signals with employing the various data transform techniques. Due to the wide spreading of medical inspection images exchange over the open environment wireless medium, the compression and encryption of transmitted medical image [1]. The hiding of transmitted medical images is proposed in [5] using the Singular Value Decomposition (SVD). The audio signals are used as a cover in this proposed technique, the various secret keys are used for encrypting the medical image before the embedding process.

Multimedia signals securing issue involves two main targets, whole multimedia protection and the multimedia contents integrity verification. The branch of multimedia files contents verifications is considered in [19], it discussed the importance of multimedia security tools for protecting the multimedia signals contents from the forgery and any manipulation from unauthorized accessing. To manipulate the data, attacker must be capable to access it firstly. The proposed technique in [37] presented combined security technique through merging different tools for preventing any unauthorized accessing to the multimedia signals [41]. The watermarking technique is proposed for protecting the data from tampering attacks is presented in [15], also, the presented technique can detect any tampering or manipulating attack in the data. Hence, the watermarking technique with the encryption process provide the data protects and data contents protection through hiding it to be unobservable.

Watermarking and steganography are effective tools for protecting the data contents through hiding the secret multimedia signal within a cover. In [47], big data exchange security is considered through presented efficient watermarking technique. Big-data such as the health care systems based on the wireless networks utilizing mainly depends on the advance in the different wireless communications. The medical information is considered sensitive and highly secret information. Because of the back bone of the new and smart health care systems is the wireless networks, it needs a robust and reliable security techniques. Hiding the medical data is an efficient method for protecting it with performing the encryption process after or before the hiding procedures [44].

The combined/hybrid security technique is proposed in [23, 32] for protecting the data from modifying or tampering by intruders. The proposed technique utilized Rabin cryptosystem and Arnold transform for constructing the cryptographic-hiding technique. The mechanism operation of the proposed technique worked based on hiding the digital multimedia files in form of

audio, video, image or text, the secret message is hidden to be not observed or noticed. In [32], the different experiments are executed to test the presented security technique, the experiments results reveal that the presented technique success for extracting the hidden data with sufficient PSNR and low MSE. In [23], the hybrid security technique is proposed using the hash function merging with the chaotic map for forming the robust cryptographic technique based on two process of data encrypting.

Krenn et al. [23] discussed the steganography data hiding techniques and its various implementating tools. Least Significant Bit (LSB) has been proposed by Deshpande Neeta, et al., this data embedding technique suggested method for data hiding within the least significant bits of the another piece of data. The presented data hiding tool has been described and tested utilizing 2, 4 and 6 LSBs to hide various images format such as bmb and png images [45]. Hidden data transferring to another side without detection from third party challenges have been presented by K. B. Raja, et al. Authors in this research paper employed image hiding steganography technique utilizing LSB, Discrete Cosine Transform (DCT) and compression tools for improving payload security [46]. LSB technique and RSA algorithm combining have been presented by Mamta Juneja, et al. for implementing robust image hiding tool [12].

Beanies Mehboob, et al. have been proposed a novel data hiding tool within colored images using LSB technique. Authors in this research paper discussed data hiding steganography mechanism and its art [29]. In [2], authors utilized pixel shuffling and confusing the pixel value of images for achieving efficient image encrypting tool by converting 2-D chaotic map into 3-D chaotic map. Also, in [40] rapid image encrypting tool has been presented employing cascaded chaotic maps to generate chaotic sequences. Gao et al. in [43] have been proposed image pixels shuffling tool and pixels confusing of secret images using chaotic maps. In [38], multi chaotic maps are utilized to secure colored images through generating robust chaotic sequences and shuffling the original image pixels.

Several papers proposed combining more than one security technique such as, encryption and data hiding tools for achieving sufficient confidentiality for the transferred data. These merged data security techniques can be executed by two model, data hiding then encryption or encryption then data hiding. In [6], secret text message has been secured by steganography technique to be hidden after encrypting the secret message. The secret message is encrypted/decrypted utilizing secret key before/after embedding/extracting processes, respectively. On the other hand, data hiding process can be executed before the encryption process as presented by Arun A.S., et al in [39]. The steganography technique has been performed firstly to hide the secret message in cover image and produces stego image. In the next security level, stego image is encrypted by 1-D chaotic map [39]. These efforts have not utilized more chaotic encryption algorithms such as 2-D Logistic map and 2-D Baker map, and in almost all cases, they depend on encrypting a secret data before the embedding process instead of encrypting the image carrying the secret data. Another limitation of these efforts is that they miss the real evaluation and implementation of their algorithms on different noisy channel models. Almost of previous related works utilized the first model (embedding encrypted secret message), These past research works did not present or devote a sufficient experiments evaluation and testing procedures as various noisy wireless channels are not considered. These drawbacks of the previous related works have been solved and covered in our research paper through merging the encryption after /before data hiding process. Also, various 2-D chaotic maps are used for executing the encryption process in a different models. In the testing and evaluating process, several experiments are carried out to prove the suitability, robustness and applicability of the proposed security models for different wireless channel conditions.

### 3 Enhancement of multimedia signals confidentiality

In the previous section, the recent research works of the multimedia signals security are presented. In this section, the various proposed secured model for enhancing the multimedia security transmission are described. These model are presented for achieving sufficient security level. Also, the presented models provide different security levels over the various fixed/mobile wireless communications channels based on the degree classifications of the processed signals. Spatial domain LSB-based steganography is chosen in the building of the presented model due to its high capacity. Also, different error control schemes have been used to improve the Bit Error Rate (BER) and increase metrics of error performance measurement of the whole system. Moreover, utilizing error control techniques aim to enhance security levels of the presented models. The various presented security models have been built based on merging concept between encryption and data hiding tools. Therefore, the combination of security techniques involves two model, modelI contains 2D baker map and steganography and modelII contains 2D logistic map combining with data hiding techniques.

Performance of the presented security model have been evaluated and measured utilizing various different transmission channel conditions models such as; noise-free channel, AWGN channel, and Rayleigh fading channel. Although the sensitive nuclear data is usually transmitted between sites through guided error-free links, the proposed algorithms should be designed and evaluated at worst cases of transmission conditions that may occur during emergency or any other unexpected transmission circumstances [24, 34, 35].

### 4 The proposed models: description

In this section, the presented models of the efficient multimedia security are described. The contents and steps of the secured signals processing are presented.

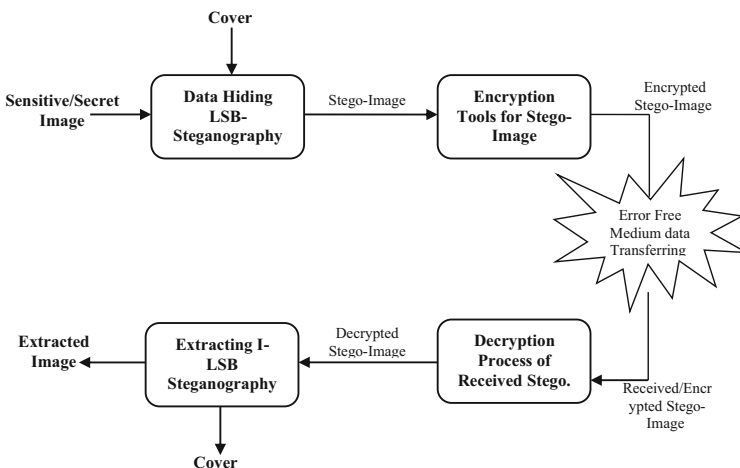
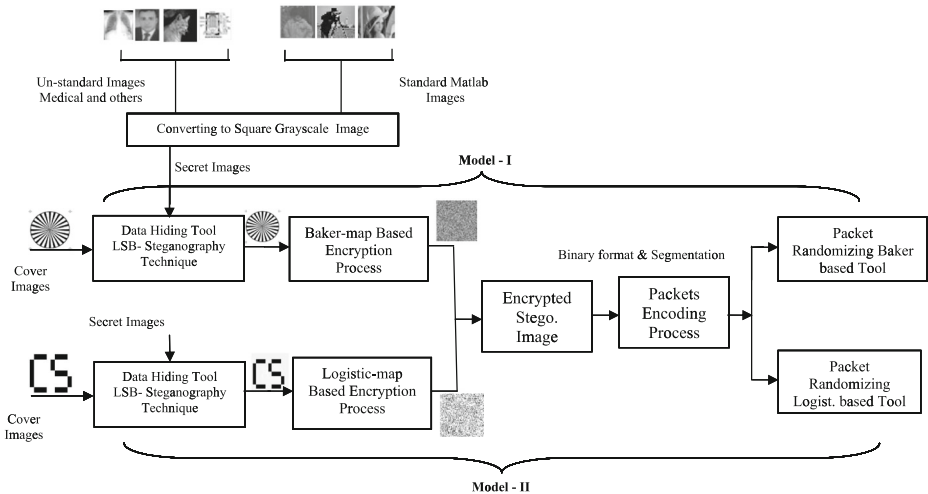


Fig. 1 Proposed security model of multimedia signals utilizing various tools



**Fig. 2** The components and details of the proposed secured model with the various security levels merging

The presented security models are constructed from a various techniques; in the following, the processing steps of the secret message have been described. At the transmitter, data hiding step is performed, firstly, spatial domain LSB-based data hiding steganography is used to embed a secret message in cover to be hidden. The embedding step produces the stego image, it is the output of embedding process. In the second step, the composed image is encrypted by one of the employed image encryption techniques to produce encrypted composed image (stego image). At the other side of the system, the processing steps are reversed; firstly, decryption process is executed on the encrypted stego and the result is received (noisy) decrypted stego version. The next step after decryption process is the extraction of secret message from the cover. In Fig. 1, the simple contents of the presented secured models for multimedia confidentiality enhancing. The details of the image processing and the steps of the proposed models mechanism are presented and cleared in Fig. 2. Also, as shown in this figure the role of encoding process and packet randomizing process based on the encryption techniques. This process is added for raising the security level of multimedia signals and its confidentiality with improving the error performance, various block and convolutional codes are employed for this purpose [20].

Multimedia signal is represented by image in the evaluating process of the proposed secured models. It is known that image has a bulk capacity, it must achieve the important properties of steganography such as, capacity and invisibility. High capacity is achieved by maximizing the embedding bits. Also, invisibility property is achieved if the cover image appearance changes is not noticeable after the embedding process for achieving the high imperceptibility. The secret-sensitive image has been embedded into the cover and followed by the encryption process starts for producing the encrypted stego-signal by using 2-D Logistic-based chaotic encryption, its mechanism is based on the substitution process or Baker-based map encryption as a permutation based encryption technique. The stego-image binary version is segmented to small packets. These packets are encoded by one of common error control schemes. The encoded packets is randomized by logistic-based or Baker-based interleaver. The last step at the transmitter side is the modulation [28].

### 5 Computer simulation experiments: evaluations

Performance of various presented secured models of multimedia/image confidentiality over the various wireless communications channels has been investigated in this section. In the evaluation process, different images and wireless channel conditions are used in the experiments, which are carried out using Matlab program. Several group of simulation experiments are carried out for evaluating the presented secured model over the different wireless communications channel using various images for testing and evaluating its suitability, applicability and robustness.

The proposed different models are tested using various gray-scale secret images such as Reactor (secret image)/Testpat (cover image) images and Woman/Boy images, the images size is  $256 \times 256$  pixels, as given in Fig. 3. In first group of experiments, stability of the security models has been evaluated and tested utilizing noise free communication channel by measuring quality level of extracted secret message and imperceptibility of the proposed models. All experiments have been implemented on different standard gray-scale images with size  $(256 \times 256)$  as shown in Fig. 3 shows the utilized images in various experiments, these gray-scale images have same  $256 \times 256$  pixels.

There are number of metrics are employed for evaluating the power and efficiency of the various presented secured models. These metrics are tabulated in Table 1 tabulates used performance metrics which are employed for measuring the efficiency and applicability of the presented security models.

#### 5.1 Error-Free channel

In this section, first group of computer simulation experiments are executed for evaluating the behavior of security models using various metrics such as the extracted image quality and time

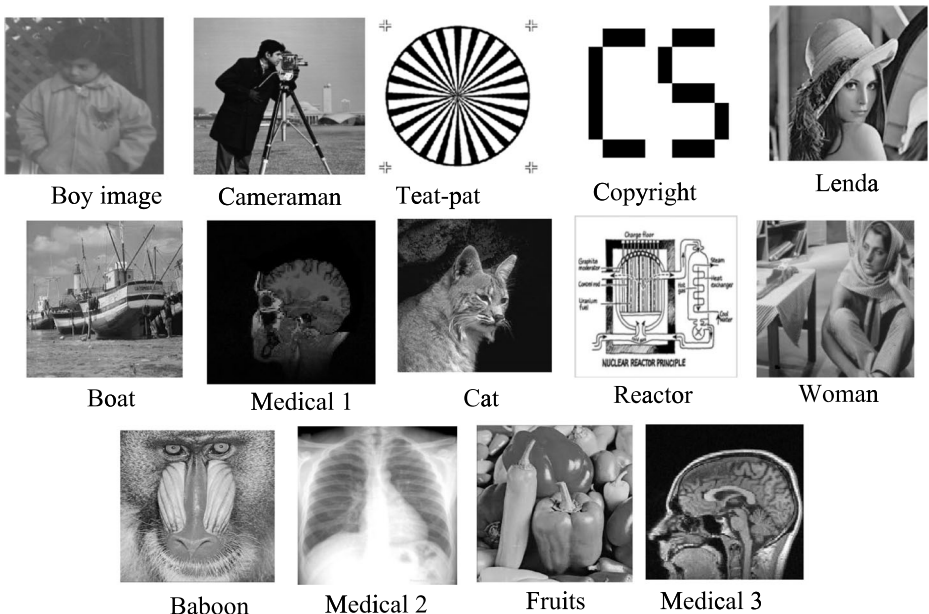
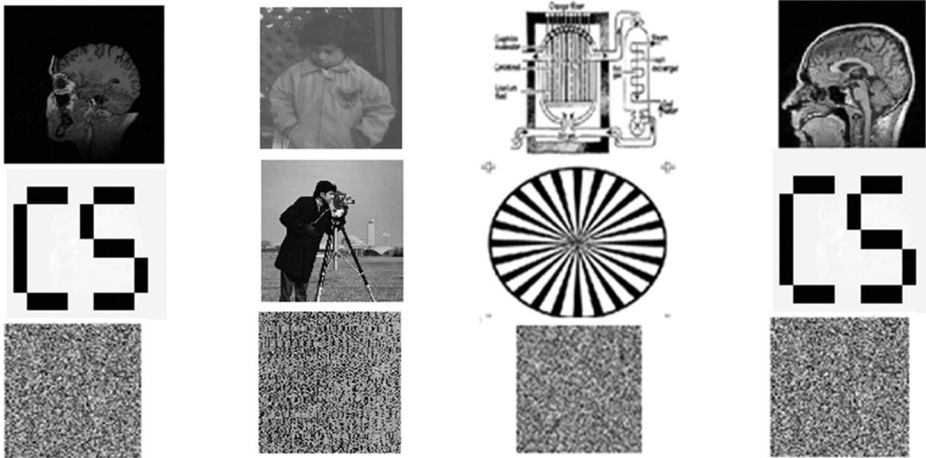


Fig. 3 The utilized images for evaluating experiments

**Table 1** Performance metrics for evaluating the various secured models and its description

Employed metrics of security		Hiding & Encryption Process		Extracting & Decryption Process			
Hid/Enc. Processing Time ( $T_{HE}$ )	Correlation Coefficient (Cr)	((PSNR))	(MSE)	Ext/Dec. Processing Time ( $T_{ED}$ )	((PSNR))	(MSE)	Histogram (Hist)
Lower values mean faster encryption process	Lower values means better security of encryption process	Higher values means better quality of encryption process	Higher values means better quality of encryption process	Lower values mean faster decryption algorithm	Higher values means better quality of decryption process	Lower values means better quality of decryption process	More uniform histogram means better quality encryption process

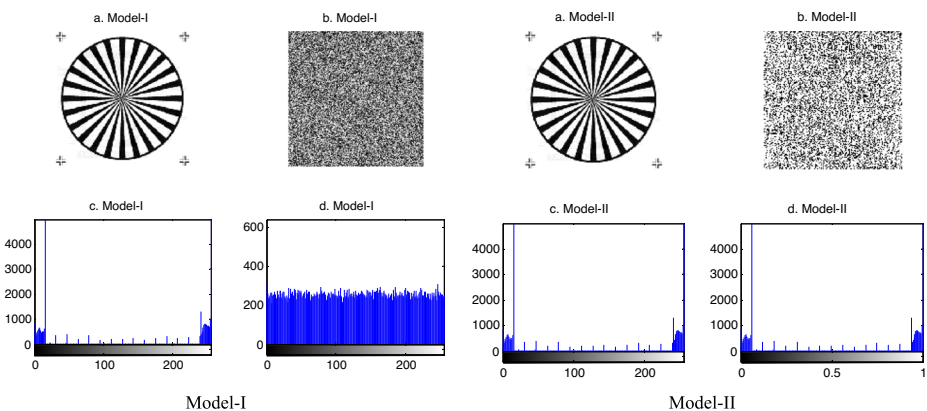




**Fig. 4** Samples original secret image, stego-image and encrypted stego-image of model-I evaluation over error free channel

of processing the embedding and encryption in model-I and model-II as shown in Fig. 2. The extracted image samples and stego-signal of the first experiments are given in Fig. 4 using error free channel.

The first experiment is carried out for evaluating the performance of Model-I over error free channel (Model-I contains:- Data hiding steganography is followed by 2-D Logistic-based encryption) are presented in Fig. 4. This figure gives image samples of Model-I over error free medium, original secret image, composed image (stego image) and encrypted stego have been shown in Fig. 4. As cleared from the results of this experiment for Model-I evaluation, the embedding process produces invisible mark, the secret message is not observable and the extraction process is performed correctly for extracting the embedded image correctly as the original secret image.



**Fig. 5** Histogram as a metric for the presented secured model-I and model-II utilizing Testpat/Reactor Images, **a** -Stego signal, **b** - Encrypted version of stego signal (logistic based), **c** -Histogram (stego signal), and **d** - Histogram (encrypted stego image)

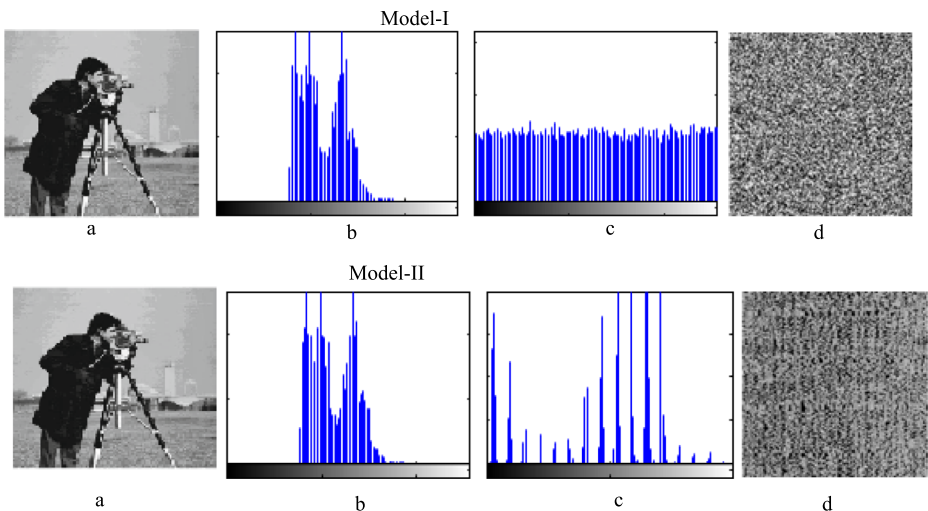
The first experiment has been repeated using other different testing images (Medical as secret image and Copyright images as cover). This experiment is devoted to test and measure the robustness and applicability of the presented security Model-I. Results of this experiment utilizing various testing images are shown in Fig. 4.

The results related to the second security model-II; (Model-II contains data hiding steganography is followed by Baker-based encryption process) have been given in Fig.5. These results prove that Model-II performs better than Model-I, it achieves high perceptibility and high extracted secret image quality. Due to the capability of chaotic Baker-map in the encrypting process (based on performing permutation in uniform geometric transform to randomize the adjacent pixels in encrypted version) the cover image and composed image appear as the same and not visual differentiated.

There are several experiments in the following for investigating the behavior of presented security models utilizing different testing images. Also, these experiments are devoted to examining the quality of extracted secret image and stego image through measuring the used metrics as presneted in Fig. 5 and Fig. 6.

From the results of the previous experiments, it is clear that extracting the secret message form the composed image by attackers is very difficult, it is proved by uniform histogram of Model-I as given in Fig. 6c. On the other hand, form results of Model-II as given in Fig.6b and c, histogram of various stego versions appear same shape. Therefore, detecting and extracting the embedded secret message is not easy process.using different testing images to evaluate model-I are given in Table 2. As cleared from these results, composed images (stego) before are after embedding process are seem same shape without any observable changes in appearance.

- The correlation coefficients of the Model-II experiments are tabulated in Table 2. These results prove that embedding process did not affected on the cover image appearance.



**Fig. 6** Histogram as a metric for the presented secured model-I and model-II utilizing Cameraman/Boy images, **a** -Stego signal, **b** - Histogram of stego signal (logistic based), **c** - Histogram of encrypted stego image, and **d** - Encrypted stego image

**Table 2** Various results of cover and embedded secret image and its metrics with respect different metrics for evaluating the robustness of the presented secured models



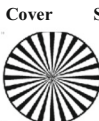













Metrics		Group of Experiment results for evaluating the presented secured model utilizing various images							
		Reactor-Testpat	Woman/Boy	Medical1-Copyright	Boy-Testpat	Boat/Boy	Medical2-Copyright		
Model -I	<b>Cr</b>	0.987	0.9797	0.9927	0.988	0.9797	0.9926		
	<b>MSE</b>	156.5	67.96	31.55	156.6	67.95	31.56		
	<b>PSNR</b>	26.2	29.84	33.20	26.1	29.841	33.21		
	<b>T<sub>p</sub>(ms)</b>	0.1325	0.12935	0.1145	0.1425	0.11935	0.1245		
Cover Image and Stego Image (Model-I)				Reactor/ Testpat Cr=0.9990		Medical/ Copyright Cr=0.9990			
Model -II	<b>Cr</b>	0.986	0.9992	0.9928	0.987	0.99909	0.9930		
	<b>MSE</b>	156.6	36.96	33.61	156.5	36.960	33.65		
	<b>PSNR</b>	26.1	32.48	33.11	26.2	32.480	33.01		
	<b>Cr</b>	0.09325	0.09135	0.1045	0.1025	0.11935	0.1045		
Cover Image and Stego Imag (Model-II)				Reactor/ Testpat Cr=0.999		Medical/ Copyright Cr=0.999			

- The utilized metrics (MSE) and (PSNR) of original secret message and extracted versions of Model-I and Model-II have been given in Table 2,  $T_{DE}$  and time of the decrypting and extracting processes at the receiving side ( $T_{EE}$ ) (ms) is calculated by sum of embedding and encrypting process at transmitter time ( $T_p$ ). Also, the average processing time of the model-I and model-II are considered as a performance metric. The average time ( $T = \frac{T_{EE}(T + )}{2 \cdot DE}$ )

These results of model-I and Model-II evaluating indicate they have acceptable results with respect to the (MSE) and (PSNR) values. Table 3 tabulates the results of the experimental results of the presented model-I and model-II over the error free channel. The various computer simulation based experiments are executed utilizing the different standard and un-standard images for testing and evaluating the robustness of the various presented models and their suitability.

As cleared in the previous experiments, the proposed models achieve double security levels by combing the data hiding and image encryption tools within one secured model. The various images are utilized for testing the presented models over error free channel to measure the robustness and suitability for the standard and un-standard images. Also, the standard image quality metrics are used for measuring the extracted secret image after decryption process of the encrypted version of stego composed image. The extracted secret images as shown form

**Table 3** Extracted images with related quality metrics, model-I and model-II

Extracted Image (Error Free Conditions)		Metrics values	Extracted Image (Error Free Conditions)		Metrics Values
Cover	Secret Image	MSE=156 PSNR=26 Cr=0.986	Cover	Secret Image	MSE=8.50 PSNR=38.1 Cr=0.996
		MSE=156.1 PSNR=26.1 Cr=0.987			MSE=18.55 PSNR=28.1 Cr=0.996
Cover	Secret Image	MSE=33 PSNR=33.1 Cr=0.989	Cover	Secret Image	MSE=156 PSNR=26.1 Cr=0.9297
		MSE=0.776 PSNR=49.2 Cr=0.9995			MSE=155 PSNR=27.1 Cr=0.9971
Cover	Secret Image	MSE=31 PSNR=33.2 Cr=0.9930	Cover	Secret Image	MSE=62.4 PSNR=30.2 Cr=0.9794
		MSE=33.6 PSNR=33.2 Cr=0.9929			MSE=62.40 PSNR=30.2 Cr= 0.9914
Cover	Secret Image	MSE=156.5 PSNR=26.10 Cr=0.9906	Cover	Secret Image	MSE=61.1 PSNR=31.1 Cr=0.994
		MSE=156.1 PSNR=26.2 Cr=0.987			MSE=33.1 PSNR=32.1 Cr=0.9894

**Table 4** Simulation setting and the various parameters of the computer simulation experiments for evaluating secured model over the different wireless communications channels

Parameter	Value of setting
Frequency Doppler shift (FD)	0Hz–250 Hz
Communications Channel Model	-AWGN -Rayleigh fading SUI-3 model Jakes model
Packet length	2024 Bits
Images	256x256pixels standard and un-standards images
Coding	RS Code (7, 3) RS Code (15, 11) CC (1, 2, 7) Hamming Code (15, 11)
Modulation	BPSK
Conv. Code rate, No. of shift register	R=1/2, K=6
SNR	0 to 40 dB
Performance Metrics	MSE, PSNR Correlation Coefficient (Cr)

previous computer simulation experiments, has an accepted quality as well as the cover image after the extracting process.

## 5.2 Wireless channels: experiments group

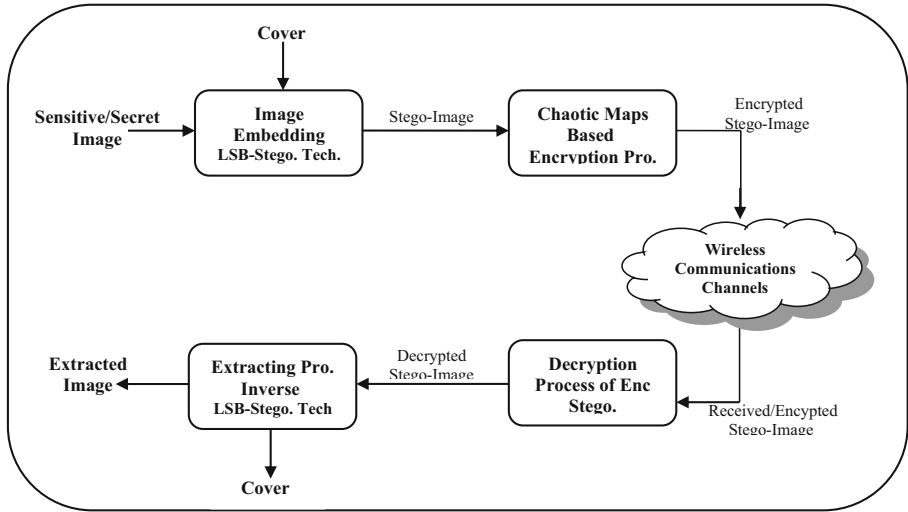
In this section, another experiments group are executed for evaluating the robustness of the proposed models. Performance of the various secured models has been investigated over; (AWGN), and Rayleigh fading channel. Table 4 gives the simulation setting parameters. This table gives the various parameters of the computer simulation experiments of the evaluating secured models I-II over the various wireless communications channels.

### 5.2.1 The AWGN channel: experiments group

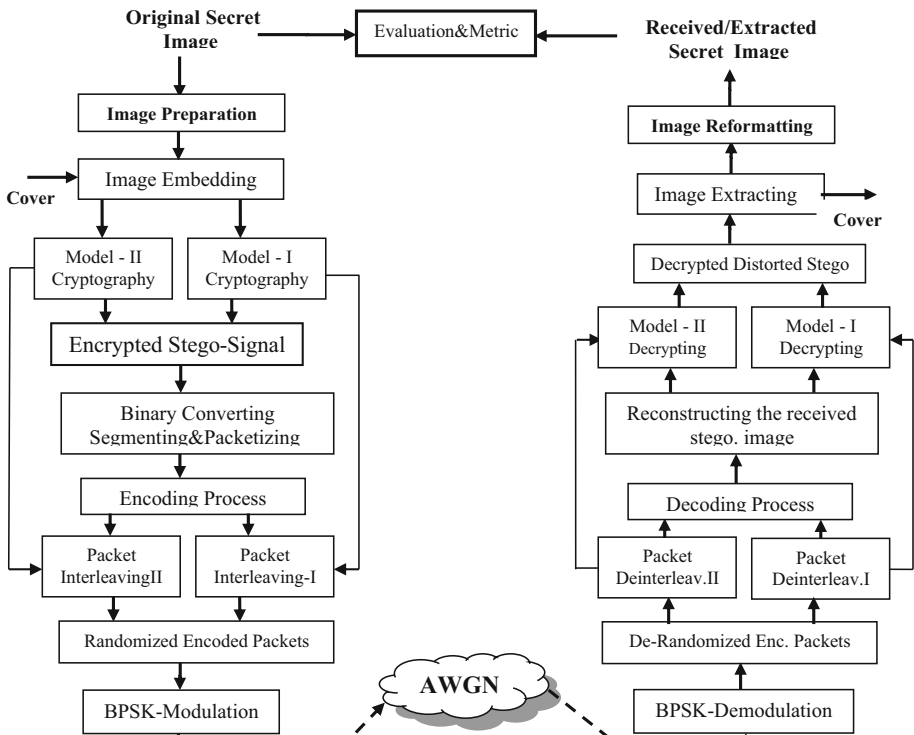
The first wireless communications channel is used as a wireless link to evaluate behavior of model-I and model-II is the (AWGN) channel. This model of wireless (AWGN)channel is used to simulate the testing process of securing transmitted secret image/multimedia signals. Various simulation experiments have been carried out for investigating the immunity and applicability of these security models for wireless link.

Performance of the presented security models is measured using many metrics such as, Cr, MSE and PSNR using AWGN channel and variations in the channel SNR (0 - 15 dB). Figure 7a shows simple block diagram contents of the proposed multimedia confidentiality enhancing models.

The results in Tables 5 and 6 indicate that model-I successes in the extracting process and working properly if SNR of channel is moderate (SNR > 12 dB), At lower level of SNR over AWGN channel, the extracting process of secret message fails. That means model-I is highly sensitive to the noise and do not resist its bad effects..



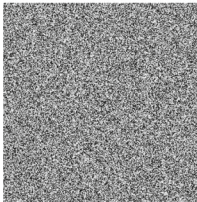
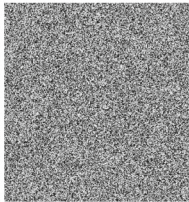
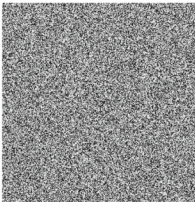

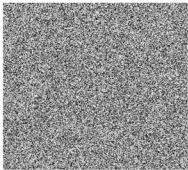
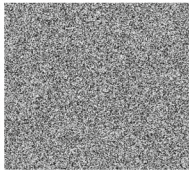
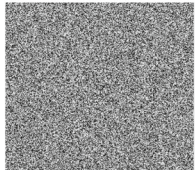
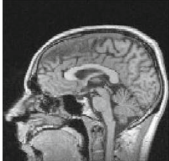
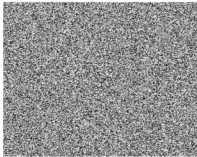
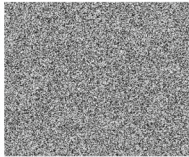
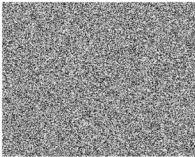

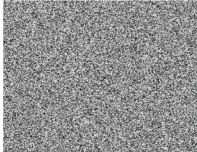
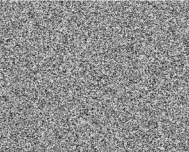
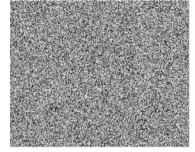
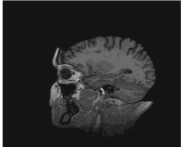
(a)



(b)

Fig. 7 Block diagram contents and steps secured multimedia transmission model, a. briefed block diagram, b. The details of secured model (contents and processing steps)

**Table 5** Extracted secret images samples with respect to the various channel SNR

<i>Model-I over wireless AWGN channel</i>			
0dB	5dB	10dB	11dB
			
10 dB	11dB	10dB	12dB
			
10 dB	11dB	10dB	10.5dB
			
10 dB	11dB	10dB	12dB
			

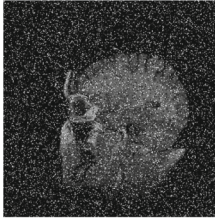
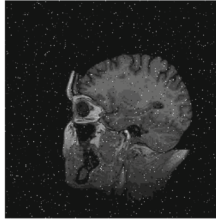
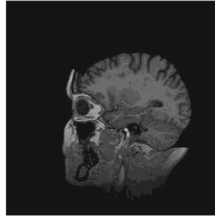
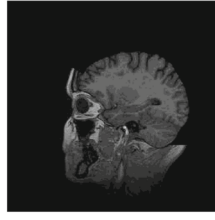
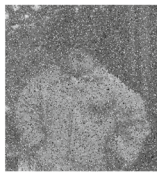



**Table 6** Samples metrics values of Model-I evaluation over AWGN channel with respect to extracted image quality

SNR	Quality of Extracted images Model-I (vImages) over wireless AWGN Channel					
	Test-pat/MedicalI			Cameraman/Boy		
	MSE	PSNR	Cr	MSE	PSNR	Cr
0 dB	16,400	6.02	0	16,200	6.04	0
5 dB	16,200	6.04	0.00334	16,200	6.04	0.00334
10 dB	16,200	6.06	0.004	16,200	6.06	0.004
12 dB	31.6	33.1	0.992	31.6	33.1	0.992
15 dB	31.6	33.1	0.9797	31.6	33.1	0.9959

Figure 7b gives the details of the processed secret-sensitive images processing in step-by-step method. In the following mechanism operation of the presented model-Is described:-

- firstly, the secret and cover images preparation and converting to  $256 \times 256$  pixels size, the embedding process to hide the sensitive image to be unobserved and unnoticed.
- The embedding process is followed by the encryption process based on (2 D logistic) in Model-I and based on (2 Baker) for model-II

**Table 7** Extracted images samples of Model-II evaluating over AWGN with respect to different SNRs

<i>Model-II over Wireless AWGN communications channel</i>			
0dB	5dB	10dB	12dB
			
0dB	5dB	10dB	12dB
			



**Table 8** Extracted image quality over AWGN with respect various metrics utilizing at different SNRs

Channel Conditions (SNR)	Image Quality Metrics of Model-II with various Image					
	Copyright/Medical1			Cameraman/Boy		
	MSE	PSNR	Cr	MSE	PSNR	Cr
0 dB	1800	16	0.49	3000	12	0.4282
5 dB	165	26	0.90	165	26	0.6969
10 dB	31.6	33.1	0.992	31	33.1	0.9348
12 dB	31.58	33.1	0.9927	31.6	33.1	0.9786
15 dB	31.6	33.1	0.9997	31.6	33.1	0.9797

- Encrypted composed image {cover involved secret message} (stego-image) has been converted to binary format and segmented to small packets (2048 bits).
- The encoding process using one of block or convolutional codes
- The encoded packets is randomized packet-by-packet) using 2-Dlogistic interleaving (Model-I) or 2-D Baker map interleaving (Model-II techniques or exchanging for more security. The randomized (encrypted) encoded packets is transmitted after the modulation stage. The end of transmitter side processes.

The previous computer simulation experiment is repeated for evaluating the model-II. The results of the second model-II employing the simulation setting and conditions as mentioned in Tables 7, 8. As indicated from the results, extracted secret image quality improves at good conditions of channel (High SNR), Also, the results prove the model-II resists the channel effects and performs better than model-I at low SNR values.,

As shown in previous, which reveal that Model-I has higher noise sensitivity, it requires high SNR and good channel conditions for successful secret-sensitive image extracting. On the other hand, the model-I is more sensitive toward any little change in the image. It can be employed for detecting tampering or modifying attacks. In the case of Model-I, it is essential employing the error control schemes for improving the extracted images and reducing the required threshold of SNR as shown in the next computer simulation experiments. The higher noise immunity is obtained model-II, efficient security model as shown in the results.

For studying the reliability and suitability the proposed secured models, various experiments have been carried out for evaluating the proposed models utilizing different cover and secret images for measuring the applicability of these security models.

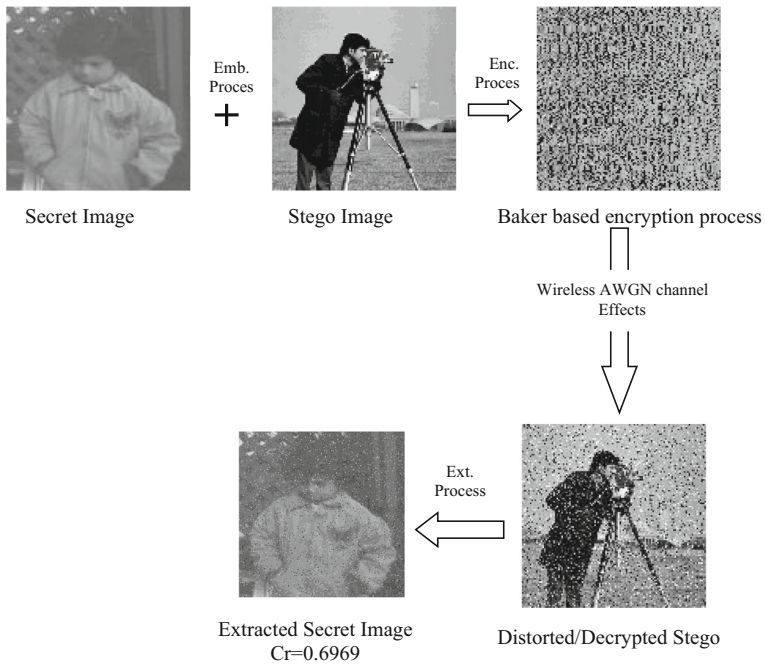
Figures 8 and 9 present the steps of images and its versions of Model-II, and Model-I respectively over the AWGN channel at SNR = 5 dB.

### 5.2.2 Model-I & Model-II:- performance investigating over AWGN channel

In this section the relation between the various SNR of AWGN and different metrics of extracted secret image is presented in a sepeate figures.

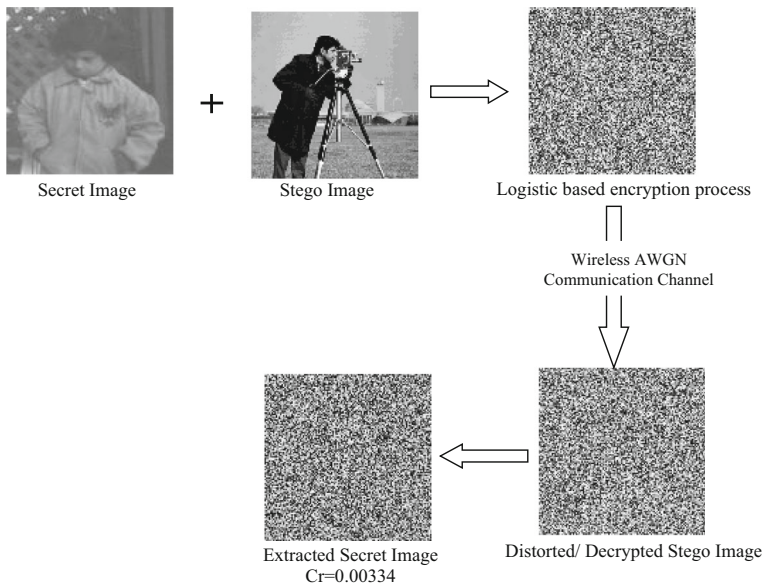
Figures 8 and 9 is presented for clearing the variation in the results and performance of Model-I and Model-II.

As cleared in Figs. 8 and 9, Model-I failed in extracted the embedded image at Eb/No <11 dB in case of wireless AWGN channel. The previous results prove that model-I is

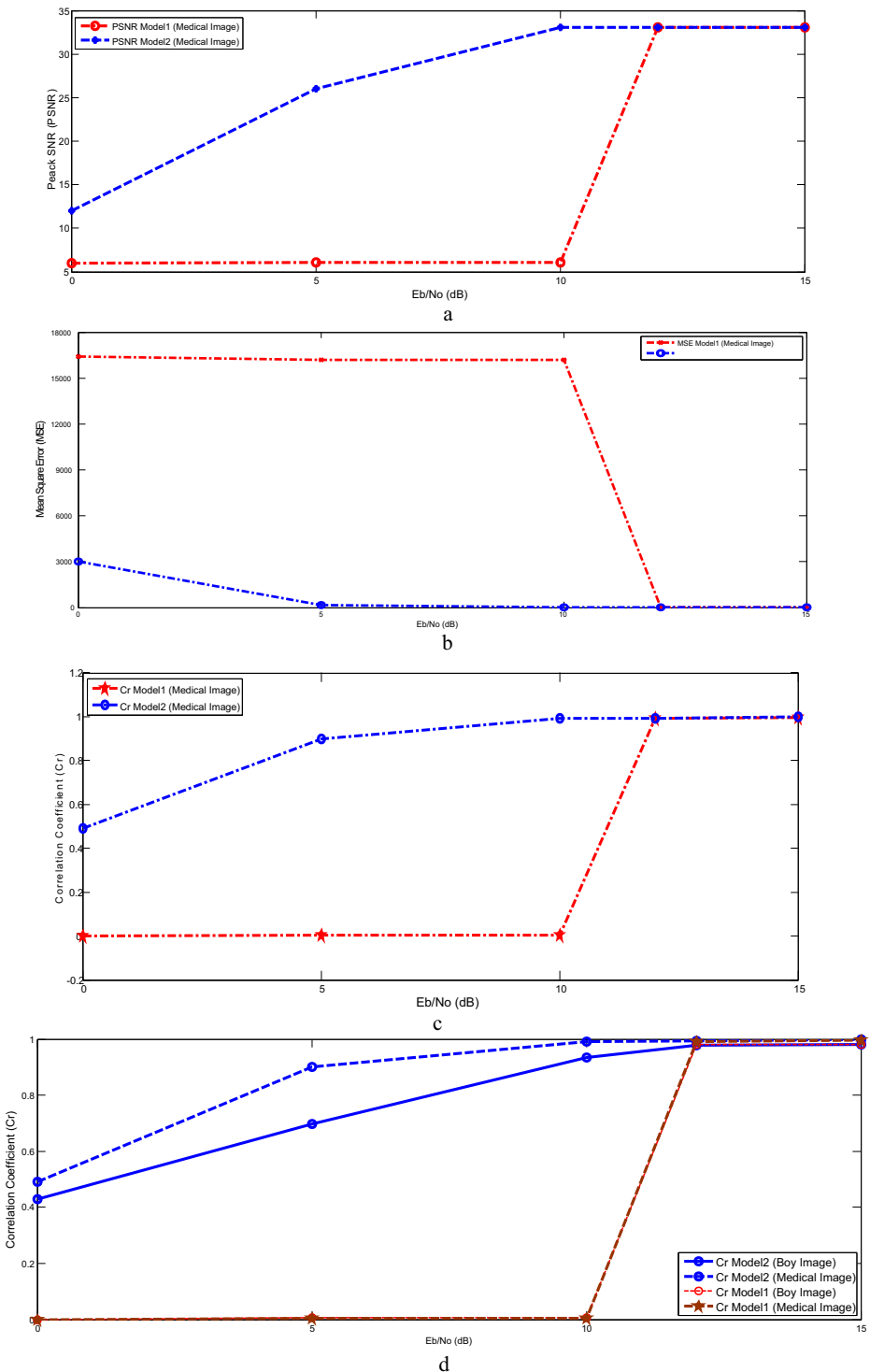


**Fig. 8** Various image version of model-II using Cameraman/Boy at SNR = 5 dB over AWGN

high sensitive towards channel noise (any changes in the composed image) due to 2D logistic map based encryption process. Also, as cleared from the results, model-I fails in extracting the embedded secret image at SNR < 12 dB. Therefore, this security model performs good and



**Fig. 9** Various Images version model-I using Cameraman and Boy, SNR = 10 dB over AWGN



**Fig. 10** Various metrics vs.  $E_b/N_0$  over AWGN wireless channel for model-I and model-II, a-PSNR, b-MSE, c-Cr, and d-Cr for boy and medical image

suitable at moderate and high channel SNR, it is not recommended and not suitable/applicable at low SNR or bad channel conditions hinders.

The change of Cr of original and extracted secret image with channel SNR variation are given in Fig. 10 for the different proposed security models. Based on the results of the various experiments, it is proved that model-II performs better than model-I at low SNR of communication channel (bad channel conditions) due to Baker-map based encryption process. For example, extracted secret image ( $Cr \approx 0$ ) for model-I at SNR of channel < 12 dB, while; at the same channel conditions,  $Cr \approx 1$  for model-II (SNR < 12 dB). So, performance of model-II at low SNR of communication channel due to its robust noise resistance.

The model-I requires good channel conditions for extracting the secret images successfully. So, the various Forward Error Correction (FEC) techniques are used for improving the quality of extracted secret image and reducing the required SNR. The results of FEC schemes utilizing with the various security models are tabulated in Table 8. The scenario of error control schemes is applied as shown in Fig. 10, this figure gives the details of the simulation model and the steps of the transmitted secret image processing, step by step.

### 5.2.3 Efficiency enhancement

Two scenarios are presented in this section for enhancing the presented security models of image transmission through employing the various FEC schemes to protect the transmitted packets over a noisy wireless channel (in first scenarios). The second scenario is based on utilizing the randomizing data technique as cleared previously in Fig. 2 for generating randomized encoded packets. These scenarios are presented for improving extracted secret image quality and enhancing the security capacities of presented models as shown in Table 9.

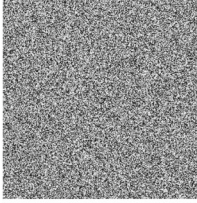
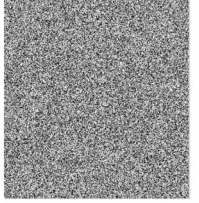
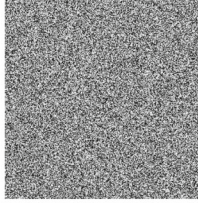

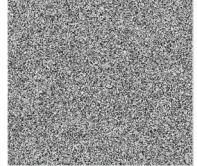
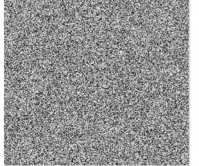
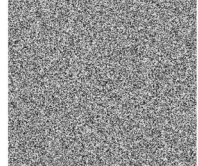
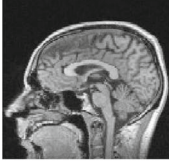
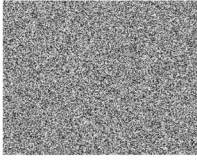
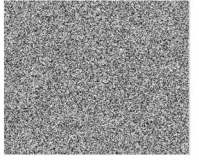
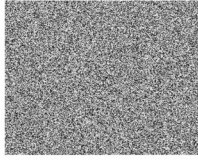

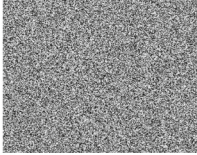
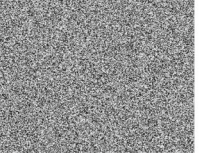
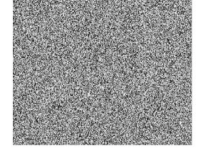
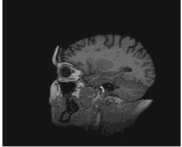
### 5.2.4 The Rayleigh fading channel:experiments group

The second group of experiments is devoted for evaluating the performance of the proposed Model-I and Model-II over the second wireless communications channel that is the fading channel for examining the applicability of these security models and evaluating its performance. Channel SNR variation is considered in measuring the extracted secret image quality. Performance Model-I “Data hiding & 2D logistic” has been investigated over fading channel, the results of this experiment have been tabulated in Table 10, it shows samples of extracted secret images. Table 11 gives the tabulation of the metrics values.

**Table 9** Results of various FEC employing over AWGN channel with respect to extracted secret image quality and multi-testing images (SNR = 8 dB)

Image for Testing		Metrics					
		No FEC		Hamming Code (15, 11)		RS(7, 3)	
		PSNR	Cr	PSNR	Cr	PSNR	Cr
Model-I	Test-pat/Medical	6.04	0.00334	23	0.962	25	0.980
	Cameraman/Boy	6.04	0.00334	24.4	0.964	27	0.990
Model-II	Test-pat/Medical	28	0.901	30	0.901	32	0.990
	Cameraman/Boy	26	0.959	28.5	0.9869	32	0.999

**Table 10** Samples of extracted image of Model-I evaluating over fading channel

<i>Model-I over wireless Rayleigh Fading channel</i>			
5dB	15dB	25dB	36dB
			
5dB	15dB	25dB	37dB
			
5dB	15dB	25dB	36.5dB
			
5dB	15dB	25dB	37dB
			

The results of model-I performance investigating prove its high sensitivity to channel noise. As cleared also, with the channel conditions (SNR<36dB) this model-I fails to successfully

**Table 11** Extracted secret image quality and the Cr metrics with SNRs variety

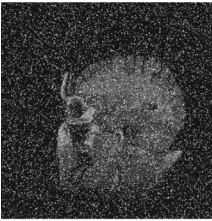
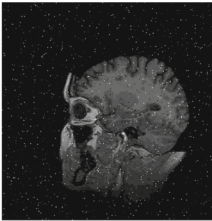
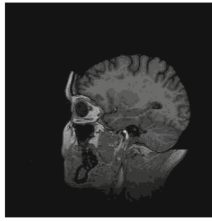
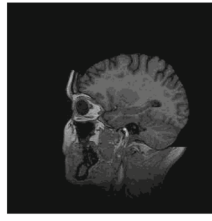




SNR	Model-I with various Images over wireless <i>wireless Rayleigh Fading channel</i>					
	Test-pat/Medical1			Cameraman/Boy		
	MSE	PSNR	Cr	MSE	PSNR	Cr
5 dB	16,500	5.02	0	16,400	6.04	0
15 dB	16,300	6.02	0.0021	16,350	6.04	0.00234
25 dB	16,200	6.06	0.0024	16,200	6.06	0.00241
37 dB	31.6	33.1	0.9977	31.6	33.1	0.9987
45 dB	31.6	33.1	0.9977	31.6	33.1	0.9989

extract the secret image, compared with results of previous experiments of model-I over AWGN channel, the required SNR for achieving success extracting process increased from 11 dB for AWGN channel to 36 dB for this channel model. While in fading channel, for guarantee successful extracting process SNR > 35 dB for Model-I.

The results of Model-II “Data Hiding & 2 D Baker map based” over fading channel have been given in Table 12. Table 13 gives the metrics value of this experiment of Model-II over Rayleigh fading channel with respect to the various metrics and SNR channel variations.

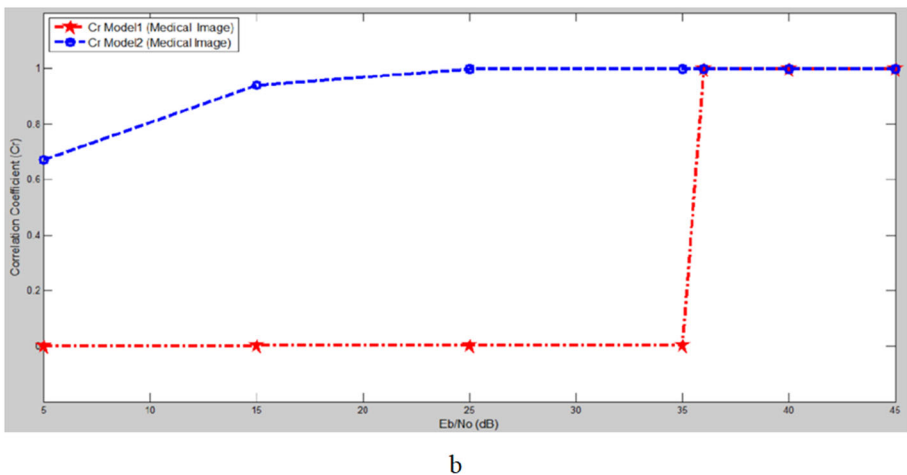
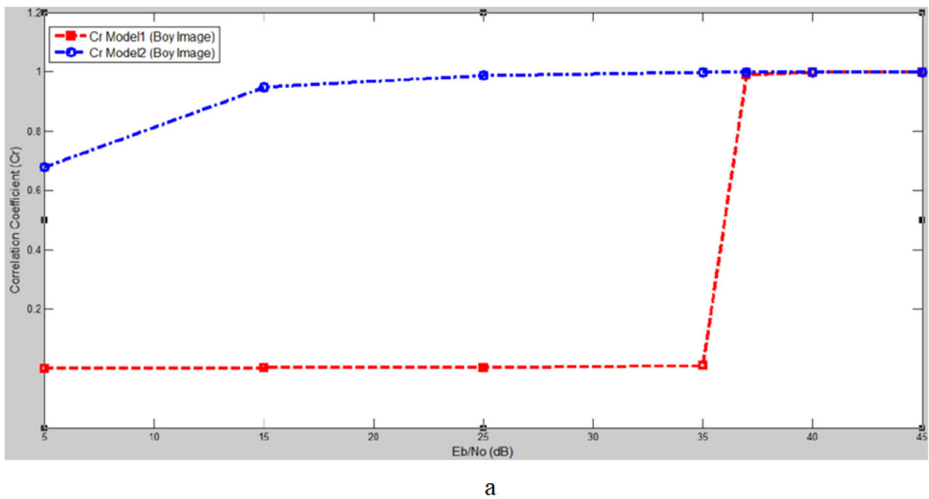
Figs. 11 and 12 show the Cr values with the SNR of fading channel variations. As cleared form these results, behavior of model-II is better than model-I as over AWGN channel. Cr of

**Table 12** Samples of extracted images of Molel-II over fading channel

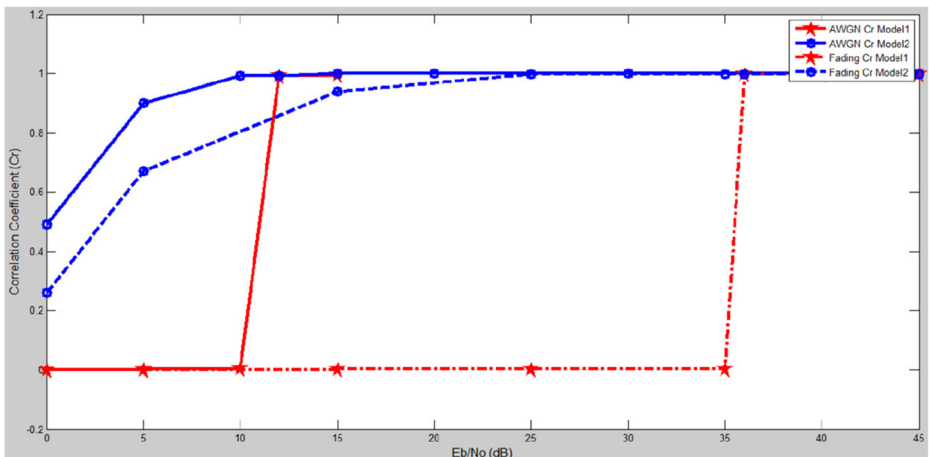
<i>Model-II over wireless Rayleigh Fading communications channel</i>			
5dB	15dB	25dB	37dB
			
5dB	15dB	25dB	37.5dB
			

**Table 13** Extracted secret images with respect various metrics with SNRs variation

SNR	Model-II with various Images					
	Copyright/Medical1			Cameraman/Boy		
	MSE	PSNR	Cr	MSE	PSNR	Cr
5 dB	1700	17	0.69	3000	12	0.6282
15 dB	165	26	0.939	165	26	0.9969
25 dB	31.6	33.1	0.997	31	33.1	0.9948
35 dB	31.58	33.1	0.9987	31.6	33.1	0.9986
45 dB	31.6	33.1	0.9987	31.6	33.1	0.9997



**Fig. 11** Various metrics vs. Eb/No over Rayleigh fading wireless channel for model-I and model-II, a- Cr using boy image, a- Cr using medical image



**Fig. 12** Cr vs. Eb/No of model-I and model-II over AWGN and Rayleigh fading wireless channels using medical image

the extracted secret image in case of model-II increases with SNR increasing, while; for model-I there is no successfully extracting process with channel SNR<35dB.

### 5.2.5 Threshold enhancing: FEC utilizing

As proposed in the previous experiments, FEC schemes can be used for decreasing the SNR which required for assuring success secret image extracting. In this section, the various FEC are employed for decreasing the SNR threshold over fading channel. The same scenarios which are presented are implemented for the security models in this section. Tables 14 and 15 show the effects of error control employing for coding the transmitted packets.

Table 15 tabulates the extracted secret images quality and utilizing the power full error control schemes for enhancing the extracted image and successfully extraction at the lower SNR of the communications channel in the case of model-II. On the other hand, the proposed model-II performs better than the model-I, it resists the distortion over the various communications channel. Therefore, the weak error control schemes are employed for this secured model.

**Table 14** FEC utilizing for model-I with respect quality metrics (SNR = 35 dB)

	Image for Testing	Metrics			
		No FEC		Hamming Code (15, 11)	
		PSNR	Cr	PSNR	Cr
Model-I	Test-pat/Medical	6.04	0.0040	31	0.932
	Cameraman/Boy	6.06	0.0039	31.5	0.904
Model-II	Test-pat/Medical	26	0.901	32	0.987
	Cameraman/Boy	27	0.959	32.5	0.987



**Table 15** Metrics of various images utilizing various error control techniques (SNR = 35dB)

Image for the Testing		Metrics			
		Convolutional (2, 1, 3) code		Convolutional (2, 1, 7) code	
		PSNR	Cr	PSNR	Cr
Model-I	Medical2	22.5	0.963	25.5	0.985
	Boy	24.3	0.962	26.51	0.989
	Lena	25	0.969	27.71	0.998
	Cat	24.3	0.961	27.3	0.971
	Fruit	24.9	0.975	27.9	0.992
	Average $T_p$	0.15935 mSec		0.17325 msec.	

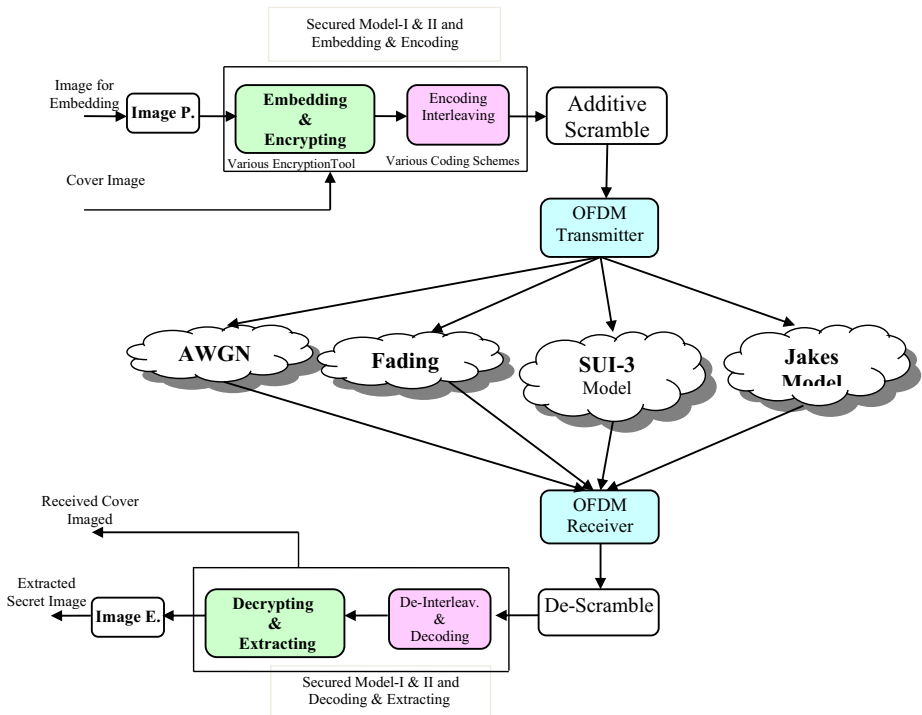
As shown in the previous Fig. 2 which describes the steps of multimedia processing for achieving the high level of confidentiality over the wireless link, there are third level of security can be merged within the proposed models through using the encryption tools for randomizing the encoded packets after the encoding process. Also, the exchanging process will enhance the confidentiality through using the Baker based randomizing tool with the model-II, while the Logistic based packet randomizing can be used with the model-I. So, the presented secured models provide three merged security level for securing the multimedia signals over the noisy wireless communications channels.

## 6 OFDM system: various channel models

The suitability and applicability of the proposed secured model for enhancing the multimedia confidentiality are tested on the OFDM system in this section. It is important in the designing of wireless communications system decreasing the bad effects of the channel such as multi-path. OFDM system has been designed to overcome problems of multi-path, it is high data rate transmission technique, through sub-carriers transmit the data simultaneously, its orthogonal achieves perfect data transmission over multi-path and noisy channel with decreasing interference and successful detection. The presented various security models have been tested and evaluated using OFDM system over a different wireless communications channels models [26].

Due to a wide using of OFDM system for achieving high data rate transmission in different wireless networks such as Long Term Evolution (LTE) and Wireless Local Area Networks (WLANs), it has been chosen for applying the various security models [13, 17, 25]. Different models of wireless channels have been employed for testing the performance and behavior the proposed security models within the OFDM system, which are AWGN, Jakes model, Rayleigh fading, and Stanford University Interim (SUI-3). All these wireless channel models are considered for testing the applicability of the proposed security schemes on OFDM system. Fig. 13 gives the proposed secured OFDM model using the various environment of data transmission [11].

The previous experiments are repeated on ODM system with using various channel models, AWGN and fading channels with another channel models. Figs. 14 and 15 give the images samples of security models testing over AWGN and Fading channels for model-I and model-II, respectively.

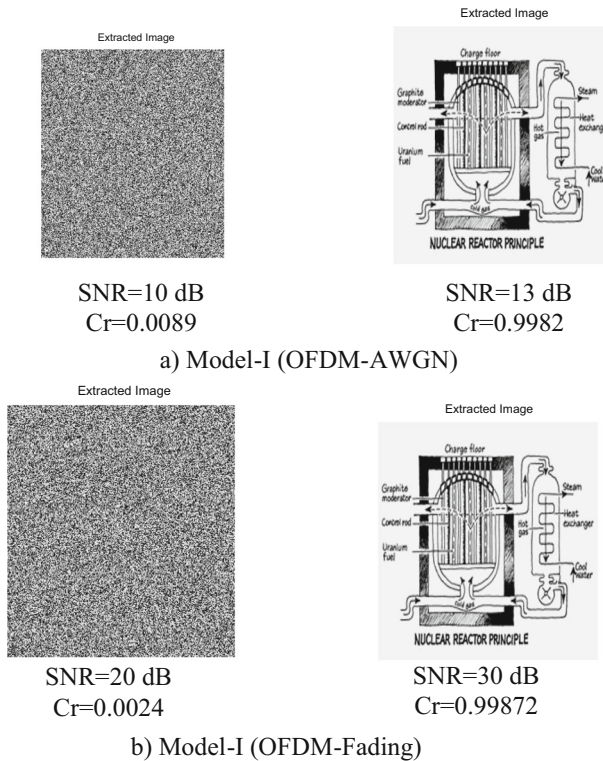


**Fig. 13** Block diagram of the proposed secured model contents for secured multimedia signal transmission over OFDM

Cr metric (with OFDM system experiments) of original and extracted secret image with channel SNR variation for AWGN and Fading has been given in Figs. 14, and 15, for model-I and model-II, respectively. These results clear that the model-II resists channel noise and Cr enhances with increasing SNR. On the other hand, model-I fails in successful secret image extracting with channel conditions  $\text{SNR} < 11$  dB for AWGN and  $\text{SNR} < 23$  for Fading channel. That means these security model need FEC schemes for decreasing the SNR threshold for assuring successful secret image extracting, specially model-I.

The third wireless communication (SUI-3) channel model-Is presented in the following experiments. This model has been utilized for evaluating and testing the presented secured model on the OFDM system. SUI-3 channel model consists of 6 models of channel conditions, they are AWGN, LOS fading, NLOS fading and variety of delay. Based on terrain nature, there are 3 categories {A, B and C}. Firstly, A category represents hilly, heavy-tree density and path-loss, B category represents and simulates medium path-loss, hilly and light-tree density. C category simulates less density of tree and lower path-loss level. In this experiments, this channel model considers various noise sources such as AWGN and fading channels (LOS/NLOS considered). Results of this experiment have given.

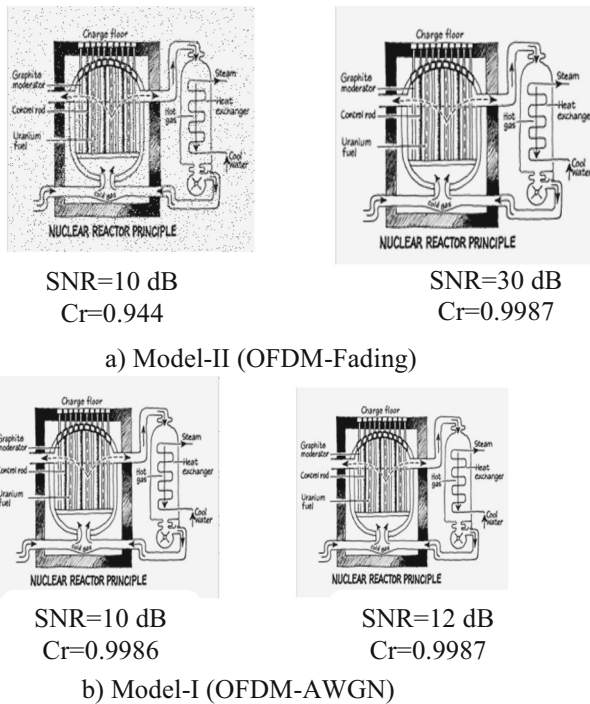
The SUI-3 model (Category B) has been used for testing the performance and behavior the security models [4]. In this experiments, this channel model considers various noise sources such as AWGN and fading channels (LOS/NLOS considered). Results of this experiment have given Fig. 16.



**Fig. 14** Received sample of extracted images samples using Model-I with OFDM wireless communications **a** AWGN channel, **b** Rayleigh fading

As proved from the previous results, model-I needs high SNR for assuring successful extracting of secret image due to the high sensitive of logistic-based encryption process. These results have been confirmed in the experiments of OFDM-SUI-3 channel mode, in this scenario; channel has worst conditions due to included fading effects in this wireless communications channel model. Therefore, model-I needs very high SNR to extract the secret image high than the previous experiments of OFDM. To decreasing this channel model effects, equalizing technique has been employed for overcoming multi-path fading effects. On the other hand, model-II also, is affected from the worst conditions of this channel model as cleared form the tabulated results in Table 16.

According to the results of OFDM experiments utilizing the presented security models over various channel models, it is cleared that model-I can be considered an efficient tool for achieving high image confidentiality if there is acceptable noise level channels, also equalization is very necessary in the presence of fading. Table 16 tabulates the experiments results of OFDM system with respect to various communications channels models and conditions. Table 17 shows the results after employing the powerful error control schemes to improve the performance of the whole systems plus decreasing the threshold of channel conditions (SNR) which permits success extraction.



**Fig. 15** Received samples of extracted images samples using Model-II with OFDM wireless communications **a** - Rayleigh fading channel, **b** AWGN channel

## 6.1 Results analysis of OFDM system

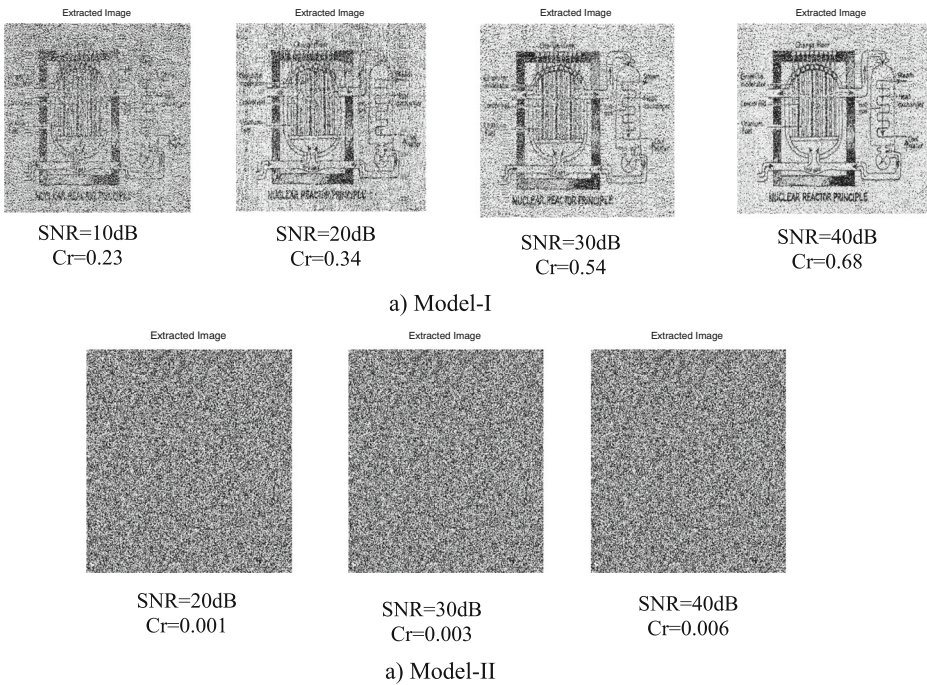
In the following, Figs. 17 and 18 show the relation between the channel condition and the extracting process.

The equalizing process is considered for enhancing the quality of the extracted secret image. From the previous results, Table 16, the presented security models achieve bad performance over the SUI-3 model and difficulty extracting secret image. Therefore, the MMSE equalizer [4, 17, 25] is employed for improving the quality of the extracted secret image. Figures 19 and 20 gives the comparison between the SUI-3 without equalizing and with employing the equalizing process.

## 7 Text confidentiality enhancing scenario

In this section, the presented efficient secured models for multimedia signals confidentiality are applied on the text files. Studying of the suitability and applicability various proposed scenarios have been presented in this section, for the classified and high secret text files. The various data transform techniques are utilized for choosing the suitable transform tool, for example, DFT, DST, DWT and DCT transforms, these technique are tested in the presented model [48].

Confidentiality of text can be essential issue; specially if this text contains high classified information. Hence, this section presents high confidential tool for securing the transmitted



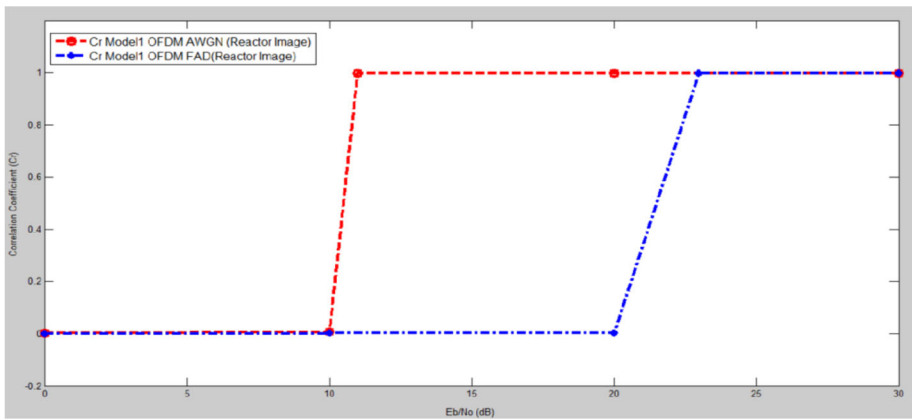
**Fig. 16** Received samples of extracted image samples over OFDM using SUI-3 model at various channel conditions, **a** Model-II results, **b** Model-I results

**Table 16** Samples of Extracted images and its quality metrics with the presented security models in OFDM system {different wireless communications model channels}

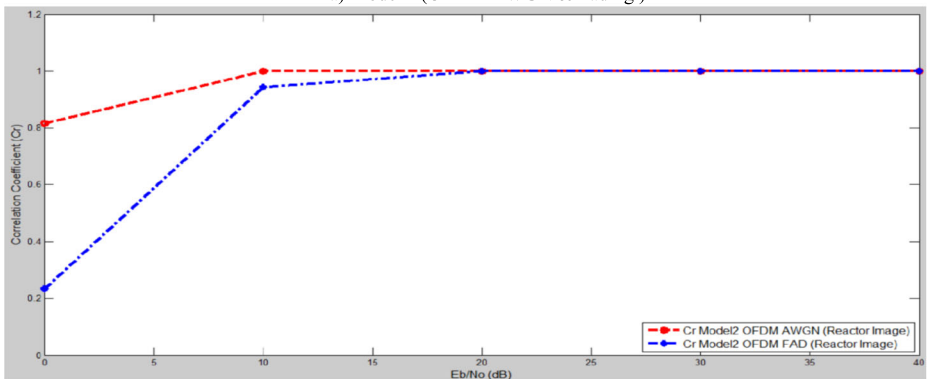
	Proposed Secured Models with OFDM System	AWGN & Fading channel with OFDM communications System									
		0 dB		10 dB		11 dB		20 dB		30 dB	
		Reactor	Medical	Reactor	Medical	Reactor	Medical	Reactor	Medical	Reactor	Medical
AWGN Channel	Model 1	0.002	0.003	0.0089	0.0090	0.998	0.999	0.998	0.998	0.998	0.998
	Model 2	0.815	0.826	0.998	0.997	0.998	0.999	0.998	0.998	0.998	0.998
	SNR	0 dB	0dB	10 dB	10dB	11dB	11dB	23 dB	23 dB	23 dB	23 dB
Fading channel	Model1	0.0005	0.0006	0.0021	0.0032	0.0024	0.0034	0.998	0.998	0.998	0.998
	Model2	0.325	0.425	0.944	0.954	0.9987	0.9987	0.998	0.9987	0.9987	0.9987
	SNR	0dB	0dB	10dB	10dB	20dB	20dB	30dB	30dB	40dB	40dB
SUI-3 Model	Model1	-0.004	-0.001	0.005	0.005	0.0016	0.0016	0.003	0.003	0.006	0.006
	Model2	0.23	0.325	0.34	0.35	0.49	0.49	0.54	0.54	0.68	0.68
SUI-3+Eq. Model	Model1	-0.004	0.006	-0.0035	-0.0035	0.0016	0.0016	0.9987	0.9987	0.998	0.998
	Model2	0.807	0.821	0.977	0.977	0.9987	0.9987	0.9987	0.9987	0.999	0.999
		Success Extracting		Failed Extracting				Equalizing Effects			

**Table 17** Error control techniques considerations and image quality metrics of OFDM experiments (SNR = 38 dB)

Image for the Testing		Metrics		
		NFEC Cr	CC (2, 1, 7) Cr	RS (15, 11) Cr
Model-I	Reactor	0.006	0.995	0.993
	Medical1	0.006	0.989	0.987
	Boy	0.006	0.989	0.9891
	Lena	0.006	0.9981	0.999
	Cat	0.006	0.971	0.991
Model-II	Fruit	0.006	0.992	0.994
	Medical1	0.67	0.9991	0.9999
	Boy	0.68	0.989	0.9976
	Lena	0.65	0.998	0.9992
	Cat	0.64	0.971	0.9995
	Fruit	0.66	0.992	0.9991

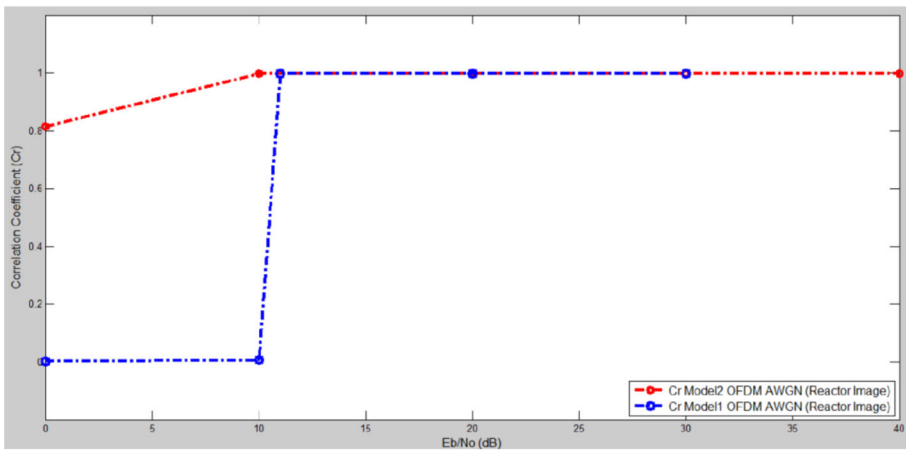


a) Model-I (OFDM AWGN & Fading )

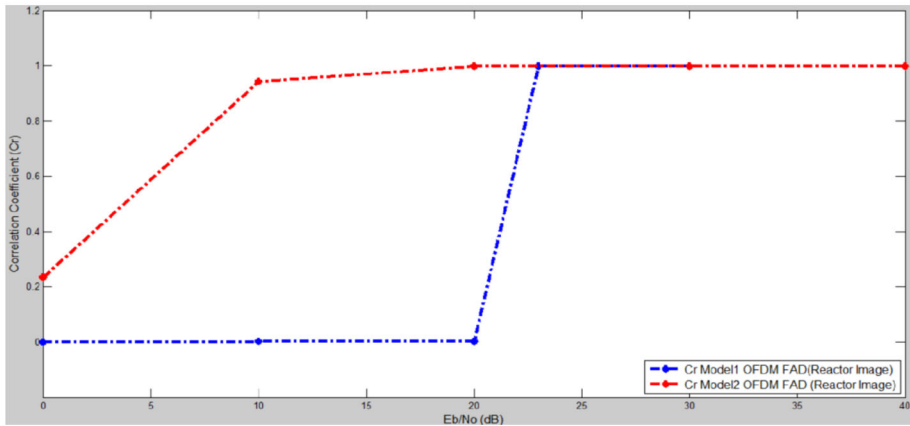


b) Model-II (OFDM AWGN & Fading )

**Fig. 17** Cr vs. Eb/No of model-I & model-II over OFDM -AWGN and Rayleigh fading wireless channels using Reactor image, **a** model-I {AWGN and Fading}, **b** Model-II {AWGN and Fading}



a) Model-I & II (AWGN )



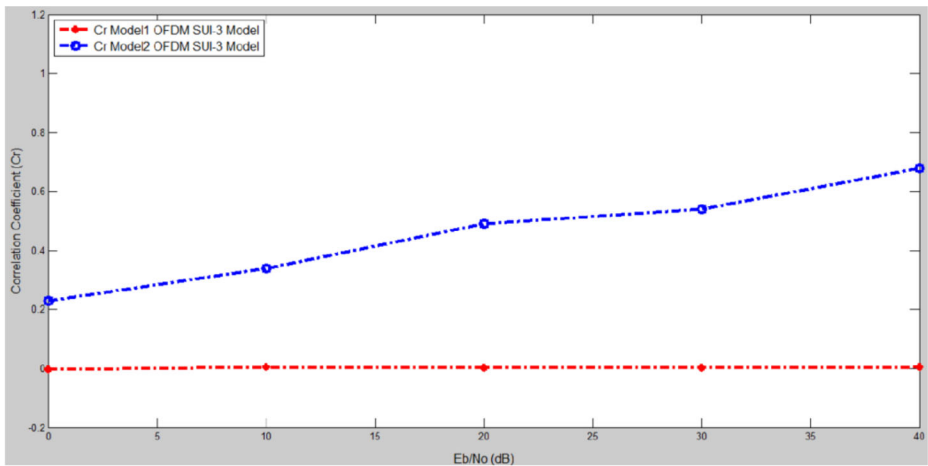
b) Model-I & II (Fading )

**Fig. 18** Cr vs. Eb/No of model-I & model-II over OFDM- various wireless channels using Reactor image, **a** OFDM - AWGN channel, **b** Fading channel

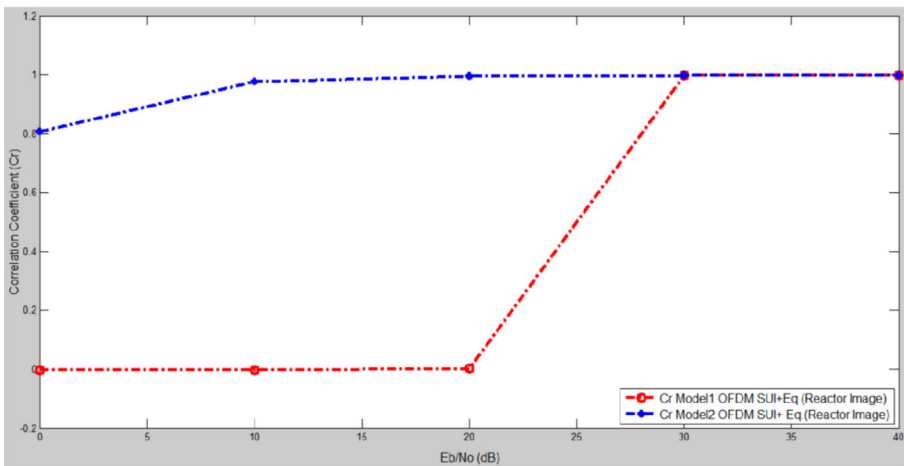
text files. This proposed tool contains multi-level of security merging; data hiding DWT-based encryption process, The presented model hides the secret text file within cover image to produce composed image/stego. The stego image is encrypted by Baker-based encryption tool. Figure 21 gives the overall processes of high sensitive/classified text files at the transmitter and in the receiver sides, as embedding process and extracting steps have been cleared in this figure.

**Text hiding Algorithm:-**

- There is the secret text file and cover image for embedding the secret text.
- First step:-Using one of the data transforming techniques (DCT, DST, DFT and DWT), DWT gives best performance, where the extracted text is very closed to the original more than the other transforms.



a) Model-I &amp; II (SUI-3 model)

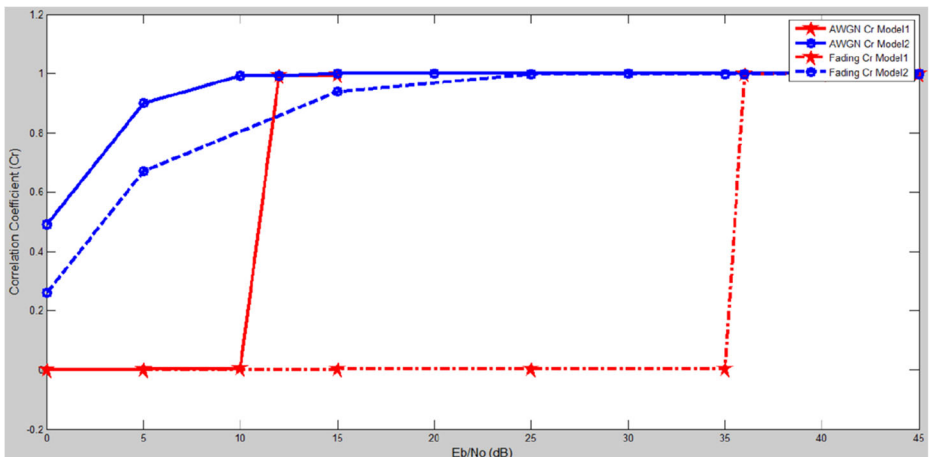


b) Model-I &amp; II (SUI-3 model &amp; Equalizing)

**Fig. 19** Cr vs. Eb/No of model-I & model-II over OFDM- SUI-3 channel mode with/without employing the equalizing process using Reactor image, **a** SUI-3 model (No Equalizing), **b** SUI-3 model (with Equalizing)

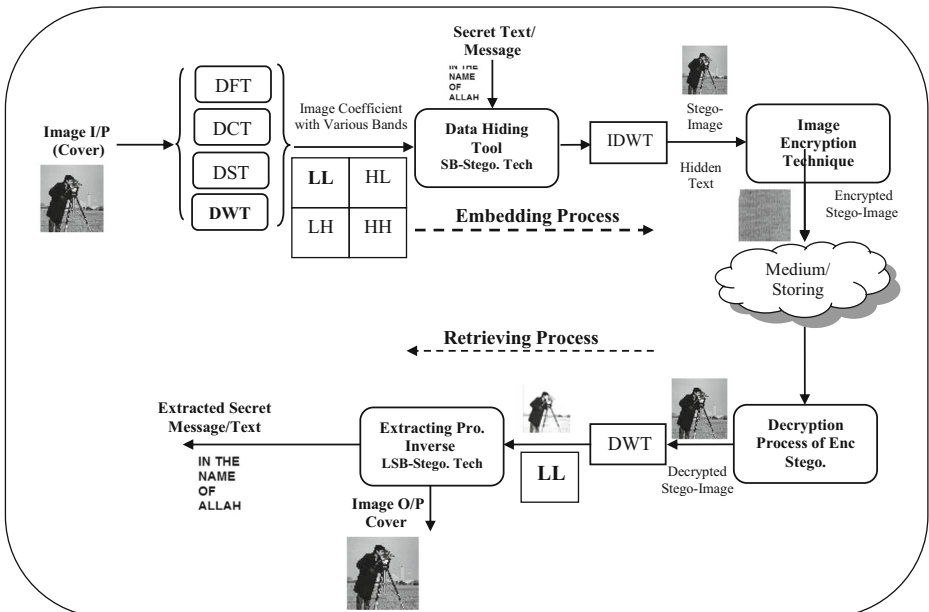
- The third step:- Choosing the lower weight data band (lower resolution partition) such as utilizing the LL band of DWT transform.
- This step ensures the high similarity between cover and composed image, hence embedded high sensitive/secret text won't be observable or noticeable.
- The fourth step:- Converting the text file to binary format and using data hiding tool (LSB-Steganography technique) for embedding this binary text file into the LL band cover.
- In the next step after hiding process, the processed LL band is processed by inverting the DWT transform and merged with the rest bands “HL, LH and HH bands” for constructing the stego-image, it involves the secret text.





**Fig. 20** Comparison Cr vs. Eb/No of model-I & model-II over OFDM- SUI-3 channel mode with/without employing the equalizing process using Reactor image

- The second level of securing process and text confidentiality enhancement is the encryption process of the stego-image using Logistic based encryption or Baker based encryption techniques.
- The encrypted Stego-image is generated containing the secret text file.
- After the last process, the encrypted file can be transmitted or stored according to the requirements. in the case of the need to this text file, the reverse process will be executed on the encrypted stego file for retrieving the secret text to its original format as shown in Fig. 21.



**Fig. 21** Secret message/text confidentiality enhancing model using combined security tools

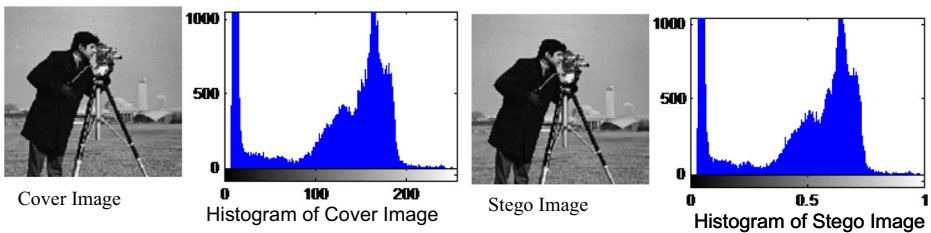


Fig. 22 The Original cover image and composed/stego image

## 7.1 TEXT confidentiality enhancing test

The proposed confidentiality enhancing model utilizes Cameraman image as a cover image, while the text message is “(In The Name of Allah, Please Check Your Results Again, The Radiation Level is Abnormal)”, as an example for testing the presented model. Figure 22 shows the original cover and composed/stego image after embedding process of secret text message and its histogram.

Table 18 tabulates the Cr of extracted classified text and original files and other quality metrics of extracted text file with the various data transform techniques.

From the experiments of text-based message, after the embedding process, appearance of original cover is very close to composed image. So, the proposed model for text confidentiality has high imperceptibility  $\{Cr=1\}$ . From the metrics values of the text confidentiality model, the presented model can be powerful security model for high sensitive and classified text files.

## 8 Comparative study

Our proposed secured model as mentioned in the introduction section, there are two security techniques are combined using the data hiding and encryption tools based on the various maps. In the proposed model, the chaotic maps are utilized twice, it is performed on the whole stego-signal after the embedding process. The second utilization of 2-D chaotic maps is executed on the packets after the encoding process for providing the packet-by-packet securing.

Hence, the robustness of the proposed multimedia security system against any type of attacks such as, adversary and eavesdropping attacks is enhanced. Also, the packet-by-packet securing process improves the error performance of the whole wireless multimedia

**Table 18** Evaluation the presented secret text confidentiality enhancing with respect to the different data transform

Data Transforms	Image Quality Metrics of Model-I with various Image over wireless AWGN Channel		
	Cameraman/Test message		
	MSE	PSNR	Cr
DFT	165	26	0.8235
DST	38.08	31.1	0.9972
DCT	37.1	33.3	0.9983
DWT	36.92	62.48	0.9999

transmission system, where, this process makes randomizing the bits in the packets that leads to spreading the adjust errors and raising the capability of FEC schemes.

PSNR of extracted data was 53 dB in [3], while in our proposed model the PSNR of the extracted text message is 62 dB. That clears the superior performance of the proposed model- In our research work compared to the pervious related work. Also, the computer simulation experiments prove the suitability and applicability of the different presented models for various multimedia signals format, text, image, and audio.

The variety in the proposed model can be employed for different scenarios of multimedia transmission according to the communications channel conditions. The variety in the security levels on the whole image level and on the packets level. This advantage of the proposed models can be used for improving the security and confidentiality of the multimedia signals.

## 9 Conclusions

In this research paper, combined of multi-levels security models are presented by merging the data hiding and cryptographic techniques for immune and enhancing the multimedia signals transmission and confidentiality over the various wireless communications channels. The standalone FEC techniques and randomized FEChave been utilized for improving performance of whole system and enhancing the extracted multimedia signals, text or image. The computer experiments covered behavior evaluation of the presented security models over various wireless channels models. The results of these experiments prove the robustness and applicability of the proposed models. Over the OFDM system, the model SUI-3 requires powerful error control schemes to ensure success extracting of secret message with accepted and sufficient quality. The timing analysis is considered, Model-I consumes more processing time more than the Model-II. Also, powerful error control schemes takes more time in the processing such as RS(15, 11) and convolutional code (1, 2, 7). Therefore, these codes is not recommended only in the bad conditions channels such as the SUI-3 model and jakes model. Finally, the presented security models enhance the confidentiality of images also, it suitable for providing confidential text message. Various data transform are utilized, DWT gives best results. The proposed secured models are suitable for various multimedia signals, such as secret - sensitive images and text files, where these models achieve high level of confidentiality over the various wireless communications channels and OFDM systems with the different communications channel models.

**Funding** Open access funding provided by The Science, Technology & Innovation Funding Authority (STDF) in cooperation with The Egyptian Knowledge Bank (EKB).

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

## References

1. Algarni AD, Soliman NF, Abdallah HA, Abd El-Samie FE (2020) Encryption of ECG signals for telemedicine applications. *Multimed Tools Appl* (2021) 80:10679–10703. <https://doi.org/10.1007/s11042-020-09369-5>
2. Al-Nuaimy W, El-Bendary MAM, Shafik A, Shawki F, Abou-El-azm AE, El-Fishawy NA, Elhalafawy SM, Diab SM, Sallam BM, El-Samie FEA, Kazemian HB (2011) An SVD audio watermarking approach using chaotic encrypted images. *Digital Signal Processing* 21 (6), 764–779
3. Al-Roithy BO, Gutub A (2021) Remodeling randomness prioritization to boost-up security of RGB image encryption. *Multimed Tools Appl*. <https://doi.org/10.1007/s11042-021-11051-3>
4. Arun AS, Joseph GM (2013) High security cryptographic technique using steganography and chaotic image encryption. *IOSR Journal of Computer Engineering (IOSR-JCE)* 12(5):49–54
5. Chandramouli EIK, Ho ATS, Kim HJ (2021) Large-scale multimedia signal processing for security and digital forensics [SI 1163]. *Multimed Tools Appl* (2021) 80:23313–23317. <https://doi.org/10.1007/s11042-021-11108-3>
6. Chang WH, Chang LW (2010) Semi-Fragile Watermarking for Image Authentication, Localization, and Recovery Using Tchebichef Moments. *Communications and Information Technologies (ISCIT)*
7. Chen GR, Mao YB, Chui CK (2004) "a symmetric image encryption scheme based on 3D chaotic cat map," *Chaos, Solitons and Fractals* 21:749–761
8. Chen H, Chang C, Shi Z, Lyu Y (2021) Hybrid features and semantic reinforcement network for image forgery detection. *Multimedia Syst J*. <https://doi.org/10.1007/s00530-021-00801-w>
9. Choudhary K (2012) Image Steganography and Global Terrorism. *Global Security Studies* 3(4)
10. El-Bendary MAM (2017) FEC merged with double security approach based on encrypted image steganography for different purpose in the presence of noise and different attacks. *Multimedia Tools and Applications* 76 (24), 26463-26501
11. El-Bendary MAM, Abou El-Azm AE (2019) Complexity considerations: efficient image transmission over mobile communications channels. *Multimedia Tools and Applications* 78 (12), 16633-16664
12. El-Bendary MAM, Abou-El-azm AE, El-Fishawy NA, Shawki F, El-Tokhy MAR, Kazemian HB (2012) Performance of the Audio Signals Transmission over Wireless Networks with the Channel Interleaving Considerations. *EURASIP Journal on Audio, Speech, and Music Processing*
13. Gao T, Gu Q, Chen Z (2008) A new image encryption algorithm based on hyper-chaos. *Phys Lett A* 372: 394–400
14. Goel S, Rana A, Kaur M (2013) Comparison of image steganography techniques. *International Journal of Computers and Distributed Systems* 3(I)
15. Himani S, Mishra DC, Sharma RK, Kumar N (2021) Multi-image steganography and authentication using crypto-stego techniques. *Multimed Tools Appl*. <https://doi.org/10.1007/s11042-021-11068-8>
16. HSE Nuclear Directorate Division 5 Office for Civil Nuclear Security (2008) The Management of Sensitive Nuclear Information during the Generic, Design Assessment of Nuclear Technologies, Version 2, 01 February
17. Huang CK, Nien HH (2009) Multi chaotic systems based pixel shuffle for image encryption. *Opt Commun* 282:2123–2127
18. International Atomic Energy Agency (2011) Computer Security at Nuclear Facilities. In: *Technical Guidance Series No.17*, IAEA, Vienna, Austria
19. Jin X, He Z, Wang Y, Yu J, Xu J (2021) Towards general object-based video forgery detection via dual-stream networks and depth information embedding. *Multimed Tools Appl*. <https://doi.org/10.1007/s11042-021-11126-1>
20. Juneja M, Sandhu PS (2009) Designing of robust image steganography technique based on LSB insertion and encryption. In: *International Conference on Advances in Recent Technologies in Communication and Computing*
21. Kamal AHM (2013) Steganography: Securing Message in wireless network. *Int J Comput Technol* 4(3) March-April
22. Kaur G, Singh K, Gill HS (2021) Chaos-based joint speech encryption scheme using SHA-1. *Multimed Tools Appl* 80:10927–10947. <https://doi.org/10.1007/s11042-020-10223-x>
23. Krenn JR (2004a) Steganography and Steganalysis
24. Krenn JR (2004b) Steganography and Steganalysis
25. Kumar A, Pooja K (2010) Steganography: A Data Hiding Technique. *International Journal of Computer Applications* (0975–8887) 9(7)
26. Kwok HS, Wallace K, Tang S (2007) "A fast image encryption system based on chaotic maps with finite precision representation," *Chaos, Solitons and Fractals* 32:1518–1529

27. Mao Y, Chen G (2005) Chaos-Based Image Encryption. In: Handbook of Geometric Computing. Springer Link, pp 231–265
28. Mehboob B, Faruqi RA (2008) A Steganography Implementation. IEEE -4244-2427-6/08/\$20.00 ©2008
29. Miller ML, Cox IJ, Linnartz JM, Kalker T (1997) A review of watermarking principles and practices. In: IEEE International Conference on image processing
30. Ming C, Zhang R, NiuXinxin YY (2006) Analysis of Current Steganography Tools: Classifications & Features. In: International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP'06), IEEE- 0-7695-2745-0/06 \$20.00 ©
31. Moerland T (n.d.) Steganography and Steganalysis. Leiden Institute of Advanced Computing Science, [www.liacs.nl/home/tmoerl/privtech.pdf](http://www.liacs.nl/home/tmoerl/privtech.pdf)
32. Musheer Ahmad M, Alam S (2009) A New Algorithm of Encryption and Decryption of Images Using Chaotic Mapping. *Int J Comput Sci Eng* 2(1)
33. Nassar SS, Ayad NM, Kelash HM, El-Sayed HS, El-Bendary MAM, El-Samie A, Fathi E, Faragallah OS (2016) Secure wireless image communication using LSB steganography and chaotic baker ciphering. *Wireless Personal Communications* 91 (3), 1023-1049
34. Nassar SS, Faragallah OS, El-Bendary MAM (2021) Reliable Mark-Embedded Algorithm for Verifying Archived/Encrypted Image Contents in Presence Different Attacks with FEC Utilizing Consideration. *Wireless Personal Communications* 119 (1), 37-61
35. Neeta D, KamalapurSnehal DJ (2004) Implementation of LSB steganography and its evaluation for various bits
36. Pareek NK, Patidar V, Sud KK (2006) Image encryption using chaotic logistic map. In: Sciencedirect, *Image and Vision Computing*
37. Patel R, Lad K, Patel M (2021) Study and investigation of video steganography over uncompressed and compressed domain: a comprehensive review. *Multimedia Systems*. <https://doi.org/10.1007/s00530-021-00763-z>
38. Petrovic R (2005) Digital Watermarks for Audio Integrity Verification, Serbia and Montenegro, Nis, September 2005 28–30
39. Radharani S, Valarmathi ML (2010) A study of watermarking scheme for image authentication. *Int J Comput Appl* 2(4):24–32
40. Rudko CS (2002) Hidden bits: a survey of techniques for digital watermarking. Independent StudyEER-290 Prof Rudko, Spring 2002
41. Sharma N, Anand A, Singh AK (2021) Bio-signal data sharing security through watermarking: a technical survey. *Computing*. <https://doi.org/10.1007/s00607-020-00881-y>
42. Srividya G, Nandakumar P (2011) A Triple-Key chaotic image encryption method. In: International Conference on Communications and Signal Processing (ICCSPP), pp 266–270
43. Tewfik AH (2000) Digital watermarking . San Mercury News, 14 August, 2000
44. Thirumarai Selvi C, Amudha J, Sudhakar R (2021) Medical image encryption and compression by adaptive sigma filtered zero certificateless signcryptive Levenshtein entropy-coding-based deep neural learning. *Multimedia Systems*. <https://doi.org/10.1007/s00530-021-00764-y>
45. Wu CW, Rul Kov NF (1993) Studying Chaos via 1-D Maps. *IEEE Transactions on Circuits and Systems: Fundamental Theory and Applications* 40(10)
46. Wu Y, Yang G, Jin H, Noonan JP (2012) Image encryption using the two-dimensional logistic chaotic map. *Journal of Electronic Imaging*
47. Zhou S, Wang X, Zhang Y, Ge B, Wang M, Gao S (2021) A novel image encryption cryptosystem based on true random numbers and chaotic systems. *Multimedia Systems*. <https://doi.org/10.1007/s00530-021-00803-8>
48. Nassar SS, Ayad NM, Kelash HM, El-Sayed HS, El-Bendary MAM, El-Samie A, Fathi E, Faragallah OS (2015) Content verification of encrypted images transmitted over wireless AWGN channels. *Wireless Personal Communications* 88 (3), 479-491



**Sabry S. Nassar** received the B.Sc. (Honors), M.Sc., and Ph.D. from the Faculty of Electronic Engineering, Menoufia University, Menouf, Egypt, in 2002, 2011, and 2016, respectively. He is currently working as Lecturer and Cyber Security Specialist for Nuclear Research Center (NRC), Inshas, Egypt. His current research interests include; cyber security of instrumentation and control, data hiding techniques, encryption techniques, data forensics, and network security.



**Mohsen A. M. El-Bendary** BSc. in Electrical Communications, Faculty of Electronic Engineering, Menoufia University, May 1998. MSc. in Communications Engineering from Faculty of Electronic Engineering, Menoufia University, 2008. PhD. in Communications Engineering, Faculty of Electronic Engineering, Menoufia University, 2012. Wireless networks, specially, the wireless personal communications such as WPANs, WSN, and WBANs. Image Processing: Enhancement of restoration of degraded and noisy images, multi-channel image processing, error of image concealment, color image processing, image watermarking, encryption, and data hiding) as well as Computational complexity of Communications systems. Implementation the different security systems such as Fire Alarm and Access control also HVAC system using the wireless technologies. 18 years' experience, Design details, installation and installation supervision, testing and commissioning, and programming for the light current systems.