International Journal of Engineering & Technology, 7 (4) (2018) 2758-2764

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.15691
Research paper

Secure image transmission over wireless network

Salah A. Aliesawi [1] *, Dena S. Alani [1], Abdullah M. Awad [1]

[1] *Department of Computer Science, College of Computer Science and Information Technology, University of Anbar, Iraq*
**Corresponding author E-mail: salaheng1996@gmail.com*

Abstract

The advances recently seen in data compression, and communication systems, have made it viable to design wireless image transmission systems. For many applications such as confidential transmission, military and medical applications, data encryption techniques should be also used to protect the confidential data from intruders. For these applications, both encryption and compression need to be performed to transmit a message in a fast and secure way. Further, the wireless channels have fluctuating channel qualities and high bit error rates. In this paper, a new scheme based on encryption and channel coding has been proposed for secure image transmission over wireless channels. In the proposed scheme, the encryption process is based on keys generator and Chaotic Henon map. Turbo codes are utilized as channel coding to deal effectively with the channel errors, multipath signal propagation and delay spread. Simulation results show that the proposed system achieves a high level of robustness against wide different of attacks and channel impairments. Further, it improves image quality with acceptable data rates.

Keywords: *Chaotic Henon Map; Turbo Code; Image Transmission; Image Compression.*

1. Introduction

The rapid development of computer networks and technology of the internet made information security an essential issue. Recently, wireless systems have become the prevailing means of communication [1]. Image transmission through wireless network is becoming more and more popular. But, the wireless communication medium is of limited bandwidth, open to intruders and noisy. So, an additional level of data security is required to make the wireless network reliable and secure [2]. People in their life need to save confidential their family albums, private documents, and films. Also, digital images are the engaging data type that is used in a wide range. So the security of images has become more and more important due to the fast development of the Internet [3]. Images are transmitted over the web for different usages like satellite images, military, database medical imaging systems, banking, broadcasting, confidential enterprise archives, and services, etc. [4]. But the constraints on bandwidth, time in several systems of the image communication, and unauthorized access, prohibit transmission the raw image data [5]. The digital transmitted image over the network can be tampered, intercepted and destroyed illegally by the attackers, so the images must be encrypted before transmitted to resist the hackers and attackers [6]. Cryptography is one of the most necessary requirements for every type of data transmitted through the wireless medium, it is the mechanism that protects data from the third-party intervention and converts it non-understandable form [7]. Due to some actual properties of the digital image such as the high correlation between picture elements (pixels) and huge data volume, the classical algorithms of cryptography such as RC4, AES, DES ...etc., it is not enough to encrypt image and convert it to a non-understandable form [8]. Modern cryptography has used chaos system, which it has many excellent advantages. It is very sensitive to a small change in initial value, pseudo-randomness, easy to execute, faster speed for encryption process, stronger against attacks [9]. However, the compressed image and encrypted image, is very sensitive to the bit errors, which can degrade the quality of the transmitted image. In the systems of digital image transmission, to improve the quality of image at the receiver side; channel coding is utilized [10].

In [2], the researchers implemented a system combine chaotic encryption and turbo coding into one processing step. In this system, the algorithm of data encryption is based on Chaotic Logistic Map. Further, the technique of error correction based on turbo coding is utilized as channel coding in order to solve the issue of limited bandwidth for channel and throughput. The results of testing show that Number Pixel Change Ratio (NPCR) is 99.44 and Unified Averaged Changed Intensity (UACI) is 31.47%, this proves that the proposed algorithm was security but it never treated the huge size of the image using the image compression to decrease the size of the transmitted image and the time of transmission. Also, Chaotic Logistic Map CLM was employed, by generating one byte for each operation, so the process of producing the keys had required a time. External private key for encryption the chaotic image have presented in [11]. The algorithm of image encryption was based on 80-bits & [2] chaotic logistic maps. The external secret key utilizes for providing various weight to its bits to generate initial conditions for two (CLM). The first CLM map is used to generate the numbers in the ranging from (1-24). The initial condition of the second CLM is modified using the numbers that produce by the first CLM. Also in this system, the process of producing the keys had required a time. In [12], discussed several aspects and proposed the improvement ways to joint source-channel coding for image data transmission over noisy channels. Efficient simple hybrid lossy image compression system is proposed, it is based on using Discrete Wavelet Transform (DWT) to decompose the image into approximation and detail sub bands. In addition to the proposed system, an Orthogonal Frequency Division Multiplexing and Interleave Division Multiple Access (OFDM -IDMA) system with joint source-channel coding [12-13] is used to transmit the compressed images/videos for multiuser over wireless multipath channels. However, the researcher did not address the security aspect of the image.

In this paper robust and secure image transmission system was proposed. The rest of the paper is organized as follows: Section 2 presents the general proposed system models. Section 3 presents simulation results and discussion. Finally, conclusions are drawn in Section 4.

2. The general proposed system

Figure 1 shows the proposed general system model. It consists of three main processes: image compression, encryption then the transmission. In this system, a joint source-channel coding is implemented for secure image transmission over wireless channels. An image file is utilized as a data source. The first stage represents the image compression. In this stage, the huge data size of the image is reduced converted from a 2-D matrix to 1 D matrix. In the second stage, Sha1 function and encryption processes are applied then the output of encryption process (E) and Sha1 function (H) are linked to generate one dimension (E-H) array. In the third stage, Turbo code is applied to the binary data (E-H) then the modulation is performed. Then, the modulated data is transmitted over wireless channel. Therefore, the noise distorts the image and added to the data when it is passed through the channel. Demodulation of the image is performed at the receiver end. After demodulation, Turbo decoding is performed, and then the spilt process is done.

The decryption process is done, and after that Hash function is applied and matching with Hash code of the transmitted image. Finally, the decompression process is implemented, and then the transmitted image is retrieved.

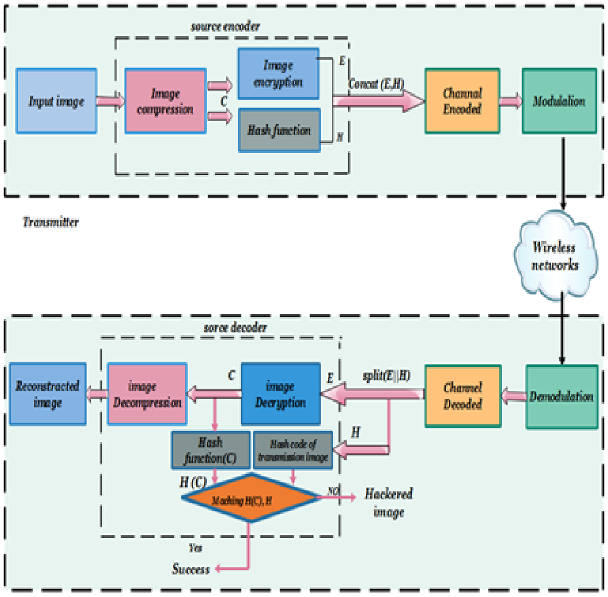


Fig. 1: The General Proposed System.

2.1. The proposed image compression & decompression techniques

The structure of the method includes two parts: the first part represents the image compression method, while the second part represents the image decompression method. In the image compression technique, the image is converted from RGB color space to YCbCr, and then each layer of (Y, Cb, and Cr) is converted from spatial domain to frequency domain utilizing DCT transformation. Quantization process is then used to lower the high frequencies, which represent less important information. The values of each layer are split with values of specific quantization table to get to lower values, which could be zeros. Then, the zigzag scan technique is utilized to convert the 2-D array to 1-D array to become more convenient and flexible to the next process that represents Run-length coding. This process works to remove the redundancy and the disposal of sequential zeros. The final process is the shift coding. This technique is used to decrease the number of bits required to represent the data after RLE. In the decompression technique, the processes are perfectly the reverse for the processes of the compression (begins from the down to top) as shown in the Figure 2b. So the first process in the decompression scheme will be the inverse shift coding then Inverse-RLE, Inverse-Zigzag, Inverse-DCT,... and ending with converting back YCbCr to RGB. Figures 2a and 2b illustrate the processes of the image compression and decompression, respectively.

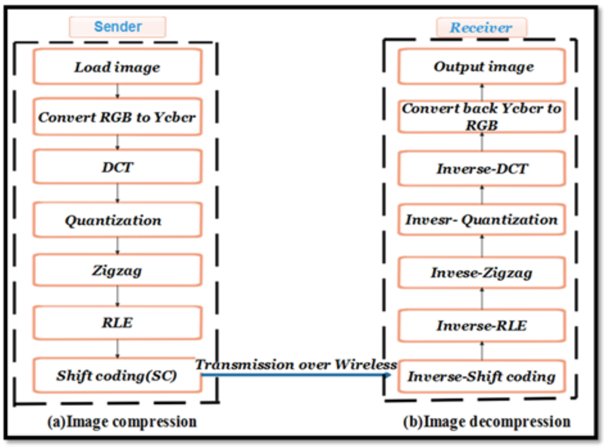


Fig. 2: A) Proposed Image Compression & B) Decompression.

2.3. The proposed image encryption model

The proposed image encryption model combines the generator with chaotic Henon Map to generate N blocks of the sub keys so that each produced key is used to encrypt one block of the compressed image. The length of the block of the keys is 256 bytes. Figure 3 shows the structure of the model. It consists of two processes generator and chaotic Henon map. Each generator has two input, the first generator has an initial S[256], which represents a vector contains the value from 0 to 255 and secret key that is input from the user to encryption and decryption. Also, the other generators have two inputs, a produced key 256 bytes from the previous generator and Chaotic key that is produced from previous Henon. Figure 3 explains the general structure of the processes of first proposed encryption model.

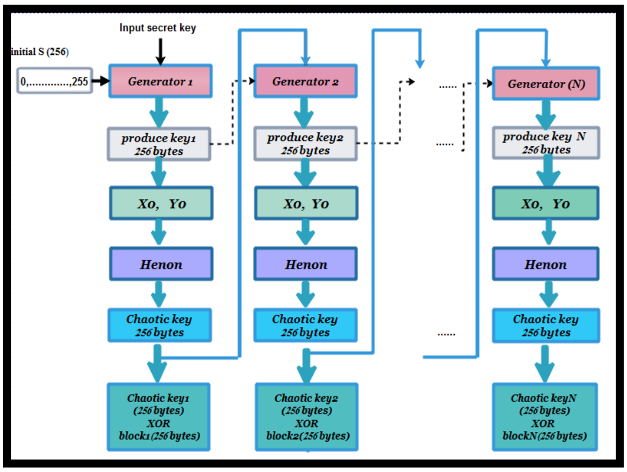


Fig. 3: The Proposed Scheme for Image Encryption.

The proposed model includes:

- The N of round is equal to the N of blocks of the compressed image.
- The N of Chaotic keys is equal to the N of blocks of compressed image.

- The length of each block of the compressed image is 256 bytes.
- The length of each generated key is 256 bytes.
- The type of encryption in this model is stream cipher, but the process of keys generation is block.
- The encryption process is XOR

The image on the computer represents a two-dimensional matrix. After the compression process, the image is converted into a one-dimensional matrix, then the compressed image is divided into blocks, the length of each block is 256 bytes. The proposed image encryption model consists of three main processes as shown in Figure 3.

- Key generator.
- Generation chaotic Henon.
- XOR_ed Chaotic key and a block of image

1) Key generator is similar to KSA of RC4, but the produced key of the generator returns as input to the generator again. The Key generator has two inputs: S[256], which represents a vector containing the values from 0 to 255 and so that state [0] = 0 and state [255] = 255, and secret key K, which is input from the user, locations of the S are permutated according to the value of the secret key. The operation that is used in the generator is the swap, so that, S[i] is swapped with another location in the state according to the value of location K[i]. The produced key has two uses: as feedback (as input) to the generator of keys in the next round, and as input for Chaotic Henon Map. To increase randomness and strength of the key against attack, Henon Map is used.
2) Generation of Chaotic Henon: Converting the produced key from the generator to the initial value for X_0, Y_0 for Henon map, the length of the produced key is 256 bytes. The process divides the produced key into two parts so that X_0 takes the values from 0 to 127, and Y_0 takes the values from 128 to 255. The values of X_0, Y_0, which are obtained from the key are converted from integer numbers to real numbers then, apply X_0 and Y_0 on following equations to calculate X_n, Y_n

$$X_{n+1} = 1 - 1.4\, x_n + y_n \quad (1)$$

$$Y_{n+1} = 0.3 y_n \quad (2)$$

After that, ″X_n"and "Y_n" will act as "X_0", and "Y_0" to calculate $X_{n+1}$and Y_{n+1} so on, X_n obtained from Henon equation represents one byte, also Y_n represents one byte. So to generate vector chaotic key of length 256 byte from Henon map involves loop from 0 to 255, loop increasing 2 every time. After x_n value and Y_n value are obtained from Henon equations, these values will be converted back into integer number. X_n, Y_n will be multiplied with 100 000 and then the result will be modulus with 255 and taken the absolute value of the result, final result of $X_n$will be stored in array chaotic key [i] and Y_n will be stored in chaotic key [i+1], where I =0, 1 ...255 . This process will be repeated until the chaotic key [255] is filled.

3) Chaotic key1 [256] bytes XOR_ed with block1 of the compressed image [256] bytes. The previous steps are repeated for an N of rounds so that the N equals to the number for blocks of compressed image.

The Steps of the first proposed encryption Algorithm can be summarized as:
Step 1: Input compressed image and secret key (K).
Step 2: Use secret key K and S [256] as inputs to the Generator.
Step 3: Generate the produced key [256] bytes from Generator.
Step 4: The produced key is feedback to the Generator, and also use the produced key as input to Chaotic Henon Map (CHM).
Step 5: Use the produced key to create initial value X_0 and Y_0 for Eq. (1), (2).
Step 6: Apply Eq. (1), (2) of Chaotic Henon Map (CHM) by using X_0 and Y_0 to produce a chaotic key, length of key 256 bytes.
Step 7: XOR_ed first chaotic key [256] bytes with first block of compressed image.
Step 8: First Chaotic key [256] bytes is feedback to Generator.
Step 9: Go to step 3.
Step 10: Repeat the previous steps for N of rounds, until N > number for blocks of the compressed image then stop. Figure 4 represents the image encryption scheme in detail.

Decryption method

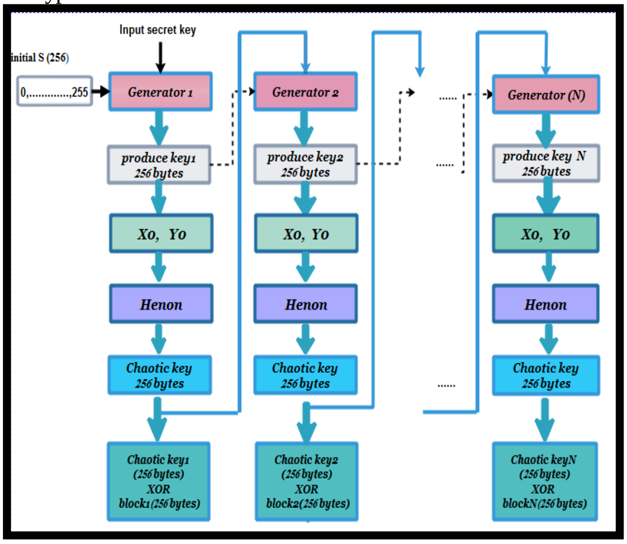


Fig. 4: Image Encryption Flowchart.

In the decryption process, the same key that was entered by the user in the encryption process is used in the decryption process to generate the key (256) bytes to decrypt the first block (256) bytes of the encrypted image. The first generated key is used as an input to the system again to generate the key to decrypt the second block of the image and so on until generating an N of the decryption keys that are equal to the N of encrypted image blocks to get the plain image.

2.3. The proposed joint source-channel coding system

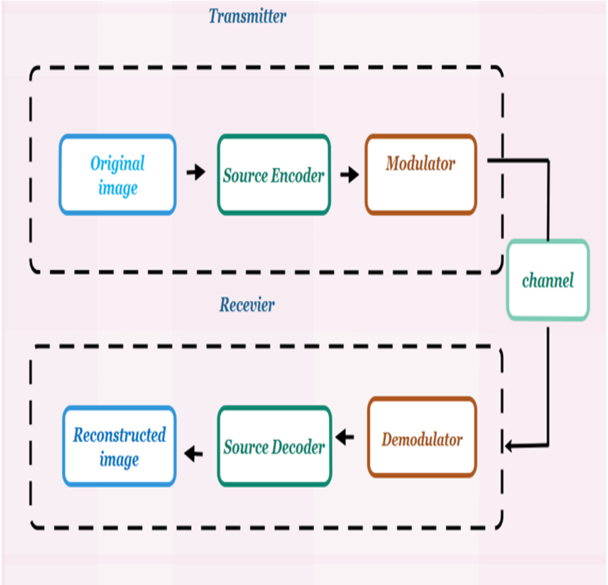
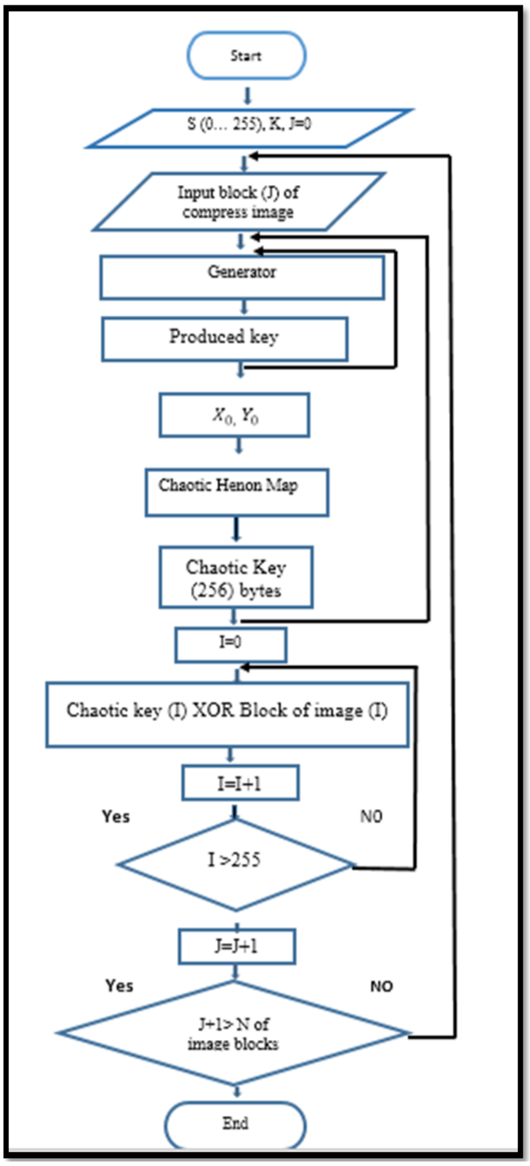


Fig. 5: The System Transmission for Single User without Channel Coding.

The proposed system of transmission in Figure 5 includes the transmitter, wireless channel and receiver. The transmitter consists of source encoder, channel encoder and modulation. The receiver includes source decoding, channel decoder and demodulation. In the proposed system, the transmitter and receiver use the simplest transmitter types of modulation Binary Phase Shift Keying (BPSK) with wireless channels.



This section concentrates on the transmission of the encoded image over the channels of the wireless noisy system. The proposed system of transmission consists of source encoder (image compression& encryption), channel coding using Turbo coding, and modulation. This represents the side of the transmitter, while the side of the receiver consists of demodulation, channel decoding using SISO and source decoder, as shown in figure 6.

In the transmitted side, the huge data size of the image is reduced using an image compression process as explained in section (2. A). the image is converted from 2-D matrix to 1-D matrix, then one dimension matrix is encrypted using Algorithm mention in section (2.B). The image compression & encryption represent the encoding image stage. The next stage is Turbo encoder. It is the best type of error correction code. Its main idea is to use two convolutions identical simple codes and one interleaver. The aim of interleaver is to permutate the locations of the input bits without changing its values before inputting to the 2nd convolution encoder. In Turbo code, the stream of the bits passes to enoder1(Upper) and also to encoder 2 (Lower) but in different order as data passes to interleaver, which works to permutate the position of input bits without changing its values. After the encoding process, the outputs of the upper and lower encoder pass to puncturing technique. In this technique, some of the parity bits are omitted from the transmitting bits for generating code words of different code rates. Finally, modulate code word from digital form to analogue and transmitted through wireless channel.

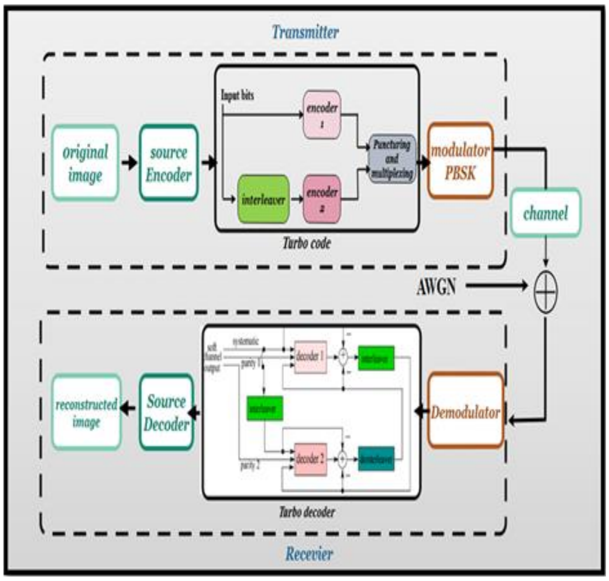


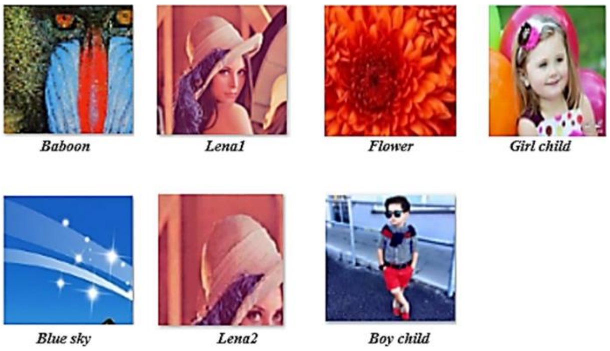
Fig. 6: Transmission System with Turbo Channel Coding.

In the side of receiver, the received signal from the transmitter is converted back to its original from analogue to digit form, by a modulation process, then moved to channel decoding stage. The encoded information bits are moved to Turbo decoder, which consists of two decoders (SISO). They work to decode the system code information and check code information, which is produced by the encoder to be then decoded. The upper SISO decoder produces the soft output and subsequently an extrinsic information (EI) is produced. The extrinsic information is interleaved and utilized by the lower SISO decoder as the estimate of the a priori probability (APP), and then the lower SISO decoder also generates the extrinsic information. The de-interleaving passes it to the upper SISO decoder to be used during the subsequent decoding operation. After many iterations, the outside information produced by the 2 SISO DEC (soft-input soft-output decoder) and the likelihood information LLR become consistent Information. After being de-interleaved, the LLR is sent into the hard decision. The decision of LLR is less than the zero and in the other cases is 1. However, the decoding process in figure 6 involves two SISO iterations to complement the decoded process. It means that each SISO is only responsible for half of the iterations and it complets the whole. The final stage is Source decoder which was explained previous in details in section (A) and (B), which is followed by the process of calculating the transmitted image and Bit BER.

3. Simulation results and discussion

3.1. Results of image compression algorithm

Image compression algorithm was applied on 7 images as shown in Figure 7. Type of used images is BMP with different sizes on PC computer with VB language and operating system is windows 7.


Baboon *Lena1* *Flower* *Girl child*

Blue sky *Lena2* *Boy child*

Fig. 7: Samples of Tested Images.

Table 1 shows the results of CR, PSNR. The compression algorithm compared with standard JPEG and the results are shown in Table 2. The results show that the proposed compression algorithm is best and faster than JPEG standard.

Table 1: Results of CR & PSNR

NO	Size of tested images in KB	CR	PSNR
1	Baboon 44.3	1:9.57	31.68
2	Lenna1 192	1:15.93	35.88
3	Girl child 28.8	1:12.01	34.02
4	Flower 19.6	1:20.11	38.54
5	Lenna2 34.6	1:17.15	40.78
6	Boy child 51.8	1:11.49	31.47
7	Blue sky 5.41	1: 16.86	36.60

Table 2: Results of JPEG & the Proposed Compression Method

No	Size of tested images in (KB)	Standard JPEG		The proposed image compression Method	
		CR	Comp/ time (Sec)	CR	Comp/ time (Sec)
1	Baboon	1:4.68	1.1094087	1:9.57	0.0072622
2	Lenna1	1:7.40	1.1153255	1:15.93	0.0055367
3	Girl child	1:6.63	0.4390390	1:12.01	0.0026940
4	Flower	1:9.19	1.1119780	1:20.11	0.0053973
5	Lenna2	1:7.81	1.7548918	1:17.15	0.0085804
6	Boy child	1:6.38	1.7372300	1:11.49	0.0090042
7	Blue sky	1:9.59	0.2775552	1:16.86	0.0010988

3.2. Results of image encryption algorithm

1) Key space analysis

Key space is meaning the total number of various keys that can be utilized in the encryption process. The good Attributes for encryption algorithm are sensitive to the secret key which has to be large enough to resist attacks. In the proposed algorithm, the length of the generated key is 256 byte, so key space is large enough to impedance the various attacks [18].

2) Sensitivity analysis

Robust encryption system must be sensitive to the original image and key, so we test the sensitivity to key using encrypted image which is obtained by the key that is little various from the original in one bit. Two measurements are used to test sensitivity of the key: NPCR and UACI, [19]

NPCR: is checking the no.of the pixels which is different between encrypted images E1, E2. NPCR that is the shortcut to the number of pixels changes rate and is defined in the following form:

$$NPCR\,(E1, E2) = \Sigma D\,(i,j)\,ij Z \times 100\,\% \quad (3)$$

Where

$Dij=\{0\ ,\ if\ E1(i,j)=E2(i,j)\ 1\ ,\ if\ E2\ (i,j)\neq E2(i,j)\ Z=W\times H$

UACI: is used to calculate the average intensity of variation between encrypted image and original image

UACI is defined by equation (4)

$$UACI = \ 1Z\left[\Sigma|E1\,(i,j) - E2\,(i,j)\,|255ij\right] \times 100 \quad (4)$$

So that, E1, E2 is representing [2] encrypted images for the same original image, which has single modified pixel.

Key sensitivity

In the proposed encryption model, [5] samples of color images with different sizes were used to encrypt by using a key, and then the same samples of the images were encrypted with a little difference in the key. The results of NPCR and UACI for encrypted images with changing one character in key are shown in table 3.

Table 3: NPCR & UACI for Encrypted Images with Changing One Character in the Key

Tested images	NPCR	UACI
Lena1	99.602885160872	33.4501000335299
Baboon	99.581223217763	33.6371517831909
Lena2	99.611292962356	33.7468710888611
Child boy	99.561850802644	33.5840915402988
Blue sky	99.759862778730	34.1348669828137

The differential attack resistances (NPCR & UACI) are calculated in the table (3). The NPCR calculates the percentage of the different pixel numbers between the 2 images. The images are encrypted and tested twice, once with a key and the second with changing one character in the same key to show the effect of difference one bit in the secret key on the images. The optimum value for NPCR is 100% if all values are changing when changing one bit from the encryption key. All values of NPCR are proximate to optimal value this indicates the efficiency of the proposed model and the values of UACI are different from an image to another, depending on the density of colors.

3) The entropy

The most important attribute for randomness is the entropy, which is calculated according to Eq. 5:

$$H(s) = \sum_{i=0}^{2N-1} P(s_i) log_2\ \frac{1}{p(si)} \quad (5)$$

For a correct random when the source is represented by 2^n symbols, the entropy H(s) must be n, or near to (n). In gray image, the pixel can take 2^n possible to represent data. So the entropy for a correct random must be 8 or closer to 8. Entropy values for the encrypted images are ordered in Table 4. The resulting values are much near to 8. That proves encryption model is secured versus the attackers. The proposed algorithm is compared with another two algorithms suggested in [21] and the results of the comparison were arranged in Table 5. The results prove that the proposed model is best.

Table 4: Results of Entropy for Encrypted Images

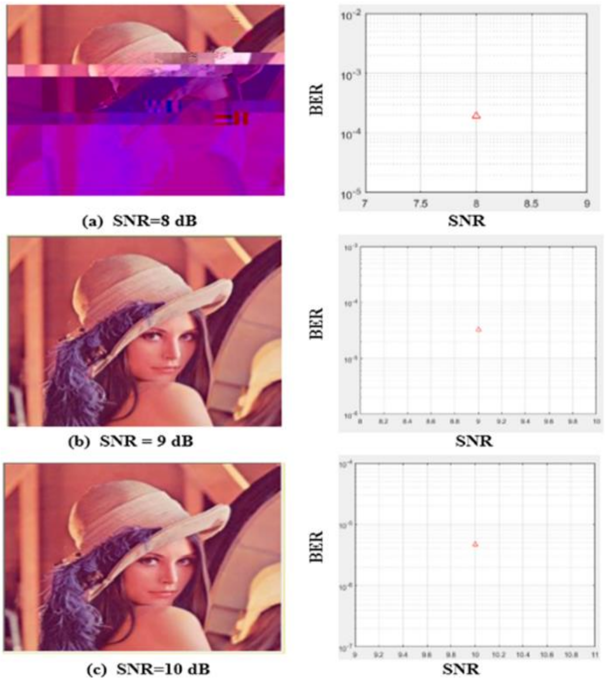
Tested images	Entropy_ Original Images	Entropy_ Encrypted Images
Lena1	7.73009821405738	7.982605323534
Baboon	7.83627286941329	7.990305823303
Lena2	7.6111719576919	7.980036896786
Child boy	7.9280384211795	7.993526832880
Blue sky	7.29599011819604	7.933965018241

Table 5: Entropy Values for the Encrypted Image of "Lena1"

Algorithms	Entropy values
Baptista's	7.926
Wong's	7.969
The proposed algorithm	7.982

3.3. Performance evaluation over wireless channels

The performance analysis of encoded image transmission through wireless channels with and without turbo coding is described in Figures 8 & 9.

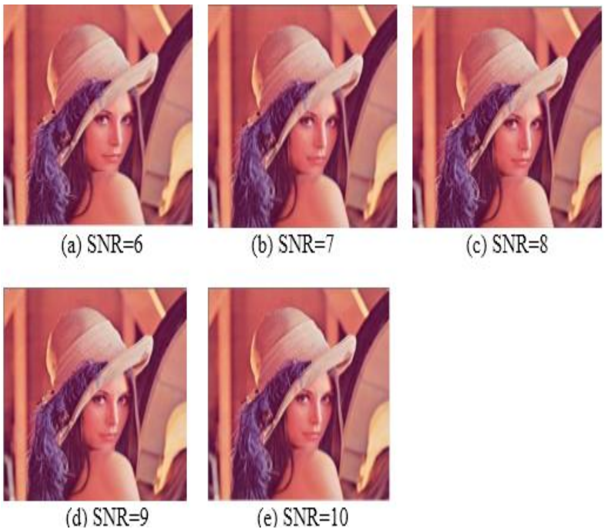


(a) SNR=8 dB

(b) SNR = 9 dB

(c) SNR=10 dB

Fig. 8: The Received Lena1 Images at Different SNR Values after Transmitting over Wireless Channel.



(a) SNR=6 (b) SNR=7 (c) SNR=8

(d) SNR=9 (e) SNR=10

Fig. 9: The Received Lena1 Images at Different SNR Values after Transmitting over Wireless Channel with Turbo Coding.

From Figure 9, it will be observed that when the channel was encrypted using Turbo codes, Lena1 images are reconstructed clearly, without distortion and without the needed for additional retransmission. Lena1 image is reconstructed clearly and efficiency with SNR values equal 6 with Turbo channel coded, while without channel coded the same image is reconstructed shattered and distorted with SNR value equal to [8]. Therefore, Turbo codes increases the throughput of the system that is defined as the useful transmission rate in bits/second accounting for the loss due to channel errors and enhances the performance of the system.

The performance of coded system is compared with the respective uncoded system under the same channel. The figures 10-12 shows the comparison between BER performance for transmitting the compressed and encrypted images over wireless channel with and without using Turbo coding for the images (Lena1, Blue sky and Girl child) respectively. The turbo code is utilized as channel coding for data communication during the wireless channel. It works to decrease BER by correct the errors that happen during the process transmission. The comparison between the 2 models explains that the quality of transmitted data during the model of transmission without Turbo code is lowest from transmission of the encoding channel due to that the second model works to detect and correct the mistakes and hence obtain a rate of mistake less than the first model.

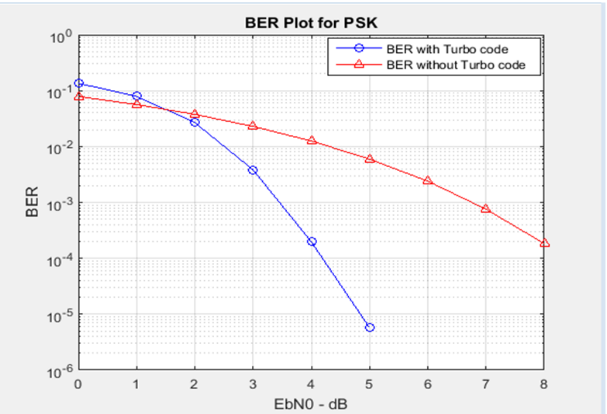


Fig. 10: BER Comparison after Lena1image Transmitting over Wireless Channel.

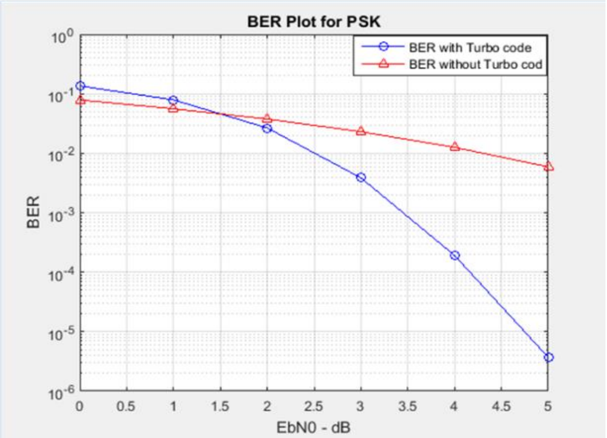


Fig. 11: BER Comparison after Blue Sky Image Transmitting over Wireless Channel.

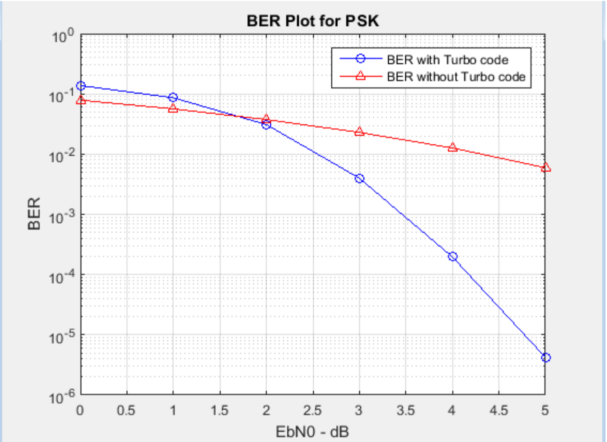


Fig. 12: BER Comparison Performance after Girl Child Image Transmitting over Wireless Channel.

4. Conclusions

This paper presents a robust and reliable scheme for transmitting the compressed and encrypted image over noisy wireless channels. In many such practical systems; jointly source and channel coding are used to enhance the system performance significantly. The source coding decreases the redundancy of the data, which exists in the image to overcome the limited transmission bandwidth problem, protect data from the third-party and convert it to non-understandable form. The channel coding adds useful redundancy to combat channel errors. The research briefly discusses the method of transmitting the encoded image over the uncoded channel, in addition to transmitting it through the encoded channel utilizing turbo coding. The results have also shown that the encoded image is more liable to channel errors; the image quality and BER value are inversely related to the SNR values. Thus, channel coding is utilized with encoded image to minimize the influence of channel errors, and the performance is improved in contrast to uncoded systems.

References

[1] Hammond, M. M., Yoshiro, K., & Sigher, A. M. (2013). RC4 stream cipher with a random initial state. In *Information Technology Convergence* (pp. 407-415). Springer, Dordrecht. https://doi.org/10.1007/978-94-007-6996-0_42.

[2] El-Iskandarani, M. A., Darwish, S. M., & Abuguba, S. M. (2010). Combination of 2D chaotic encryption and turbo coding for secure image transmission. *IJCSNS*, *10* (11), 179.

[3] Sagheer, A. M., & Abed, L. H. (2015). Visual secret sharing without pixel expansion. *International Journal of Digital Crime and Forensics (IJDCF)*, *7*(2), 20-30. https://doi.org/10.4018/IJDCF.2015040102.

[4] Pande, A. P., & Thakur, N. V. (2018). A Survey on Different Ways of Secure Image Transmission.

[5] Ramasamy, K., Siddiqi, M. U., & Alias, M. Y. (2006). Performance of JPEG image transmission using proposed asymmetric turbo code. *EURASIP Journal on Advances in Signal Processing*, *2007*(1), 075757. https://doi.org/10.1155/2007/75757.

[6] Setyaningsih, E., & Wardoyo, R. (2017). Review of image compression and encryption techniques. *International Journal of Advanced Computer Science and Applications*, *8* (2). https://doi.org/10.14569/IJACSA.2017.080212.

[7] Mohamed, M. A., Zaki, F. W., & El-Mohandes, A. M. (2013). Improved mobile WiMAX image privacy using novel encryption techniques. *International Journal of Computer Science Issues (IJCSI)*, *10* (Part 2), 488.

[8] Hammood, M. M., Yoshigoe, K., & Sagheer, A. M. (2013). RC4-2S: RC4 stream cipher with two state tables. In *Information Technology Convergence* (pp. 13-20). Springer, Dordrecht. https://doi.org/10.1007/978-94-007-6996-0_2.

[9] Jiang, Y., & Li, B. (2016, December). A novel image encryption algorithm based on logistic and henon map. In *Wavelet Active Media Technology and Information Processing (ICCWAMTIP), 2016 13th* IEEE *International Computer Conference* (pp. 66-69).

[10] Mishra, A., Sharma, K., & De, A. (2014). Quality image transmission through AWGN channel using polar codes. *International Journal of Computer Science and Telecommunications*, *5*(1).

[11] Kadir, R., Shahril, R., & Maarof, M. A. (2010, May). A modified image encryption scheme based on 2D chaotic map. In *Computer and Communication Engineering (ICCCE), 2010 International* IEEE *Conference* (pp. 1-5).

[12] Aliesawi, S. A., & Rajab, M. A. (2015). Joint Source-Channel Coding for Wireless Image Transmission based OFDM-IDMA Systems. *Iraqi Journal of Science*, *56* (2A), 1185-1197.

[13] Aliesawi, S. A., Mustafa, S. S., & GATHBAN, S. A. (2017). Motion estimation and convolutional coding for video streaming over wireless channels. *Journal of Theoretical & Applied Information Technology*, *95* (22).