

Combination of 2D chaotic Encryption and Turbo Coding for Secure Image Transmission

M. A. El-Iskandarani, Saad M. Darwish, Saad M. Abuguba

Institute of Graduate Studies and Research University of Alexandria Egypt

Summary

Robust and secure transmission strategy for high-quality image through wireless networks is considered a great challenge. However, majority of encrypted image transmission schemes do not consider well the effect of bit errors occurring during transmission and this issue is considered a problem that should be handled by an efficient coding scheme. In this paper, a modified wireless image transmission scheme that combines chaotic encryption and turbo coding technique into one processing step is proposed. In the proposed scheme, selective encryption algorithm based on two-dimensional chaotic map is utilized for data security. Furthermore, error correction technique based on turbo coding is employed as channel coding for data communication in order to solve the problem of channel's limited bandwidth and throughput. Simulation results show that the proposed scheme achieves high degree of robustness against channel impairments and wide varieties of attacks. In addition, it improves image quality with acceptable data rates.

Keyword

Error correction code, Image transmission, DWT, Image encryption

1. Introduction

The wireless communication medium, as opposed to the wired counterparts, is noisy and open to intruders. Hence, additional level of error protection and security is required to make the wireless network as reliable and secure as the wired network. The issue of using cryptographically secure ciphers in wireless noisy channel is that the very same property that gives ciphers their cryptographic strength makes them sensitive to channel errors. This sensitivity causes retransmissions thus reducing the overall throughput.

To improve the throughput in noisy environments, channel coding is performed after encryption. Unfortunately, performing both encryption and coding separately can potentially prove to be too computationally intensive for many wireless end devices (e.g., personal data assistants (PDA), mobile phones). In fact, as both encryption and coding can be performed at the link layer, a single operation which does both encryption and error correction would be preferable [1,2]. Error control codes (ECC) are

important issue in wireless transmission, and are used to protect data from channel errors. ECC codes work by adding redundancy to data transmission to retrieve the data in the receiver side. In the literature, ECC can be classified into two categories: convolutional codes and linear block codes [3]. Convolutional codes process the information on a bit-by-bit basis and this is used in stream cipher [4]. Linear codes process the information on a block-by-block basis and this is used in block cipher, i.e. linear code operates on a fixed block length of data at a time. The main weakness of linear block code is that a single bit flip in the encrypted data can cause a complete decryption failure. This sensitivity causes retransmissions thus dropping the overall throughput (avalanche effect) [2].

Generally, the encryption can be applied in special domain or in frequency domain. Spatial domain schemes are mainly related to the position of the pixels in the image. Encryption in spatial domain does not satisfy the security application because they cannot survive most image processing attacks and geometric attacks [1]. In the other hand, frequency domain schemes deal with the digital transformation of the image and therefore can resist the image processing attacks [5]. An example of frequency transform is wavelet transforms, which have several properties that make them good candidates. First, the approximation coefficients provide a good low-resolution estimate of the image, while minimizing aliasing artefacts resulting from the reduction in resolution. Second, the wavelet coefficients are localized, so a corruption of a coefficient through channel errors has only local effect on the image [6].

Traditionally, error correction and encryption in communication networks have been addressed independently such as in Refs.[7-8]. Several researchers have studied the trade-off between encryption and error correction by trying to combine these functionalities in one unit. For instance, Gligoroski et al. [9] proposed technique for joint error correction and encryption, this technique achieves both security and error correction but the decoding procedure is extremely complicated and cannot be used in a wireless environment because it needs more computation time. Another work of Cam et al. [10] that combine the advanced encryption standard (AES) and turbo coding into single processing step in order to reduce the processing time. However, the work of Asim et al. [11] compared between

AES and chaotic based encryption. Their results show that chaotic encryption scheme is less computationally intensive compared to AES, and provides the same level of security.

The main contribution of this paper is to build a secure and reliable image transmission scheme that combine turbo coding based on error correction code and 2D chaotic map based encryption functionality into one single step in order to reduce the overall processing cost. The advantages of our scheme are achieving better security by utilizing 2D chaotic map instead of 1D chaotic map used by [12] and improving the throughput of an image transmission system by using turbo coding. The systematic block diagram of the proposed scheme is shown in Figure 1, and the following subsections briefly outline each step.

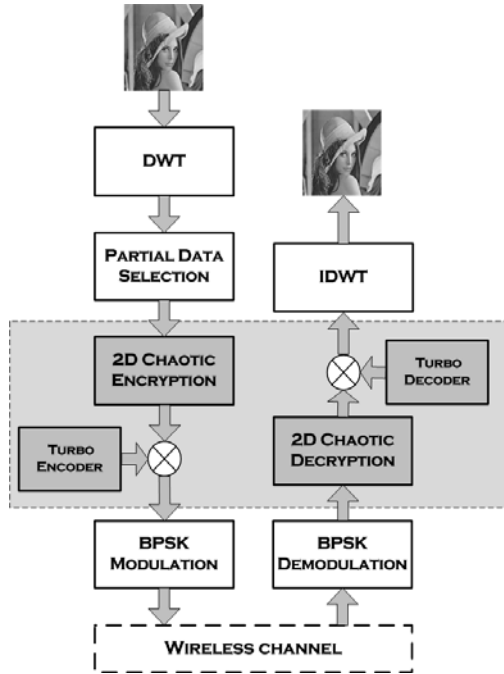


Figure 1. Block diagram of the proposed scheme.

The rest of this paper is organized as follows. Section II, describes the DWT data selection briefly. Section III, discusses the selective image encryption based on two dimensional chaotic maps. An efficient error correction scheme is presented in section IV. Section V discusses the combination of chaotic encryption and turbo coding. The simulation results are given in section VI and finally in Section VII, the conclusion.

2. Partial Data Selection of DWT

Discrete wavelet transform (DWT) is becoming popular in many image/video applications due to its multi-

resolution representation feature. The basic idea of the DWT for a 2D image is described as illustrated in Figure 2. With the pyramid-structured wavelet transform, the original image will encounter different combinations of a low-pass filter and a high-pass filter and then based on the convolution with these filters to generate the low-low (LL), low-high (LH), high-low (HL) and high-high (HH) sub-bands [13].

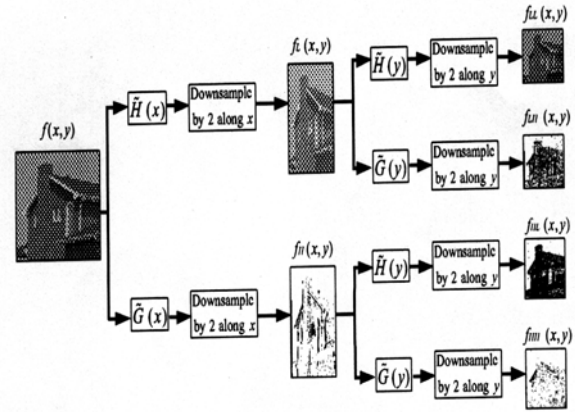


Figure 2. 2D forward wavelet transform

The most of the previous works for DWT [14,15] noticed that with only LL4, a large amount of image information can be extracted, but encrypting only LL4 may reveal higher frequency information such as edge components and it can be used to infer useful information. The experimental results of Seo et al. [14] showed that the encryption of all the sub-bands in level 4 and HH3 from level 3 give us the ability to reduce the computation time to implement the encryption and therefore preserve wireless energy. The proposed scheme utilizes the same technique in order to meet the requirement of computational time.

3. Cryptographic of Chaotic Map

This section discusses the methodical procedure of the proposed image encryption as well as decryption process using two chaotic logistic maps [12]. The basic logistic-map is formulated as:

$$X_{n+1} = \mu X_n (1 - X_n) \quad (1)$$

where μ represents the parameter of chaotic map. To satisfy the best encryption, i.e. chaotic sequence is unpredictable, μ must lies between $3.569 < \mu < 4.0$ [16]. Consequently the chaotic encryption and decryption provides guaranteed high security. The encryption using chaotic sequence produced by 1-D logistic system as depicted in Figure 3 is known to be weak in security, since it cannot resist known/chosen-

plaintext attacks. More information about the implementation of 1-D chaotic map can be found in [17,18].

In order to deal with the problem of the previous scheme, the proposed scheme utilizes 2-D chaotic logistic map as drawn in Figure 4. Mathematically, the 2-D chaotic map is defined as follows:

$$\begin{cases} x_{n+1} = 4\mu_1 x_n (1 - x_n) + \gamma y_n \\ y_{n+1} = 4\mu_2 y_n (1 - y_n) + \gamma x_n \end{cases} \quad (2)$$

where (x_n, y_n) represent image pixels, γ is simple coupled term and μ_1, μ_2 are control parameters of chaotic system. See [13] for further details.

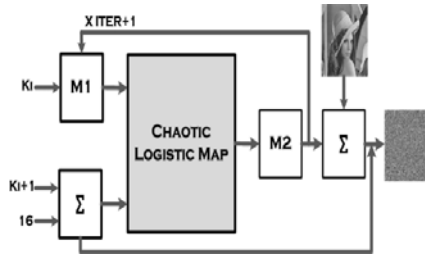


Figure 3: 1D Chaotic image encryption

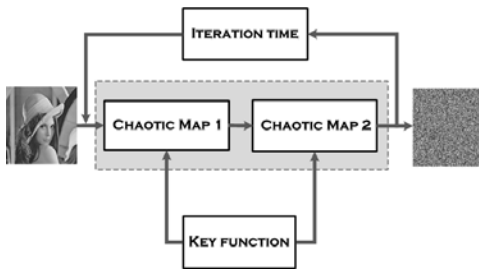


Figure 4: 2D chaotic image encryption

4. Turbo Channel Coding

Error corrective coding is used to enhance the efficiency and accuracy of transmitted information. In this work, turbo codes are used as channel coding for data communication over wireless channels with burst errors. Turbo-codes consist of particular concatenation of two recursive systematic codes linked together by non-uniform interleaving [14]. Formally, the redundancy information for turbo coder is computed as follows:

$$L(u_k) = \log \left[\frac{\sum_{u^+} P(s_{k-1} = s' \mu_k = 1, y_1^{k-1}, y_k, y_{k+1}^N) / P(y_1^N)}{\sum_{u^-} P(s_{k-1} = s' \mu_k = 0, y_1^{k-1}, y_k, y_{k+1}^N) / P(y_1^N)} \right] \quad (3)$$

where $\sum_{u^+}$ and $\sum_{u^-}$ are the summation over the entire possible transition branch pair (s_{k-1}, s_k) at time K given input $u_k = 1$, and input $u_k = 0$ respectively. At the receiver side, the following equation is used to estimate the lost information due to channel errors.

$$L(u_k) = \log \left(\frac{P(y_1^N / u_k = 1)}{P(y_1^N / u_k = 0)} \right) + \log \left(\frac{P(u_k = 1)}{P(u_k = 0)} \right) \quad (4)$$

For more details about turbo coding and decoding, readers can refer to [19].

5. Cryptcoding: Combination of 2-D Chaotic Encryption and Turbo Coding

Figure 5 shows the proposed combination between 2-D chaotic encryption and turbo coding, which is implemented in a synchronous way to improve both the security and throughput. The algorithm of the combination is as follows:

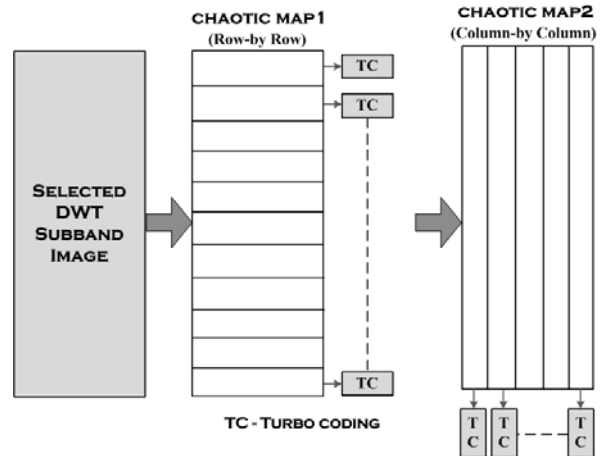


Figure 5: Combination of encryption and turbo coding

Algorithm 1 : at the sender side

1. **For each row (R) of the selected sub bands**
 $\text{Encr}(\text{Map1}, R) = E1$
// encryption step using chaotic map1.

```

T.coder (E1) =TC1
// encoding step using turbo coder in which
the cipher row is encoded

End for

2. For each column (C) of the TC1
Encr (Map2, C) = E2
// encryption step using chaotic map2.
T.coder (E2) =TC2
// encoding step using turbo coder in which
the cipher column is encoded

End for

```

Algorithm2 : at the reciever side

```

1. For each column (C) of the TC2
Decr (Map2, C) = D1
// decryption step using chaotic map2.
T.decoder (D1) =TD1
// decoding step using turbo decoder in which
the plain-image column is decoded

End for

2. For each row (R) of the TD1
Decr (Map1, R) = D2
// decryption step using chaotic map1.
T.decoder (D2) =TD2
// decoding step using turbo decoder in which
the
Plain-image row is decoded

End for

```

6. Simulation Results

6.1 Key Space Analysis

Key space size is the total number of different keys that can be used in the encryption. For a secure image encryption, the key space should be large enough to make brute force attacks infeasible [20]. The proposed cipher has different combinations of large set of parameters (keys). An image cipher with such a long key space is sufficient for reliable practical use. Figure 6 clearly shows that the decryption with a slightly different key fails completely and hence the proposed

encryption procedure is highly key sensitive and large enough to resist brute force attack.

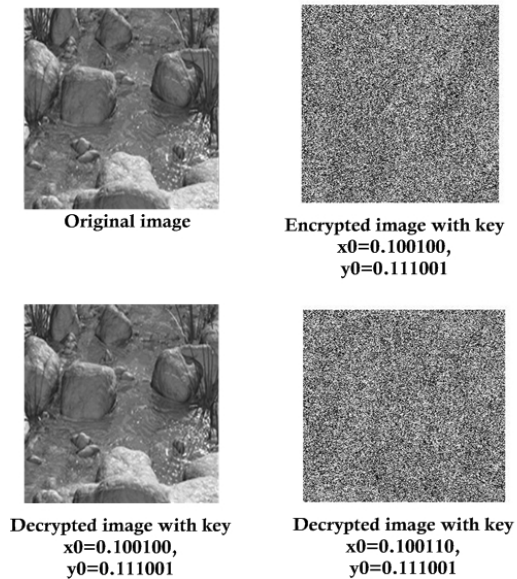


Figure 6: Key space analysis

6.2 Statistical Analysis

It is well known that many ciphers have been successfully analyzed with the help of statistical analysis and several statistical attacks have been devised on them. Therefore, an ideal cipher should be robust against any statistical attack. To prove the robustness of the proposed cipher, we have performed statistical analysis by calculating the histograms as well as the correlations of two adjacent pixels in the plain-image/cipher-image.

6.2.1 Histogram of Encrypted Images

To prevent the leakage of information to an opponent, it is also advantageous if the cipher-image bears little or no statistical similarity to the plainimage. An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each intensity level. We have calculated and analyzed the histograms of several encrypted images as well as its original images that have widely different content. One typical example among them is shown in Fig.7 (b). The histogram of a plain-image Fig.7 (a) (Pepper image of size 256x256 pixels) contains large spikes. From Fig. 7(d), it is clear that the histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure.



Figure 7 (a) Original image

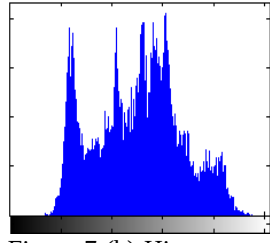


Figure 7 (b) Histogram of original image

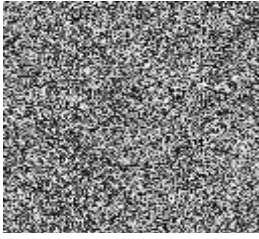


Figure 7 (c) Encrypted image

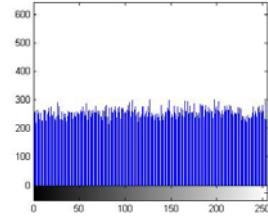


Figure 7 (d) Histogram of encrypted image

Figure 7: Histogram analysis

6.2.2 Correlation of Adjacent Pixels

In addition to the histogram analysis, we have also analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels and two diagonally adjacent pixels in plain-image/cipher-image respectively. The procedure is as follows: First, randomly select 1000 pairs of two adjacent pixels from an image. Then, calculate their correlation coefficient using the following two formulas:

$$\text{cov}(x, y) = E(x - E(x))(y - E(y)),$$

$$r_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \quad (5)$$

where x and y are grey-scale values of two adjacent pixels in the image. In numerical computations, the following discrete formulas were used:

$$E(x) = \frac{1}{N} \sum_{i=1}^N x_i \quad (6)$$

$$D(x) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))^2, \quad (7)$$

$$\text{cov}(x, y) = \frac{1}{N} \sum_{i=1}^N (x_i - E(x))(y_i - E(y)), \quad (8)$$

here N is the number of image pixels. Figure 8 and 9 demonstrate the correlation distribution of two horizontally adjacent pixels in plain-image/cipher-image (Baboon image of size 256x256) for the modified cipher. The correlation coefficients are 0.9452 and -0.0112 respectively for both plain-image/cipher-images, which are far apart. Similar results for diagonal and vertical directions were obtained as shown in Table 1. It is clear that there is negligible correlation between the two adjacent pixels in the cipher-image. However, the two adjacent pixels in the plain-text are highly correlated.

Table 1: Correlation coefficient of two adjacent pixels in original and Encrypted image

Direction	Plain -image	Cipher-image
Horizontal	0.9650	0.0012
Vertical	0.9250	-0.0561
Diagonal	0.8919	0.0315

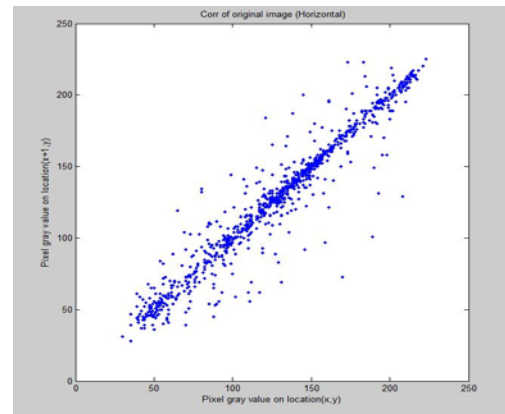


Figure 8: Horizontal adjacent pixels Correlation in plain-image

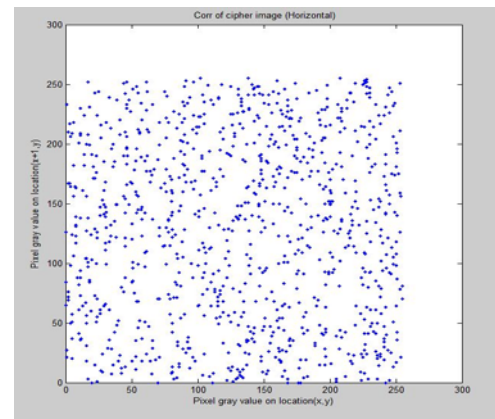


Figure 9: Horizontally adjacent pixels Correlation in cipherimage

6.2.3 Information Entropy Analysis

Information entropy is the mathematical theory of data communication and storage founded in 1949 by C.E. Shannon [21]. Modern information theory is concerned with error- correction, data compression, cryptography, communications systems, and related topics. To calculate the entropy $H(m)$ of a source m , we have:

$$H(m) = \sum_{i=0}^{2^N-1} P(m_i) \log_2 \frac{1}{P(m_i)} \text{ bits} \quad (9)$$

P represents the probability of symbol m_i and the entropy is expressed in bits. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. It can be noted from Table 2 that the entropy of the encrypted images (in average using 50 images) the proposed scheme are very near to 8 compared the image encryption scheme presented in [22].

Table 2: Entropies of the encrypted images

Encryption algorithm	Entropy Value (average)
Modified AES [22]	7.910
Proposed scheme	7.995

6.3 Differential Attack

Two common measures, NPCR and UACI [23-25], are used to test the influence of changing a single pixel in the original image on the whole image encrypted by the proposed scheme. NPCR stands for the number of pixels change rate while-pixel of plain image are changed. Unified Average Changing Intensity (UACI) measures the average intensity of difference between the plain image and cipher image. For calculation of NPCR and UACI, let us assume two ciphered images $C1$ and $C2$ whose corresponding plain images have only one-pixel difference. Define a bipolar array, D , with the same size as images $C1$ and $C2$. Then, $D(i,j)$ is determined by $C1(i,j)$ and $C2(i,j)$, namely, if $C1(i,j) = C2(i,j)$ then $D(i,j) = 1$; otherwise, $D(i,j) = 0$. NPCR and UACI are defined through the following formulas:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \quad (10)$$

$$UACI = \frac{1}{W \times H} \left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{255} \right] \times 100\%, \quad (11)$$

W and H are the width and height of $C1$ or $C2$. Tests have been performed on the proposed algorithm, about one-pixel change influence on a 256 gray-scale image of size 256×256 . We obtained $NPCR=99.44\%$ and $UACI=32.63\%$. The results show that a swiftly change in the original image will result in a significant change in the ciphered image, so the algorithm proposed has a good ability to anti differential attack. The results is illustrated in table 3, shows that a swiftly change in the original image will result in a significant change in the ciphered image, so the algorithm proposed has a good ability to anti differential attack with compared to image encryption based on 3D chaotic map [26].

Table 3: Comparison of differential attack analysis.

Experiments	Giesl et al. scheme [26]	Proposed scheme
NPCR	98.53%	99.44%
UACI	31.47%	32.63%

6.4 Encryption Effect Measurement

The peak signal to noise ratio (PSNR) in decibels (dB) is defined as:

$$PSNR = 20 \log_{10} \frac{MAX}{RMSE} \quad (12)$$

MAX is the image depth, in this study 8 pixels depth image are used which is gray scale level, so $MAX = 2^8 - 1 = 255$, and $RMSE$ is the root mean square error and defined as:

$$RMSE = \sqrt{\frac{1}{NM} \sum_{x=1}^N \sum_{y=1}^M [f(x,y) - \hat{f}(x,y)]^2} \quad (13)$$

where, N and M are the width and height of the images in pixels. f is the original image and $\hat{f}$ is the cipher-image. As illustrated in Table 4, the PSNR values according to DWT selected sub-band of the proposed scheme compared to the values in Seo et al. scheme [14].

Table 4: The encryption effect in terms of PSNR (in dB)

Selected DWT sub-band	Seo et al scheme [14]	Proposed scheme
LL4	9.244	8.110
LL4-HH4	7.760	7.340

Selected DWT sub-band	Seo et al scheme [14]	Proposed scheme
Level 4	7.669	7.193
Level 4-HH3	7.624	6.934

It is showed that the best image quality is obtained when the all Level 4 sub-bands and HH3 sub-band from level 3 are utilized for combined encryption and turbo coding, which give us the ability to reduce the computation time to implement the encryption and therefore preserve wireless energy.

6.5 Encryption speed analysis

Apart from the security considerations, some other issues for image encryption algorithm are important aspect, includes the running speed, particularly for real time image encryption in wireless-related applications. Some experimental tests are given to demonstrate the efficiency of our scheme compared with other algorithm with respect to the fastness issue for Lena image with different sizes. The time analysis has been done on a desktop computer has the following specification: Pentium-dual-core processor with 1024 MB RAM running with Microsoft windows 7 as operating system. Table 5 shows the test results of enciphering speeds of the proposed encryption algorithm compared with Chuanmu et al Algorithm [20] for Lena image with different sizes.

Table 5: Performance of encryption speed analysis

Image size	Chuanmu et al. [20]	Proposed scheme
256X256	2.01	0.78
512X512	4.12	1.62
1024X1024	8.74	3.29
2048X2048	15.87	7.03

We can see from Figure 10 the proposed algorithm reduce the computation time of encryption process to the half with compared to Chuanmu et al. Algorithm [18] and this serve the requirement of wireless channel.

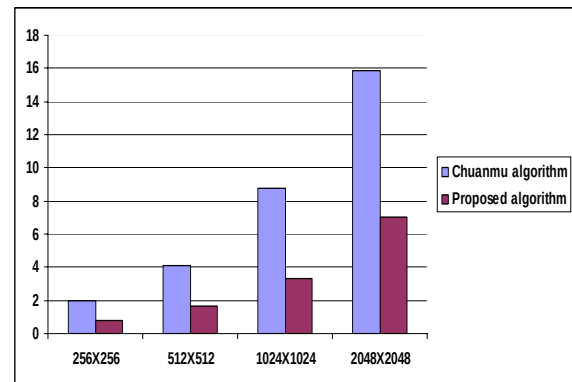


Figure 10: Encryption speed comparison

6.5 Bit Error Rate Performance

Additive White Gaussian Noise (AWGN) channel and Binary Phase Shift Keying (BPSK) modulation are considered. The bit error rate performance of overall system is investigated over mobile communication channels for various Signals to Noise Ratios. The bit error rate (BER) is computed after decoding, as a function of signal to noise ratio E_b/N_0 where E_b is the energy received per information bit and N_0 is the noise power spectral density. The reconstructed image for channel with $E_b/N_0=8$ dB without and with combination of turbo coding and 2D chaotic encryption are shown in Figures 11 (a) and (b), respectively.

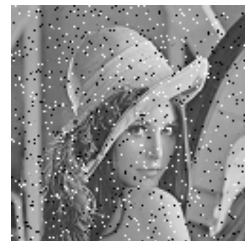


Figure 11 (a) Reconstructed image without turbo coding, PSNR=18.86

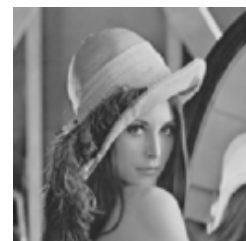


Figure 11 (b) Reconstructed image with turbo coding, PSNR=27.46

From Figure 11(a), it is observed that it is not possible to reconstruct the image clearly without the combination of turbo coding. But with combined encryption and turbo channel coding (1 iteration decoding), the image is reconstructed without distortion and no additional retransmission therefore 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. The E_b/N_0 vs. bit error rate (BER) with and without turbo channel coding (with single iteration decoding) is shown in Figure 12 ,

which obviously clears that the proposed scheme is effective for secure image communication over wireless noisy channel.

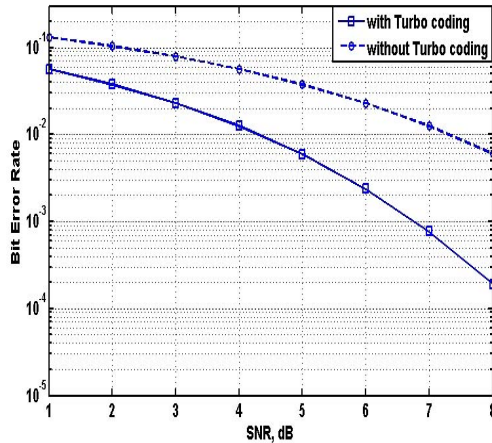


Figure 12: Bit Error Rate (BER) Performance over AWGN Channel

7. Conclusions

In this paper, combination of image encryption and error correction code has been proposed. Image encryption based on 2D chaotic maps and error control coding based on turbo channel coding. Simulation results show that the proposed scheme is effective and secure. The proposed scheme has larger key space. It can resist differential attack, plaintext attack, chosen-text known attacks and various brute-force attacks. The proposed scheme is suggested for secure image communication over wireless channels. From the results, it is concluded that the scheme is very effective for secure image communication over wireless noisy channels. Further works purpose an optimization scheme for the security issues and error correction code for wireless image transmission.

References

- [1] C. Nanjunda, M. Haleem and R. Chandramouli, "Robust Encryption for Eecure Image Transmission over Wireless Channels," IEEE ICC Conference, pp.287-1291, Korea, May 2005
- [2] C. Mathur, K. Narayan and K. Subbalakshmi, "On the Design of Error-Correcting Ciphers," EURASIP Journal on Wireless Communications and Networking, Vol.2006, pp.1-12, November 2006.
- [3] M.Williams, F. J. and N. A. Sloane: The Theory of Error Correcting Codes. I and II. Amsterdam: North-Holland Publishing Co., Vol. 16, 1977.
- [4] W. Stallings, Cryptography and Network Security: Principles and Practice, Prentice-Hall, USA, 2nd edition, 1999.
- [5] Stinson, D., Cryptography: Theory and Practice, Second Edition. CRC/C&H., 2002.
- [6] J. Fowler and B. Popescu, "An Overview on Wavelets in Source Coding, Communications, and Networks," EURASIP Journal on Image and Video Processing, Vol. 2007, pp. 1-27, April 2007.
- [7] Deerga Rao, "A Robust and Secure Scheme for Image Communication over Wireless Channels", IEEE CAS on ETW Conference, pp.88-91, 2005.
- [8] A. Padmaja and M. Shameem, "Secure Image Transmission over Wireless Channels", IEEE ICCIMA Conference, Sivakasi, Tamil Nadu, pp.44-48, January 2007.
- [9] D. Gligoroski, S. Knapkog, and S. Andova, "Cryptcoding - Encryption and Error Correction Coding in a Single Step," International Conference on Security and Management, pp.1-7, June 2006.
- [10] H. Cam, V. Ozduran and O. Ucan, "A Combined Encryption and Error Correction Scheme: AES-Turbo", Journal of electrical & electronics engineering, Vol.1, 2009, pp.861-866.
- [11] M. Asim and V. Jeoti, "On Image Encryption: Comparison between AES and A Novel Chaotic Encryption Scheme", IEEE ICSCN Conference, 2007, pp.65 - 69.
- [12] H. Ahmed, H. Kalash, and O. Farag Allah. , "An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption," IEEE Informatica, Vol.31, pp. 121-129, October 2007.
- [13] G. Sheng and G.Qiang , " The application of Chaos and DWT in Image Scrambling," Informatica Vol.31, pp. 3729-3733, October 2006.
- [14] Seo Y., Kim D., Yoo J., Dey S. and A. Agrawal, "Wavelet Domain Image Encryption by Subband Selection and Data Bit Selection", World Wireless Congress (3G Wireless) Conference, pp.1-6, May 2003.
- [15] A. Pommer and A. Uhl, "Selective Encryption of Wavelet Packet Subband Structures for Obscured Transmission of Visual Data", IEEE Benerux Signal Processing Symposium, pp. 25-28, 2002.
- [16] M. El-Iskandarani, S. Darwish and S. Abuguba, "A Robust and Secure Scheme for Image Transmission over Wireless Channels," IEEE ICCST Conference, Prague, Czech Republic, pp. 51-55, October 2008.
- [17] K.Deerga and K.Sudha, "Chaotic Image Encryption and Decryption -A Comparative Study", Proc. of International Conference on Systemics, Cybernetics and Informatics, Hyderabad, pp.433-438, 12-15 Feb.2004.
- [18] J. Luo and H. Shi, "Research of Chaos Encryption Algorithm Based on Logistic Mapping", IEEE International Conference on Intelligent Information Hiding and Multimedia, Pasadena, CA, USA pp.381-383, December 2006.
- [19] C.Berrou and A. Glavieux, "Near Optimum Error Correcting Coding and Decoding: Turbo Codes." IEEE transactions on communications Vol.44, No: 10, pp.1261-1271, 1996.
- [20] Chuanmu L., Lianxi H., "A New Image Encryption Scheme based on Hyperchaotic Sequences", IEEE IWASID Workshop, 2007, pp.237-240.
- [21] Shannon CE., Communication Theory of Secrecy System, Bell Syst Tech. J 1949;28:656-715.
- [22] M. Zeghid, M. Machhout, And R. Tourki, " A Modified AES Based Algorithm for Image Encryption", Waset, Vol.1, 2008.

- [23] S. Behnia, A. Akhshani, and A. Akhavan, "A Fast Chaotic encryption scheme based on piecewise nonlinear chaotic Maps". *Physics Letters A* 366 (2007) 391-396
- [24] Fuyan S., Shutang Liu, Zhongqin Li, and Zongwang Lü, "A Novel Image Encryption Algorithm based on Spatial Chaos Map," *Chaos Solutions and Fractals* 38 (2008) 631-640.
- [25] Ibrahim F. Elashry, S. El-Rabaie, and Fathi E. Abd El-Samie, "Homomorphic Image Encryption," *J. Electron. Imaging* Vol. 18, 033002 Jul. 14, 2009.
- [26] Giesl J. and Vlcek K., "Image Encryption Based On Strange Attractor", *International Journal on Graphics, Vision and Image Processing*, Vol.9, No.2, pp.19-26, 2009.