Research Journal of Applied Sciences 11 (10): 1159-1165, 2016
ISSN: 1815-932X

Design and Implementation a New Encryption System for True Images

Bahigah Khudair, Zainab Abdullah and Sawsan Hadi
Faculty of Information Technology, Babylon, Iraq

Abstract: Image encryption is a very effective method used in information security. In this study, a new and secure method for image encryption is proposed. This method is implemented firstly by doing a circular rotation (right and left) operation on all pixels of the image; each row in the image is rotated number of times depending on number of row. Secondly, making a sequential XOR operation between the pixels in the image and secret key. During the encryption phase, the two operations are repeated several times. On the other hand, the proposed system uses hybrid generator to generate initial secret key. The hybrid generator is based on the combination of Pless and Groth generators algorithms to increase the complexity on attackers which improves the security In order to evaluate the security and performance of the proposed system, the recorded results from applying it on images are analyzed using statistical analysis, key space analysis and key sensitivity analysis. According to experimental results, the proposed method has the best performance with lower MSE, higher PSNR, higher entropy and the correlation was significantly decreased. Also the results showed that the method is sensitive to any changes in the secret key. The proposed system is implemented in Vb6 programming language.

Key words: Image processing, cryptography, key sensitivity, histogram, entropy, correlation coefficient, confusion and diffusion, XOR, rotation, key space analysis

INTRODUCTION

With the rise of the internet, the world become relies totally on communication and information technology. As a result of high growth in multimedia applications and rapid development networking technology, one of a prime important issue in data communication is information security. Encryption is one the way to ensure securely transmit data in networks. It is very important to protect the data from unauthorized access (Zhu, 2012).

Encryption employed a variety of methods in mathematics to be used in data encryption and decryption code. This makes writing the data format will be more difficult to understand except the recipient who has the key of opening. Where it was easy for our sensitive data storage (confidential data) or secure transmission of data in the internet to protect it from thieves and attackers. So, writing the data in complicated format will makes it a very hard to be known by everyone except the person concerned (Patel and Belani, 2011; Ghebleh *at al*., 2014). Encryption algorithms are always striving to be more secure in order to make the code breaker find it so difficult to get the algorithm and thus obtain the explicit text. The force algorithm security depends on the construction method, the strength of key generation and measurement. Image encryption plays a major role to guarantee transmission of image over web. Image encryption has applications in satellite imagery, internet communication, industrial processes, military communication, astrophysics, etc. Image encryption methods attempt to convert original image to a different image that is difficult to understand to avoid the information theft and keep the image confidential between users (Patel and Belani, 2011). There are different image encryption methods to encrypt and decrypt image, and there is no single encryption algorithm satisfies the different image types.

Yaghoobi (2008) presented a technique for image encryption relies on a chaotic map. The proposed technique using chaotic map system to replacing the image pixels then changing the gray level value used simultaneously (Yaghoobi, 2008). Singh suggested a new encryption technique that is based on shuffling the image pixels using affine transform and resulting image was encrypting by using XOR operation (Nag *et al*., 2011).

Al-Husainy (2012) presented a encryption method that depend on the bit level permutation. The proposed method mixing two Boolean operations: XOR and Rotation on the bits of the pixels to satisfy the confusion and diffusion properties that ensures better security (Husainy, 2012).

Ginting and Dillak (2013) have proposed new encryption algorithm which based on RC4 stream cipher algorithm and chaotic logistics map.

Coressponding Author: Bahigah Khudair, Faculty of Information Technology, Babylon, Iraq

MATERIALS AND METHODS

Proposed method for key generation: The proposed key generation method used nonlinear generators. To increase the complexity of these generators increasing their numbers after linking them by a nonlinear hybrid function to get a complex nonlinear generator. Here, some of the algorithms that were based on this principle in the design are reviewed which has been built upon the design of hybrid generators including pless and groth generators. This will explain briefly two algorithms that will be built including hybrid generator to create the key.

Pless generator algorithm: It is a realistic and complex system has been used to generate randomization in a row. This system consists of eight feedback shift registers. These registers are arranged in four pairs as the greatest common denominator for the longest each pair of them is equal to to give the greatest cycle of the final relay output of all registers. This system has come to overcome the weaknesses in the system (J-K FF).

Groth generator algorithm: This algorithm consists of the removal of one registered with a feedback function. The output registers characteristic are resulted from group of operations which progress on the content of the group stages.

The proposed generator (hybrid generator): Pless and Groth algorithms have been hybridized together by Boolean connect nonlinear function where they are put the sequential resulting from pless generator in file with certain length. Also, putting the output key that was generated by the Groth algorithm in another file then combining them with a nonlinear functions function, which illustrated in Fig. 1 and 2.

The proposed technique for encryption: The structure of the proposed system is appeared in Fig. 1:

Encryption phase

Confusion process: The plain image of size h×w×3 is converted into its RGB components and then obtain the R, G and B matrixes (the three color components Red, Green and Blue) respectively. R represents h×w matrix for the red, G represents h×w matrix for the green and B represents h×w matrix for the blue:

- Circular rotate-right for each row in R several of times equal to row number
- Circular rotate-lefts for each row in B several of times equal to row number

Diffusion process: Generate a secret key of length (number of bit) = h×w×24 using hybrid generator (h, w is height and width of image). Divide the secret key into sub key each key's length is 8 bit and store them in a list called key list where each number of sub key = length/8.

- XOR the pixels with secret key
- R [i, j] = R [i,j] XOR keylist [index]
- G [i, j] = G[i,j] XOR keylist [index+1]
- B [i, j] = B[i,j] XOR keylist [index+2]
- Index = index+3 where index = 0 to numbers of sub key

Repeat all above steps for each pixel in the image to be sure that all pixels in the image are affected by secret key.

Decryption phase

Inv-diffusion process: Generate a secret key of length (number of bit) = h×w×24 by using hybrid generator (h, w is height and width of image). Divide the secret key into sub key each key's length is 8 bit and store them in a list called keylist where each number of sub key = length/8.

The cipher image of size h×w×3 is converted into its RGB components and then Obtain the R, G and B matrixes (the three color components Red, Green and Blue), respectively. R represents h×w matrix for the red, G represents h×w matrix for the green and B represents h×w matrix for the blue.

- XOR the pixels with secret key
- R [i,j] = R[i,j] XOR keylist[index]
- G [i,j] = G[i,j] XOR keylist[index+1]
- B [i,j] = B[i,j] XOR keylist[index+2]
- Index = index+3 where index = 0 to numbers of sub key

Repeat all above steps for each pixel in the image to be sure that all pixels in the image are affected by secret key.

Inv-confusion process: Circular Rotate-Left for each row in R several of times equal to row number. Circular Rotate-Right for each row in B several of times equal to row number.

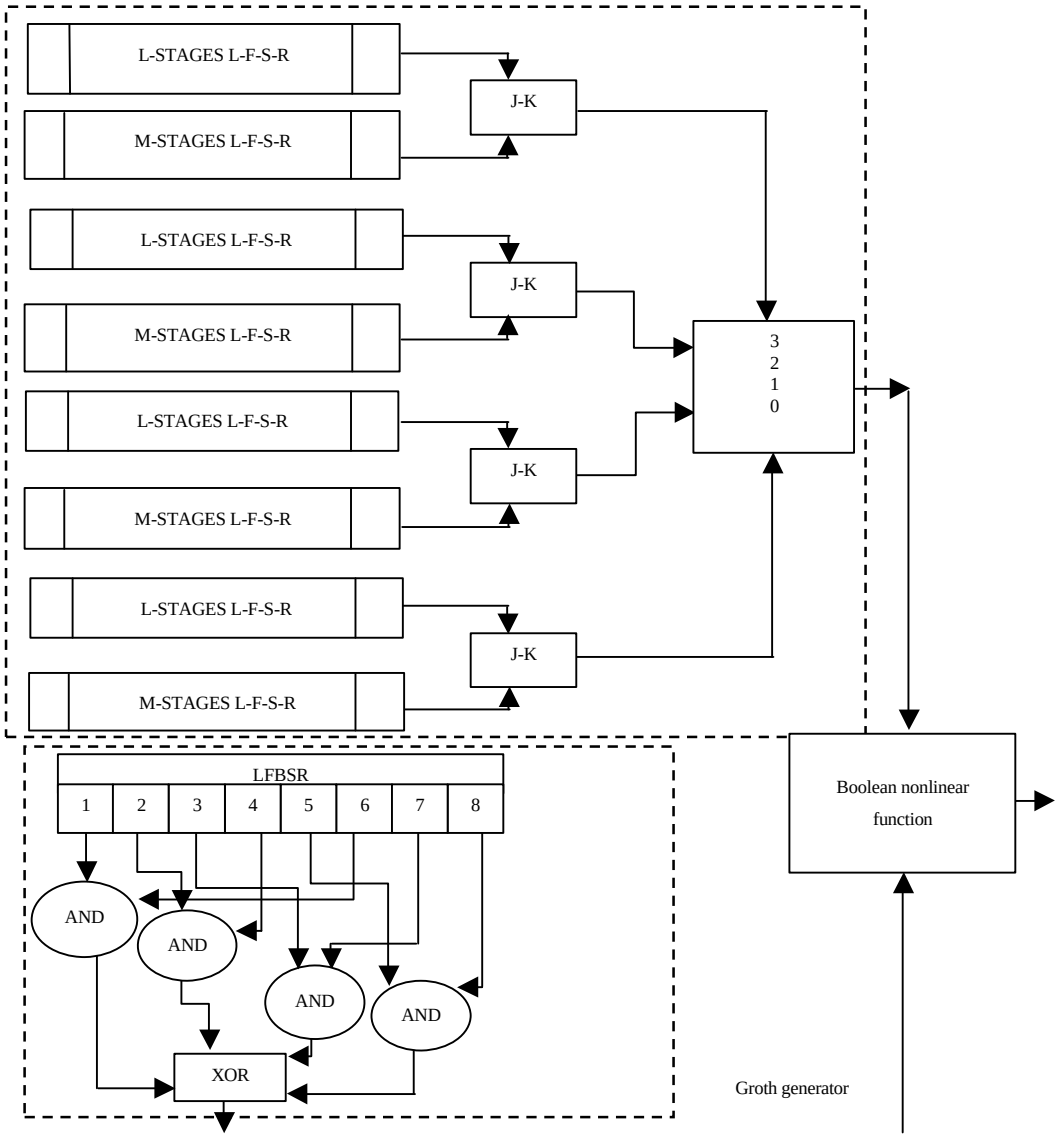

Fig. 1: Hybrid generator

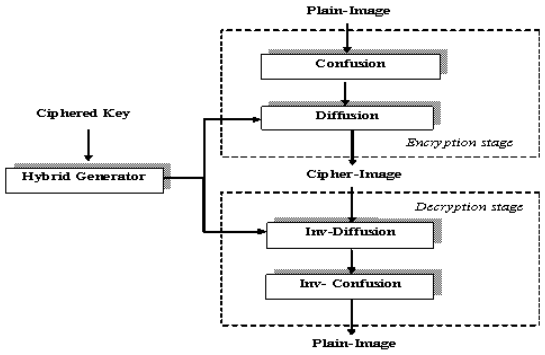

Fig. 2: The general structure of the encryption and decryption system

RESULTS AND DISCUSION

Evaluation and performance results: In order to assess the proposed encryption system, the method is tested on various images. Some security analysis has been performed including the most well-known such as: histogram, entropy, correlation and key space analysis. The performance results are more efficiency and confidentiality which demonstrate the strength of the proposed cryptosystem against any attack.

Histogram for ciphered images: A histogram is a graphical creation which explains the allocation of numerical data. It is a guess of the likelihood spreading of

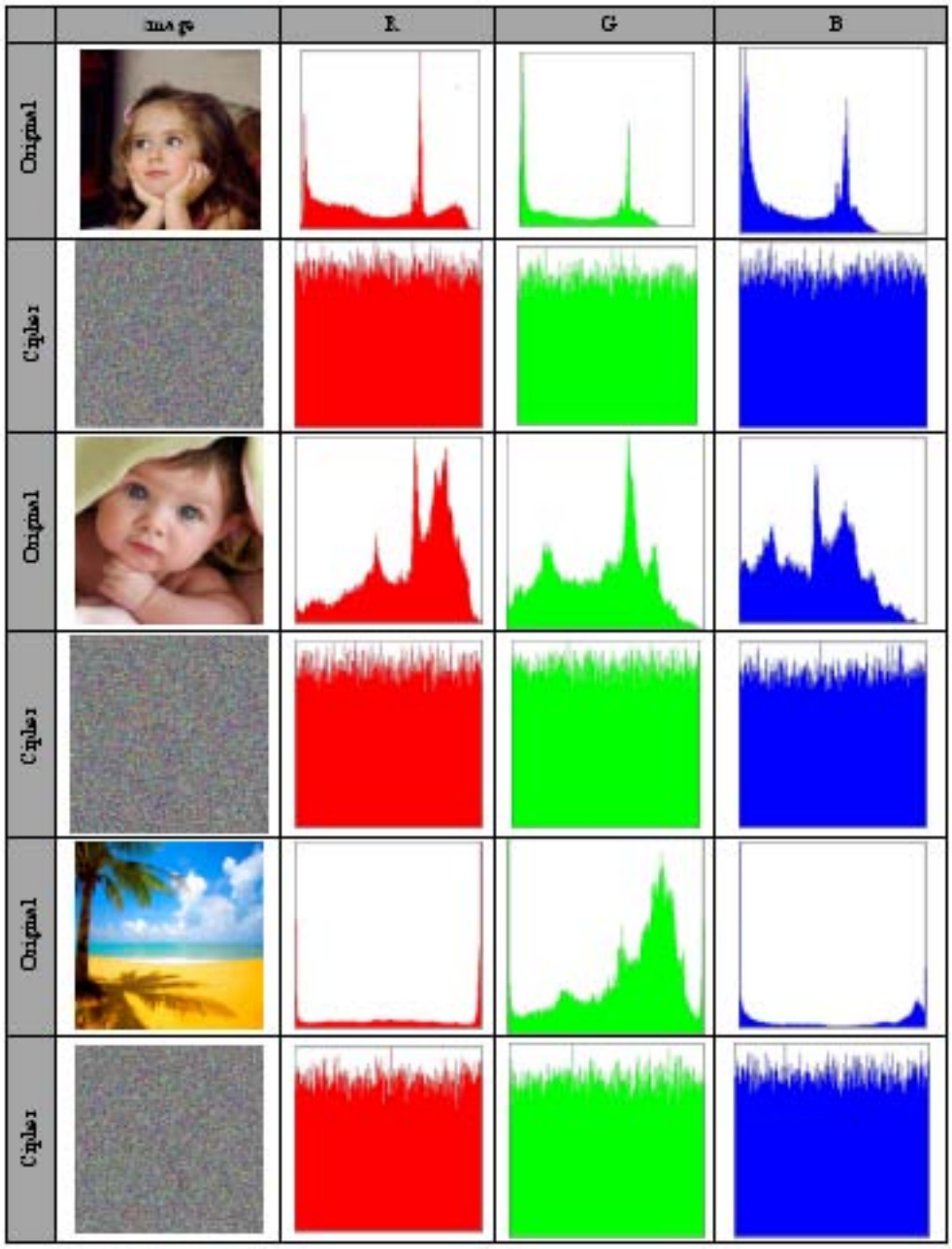

Fig. 3: Original images, ciphered images and their histograms

a continuous variable (quantitative variable). Histograms denote an estimate for information density. As apparent in Fig. 3 the histograms completely of encryption images are uniformly spread and greatest different from original images. Therefore, this system produce defends the original image data against statistical attack.

Entropy of image: Entropy is an instability relationship measure with arbitrary variable. Image entropy is an amount which is utilized to characterize the texture of image. The security system must achieve a requirement on image entropy in which the encrypted image does not show any relation with the original image (Jawad and Fawad, 2013). The image entropy is considered using equality:

$$\text{Entropy} = \sum_{k=0}^{N-1} p(k) \times \log_2 P(k) \quad (1)$$

Where:

N = The number of gray level in the image

P(k) = The probability of frequency of a pixel with gray level valuable k

The perfect entropy of a 256 gray level image should be 8, he entropy values for the test images are shown in Table 1. It's obvious that the entropy values of cipher images are very near to 8 unlike to their original image. This implies that the proposed system is safe on to entropy attack.

Correlation analysis

Correlations of two adjacent pixels: Correlation is computed by selecting K pairs of two adjacent pixels from original image and cipher image in diagonal, vertical and horizontal direction and then calculating correlation coefficients by using the following equation:

$$M(V) = \frac{1}{K}\sum_{1}^{K} Vi \quad (2)$$

$$D(V) = \frac{1}{K}\sum_{1}^{K} [Vi - M(V)]^2 \quad (3)$$

$$Con = \frac{1}{K}\sum_{1}^{K} [Vi - M(V)][Wi - M(W)] \quad (4)$$

$$C_{vw} = \frac{Con(v,w)}{\sqrt{D(V)}\sqrt{D(W)}} \quad (5)$$

with D (V)≠0 and D (W)≠0. Here, v and w denote gray level values of two-adjacent pixels and K is the total number of pixel pairs (Gao *et al*., 2006). Illustrates the result of correlation analysis for adjacent pixels in the diagonal, vertical and horizontal directions of the original images and ciphered image. It's obvious that the correlation values of the original images are close to one, implying that strong correlation between pixels. Unlike those observed for the ciphered images which are zero, meaning that no detectable correlation exists between pixels. This security test demonstrates that the proposed system achieves zero coefficient correlation.

Table 1: The entropy of the testing and ciphered images

Images	R(1)	G (2)	B(3)
Plain	7.6107	7.0233	7.0613
Cipher	7.9972	7.9968	7.9970
Plain	7.5978	7.6972	7.6629
Cipher	7.9989	7.9975	7.9974
Plain	7.3092	7.6493	7.9434
Cipher	7.9970	7.9969	7.9974

Correlations between original image and ciphered image: The correlation between original and ciphered images is analyzed by calculating the 2D Correlation Coefficients (CC) between original and ciphered images. The CC is computed as follows:

$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(AA_{ij} - \overline{AA})(BB_{ij} - \overline{BB})}{\sqrt{(\sum_{i=1}^{M}\sum_{j=1}^{N}(AA_{ij} - \overline{AA})^2)(\sum_{i=1}^{M}\sum_{j=1}^{N}(BB_{ij} - \overline{BB})^2)}} \quad (6)$$

$$\overline{AA} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} AA_{ij} \text{ and } \overline{BB} = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} BB_{ij} \quad (7)$$

Here, AA is the original image, BB is the ciphered image i, j are the number of rows and the number of columns nd are the mean values of matrices $\bar{A}\bar{A}$ and $\bar{B}\bar{B}$. M and N are the height and width of the image. Table 2 illustrates the correlation values between the ciphered and original images. It is obvious that no correlation exists between the two images which mean the original image and it encryption are totally different.

Key space analysis: Key space is the total aggregate of bits in a key that can be utilized in the encryption. For an efficient encryption system, the key space should be large enough to make brute-force attack infeasible.

Key sensitivity test: Encryption algorithm must be high sensitive to cipher key. This implies that a small exchange in the key should result in a big change in the encrypted or decrypted image. To explain the key sensitivity of the proposed system, the following steps are performed:

Table 2: The Correlations for the test images and ciphered images

	Horizontal (1)			Vertical (2)			Diagonal (3)		
Images	R	G	B	R	G	B	R	G	B
Plain	0.9888	0.9844	0.9752	0.9865	0.9851	0.9814	0.9822	0.9851	0.9757
Cipher	0.0034	-0.0028	-0.0034	-0.0002	-0.0034	0.0030	-0.0010	0.0000	-0.0008
Plain	0.9893	0.9896	0.9889	0.9905	0.9916	0.9908	0.9803	0.9916	0.9805
Cipher	-0.0018	-0.0020	-0.0057	-0.0056	-0.0031	0.0038	-0.0007	0.0002	-0.0063
Plain	0.9844	0.9752	0.9910	0.9830	0.9666	0.9873	0.9753	0.9666	0.9838
Cipher	-0.0034	0.0019	0.0009	-0.0333	-0.0022	0.0035	0.0021	-0.0016	0.0079-

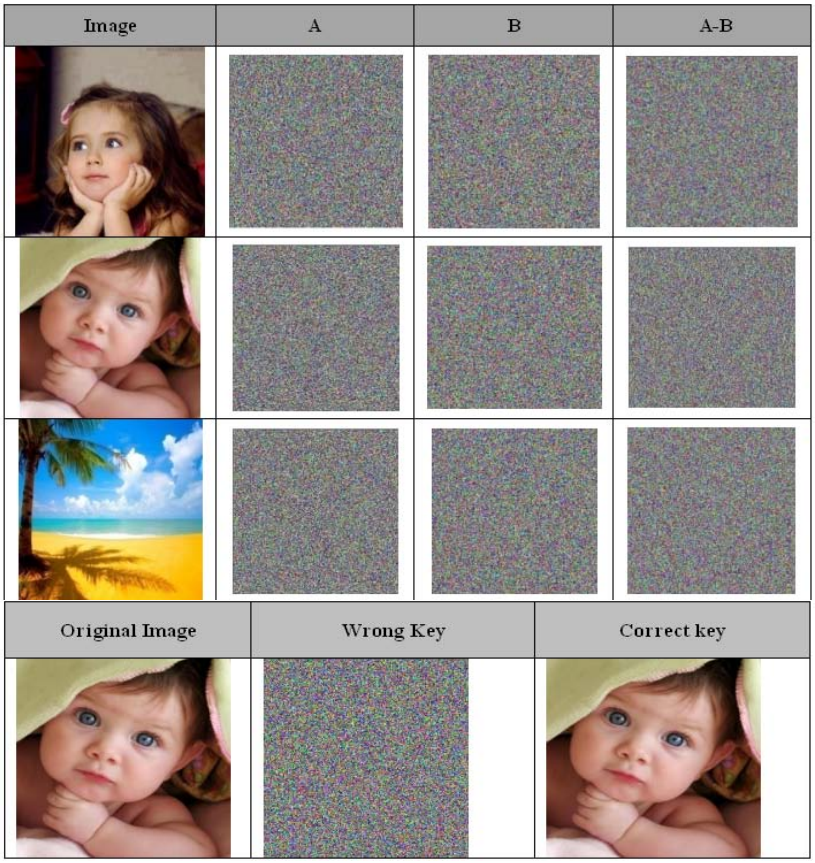

Fig. 4: The original, decrypted image with wrong key and decrypted image with correct key

Table 3: Correlation coefficients between ciphered and original images

	Images		
Variables	1	2	3
R	-0.0054	-0.0009	-0.0019
G	-0.0074	-0.0080	-0.0031
B	-0.0053	-0.0038	-0.0037

Table 4: Correlation coefficients and pixel difference between the result encrypted images using slightly different keys

	Correlation coefficients			Pixel eifference (%)		
Images	R	G	B	R	G	B
1	-0.0027	-0.0021	-0.0016	99.55	99.65	99.50
2	0.0003	-0.0053	-0.0006	99.56	99.66	99.56
3	-0.0013	-0.0004	-0.0042	99.55	99.70	99.56

- The original image is encrypted by using the secret key and is called encrypted image A
- The original image is encrypted by making a small modification in the key (i.e., the most significant bit is exchanged) and is called encrypted image B

The test of key sensitivity: The original images, encrypted images and difference images and Table 3 and 4 display the correlation coefficient and pixels difference between the two encrypted images A, B. It's obvious that there is no correlation between two encrypted images despite they have been encrypted by using slightly different keys.

Another test to illustrate the key sensitivity feature is to change one bit in the key and then use it to decrypt the cipher image, the decryption completely fails as show in Fig. 4.

CONCLUSION

Pless method is the best way to get the greatest complexity and when hybridized with other generators was increased complexity of other generators. The proposed cryptosystem is simple and powerful, the simplicity originated from utilizing two XOR and Rotate operations. The powerful came from utilize a big number of bits in the secret key. The tests results illustrate that the proposed cryptosystem has good security features and high performance in encryption. The proposed cryptosystem has high sensitive to any slight difference in encryption key.

REFERENCES

Al-Husainy, M.A.F.A., 2012. A novel encryption method for image security. Intl. J. Secur. Appl., 6: 1-8.

Gao, H., Y. Zhang, S. Liang and D. Li, 2006. A new chaotic algorithm for image encryption. Chaos Solitons Fractals, 29: 393-399.

Ghebleh, M., A. Kanso and H. Noura, 2014. An image encryption scheme based on irregularly decimated chaotic maps. Signal Proc. Image Commun., 29: 618-627.

Ginting, R.U. and R.Y. Dillak, 2013. Digital color image encryption using RC4 stream cipher and chaotic logistic map. Proceedings of the International Conference on Information Technology and Electrical Engineering (ICITEE), October 7-8, 2013, IEEE, New York, USA., ISBN:978-1-4799-0425-9, pp: 101-105.

Jawad, A. and A. Fawad, 2013. Efficiency analysis and security evaluation of image encryption schemes. Int. J. Video Image Process. Network Secur., 12: 18-31.

Nag, A., J.P. Singh, S. Khan, S. Ghosh and S. Biswas *et al*., 2011. Image encryption using affine transform and XOR operation. Proceedings of the International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), July 21-22, 2011, IEEE, New York, USA., ISBN:978-1-61284-653-8, pp: 309-312.

Patel, K.D. and S. Belani, 2011. Image encryption using different techniques: A review. Intl. J. Emerging Technol. Adv. Eng., 1: 30-34.

Yaghoobi, M., 2008. A new approach for image encryption using chaotic logistic map. Proceedings of the 2008 International Conference on Advanced Computer Theory and Engineering, December 20-22, 2008, IEEE, New York, USA., ISBN:978-0-7695-3489-3, pp: 585-590.

Zhu, C., 2012. A novel image encryption scheme based on improved hyperchaotic sequences. Opt. Commun., 285: 29-37.