Asian Journal of Scientific Research

ISSN 1992-1454

science alert
http://www.scialert.net

ANSInet
an open access publisher
http://ansinet.com

Asian Journal of Scientific Research 8 (3): 359-366, 2015
ISSN 1992-1454 / DOI: 10.3923/ajsr.2015.359.366

Chain of Shuffling and Chaos: A Tied Encryptic Approach

Padmapriya Praveenkumar, G.U. Priyanga, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India

Corresponding Author: Padmapriya Praveenkumar, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613 401, India Tel: +91 4362-264101-108 Fax: +91-4362-264120

ABSTRACT

The intellectual growth of computer communication lead to drastic improvement in wireless technology and shrunken the world into palms of the user which paved the path for the security attack issues. The development of the security system became the ultimate. Popular technique widely used in present scenario that provides a better security to secret information is image encryption. Multiple encryption technique has been adopted in this study. The secret image is block shuffled and then chaotic maps such as baker map, skew tent map and Arnold cat map are used to encrypt the image. Further the image is encrypted using Cipher Block Chaining (CBC) to contribute the final encrypted image. Metrics such as horizontal, vertical, diagonal correlation, Number of Changing Pixel Rate (NPCR) and entropy were calculated for various Digital Imaging and Communication in Medicine (DICOM) test images and the performance of the algorithm was analyzed.

Key words: Arnold cat map, baker map, CBC, DICOM, image encryption, skew tent map

INTRODUCTION

As like olden days keeping all valuable documents in paper format becomes tiresome and then we go for computer database management and computer communication. Ultimately the advancement of productive telecommunications have accompanied with the hike in fruitless technology such as security attacks, internet attacks and hacker attacks. Hence it is decided to know about the attacks and flourish security system to prevent computer communication from security issues. Information security system comprises of classifications such as cryptography, steganography and watermarking (Zhang *et al*., 2014; Korrai *et al*., 2012).

Cryptography is the method of securing the secret information by modifying the originality of the information and presenting it in an unpredictable format. Under cryptography image encryption is the widely used technique (Aarthie and Amirtharajan, 2014; Amirtharajan *et al*., 2013; Mahmood *et al*., 2013a; Mahmood and Dony, 2013b; Dong *et al*., 2012). This confuses the secret image so that third party has no knowledge about the original information. The success of the crypto system falls in the robustness of the algorithm proposed and then multiple stages of encryption were preferred (Praveenkumar *et al*., 2014a, b, c, d, 2015; Rajagopalan *et al*., 2014a, b, c). Shuffling is the process of randomizing the position of the object to the position in the modified output (Chen *et al*., 2014a, b).

In image encryption shuffling can be described as the randomization of the pixel position in order to expose an uncorrelated image. The block shuffling is the procedure of shuffling small blocks of an image (Tang *et al*., 2014; Patidar *et al*., 2011). Image is divided into smaller blocks and

then their positions are randomized without any prescribed format. The block shuffling procedure reduces to pixel shuffling when the block size is chosen as 1×1. Chaos is the study of dynamic systems. Though chaotic systems have deterministic nature they are unpredictable. The output of the deterministic systems is completely dependent on the initial conditions (Dai and Wang, 2012; Naeem *et al*., 2014). A small variation in the initial condition will result in completely different output and the selection of range of initial condition also plays a major role. Detailed studies on the chaos system have made such selection easier. Hence the chaotic map output is not a random one and it is well defined by its equations.

Cipher block chaining is the process of encrypting the first pixel of an image with a predefined key and the following pixels using the previous cipher (Tong *et al*., 2014). Arnold transformation deals with geometric transformation (Liu *et al*., 2012; Veena *et al*., 2012) i.e., the image are tilted to an angle and then pieces of image were combined to form a square image as of the original image size. More number of iterations gives better confused image than the lesser iteration.

The Arnold transformation itself has the property that after certain number of iterations the original image will be reconstructed. Tang *et al*. (2014) have proposed the block shuffling procedure and chaotic maps for image encryption. Naeem *et al*. (2014) have proposed baker map encryption. In this study block shuffling and CBC along with three chaotic maps namely skew tent map, Arnold cat map and baker map were proposed so as to give better performance.

PROPOSED ALGORITHM

The secret input image is divided in to number of smaller blocks and shuffled twice using the key generated by pseudo random generator. The initial shuffled image is then encrypted using baker map which involves block division and mapping elements of each sub-block in to a single row of the corresponding block taking elements from right to left and bottom to top fashion. In the third stage a chaotic sequence is generated using skew tent map and a secret matrix is formed with these elements. The secret matrix undergoes Arnold transformation and each stage output is XORed with unique block of the image of same size as secret matrix. The final stage of encryption is Cipher Block Chaining (CBC) encryption. The CBC is applied twice first in column wise and then in row wise manner thus offering the final encrypted image. The decryption process follows the reverse of encryption. The following is the encryption algorithm in detail and Fig. 1a explains step by step procedure of encryption.

Encryption algorithm:

- Get the input image and the size of image be M×N
- Image is divided into S×S blocks and shuffled twice using the random permuted key
- The shuffled image is further divided into blocks of size S1×S1, then circular shifting based on key and Baker map are applied to each block
- For baker encryption each block is divided into number of non-square sub-blocks horizontally and vertically so that each sub-block will have same number of elements as M
- Each sub-block is transformed to a single row of a block
- Selection of sub-block and its elements are done from right to left and bottom to top fashion
- A chaotic sequence is generated using skew tent map which can be defined by the equation:

$$F(x)=\begin{cases} x/p, x\in[0,p] \\ (1-x)/(1-p), x\in(p,1] \end{cases} \quad (1)$$

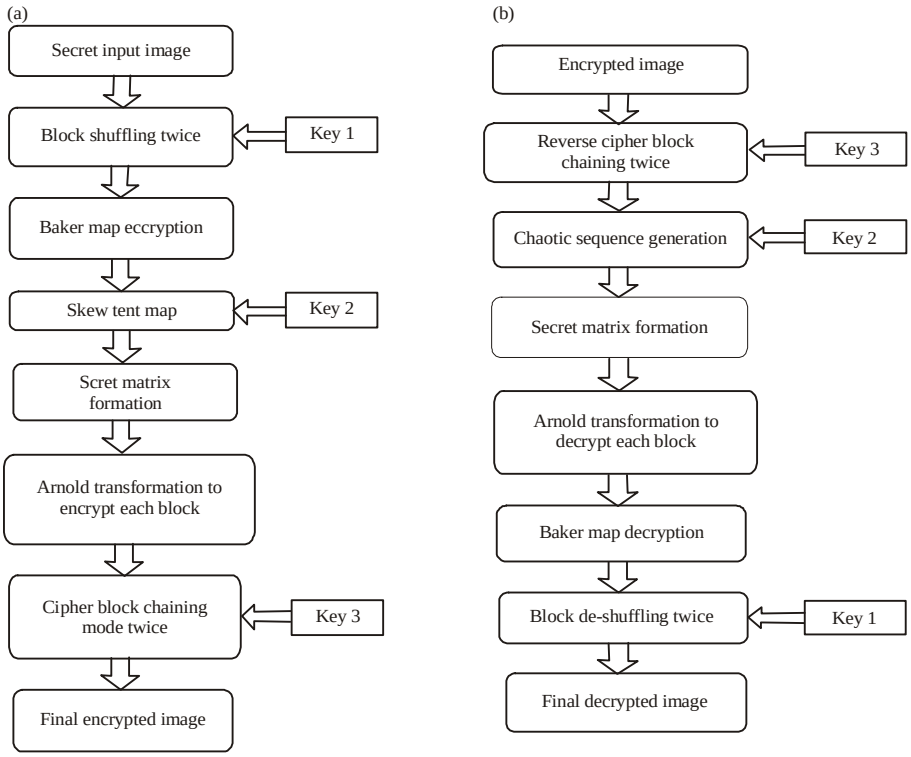

Fig. 1(a-b): (a) Encryption block diagram and (b) Decryption block diagram

- The initial values are taken in the range x_0 = (0-1) and p = (0-1)
- The elements of chaotic sequence are converted to the range of 1-256 using the equation:

$$Y(x) = \mathrm{mod}(\lfloor F(x) * 2^{10} \rfloor, 256) \tag{2}$$

- B^2 number of elements are taken from generated chaotic sequence to form a secret matrix of size B×B
- Secret matrix undergoes Arnold transformation that can be given by the equation:

$$\begin{pmatrix} s' \\ t' \end{pmatrix} = \begin{pmatrix} 1 & P \\ Q & P*Q+1 \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix} (\mathrm{mod}\, 4) \tag{3}$$

- At each stage Arnold transformed secret matrix is XORed with B×B blocks of the image
- Cipher block chaining is applied in column wise and then row wise manner
- Hence the encrypted image is formed

Decryption algorithm:

- The encrypted image is read and reverse CBC is applied first in row wise and then column wise manner
- Using the key from encryption side secret matrix is formed and XORed with the B×B blocks of image

- Reverse of baker map and circular shifting are carried out for the resultant image
- Then block de-shuffling is carried out to get the original reconstructed image
- Figure1b explains step by step procedure of decryption

RESULTS AND DISCUSSION

For analysis, 2 gray scale images and 4 medical images were taken and metrics were calculated in order to prove the performance of the algorithm.

Correlation coefficient: The correlation coefficient is classified as horizontal correlation, vertical correlation and diagonal correlation. The term which represents the correlation between the adjacent pixels is called correlation coefficient. This correlation coefficient can be given by the following equation:

$$\text{Correlation cofficient } r(x,y) = \frac{\text{cov}(x,y)}{\sqrt{V(x)+V(y)}} \tag{4}$$

In which numerator of the fraction is the covariance and the denominator is the square root of sum of the variances. The Eq. 5, 6 and 7 are used to calculate the covariance and variance. The calculation of variance needs mean which can be determined using Eq. 8 and 9.

$$\text{Co var iance, } \text{cov}(x,y) = \frac{1}{n}\sum_{i=1}^{n} E[(x(i)-E(x))(y(i)-E(y)] \tag{5}$$

$$\text{Variance, } V(x) = \frac{1}{n}\sum_{i=1}^{n}\left[x(i)-E(x)\right]^2 \tag{6}$$

$$V(y) = \frac{1}{n}\sum_{i=1}^{n}\left[y(i)-E(y)\right]^2 \tag{7}$$

$$\text{Mean, } E(x) = \frac{1}{n}\sum_{i=1}^{n} x(i) \tag{8}$$

$$E(y) = \frac{1}{n}\sum_{i=1}^{n} y(i) \tag{9}$$

NPCR: PCR is expanded as Number of Changing Pixel Rate and it is used to determine the strength of the encryption algorithm beyond attacks. NPCR can be calculated using the following equation:

$$\text{NPCR} = \left(\frac{1}{n}\sum_{i=0}^{n-1} d_i\right)\times 100\% \tag{10}$$

where, d_i is decided by comparing the pixels of encrypted image and the original image at same position. This process is explained using the following equation:

$$d_i = \begin{cases} 0, \text{If } X_i^2 = Y_i^2 \\ 1, \text{If } X_i^2 \neq Y_i^2 \end{cases} \quad (11)$$

X and Y are the pixel from original image and encrypted image of same index i:

Entropy: The entropy of an encrypted image is the average information in an image after encryption and this can be determined by the Eq. 12:

$$H(x) = \sum_{i=0}^{L-1} p(x_i) \log_2 p(x_i) \quad (12)$$

H(x) is the entropy of an image, x is the information source, $p(x_i)$ is the probability of symbol x_i.

The following Table 1, containing the metrics calculated for various test images and the values are compared with the previous existing works. Since the correlation values are obtained in negative range and comparatively lesser as compared to (Zhang *et al*., 2014; Dai and Wang, 2012).

The output images obtained after execution of test image in the proposed methodology was displayed below.

Figure 2, 3 and 4 describe the encryption stages. Figure 2a and 2b are the original medical test image and its histogram respectively. Figure 3a is the first stage encrypted image obtained using block shuffling and baker map. Figure 3b is the second stage encrypted image obtained using Skew tent map and Arnold transformation.

Figure 4a and 4b are the final encrypted image and its histogram, respectively. Figure 5 and 6 describe the decryption stages. Figure 5a is the decrypted image after applying inverse CBC.

Table 1: Metrics for different test images

Images/metrics	Diagonal correlation	Vertical correlation	Horizontal correlation	NPCR	Entropy
Test image 1.dcm	-0.00089	-0.0365	-0.0112	100	7.9973
Zhang *et al*. (2014)	0.0032	-0.0154	0.0193	-	-
Test image 2.dcm	-0.0024	-0.0018	-0.0064	100	7.9971
Dai and Wang (2012)	0.2027	0.2056	0.3992	-	-
Brain-016.dcm	-0.0036	-0.0175	-0.0120	100	7.9972
Brain-008.dcm	-0.0048	-0.0042	-0.0141	100	7.9971
Baboon.jpg	-0.000615	-0.00168	-0.000477	100	7.9994
Barbara.png	-0.00232	-0.0021	-0.0020	100	7.9993

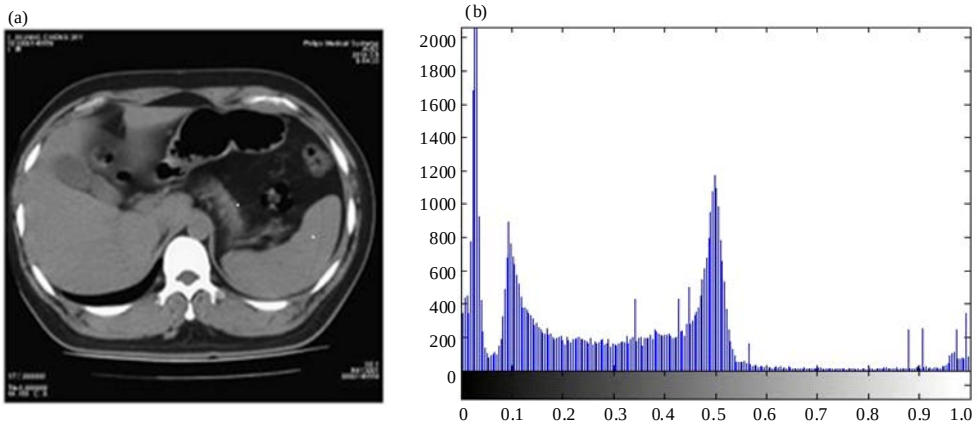

Fig. 2(a-b): (a) Original test image and (b) Histogram of original image

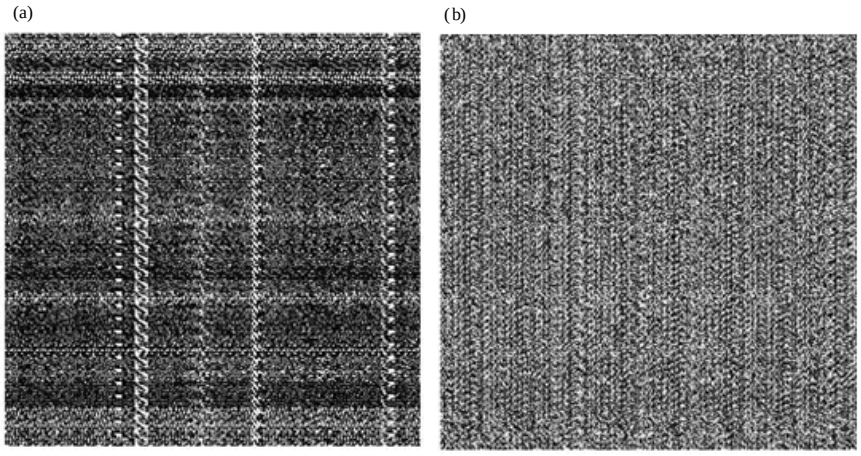

Fig. 3(a-b): (a) Encrypted image using block shuffling and baker map and (b) Encrypted image using skew tent map and arnold transformation

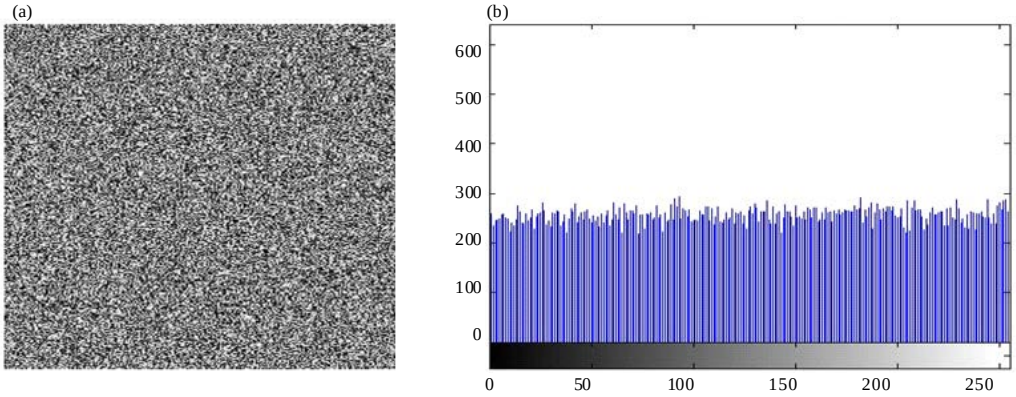

Fig. 4(a-b): (a) Final encrypted image using CBC and (b) Histogram of encrypted image

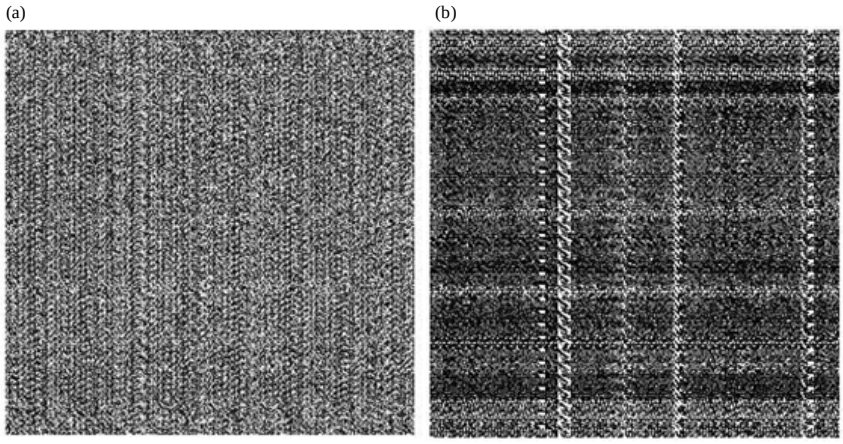

Fig. 5(a-b): (a) Decrypted image after CBC and (b) Decrypted image after arnold transformation and skew tent map

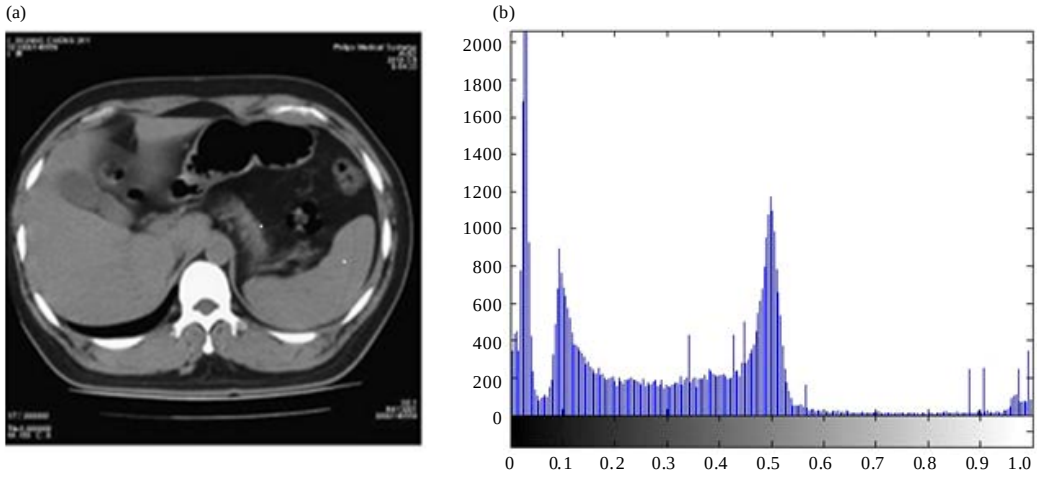

Fig. 6(a-b): (a) Final decrypted image and (b) Histogram of decrypted image

Figure 5b is the decrypted image obtained using reverse Arnold transformation and Skew tent map. Figure 6a and 6b are the final decrypted image and its histogram, respectively.

CONCLUSION

It is evident that information security is most needed in present world either in preserving personal information or social information. The leakage of information may lead to severe consequences. Hence it is mandatory to test the robustness of the encryption. Since the adopted encryption technique is multiple encryptions, it is more robust and safer. The calculated metrics are compared with available literature and also proves to be the efficient image encryption algorithm.

REFERENCES

Aarthie, N. and R. Amirtharajan, 2014. Image encryption: An information security perceptive. J. Artif. Intell., 7: 123-135.

Amirtharajan, R., P. Archana and J.B.B. Rayappan, 2013. Why image encryption for better steganography. Res. J. Inform. Technol., 5: 341-351.

Chen, J.X., Z.L. Zhu, C. Fu, H. Yu and L.B. Zhang, 2014a. An efficient image encryption scheme using gray code based permutation approach. Opt. Lasers Eng., 67: 191-204.

Chen, J.X., Z.L. Zhu, C. Fu, L.B. Zhang and Y. Zhang, 2014b. An image encryption scheme using nonlinear inter-pixel computing and swapping based permutation approach. Commun. Nonlinear Sci. Numer. Simul., 23: 294-310.

Dai, Y. and X. Wang, 2012. Medical image encryption based on a composition of logistic maps and chebyshev maps. Proceeding of the IEEE International Conference on Information and Automation, June 6-8, 2012, Shenyang, China, pp: 210-214.

Dong, C., J. Li, M. Huang and Y. Bai, 2012. The medical image watermarking algorithm with encryption by DCT and logistic. Proceedings of the 9th Web Information Systems and Applications Conference, November 16-18, 2012, Haikou, pp: 119-124.

Korrai, P.K., M.N.S. Swamy and K.D. Rao, 2012. Robust transmission of watermarked medical images over wireless channels. Proceedings of the IEEE Global Humanitarian Technology Conference (GHTC), October 21-24, 2012, Seattle, WA., pp: 242-246.

Liu, Z., M. Gong, Y. Dou, F. Liu and S. Lin *et al*., 2012. Double image encryption by using Arnold transform and discrete fractional angular transform. Opt. Lasers Eng., 50: 248-255.

Mahmood, A., R. Dony and S. Areibi, 2013a. An adaptive encryption based genetic algorithms for medical images. Proceedings of the IEEE International Workshop on Machine Learning for Signal Processing, September 22-25, 2013, Southampton, pp: 1-6.

Mahmood, A.B. and R.D. Dony, 2013b. Adaptive encryption using pseudo-noise sequences for medical images. Proceedings of the 3rd International Conference on Communication and Information Technology, June 19-21, 2013, Beirut, pp: 39-43.

Naeem, E.A., M.M. Abd Elnaby, N.F. Soliman, A.M. Abbas and O.S. Faragallah *et al*., 2014. Efficient implementation of chaotic image encryption in transform domains. J. Syst. Software, 97: 118-127.

Patidar, V., N.K. Pareek, G. Purohit and K.K. Sud, 2011. A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. Opt. Commun., 284: 4331-4339.

Praveenkumar, P., G. Ashwin, S.P.K. Agarwal, S.N. Bharathi, V.S. Venkatachalam, K. Thenmozhi and R. Amirtharajan, 2014a. Rubik's cube blend with logistic map on RGB: A way for image encryption. Res. J. Inform. Technol., 6: 207-215.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014b. Why information security demands transform domain, compression and encryption? J. Artif. Intell., 7: 136-144.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014c. Double layer encoded encrypted data on multicarrier channel. J. Applied Sci., 14: 1689-1700.

Praveenkumar, P., R. Hemalatha, R. Uma, K. Madhunisha, K. Thenmozhi and R. Amirtharajan, 2014d. Image $\xrightarrow{Zoning}$ encryption. Res. J. Inform. Technol., 6: 368-378.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015. Pixel scattering matrix formalism for image encryption-A key scheduled substitution and diffusion approach. AEU-Int. J. Electron. Commun., 69: 562-572.

Rajagopalan, S., H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014a. Dual cellular automata on FPGA: An image encryptors chip. Res. J. Inform. Technol., 6: 223-236.

Rajagopalan, S., H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014b. Galois field proficient product for secure image encryption on FPGA. Res. J. Inform. Technol., 6: 308-324.

Rajagopalan, S., H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014c. Logic elements consumption analysis of cellular automata based image encryption on FPGA. Res. J. Inform. Technol., 6: 291-307.

Tang, Z., X. Zhang and W. Lan, 2014. Efficient image encryption with block shuffling and chaotic map. Multimedia Tools Applic. 10.1007/s11042-014-1861-1

Tong, X.J., Z. Wang, Y. Liu, M. Zhang and L. Xu, 2014. A novel compound chaotic block cipher for wireless sensor networks. Commun. Nonlinear Sci. Numer. Simul., 22: 120-133.

Veena, V.K., G.J. Lal, S.V. Prabhu, S.S. Kumar and K.P. Soman, 2012. A robust watermarking method based on compressed sensing and Arnold scrambling. Proceedings of the International Conference on Machine Vision and Image Processing, December 14-15, 2012, Taipei, pp: 105-108.

Zhang, S., T. Gao and L. Gao, 2014. A novel encryption frame for medical image with watermark based on hyperchaotic system. Math. Problems Eng. 10.1155/2014/240749