# Research Journal of Information Technology

ISSN 1815-7432

Academic Journals Inc.

www.academicjournals.com

OPEN ACCESS Research Journal of Information Technology

ISSN 1815-7432
DOI: 10.3923/rjit.2016.10.16

# Research Article
# Image Merger Encryptor: A Chaotic and Chebyshev Key Approach

Padmapriya Praveenkumar, R. Nisha, K. Thenmozhi, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan

School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613401, India

## Abstract
In the rapid development of various expertises, the information can be misplaced, misused and damaged. To overcome these vulnerabilities, the information security is eminent. Information security ensures the authorized people to access the precise information when they are needed and cannot be customized without authorization. To prevent the access of information from the illegal user and destruction several encryption techniques are used. Multilevel and double image encryption method are proposed this work to achieve the high level secrecy and better performance. The novel double image encryption technique based on cross image pixel scrambling in Fourier domain and chaotic maps are used to achieve the multilevel encryption. The statistical and security test are tested on Digital Imaging and Communication in Medicine (DICOM) images.

Key words: Chaotic mapping, DICOM, Image encryption, NPCR

Received: July 18, 2015 Accepted: October 30, 2015 Published: March 15, 2016

Citation: Padmapriya Praveenkumar, R. Nisha, K. Thenmozhi, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan, 2016. Image Merger Encryptor: A Chaotic and Chebyshev Key Approach. Res. J. Inform. Technol., 8: 10-16.

Corresponding Author: Padmapriya Praveenkumar, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, 613401, India
Tel: +91 4362-264101-108 Fax: +91-4362-264120



Competing Interest: The authors have declared that no competing interest exists.

Data Availability: All relevant data are within the paper and its supporting information files.

## INTRODUCTION

Due to the development of multimedia and network technologies, the information is transmitted through communication network. The intruder can capture the information and it can be altered (Dang and Chau, 2000). Wireless security is used to protect against the illegal copying and distribution of the information (Praveenkumar *et al*., 2014c). The wireless network provides to access and share the information from any place. Information security such as encryption is used for providing security. Security system is classified into information hiding and cryptography. Steganography and water marking are sub disciplines of information hiding (Amirtharajan *et al*., 2013).

Cryptography is used for protecting the content of the message from an unauthorized user. The main objective of cryptography is authentication, confidentiality, integrity, non repudiation and availability. It is classified as symmetric key cryptography, asymmetric key cryptography and hashing functions. In symmetric key cryptography identical keys are used for both encryption and decryption. The DES and AES are frequently used techniques in symmetric cryptography. Asymmetric key cryptography uses public key and private key for encryption and decryption. Most popularly used asymmetric cryptography techniques are RSA, DSA and Diffie-Hellman (Wang *et al*., 2010).

Encryption is the process of altering of information using a secret key which cannot be retrieved by an unauthorized user. Decryption is the reverse process of encryption (Dang and Chau, 2000), with the development in the technology multiple image encryption is proposed in this work. Here double image is encrypted using Arnold cat map and chaotic chebyshev map (Zhong *et al*., 2012; Li and Dai, 2010). Multiple secret images can be hidden at the same time using multiple image encryptions algorithm. Scrambling is the process of encoding of message in a form which makes the image in an unintelligible form (Aarthie and Amirtharajan, 2014; Amirtharajan *et al*., 2013; Praveenkumar *et al*., 2014a,b,c,d, 2015a,b,c,d; Rajagopalan *et al*., 2014a,b,c). Scrambling of images is defined as the process of change in the position of pixels in a particular order.

Two input images are combined to processed further. This image is split into several bit planes and shuffled iteratively using logistic map algorithm along with Arnold cat map. The Arnold cat map used to scramble and shuffle the pixel of an image (Liu *et al*., 2012; Veena *et al*., 2012; Prusty *et al*., 2013). The properties of the chaos are sensitive to the initial condition and dense orbits. The chaos maps are deterministic dynamical system and have random behaviour. Finally obtain the random binary matrix by chaotic map (Zhe *et al*., 2009; Li and Liu, 2013; Zhang *et al*., 2014; Desai *et al*., 2012).

The chaotic logistic map is depicted by Eq. 1:

$$X_n+1 = \mu x_n (1-x_n) \quad (1)$$

The bit xor operation is performed between the unique key and shuffled image by Arnold cat map which produce the ciphered image. The chebyshev map is used to generate the key for shuffled image and generate the row confusion vector. The chaotic state variable is generated by chebyshev map (Fu *et al*., 2013; Dai and Wang, 2012; Prasadh *et al*., 2009; Wang *et al*., 2008). The row and column of the shuffled image are rearranged by row confusion vector and finally produce the scrambled cipher image.

Zhong *et al*. (2012) proposed double image encryption by scrambling the matrix and encoding one image into phase and other image into amplitude of the complex function. In fractional Fourier domain, double random phase encoding is applied to this complex function and the resultant is the encrypted image.

Liu *et al*. (2012) proposed the encryption method for double image using Arnold and discrete fractional angular transform. The two images are converted into phase and amplitude of the complex function. Arnold transform is used to scramble the pixel position and it is transformed into fractional angular domain. In this process phase is considered as the key and amplitude of the image is the encrypted image.

In this study, a combination of two images into single image using Arnold transform to scramble the pixel position using chaotic logistic sequence is proposed. It is used as the key for encryption. Further image is encrypted using chaotic chebyshev map. The chaotic logistic and chebyshev maps are used as the key for both encryption and decryption process.

## MATERIALS AND METHODS

In this study, a combination of two images into single image using Arnold transform to scramble the pixel position using chaotic logistic sequence is proposed shown in Fig. 1. It is used as the key for encryption. Further image is encrypted using chaotic chebyshev map. The chaotic logistic and chebyshev maps are used as the key for both encryption and decryption process.

### Encryption algorithm:

- Read the double input DICOM images of size 256×256
- Split the image into 8 bit planes and apply Arnold cat map to shuffle the bit planes

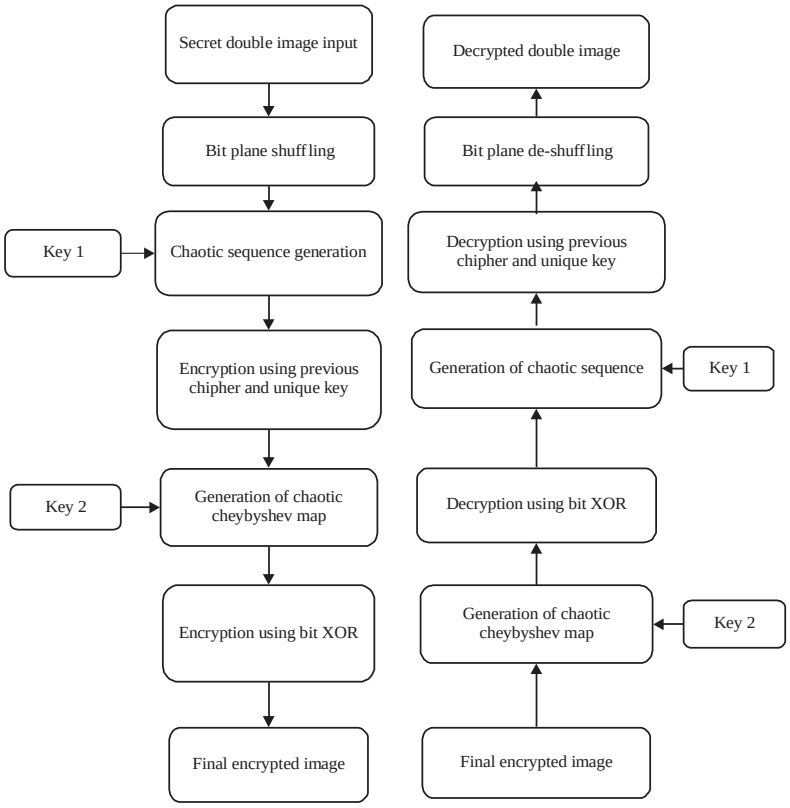


Fig. 1: Block diagram of encryption and decryption

- Then the resultant image forms the encrypted image of level 1
- The chaotic logistic key is generated by Eq. 1 and Bit xor with the previous cipher from step 2
- Then the resultant image forms the encrypted image of level 2
- Row confusion vector is calculated by Eq. 2:

$$r_m = m+\text{mod}(\text{floor}(\text{floor}(\text{state\_variable}\times 10^{15})\ M-m+1) \quad (2)$$

The values of $r_m$ is restricted within the region (m, M). The chaotic state variables are generated from chebyshev map as expressed by Eq. 3:

$$x_{n+1} = \cos(k \cos^{-1} x_n) \quad (3)$$

- Apply this row confusion vector to step 6 then it forms the resultant image as the scrambled image of level 3
- Store the resultant image as the multilevel encrypted image

The block diagram of encryption and decryption is shown in Fig. 1.

**Decryption algorithm:**

- Read the double input multilevel encrypted image
- Decrypt the image using the key generated by chaotic chebyshev map Eq. 3
- The resultant image is the descrambled image of level 1
- Generate the key using chaotic logistic map Eq. 2
- Bit Xor is applied between the step 3 and 4 then the resultant image is the decrypted image of level 2
- Then to the decrypted image obtained from step 5 apply Arnold cat map to reshuffle the image to form the final decrypted image of level 3
- Combine 8 bit planes into single plane
- Store the resultant image as the decrypted image

## RESULTS AND DISCUSSION

In this study a double image encryption is proposed. Double image is encrypted using Arnold logistic cat map and chaotic chebyshev map. To prove the performance of the proposed method various metrics were calculated such as correlation coefficient, Number of Changing Pixels Rate (NPCR) and information entropy.

Several metrics were calculated for sample images shown in Table 1 and compared with recent work on image encryption (Zhang *et al*., 2014; Dai and Wang, 2012). Consider image 1 and 2 as the double input image for which horizontal, vertical, diagonal correlation, NPCR and entropy were calculated as -0.0044, -0.00046, 0.0039, 99.5750 and 7.9962, respectively and these values are comparable with various studies (Praveenkumar *et al*., 2015a b, c, d; Zhang *et al*., 2014; Dai and Wang, 2012), the correlation values, NPCR and entropy are better.

In Fig. 2a depicts the double input medical image and Fig. 2b depicts the uniform pixel distribution of Fig. 2a. The encryption using Chaotic Arnold cat map of Fig. 2a is depicted in Fig. 2c. The encryption using chaotic chebyshev of Fig. 2c is illustrated in Fig. 2d. The uniform pixel distribution of Fig. 2d is represented in Fig. 2e. There is no correlation between the original and ciphered image. The decryption using chaotic chebyshev of Fig. 2e is illustrated in Fig. 2f. The final decrypted image is depict in Fig. 2g. The uniform pixel distribution of Fig. 2g is illustrated in Fig. 2h.

**NPCR:** Number of pixel change rate (NPCR) is used to find the effect one pixel modification on the entire image. It used to find the difference between original and encrypted image pixels. NPCR, correlation coefficients and entropy were calculated using the Eq. 4:

$$NPCR = \left(\frac{1}{n}\sum_{i=0}^{n-1} d_i\right)\times 100\% \quad (4)$$

X, Y is the adjacent pixel from original image and encrypted image:

Table 1: Metrics considering images of size 256×256

| Metrics/images | Proposed image 1 and 2 (dcm) | Zhang *et al*. (2014) | Dai and Wang (2012) | Proposed image 3 and 4 (dcm) | Proposed image 5 and 6 (dcm) |
|---|---|---|---|---|---|
| Vertical correlation | -0.00046 | 0.3992 | 0.0122 | 0.00059 | -0.0011 |
| Horizontal correlation | -0.0044 | 0.2027 | -0.006 | -0.0015 | -0.0079 |
| Diagonal correlation | 0.0039 | 0.2056 | -0.0197 | 0.0067 | 0.0095 |
| NPCR | 99.575 | na | na | 99.6368 | 99.6223 |
| Entropy | 7.9962 | na | na | 7.9971 | 7.9967 |

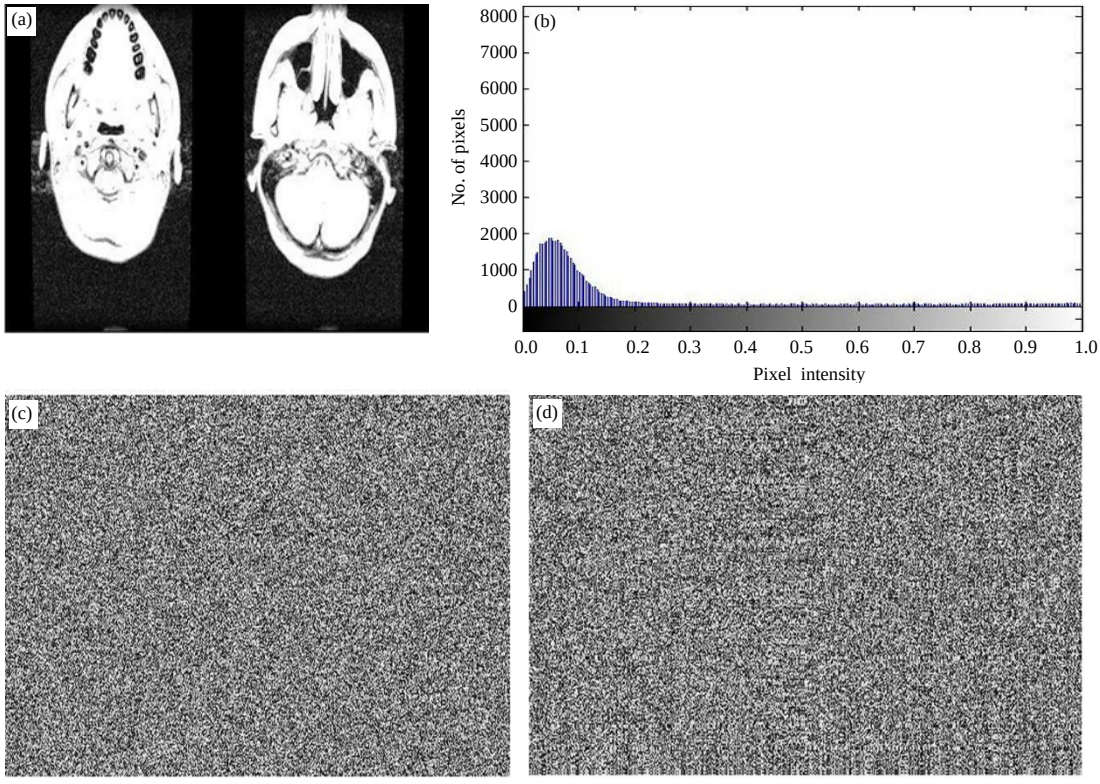


Fig. 2(a-h): Continue

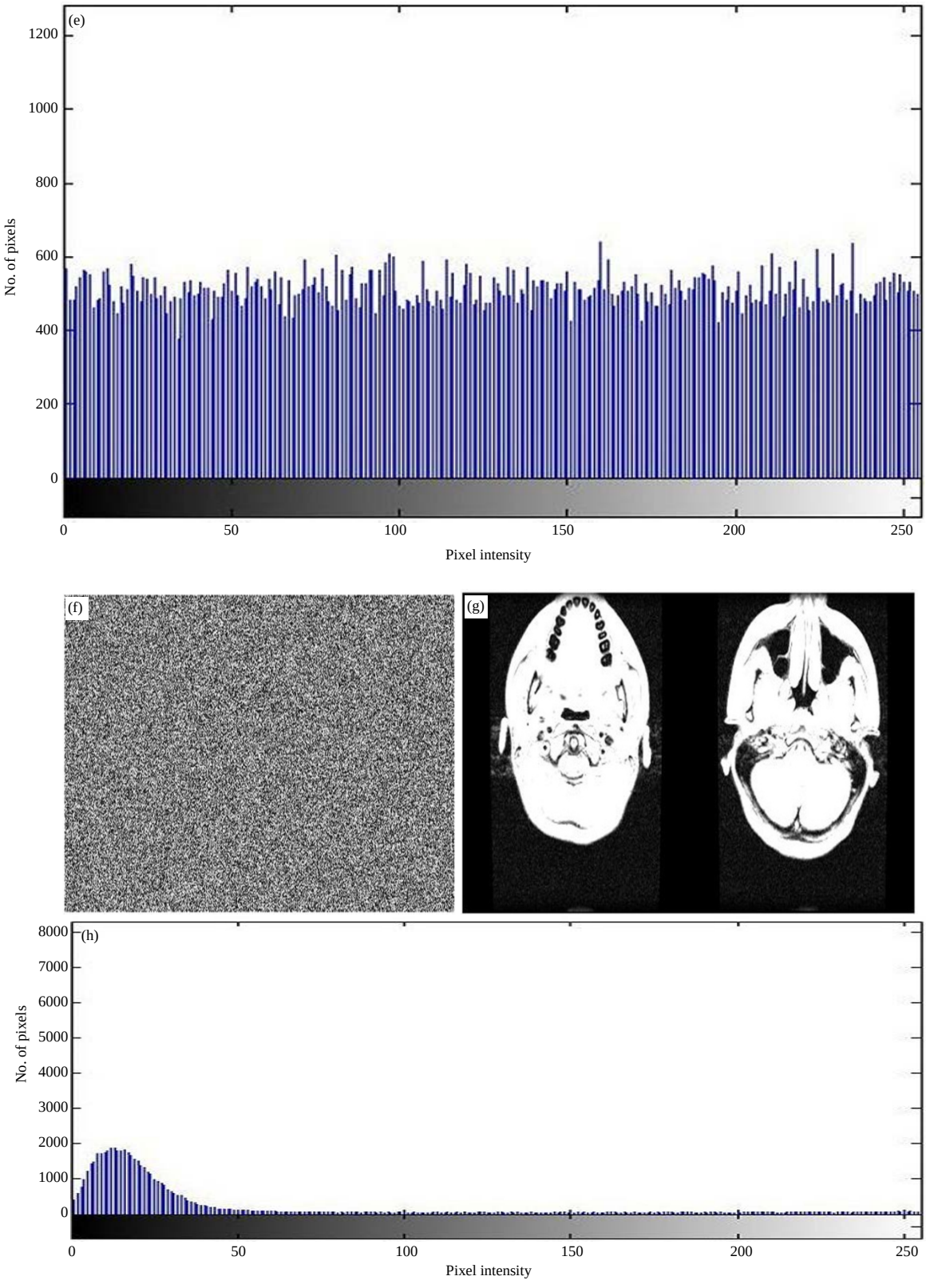


Fig. 2(a-h): Sample double image with their multiple encrypted decrypted outputs and histograms (a) Original double image, (b) Histogram of Fig. 2a, (c) Encryption using Arnold cat map, (d) Encryption using chaotic chebyshev, (e) Histogram of Fig. 2d, (f) Decryption using chaotic chebyshev, (g) Final decrypted image and (h) Histogram of Fig. 2g

- $d_i = 0$ if $X_i^2 = Y_i^2$
- $d_i = 1$ if $X_i^2 \neq Y_i^2$ for any $i \in \{0,1,...,n-1\}$

**Correlation coefficient:** Correlation is used to find the degree of similarity between the two adjacent vertical, horizontal and diagonal pixels are given in Eq. 5:

$$\rho(X,Y) = \frac{E\left[\left(X - \mu_X\right)\left(Y - \mu_Y\right)\right]}{\sigma \times \sigma_Y} \quad (5)$$

where, μ is the mean value, s is the standard deviation, E [.] is the expected value.

**Entropy:** Average quantity of information enclosed in the each received message and the formula is given in Eq. 6:

$$H(X) = \sum_{i=0}^{i=L-1} p(x_i) \log_2 p(x_i) \quad (6)$$

Where:

H(X) = Information entropy
X = Information source X
L = Length
$p(x_i)$ = Probability of symbol

## CONCLUSION

To tackle the robustness, tamper detection and security issues double image multilevel encryption scheme is proposed. The double image is scrambled using Arnold cat map and chaotic Chebyshev map. The bit-XOR operation is performed between unique key generated by chaotic chebyshev map and scrambled image. The resultant image is the multi level encrypted image. The various metrics such NPCR, information entropy and correlation values of horizontal, vertical, diagonal were calculated for various medical image and compared with available literature and found to be superior. The negative correlation values expose that they defend against discrepancy and brute force attack.

## 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.

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.

Dang, P.P. and P.M. Chau, 2000. Image encryption for secure internet multimedia applications. IEEE Trans. Consumer Elect., 46: 395-403.

Desai, D., A. Prasad and J. Crasto, 2012. Chaos-based system for image encryption. Int. J. Comput. Sci. Inform. Technol., 3: 4809-4811.

Fu, C., W.H. Meng, Y.F. Zhan, Z.L. Zhu, F.C.M. Lau, C.K. Tse and H.F. Ma, 2013. An efficient and secure medical image protection scheme based on chaotic maps. Comput. Biol. Med., 43: 1000-1010.

Li, J. and H. Liu, 2013. Colour image encryption based on advanced encryption standard algorithm with two-dimensional chaotic map. IET Inform. Secur., 7: 265-270.

Li, X.M. and L. Dai, 2010. A novel approach for double image encryption. Proceedings of the IEEE Region 10th Conference on TENCON, November 21-24, 2010, Fukuoka, pp: 697-701.

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.

Prasadh, K., K. Ramar and R.G. Araman, 2009. Public key cryptosystems based on chaotic-chebyshev polynomials. Proceedings of the International Conference on Advances in Recent Technologies in Communication and Computing, October 27-28, 2009, Kottayam, Kerala, pp: 4-8.

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 Zoning→ encryption. Res. J. Inform. Technol., 6: 368-378.

Praveenkumar, P., G.U. Priyanga, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2015a. Chain of shuffling and chaos: A tied encryptic approach. Asian J. Scient. Res., 8: 359-366.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015b. Medical data sheet in safe havens-a tri-layer cryptic solution. Comput. Biol. Med., 62: 264-276.

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

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2015d. Triple chaotic image scrambling on RGB: A random image encryption approach. Secur. Commun. Networks. 10.1002/sec.1257

Prusty, A.K., A. Pattanaik and S. Mishra, 2013. An image encryption and decryption approach based on pixel shuffling using Arnold cat map and Henon map. Proceedings of the International Conference on Advanced Computing and Communication Systems, December 19-21, 2013, Coimbatore, pp: 1-6.

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.

Veena, V.K., G.J. Lal, S.V. Prabhu, S.S. Kumar and K.P. Soman, 2012. A robust water marking 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.

Wang, C.H., C.L. Chuang and C.W. Wu, 2010. An efficient multimode multiplier supporting AES and fundamental operations of public-key cryptosystems. IEEE Trans. Very Large Scale Integration Syst., 18: 553-563.

Wang, L., Q. Ye, Y. Xiao, Y. Zou and B. Zhang, 2008. An image encryption scheme based on cross chaotic map. Proceedings of the Congress on Image and Signal Processing, Volume 3, May 27-30, 2008, Sanya, China, pp: 22-26.

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

Zhe, Z., Y. Haibing, Z. Yu, P. Wenjie and Z. Yunpeng, 2009. A block encryption scheme based on 3D chaotic Arnold maps. Proceedings of the International Asia Symposium on Intelligent Interaction and Affective Computing, December 8-9, 2009, Wuhan, pp: 15-20.

Zhong, Z., J. Chang, M. Shan and B. Hao, 2012. Double image encryption using double pixel scrambling and random phase encoding. Optics Commun., 285: 584-588.