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.2016.1.9

Research Article
Horse DNA Runs on Image: A Novel Road to Image Encryption

Padmapriya Praveenkumar, P. Rajalakshmi, K. Thenmozhi, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan

School of Electrical and Electronics Engineering, Shanmugha Arts, Science, Technology and Research Academy University, Thanjavur, 613401, India

Abstract
As there are formations there will also be every possible ways to obstruct the growth or to destruct the grown. So the world filled with technologies needs improvisation at every stride of its way to be reached out. This is more predominant when it comes to the plight of communication a major surface without which life has become a nihility. There is always a thrive to overcome the security attack and every time produce a next step ahead technology to avoid invaders via communication. And in such way boomed a technology called cryptography, where different encryption techniques emerged with their own specialities in safeguarding the essential data from out the window access. Here in this paper a combo of two techniques namely Deoxyribo Nucleic Acid (DNA) encryption and famous rule set encryption have been proposed for various Digital Imaging and Communication in Medicine (DICOM) images. This encryption technique has proven good results when checked with their correlations, Number of Pixels Change Rate (NPCR), information entropy and histogram analysis.

Key words: DNA encryption, NPCR, DICOM, correlation, entropy

Received: July 19, 2015 **Accepted:** October 26, 2015 **Published:** March 15, 2016

Citation: Padmapriya Praveenkumar, P. Rajalakshmi, K. Thenmozhi, John Bosco Balaguru Rayappan and Rengarajan Amirtharajan, 2016. Horse DNA Runs on Image: A Novel Road to Image Encryption. Res. J. Inform. Technol., 8: 1-9.

Corresponding Author: Padmapriya Praveenkumar, School of Electrical and Electronics Engineering, Shanmugha Arts, Science, Technology and Research Academy 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

Information security has become a paramount factor for us to be noted. Hence, the augmenting growth of this particular field in present scenario and it will keep being burgeoning in future too. Information security is simply the way how we protect the cardinal information from getting slipped out either deliberately or unwittingly. Cryptography is a field with infinite ways to encrypt the information that needs to be surpassed safely without being identified. There are also few other ways such as steganography and water marking serving the purpose of information security. Apart from information in form of text, audio, video and images also carry more of integral part of information. So, image encryption has been growing recently in a tremendous way.

Traditionally digital image scramblers were used in simple ways so as to confuse the image data and display will finally result to be unidentifiable (Aarthie and Amirtharajan, 2014; Amirtharajan *et al*., 2013; Praveenkumar *et al*., 2014a, b, c, d, 2015a, b, c; Rajagopalan *et al*., 2014a, b). Recently there are surplus techniques kept as the base for scramblers used in image encryption (Tong *et al*., 2015; Kishore *et al*., 2014; Kester *et al*., 2013; Paul *et al*., 2013; Dascalescu *et al*., 2013). One of the new-fangled eras has started with famous rule set based scramblers for image encryption and few of them like Rubik's cube principle based (Loukhaoukha *et al*., 2012; Diaconu and Loukhaoukha, 2013) Sudoku puzzle based (Wang *et al*., 2012; Delei *et al*., 2008; Wu *et al*., 2012), Poker's shuffling rule based (Wang and Zhang, 2008), etc. Along the line knights move (Diaconu *et al*., 2014; Delei *et al*., 2008; Lei *et al*., 2010) in a chess board can also be used noticeably.

In this study, an amalgamation of transposition of pixels between RGB planes and logistic chaotic mapping is used at a stage of encryption (Borujeni and Eshghi, 2009; Li *et al*., 2013; Zou *et al*., 2011). Apart from this rule set based encryption another alluring and contemporary technique for image encryption is DNA based encryption (Belazi *et al*., 2014). In this work an encryption is percolated using DNA coding, complement, XOR and swapping between pixels in every planes separately. This is also accomplished along with the help of logistic chaotic mapping. The DNA encryption is applied before and after the knights move scrambling.

MATERIALS AND METHODS

DNA encryption: More the complexity would offer more the security of the system. Chaotic systems were predominantly used for greater confusing purpose in many encryption techniques. With the insight wanting for more complexity the idea turned out to molecular biology based information (Wang *et al*., 2010; Jain and Bhatnagar, 2014; Yunpeng *et al*., 2011; Som *et al*., 2013; Zhang *et al*., 2012). Images are generally represented in binary and this can be encoded into DNA representation. A DNA molecule is generally comprised of basically four types of nucleic acids viz., Thymine (T), Cytosine (C), Adenine (A) and Guanine(G), the standard pairing occurs between T-A and G-C. Different operations such as DNA addition, subtraction, complement and XOR are used widely. Table 1 provides the binary representation of various DNA code.

Table 1: DNA encoding

Binary representations	DNA code
00	A
01	C
10	G
11	T

Rule set based encryption: Knights moving rule takes a form of letter L i.e., vertical displacement of two squares and a horizontal displacement of one square or horizontal displacement of two squares and a vertical displacement of one square. The use of Knights move of chess board has found a vital part of this encryption technique in this study. There are generally 8 possible moves for a knight from an initial position.

The choice of a particular move is manipulated using essential data from chaotic sequence. The number of times n a move needs to be enforced is left to the choice of the particular user. There are certain things that need to be clarified before getting into the details of algorithm. The n can take any possible values from 0-255 so that its value is curbed into 8 bit representation. There might be a possibility that the moves can outpace the image dimension and so as to avoid this problem the image is considered as virtually cyclic. So, that when the pixel exits through one side it might emerge at other side forming a cyclic nature. And finally for efficient transposition the pixels should necessarily be removed from their original plane and has to be transposed into either of other planes (Diaconu *et al*., 2014; Lei *et al*., 2010).

Chaotic sequence: A chaotic sequence is used at various stages of the encryption in this study (Chen *et al*., 2015; Ahmad and Farooq, 2010). A sequence x_n is generated with the help of certain initial values such as x_0 and μ in Eq. 1:

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

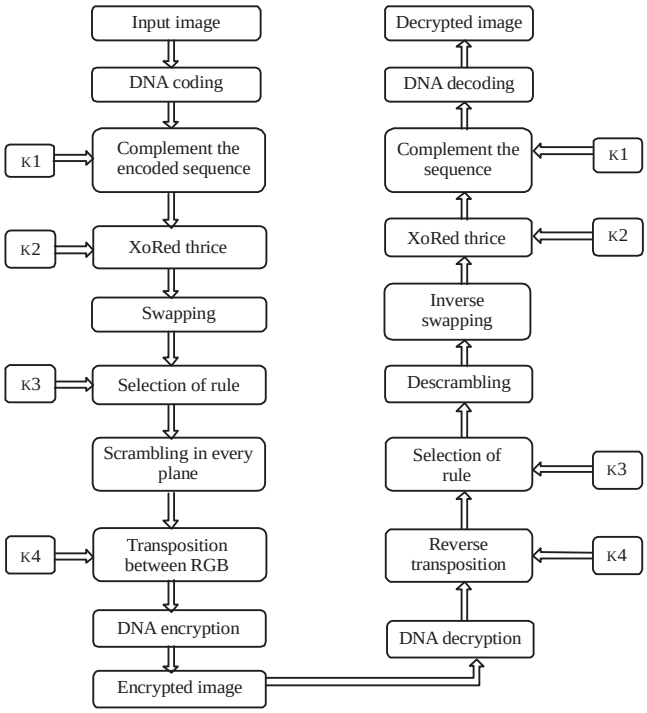

Fig. 1: Proposed methodology

This sequence is not as such used through the encryption technique. It is multilevel discretized to form binary sequence which is further used. In case of knights move encryption this multilevel discretization is done in four stages and a dibit is generated. Out of the dibit the first bits are stored in a separate text file and second bits are stored in another file. This is further retrieved for manipulation of various factors such as km1, km2, Py and Pz.

Proposed methodology: The methodology that is proposed in this paper is that a combination of multiple encryption techniques such as DNA encryption and rule set based encryption. This is used in the order as DNA encryption-rule set based encryption-DNA encryption. An input image is initially separated into three separate planes and only then further encryption operation is performed. This standard is equally applicable to both RGB images and RGB medical images. The complete encryption and decryption algorithm is explained below in Fig. 1.

Encryption algorithm:

- Get the input image and extract the three color planes separately
- Convert the pixel values into binary and store them in an array
- This binary image is then DNA encoded
- Generate a sequence 'x' using logistic map as per Eq. 1 and using a threshold function convert it into a binary sequence

$$f(x) = \begin{cases} 0, 0 < x \le 0.5 \\ 1, 0.5 < x \le 1 \end{cases} \quad (2)$$

- Based on this binary sequence criterion the DNA coded image is complemented into respective codes. If f(x) = 0 then the value is not complemented and if f(x) = 1 then the value is complemented
- The DNA matrices are now decoded back to binary matrices and stored in 'X'
- A chaotic sequence using logistic map is produced and it is multilevel discretized into binary values. And it is stored in an array 'C'
- A XOR operation is performed between the matrix 'C' and 'X' and stored in 'V'
- Step 7 is repeated with different initial values and is again XORed with the output 'V'
- Step 7 and 8 are again repeated using another set of initial values
- In each plane every two pixels are selected in a random manner and they are swapped

- Using chaotic logistic mapping and multilevel discretization generate a dibit sequence and store first and second bits in two separate files
- Using this bit sequence generated, every 8 bits are taken and stored in a variable
- Out of these 8 bits four values are computed namely km1, km2, py, pz
- There are 8 possible knights move from a particular position. One of these 8 moves is chosen using km1
- Input from user is obtained for the number of times 'n', the rule is to be applied
- Every individual planes are scrambled using this rule and n
- Step 17 is repeated using km2 and n
- Using the values of py and pz and its respective rule set for each plane, the pixels are transpositioned between three planes
- Steps 1 to 11 are repeated again
- Hence the encrypted image is obtained

Decryption algorithm:

- The three different planes are inverse swapped
- Using the respective keys three steps of XOR is performed
- They are DNA encoded and complemented using the key
- It is again DNA decoded to obtain the binary matrix of values
- The encrypted image is reverse transposition between their respective planes
- Similarly reverse scrambling is performed twice with the respective keys
- Steps 1-4 are repeated again and converted to decimal to form the original image

RESULTS AND DISCUSSION

For analysis of the encryption standard used here various RGB and colour medical images were taken and their diagonal, vertical and horizontal correlations, NPCR and entropy were calculated and compared with the results of (Tong *et al*., 2015; Kishore *et al*., 2014; Kester *et al*., 2013; Paul *et al*., 2013; Dascalescu *et al*., 2013; Diaconu *et al*., 2014; Delei *et al*., 2008; Lei *et al*., 2010) and the values were intact the encryption schemes in the available literature. Considering the colour DICOM images 1 and 2 from the Table 2, the encryption metrics such as correlation, NPCR and entropy of the proposed scheme was found to better than (Liu *et al*., 2014; Kanso and Ghebleh, 2015).

Table 2: Metrics of different sample images

Image/metrics	Diagonal correlation	Horizontal correlation	Vertical correlation	NPCR	Entropy
Colormedical1. dcm	-0.0030	0.0069	-0.0037	100.00	7.999
Liu *et al*. (2014)	0.00022	0.0036	-0.0012	99.54	7.987
Colormedical2. dcm	0.00024	-0.0047	-0.0025	100.00	7.9989
Kanso and Ghebleh (2015)	0.0043	0.00185	-0.00739	99.609	7.99
Img1. dcm	0.00124	-0.0016	-0.0018	100.00	7.9987
Lungs. dcm	-0.0027	0.0025	-0.000477	100.00	7.9991
Baboon. jpg	-0.0026	0.0058	0.00079	100.00	7.9999

NPCR: Number of pixels change rate

Correlation: The correlation is found out between two pixel values in an image so as to determine the quality of the encryption technique applied to the image. This correlation can be calculated for an encrypted image diagonally, vertically and horizontally along their adjacent pixels and they are respectively termed as diagonal, vertical and horizontal correlation. As far the correlation values are lesser the encryption methodology can be claimed as better efficient. In order to calculate the correlation we need to find out mean, variance and covariance. Then the correlation is found out using the following Eq. 3-6.

Correlation coefficient:

$$r(x,y) = \frac{\text{cov}(x,y)}{\sqrt{V(x)+V(y)}} \tag{3}$$

Covariance:

$$\text{cov}(x,y) = \frac{1}{n}\sum_{i=1}^{n} E[(x(i)-E(x))\,(y(i)-E(y)] \tag{4}$$

Variance:

$$V(x) = \frac{1}{n}\sum_{i=1}^{n}\left[x(i)-E(x)\right]^2 \tag{5}$$

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

Mean:

$$\text{Mean, } E(x) = \frac{1}{n}\sum_{i=1}^{n} x(i) \tag{6}$$

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

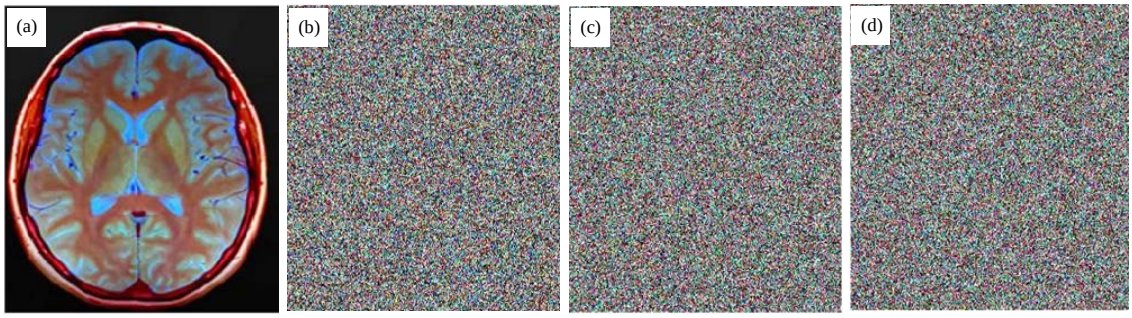

Fig. 2(a-d): (a) Input image, (b) DNA encrypted image, (c) Knights move encryption and (d) Final encrypted image

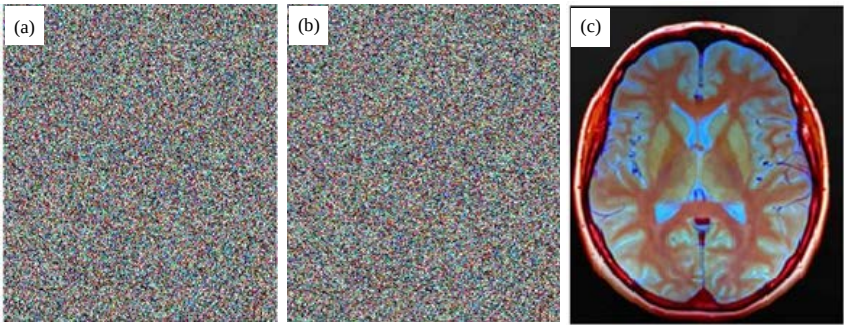

Fig. 3(a-c): (a) DNA decryption, (b) Knightsmove decryption and (c) Final decrypted image

The correlation values are found to be minimum or negative for different values. It has also been compared with (Liu *et al*., 2014; Kanso and Ghebleh, 2015) and the results are found superior.

Number of pixels change rate: The number of changing pixel rate is commonly used tool to evaluate the strength of the encrypted image subject to certain differential attacks. i.e., the higher value of NPCR, higher the security of the algorithm against differential attacks. The NPCR is calculated using the following Eq. 7:

$$NPCR = \left(\frac{1}{n}\sum_{i=0}^{n-1} d_i\right)\times 100\% \quad (7)$$

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

$$d_i = 0 \text{ If } X_i^2 = Y_i^2$$

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

The NPCR values for different sample images are found to be 100 in this paper as compared to (Liu *et al*., 2014; Kanso and Ghebleh, 2015).

Information entropy: Information entropy is the average amount of information from an event. The H(X) is the represent the information entropy, X = information source and L = Length of the information.

$p(x_i)$ is the probability of x_i:

$$H(X) = \sum_{i=0}^{i=L-1} p(x_i)\log_2 p(x_i) \quad (8)$$

The entropy of this algorithm is calculated and is determined to be efficient when compared with different algorithms.

Four different colour medical images and one RGB image were taken and the above mentioned metrics were calculated and results are shown below in Table 2.

Figure 2a provides the original DICOM image. Then the four encryption stages for a colour medical image are given in Fig. 2b-d, respectively. Initially it is DNA encrypted then knights move encryption is applied and finally again DNA encryption is performed to obtain the final encrypted image.

At the decryption the three stages are obtained. Initially DNA decryption is given in Fig. 3a, then knights move decryption is given in Fig. 3b and then again DNA encryption is performed to obtain the final decrypted image as in Fig. 3c.

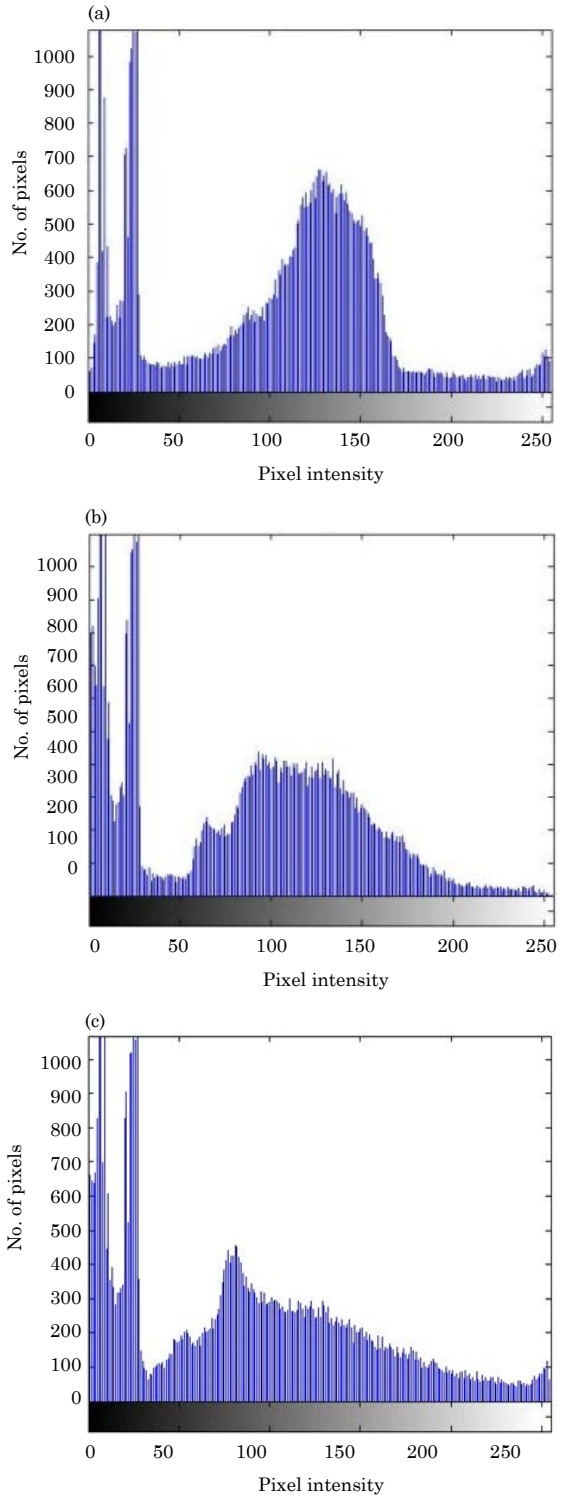

Fig. 4(a-c): Histogram of (a) Red, (b) Green and (c) Blue planes of the original images

The histograms of every planes of original image and the encrypted image are shown below. The histogram of original image planes (R, G and B) are shown in Fig. 4a-c. and the encrypted image planes are shown in Fig. 5a-c. it is seen that the encrypted image has its pixel values evenly distributed with a range of intensity values. Hence, it is well encrypted.

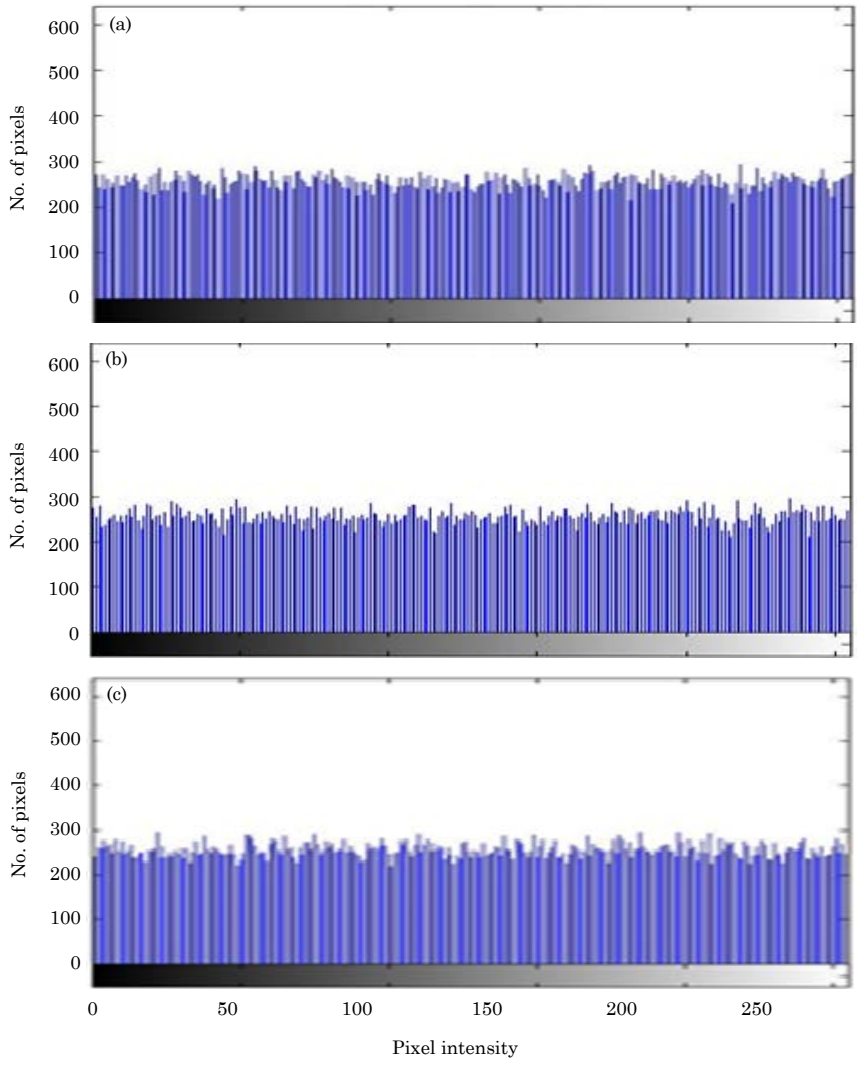

Fig. 5(a-c): Histogram of (a) Red, (b) Green and (c) Blue planes of the encrypted images

CONCLUSION

In the present study a technique for encryption was proposed using a combination of DNA encryption, digital image scrambler using knights move and chaotic logistic mapping. It has been desisted that this encryption standard is more apt for color images and for color medical images. The result analysis has been done for various parameters such as diagonal, vertical and horizontal correlation, NPCR, information entopy and histograms. It has been compared with few other previously existing algorithms and the results are found to better efficient. Thus this methodology serves to be a another alluring one with respect to numerous techniques available.

REFERENCES

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

Ahmad, M. and O. Farooq, 2010. A multi-level blocks scrambling based chaotic image cipher. Proceedings of the 3rd International Conference on Contemporary Computing, August 9-11, 2010, Noida, India, pp: 171-182.

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

Belazi, A., H. Hermassi, R. Rhouma and S. Belghith, 2014. Algebraic analysis of a RGB image encryption algorithm based on DNA encoding and chaotic map. Nonlinear Dyn., 76: 1989-2004.

Borujeni, S.E. and M. Eshghi, 2009. Chaotic image encryption design using Tompkins-Paige algorithm. Math. Prob. Eng. 10.1155/2009/762652

Chen, J.X., Z.L. Zhu, C. Fu, H. Yu and L.B. Zhang, 2015. An efficient image encryption scheme using gray code based permutation approach. Opt. Lasers Eng., 67: 191-204.

Dascalescu, A.C., R.E. Boriga and A.V. Diaconu, 2013. Study of a new chaotic dynamical system and its usage in a novel pseudorandom bit generator. Math. Problems Eng. 10.1155/2013/769108

Delei, J., B. Sen and D. Wenming, 2008. An image encryption algorithm based on knight tour and slip encryption-filter. Proceedings of the International Conference on Computer Science and Software Engineering, December 12-14, 2008, Wuhan, China, pp: 251-255.

Diaconu, A.V. and K. Loukhaoukha, 2013. An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher. Math. Prob. Eng. 10.1155/2013/848392

Diaconu, A.V., A. Costea and M.A. Costea, 2014. Color image scrambling technique based on transposition of pixels between RGB channels using knight's moving rules and digital chaotic map. Math. Problems Eng. 10.1155/2014/932875

Jain, S. and V. Bhatnagar, 2014. Bit based symmetric encryption method using DNA Sequence. Proceedings of the 5th International Conference on the Next Generation Information Technology Summit (Confluence), September 25-26, 2014, Noida, pp: 495-498.

Kanso, A. and M. Ghebleh, 2015. An efficient and robust image encryption scheme for medical applications. Commun. Nonlinear Sci. Numer. Simul., 24: 98-116.

Kester, Q.A., L. Nana, A.C. Pascu and S. Gire, 2013. A new encryption cipher for securing digital images of video surveillance devices using diffie-hellman-MD5 algorithm and RGB pixel shuffling. Proceedings of the European Modelling Symposium, November 20-22, 2013, Manchester, UK., pp: 305-311.

Kishore, P.V.V., N. Venkatram, C. Sarvya and L.S.S. Reddy, 2014. Medical image watermarking using RSA encryption in wavelet domain. Proceedings of the 1st International Conference on Networks and Soft Computing, August 19-20, 2014, Guntur, pp: 258-262.

Lei, Z.K., Q.Y. Sun and X.X. Ning, 2010. Image scrambling algorithms based on knight-tour transform and its applications. J. Chin. Comput. Syst., 5: 44-44.

Li, S., Y. Zhao, B. Qu and J. Wang, 2013. Image scrambling based on chaotic sequences and Veginere cipher. Multimedia Tools Applic., 66: 573-588.

Liu, G., J. Li and H. Liu, 2014. Chaos-based color pathological image encryption scheme using one-time keys. Comput. Biol. Med., 45: 111-117.

Loukhaoukha, K., J.Y. Chouinard and A. Berdai, 2012. A secure image encryption algorithm based on Rubik's cube principle. J. Electr. Comput. Eng. 10.1155/2012/173931

Paul, A., N. Das, A.K. Prusty and C. Das, 2013. RGB image encryption by using discrete log with and Lorenz's chaotic function. Proceedings of the 4th International Conference on Computer and Communication Technology, September 20-22, 2013, Allahabad, pp: 199-204.

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, 2015a. 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, 2015b. 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, 2015c. Triple chaotic image scrambling on RGB: A random image encryption approach. Secur. Commun. Networks. 10.1002/sec.1257

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. Logic elements consumption analysis of cellular automata based image encryption on FPGA. Res. J. Inform. Technol., 6: 291-307.

Som, S., A. Kotal, A. Chatterjee, S. Dey and S. Palit, 2013. A colour image encryption based on DNA coding and chaotic sequences. Proceedings of the 1st International Conference on Emerging Trends and Applications in Computer Science, September 13-14, 2013, Shillong, pp: 108-114.

Tong, X.J., Z. Wang, Y. Liu, M. Zhang and L. Xu, 2015. A novel compound chaotic block cipher for wireless sensor networks. Commun. Nonlinear Sci. Numer. Simul., 22: 120-133.

Wang, Q., Q. Zhang and X. Wei, 2010. Image encryption algorithm based on DNA biological properties and chaotic systems. Proceedings of the 5th International Conference on Bio-Inspired Computing: Theories and Applications, September 23-26, 2010, Changsha, pp: 132-136.

Wang, X. and J. Zhang, 2008. An image scrambling encryption using chaos-controlled poker shuffle operation. Proceedings of the IEEE International Symposium on Biometrics and Security Technologies, April 23-24, 2008, Islamabad, Pakistan, pp: 1-6.

Wang, Y.Y., B. Sen and D. Wenming, 2012. An encryption algorithm by scrambling image with sudoku grids matrix. Adv. Mater. Res., 433-440: 4645-4650.

Wu, Y., S.S. Agaian and J.P. Noonan, 2012. Sudoku associated two dimensional bijections for image scrambling. http://arxiv.org/pdf/1207.5856v1.pdf.

Yunpeng, Z., Z. Yu, W. Zhong and R.O. Sinnott, 2011. Index-based symmetric DNA encryption algorithm. Proceedings of the 4th International Congress on Image and Signal Processing, Volume 5, October 15-17, 2011, Shanghai, pp: 2290-2294.

Zhang, Q., X. Xue and X. Wei, 2012. A novel image encryption algorithm based on DNA subsequence operation. Scient. World J. 10.1100/2012/286741

Zou, Y., X. Tian, S. Xia and Y. Song, 2011. A novel image scrambling algorithm based on Sudoku puzzle. Proceedings of the 4th International Congress on Image and Signal Processing, October 15-17, 2011, Shanghai, China, pp: 737-740.