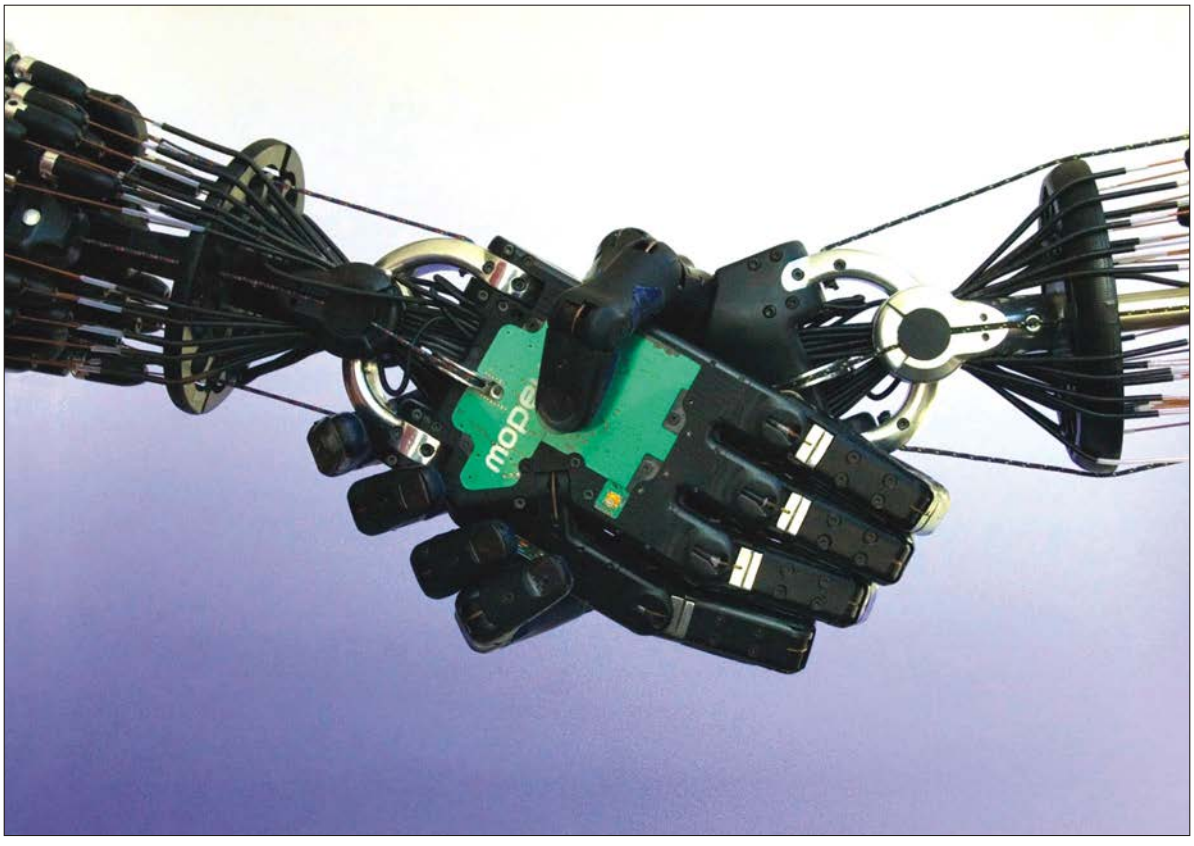

Journal of Artificial Intelligence

ISSN 1994-5450

science alert

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

Journal of Artificial Intelligence 7 (3): 123-135, 2014
ISSN 1994-5450 / DOI: 10.3923/jai.2014.123.135

Image Encryption: An Information Security Perceptive

[1]Narasimhan Aarthie and [2]Rengarajan Amirtharajan
[1]School of Computing, SASTRA University, Thanjavur, Tamil Nadu, India
[2]School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Corresponding Author: Rengarajan Amirtharajan, School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

ABSTRACT

Information security purported, yet another retrospected technique for secret sharing, highlighted by image encryption. Encryption of images is proven a successful method to communicate confidential information for which countless procedures are unearthed. Still, it continues attracting researchers as usage of images in every means of digital communication has phenomenally increased. Cryptography embraces various encryption methods and offers four chief modes where each one has found its place in many journals. This study takes cryptographic Cipher Block Chaining (CBC) mode as the fundamental footing which is manipulated in a unique fashion to achieve the goal. This script is coalescing of both Steganography and Cryptography thus ensuring enhanced security. Tentative results testify the routine and thus making it more upright of previously existing image encryption techniques.

Key words: Data security, CBC, Cryptography, image encryption

INTRODUCTION

Information security is the most common word uttered by any man any device or any peripheral since past two centuries. Protection from malicious sources has become a part of the invention or the discovery cycle. Myriad methods of protection are used ranging from a simple authentication password to most complex Cryptography (Amirtharajan and Rayappan, 2013) or Steganography algorithms (Amirtharajan *et al*., 2013a-j; Cheddad *et al*., 2010; Janakiraman *et al*., 2014a, b; Luo *et al*., 2011; Praveenkumar *et al*., 2014a-m, 2012a, b; Rajagopalan *et al*., 2014a-e; Ramalingam *et al*., 2014a, b; Thanikaiselvan *et al*., 2012a-c, 2013a, b, 2014; Thenmozhi *et al*., 2012; Zhao and Luo, 2012) for hiding the extreme sensitive data. The other useful information security (Amirtharajan and Rayappan, 2012a, b, 2013) scheme for proving the ownership is through watermarking (Amirtharajan *et al*., 2012).

One such exclusive method for the data security and protection is the image encryption (Akhshani *et al*., 2012; Amin *et al*., 2010; Diaconu and Loukhaoukha, 2013). The definition is quite simple from the terms, encryption meaning the data or bits of any particular source are changed in a definite pattern which is known to only sender and receiver. This is generally done with normal bits of any passwords or Secure SSL encryption systems. But the concept of introducing the similar encryption algorithm on an image creates a revolution in the field secret message transfer through images.

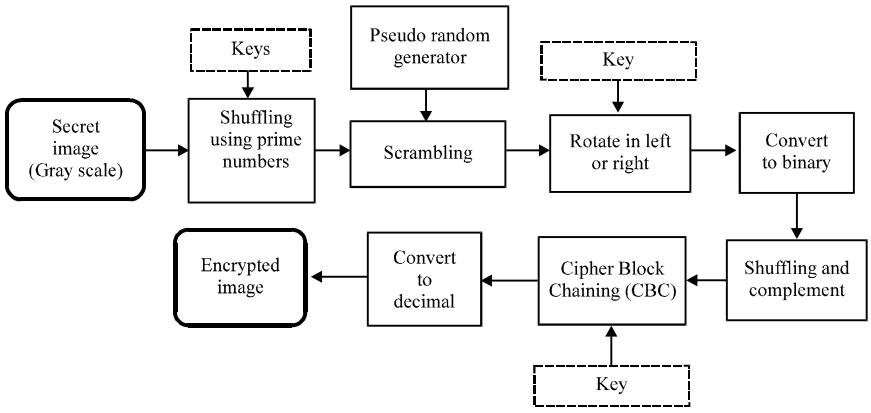

Fig. 1: Block diagram for proposed method

Image encryption works on the innovative idea of taking the consecutive or random pixel bits of an image and collectively worked and modified with logic, thereby leading to a complete set of new of pixel, which is typical from the original bits (Huang and Zhang, 2013; Luo *et al*., 2011; Wang *et al*., 2011; Xu *et al*., 2012; Yang *et al*., 2010a, b; Ye, 2010). Hence, giving rise to a new mode of information transfer. A further complication can be added to the malignant attacker, by incorporating the CBC (Cipher Block Chaining) method by which the plain text is monumentally embedded in the encrypted image, thereby making the data transfer very secure. A further addition of a key in the process makes the image tight/closed from any external agency.

The CBC (Cipher Block Chaining) works with the least complication of considering an N bit block of plain text and another M bit block of initialization vector and the bits of the N and M is "EXOR"ed. Thus, the EXORed bit represent a binary bit value resembling none like the original message. Hence a block of data, say M×N is obtained. Further, a secret key is added/embedded to the newly created plain text and initialization vector combination by using the Block Cipher Encryption. This would result in an encrypted cipher text or image as applicable.

This newly formed cipher text will act as the initialization vector for the next plain text block and then the cycle continues to produces a new piece of cipher text. Thereby, the image is completely covered in this process by three means, firstly RASTER SCAN wherein, the bits are horizontally taken and the scanning is done in the same fashion till the last line and hence the last pixel of the image. Secondly, using the VERTICAL SCAN method, wherein the columns are effectively taken and the pixel data are converted to cipher text. Finally, the random method, wherein the position is instantly determined and then cipher text is produced for that block of pixel that were considered.

The other two information security paradigms Steganography and watermarking are briefly explained in Amirtharajan and Rayappan (2013). The classification in image Steganography is available in Amirtharajan *et al*. (2012), Amirtharajan and Rayappan (2013) and Cheddad *et al*. (2010). Even though, this study address only in image encryption. If the encrypted confidential information (i.e., image) embedded in image Steganography, then it would heighten the security level manifold. For image Steganography, several authors suggested spatial domain as a good choice for high payload, if imperceptibility and robustness alone is of user's choice, then transform domain image Steganography would be the best candidate.

In this study, block diagram for proposed method is presented in Fig. 1 and the corresponding flowchart is given in Fig. 2.

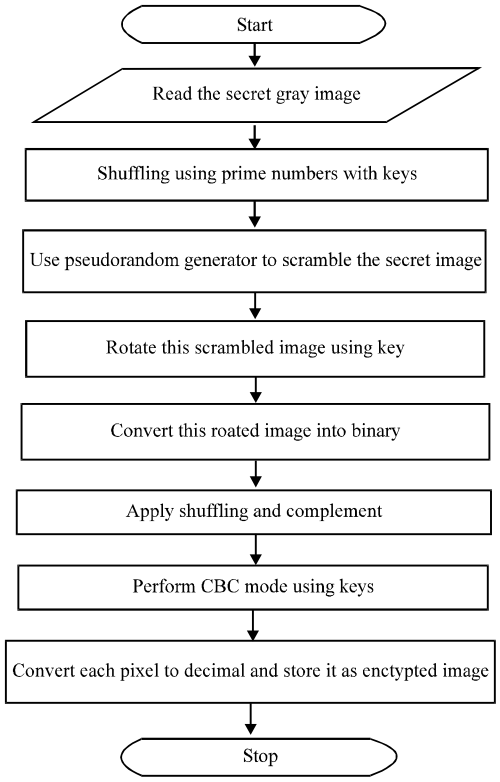

Fig. 2: Flowchart for proposed method

METERIALS AND METHODS

In this method, a new way of image encryption is presented. First, the secret gray image is scrambled using the run of prime numbers and pseudorandom generator, this increases the complexity of the algorithm. To make it more difficult to retrieve, CBC is introduced. To increase the security, intensity values are complemented. This provides better robustness in this system.

Encryption: Encryption is governed by:

$$Ci = Ek (Pi \otimes Ci\text{-}1)$$

$$C0 = IV \text{ (initialization vector)}$$

where, Ek is encryption key, Pi is plain text, Ci-1 is cipher text of the previous block of pixels and Ci is current cipher text.

Decryption works in the similar with a few modifications, wherein the cipher text is sent to the block cipher decryption for whose key is also an input. So, the key is used to decrypt the block of the data and then the data block is worked again with initialization vector and the plain text is de-embedding rather retrieved out of the cipher text.

Decryption: Decryption is governed by:

$$Pi = Dk (Ci \otimes Ci\text{-}1)$$

$$C0 = IV$$

where, Pi is plain text, Dk is decryption key, Ci is current cipher text and Ci-1 is previous cipher text.

Encryption algorithm:

- Read the secret image (gray image) with size 256×256
- Create the sequence of prime numbers, based on this, shuffle the image
- Again scramble the image with the help of pseudorandom generator
- Shift the resultant image right or left key times, then convert it into binary
- Perform bitwise complement in each pixel, prior to that shuffle each bit in every pixel
- Apply Cipher Block Chaining mode here, then change it into decimal again
- Once all the steps are performed, name the image as encrypted image

Decryption algorithm:

- Get the encrypted image, shift it in the reverse direction of encryption process
- Apply Cipher Block Chaining mode with their private and public keys and change every pixel into binary
- Take bitwise complement of every pixel and shuffle it as in transmitting process
- Descramble the image using pseudorandom generator and prime numbers
- Finally, original image is recovered

RESULTS AND DISCUSSION

For analysis, Mahatma Gandhi, Baboon, Lena and Kovil images are taken which are of dimension 256×256. The code is simulated in MATLAB 7.10. They are shown in Fig. 3-6. Apart from secret images, their two shuffled versions and the resultant encrypted images are also shown. First one is a scrambled version as per the code. Second one is the image as per the key defined by the user for shuffling the image. Histograms are also given for all the images for better understanding.

As far as randomness is considered, no third party can relate the resultant with the original. There is not even a single thing that relates the two images. Moreover, as the secret image gets scrambled twice, cryptanalysis becomes possible only if the invader knows about the tactics followed. Thus, the resultant output does not give a clue about the original components of the image or its pattern.

Histograms can also come under investigation in image encryption. It is vivid that for the original and two scrambled images, histograms follow a pattern; for encrypted version the case is flat. So, the algorithm is prone to examination based on frequencies. In order to prevent attacks, the need for distinct histograms is crucial. The pattern is spiky and has notable ups and downs in the first three, whereas in output, distinguishing cannot be done since it has no absolute variations.

Pixel correlation is most important of all the criteria since even a small clue can definitely be of great help in decrypting. It indicates the performance of the algorithm; in this study, all the three

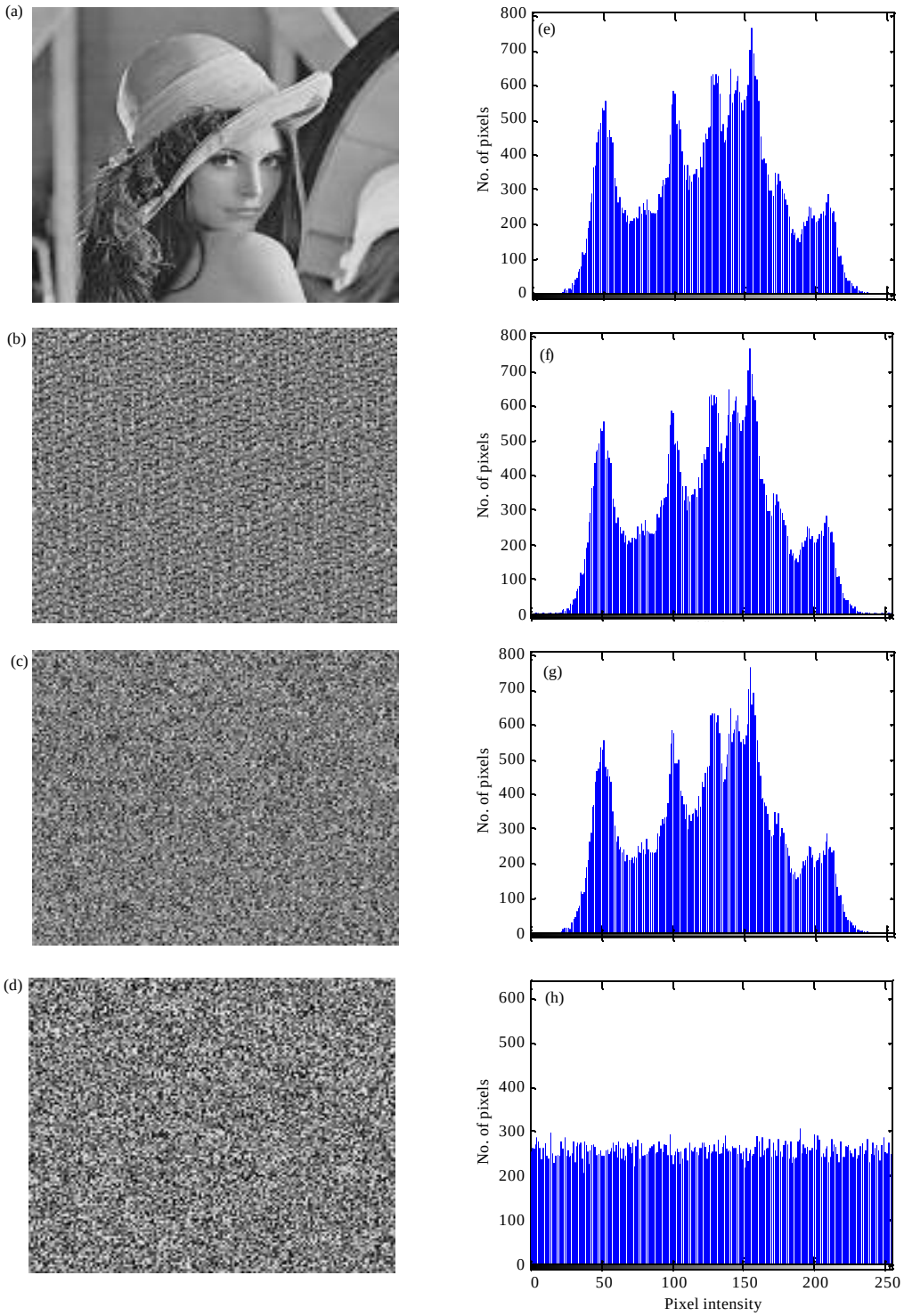

Fig. 3(a-h): (a, e) Secret image Lena and it's histogram, (b, f) First shuffled image and it's histogram, (c, g) Second shuffled image and it's histogram and (d, h) Encrypted image and it's histogram

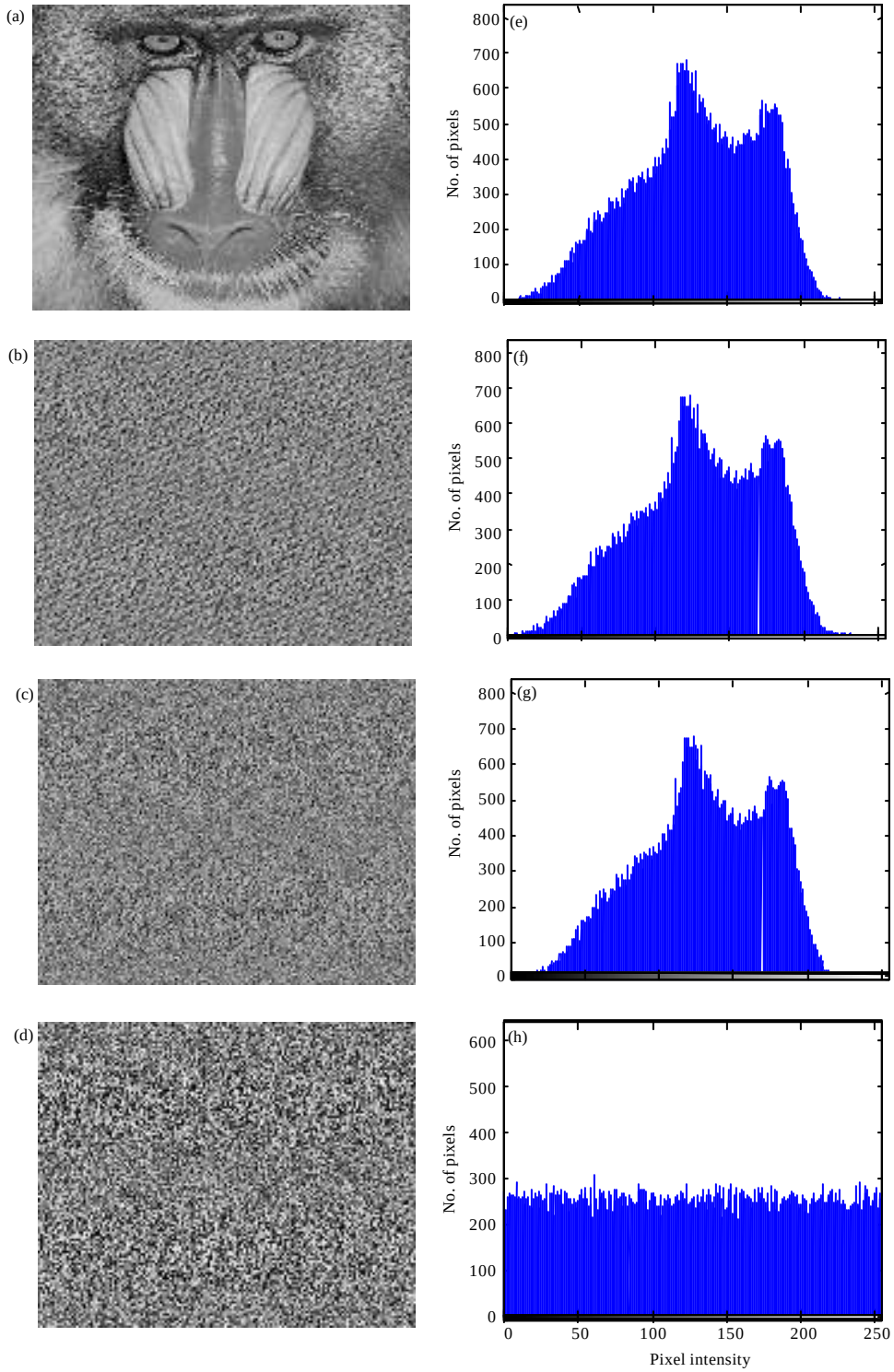

Fig. 4(a-h): (a, e) Secret image Baboon and it's histogram, (b, f) First shuffled image and it's histogram, (c, g) Second shuffled image and it's histogram and (d, h) Encrypted image and it's histogram

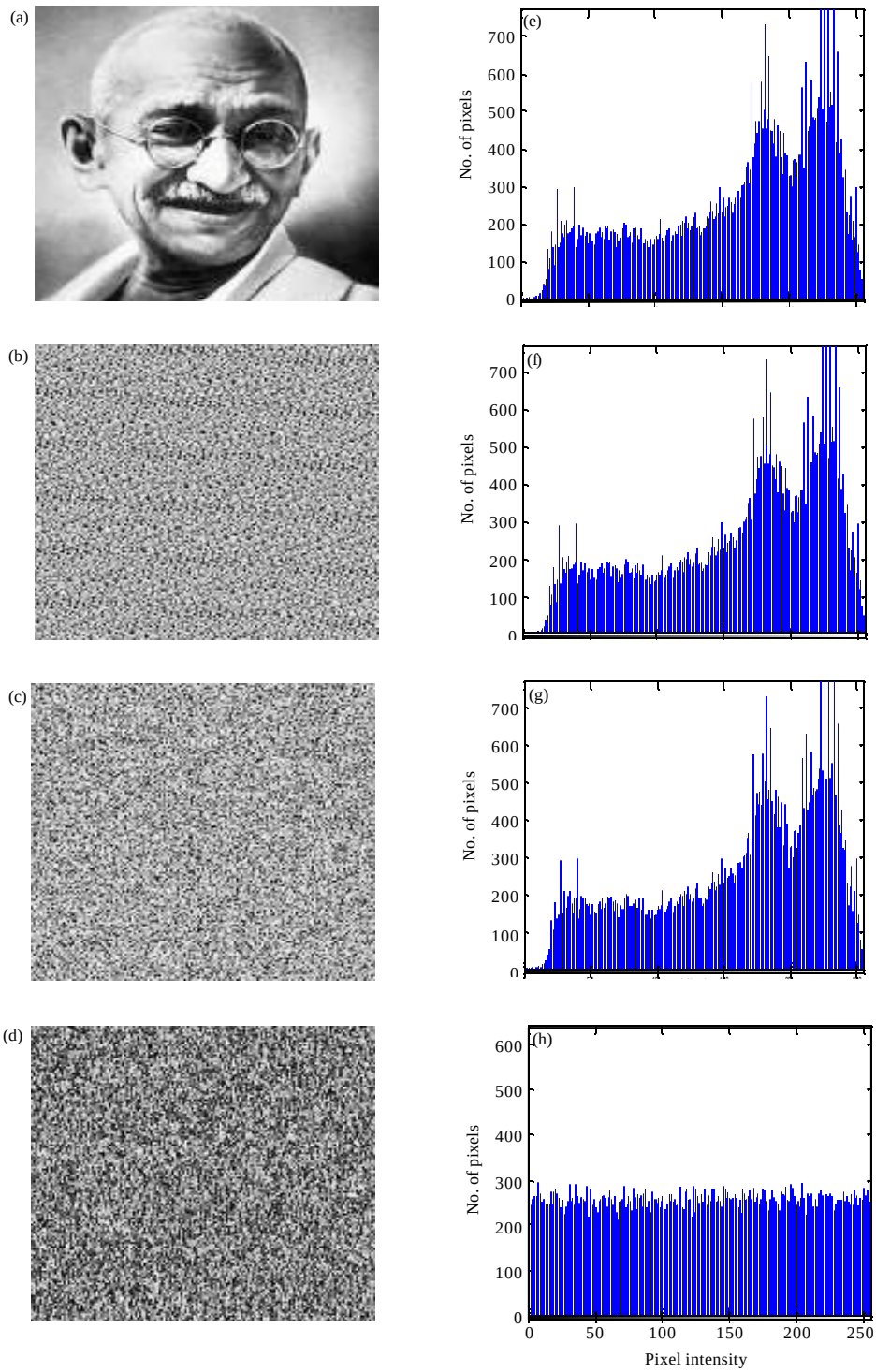

Fig. 5(a-h): (a) Secret image Gandhi and it's histogram, (b, f) First shuffled image and it's histogram, (c, g) Second shuffled image and it's histogram and (d, h) Encrypted image and it's histogram

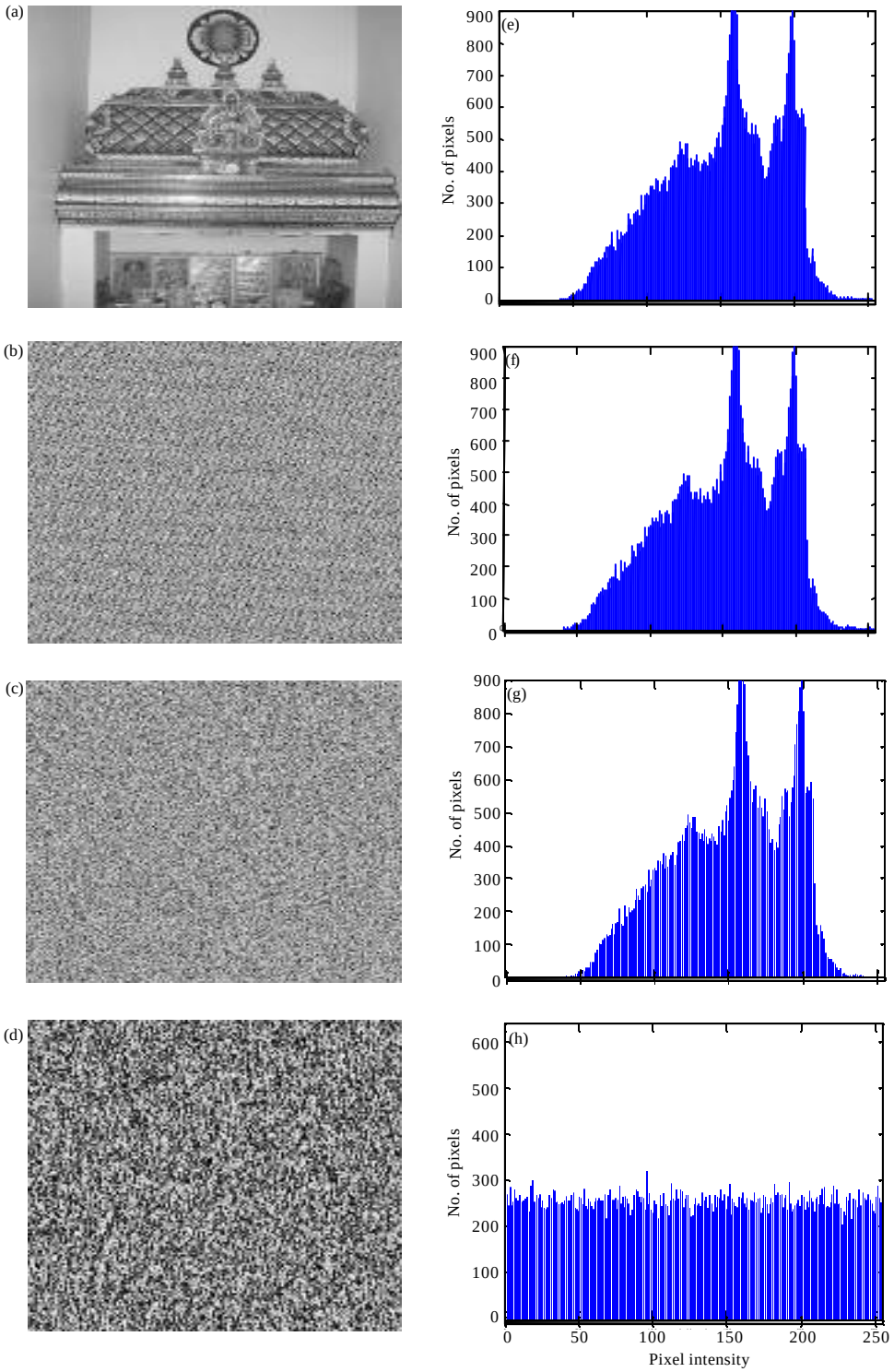

Fig. 6(a-h): (a) Secret image Kovil and it histogram, (b, f) First shuffled image and it's histogram, (c, g) Second shuffled image and it's histograms and (d, h) Encrypted image and it's histogram

correlation values are tabulated. A perfect encryption routine should give these values very far from 1 i.e., it should be as less as possible. Therefore, values of almost 0 are obtained which indicates there is absolutely no correlation between the pixels in all three patterns. So, this proposal possesses superior correlating properties which are very essential. The correlation coefficient is calculated by following equations:

$$r_{x,y} = \frac{\text{cov}(x,y)}{\sqrt{R(x)}\sqrt{R(y)}} \tag{1}$$

$$\text{cov}(x,y) = \sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{j=1}^{N}x_j)(y_i - \frac{1}{N}\sum_{j=1}^{N}y_j) \tag{2}$$

$$R(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{j=1}^{N}x_j)^2 \tag{3}$$

$$R(y) = \frac{1}{N}\sum_{i=1}^{N}(y_i - \frac{1}{N}\sum_{j=1}^{N}y_j)^2 \tag{4}$$

Security is the major concern and is measured by means of differential attack. A small change in pixel value can give deviated results which cannot be termed as a good encryption. This test is characterized by NPCR and UACI. Exposing all the images to this run, approximately 99% of first one and 33% of second parameter is observed which takes the pride of beneficial routine. As a result shown in Table 1, one is unable to study even the minute similarities existing between the images.

Besides these, three image metrics are also examined namely PSNR, BER and MSSIM. If BER of less than 35% is produced, then the routine is believed to be good. This study outperforms the other techniques by producing BER nearly 0.5 approximately for all the images which clears that the error is too small to be considered and thus making this mechanism very beneficial and efficient. The MSSIM gives the similarity test between the original and the resultant; if the value is closer to 1, there rendered high similarity. Since, this study exhibits MSSIM of much below 0.1, it escapes this test and does not even give a hint about this. The PSNR generally qualifies

Table 1: Experimental results for the proposed method (Amirtharajan *et al.*, 2013a)

	Secret image			Encrypted image							
Secret image	Vertical correlation	Horizontal correlation	Diagonal correlation	Vertical correlation	Horizontal correlation	Diagonal correlation	BER	PSNR	MSSIM	NPCR	UACI
Lena	0.9683	0.9383	0.9133	0.0262	-0.0089	-0.0064	0.5002	9.250	0.0089	99.6292	33.4985
	0.9699	0.9413	0.9155	0.0160	-0.0086	0.0044	0.5002	9.2391	0.0103	99.5758	33.6274
Baboon	0.6351	0.7133	0.6239	0.0542	-0.0044	0.0025	0.5008	9.530	0.0079	99.5972	33.3653
	0.6337	0.7121	0.6230	0.0433	-0.0087	-0.0022	0.5011	9.4977	0.0108	99.6262	33.6629
Mahatma Gandhi	0.9766	0.9752	0.9524	0.0029	-0.0094	-0.0079	0.4999	7.810	0.0065	99.5987	33.4264
	0.9767	0.9753	0.9526	0.0243	-0.0014	0.0016	0.5007	7.7745	0.0091	99.6033	33.6108
Kovil	0.8597	0.9139	0.8157	-0.0098	0.0072	0.0048	0.5001	9.360	0.0106	99.6399	33.6399
	0.8566	0.9113	0.8137	0.0247	-0.0039	-0.0091	0.4991	9.3307	0.0078	99.6002	33.6668

imperceptibility in images; since it is a encryption methodology, PSNR of about 9 vindicate that one cannot sense the relation between images and it is totally unpredictable about the surreptitious information.

CONCLUSION

In the field of information security, growth plays a main concern, growth means change, change starts when we think an innovative concept. In this study, we introduce one in the field of information security under image encryption topic. Image encryption can be defined in such a way that it is the process of encoding secret image with the help of some encryption algorithm in such a way that unauthorized users can't access it. This process, though sounds complicated, is very effective and easy implementation is the added feather to the advantage crown of image encryption with CBC incorporation. Though, the image through data encryption is completely distorted or unclear, the ultimate output i.e., the cipher text can be extra modified with the help of the key in picturing a more aesthetic image for the hacker which, when deeply checked, will not leave a single trace of the randomization that has been introduced to the image. Analytical results show that this proposal brags about its creation having improved security and complexity.

REFERENCES

Akhshani, A., A. Akhavan, S.C. Lim and Z. Hassan, 2012. An image encryption scheme based on quantum logistic map. Commun. Nonlinear Sci. Numer. Simul., 17: 4653-4661.

Amin, M., O.S. Faragallah and A.A. Abd El-Latif, 2010. A chaotic block cipher algorithm for image cryptosystems. Commun. Nonlinear Sci. Numer. Simul., 15: 3484-3497.

Amirtharajan, R., J. Qin and J.B.B. Rayappan, 2012. Random image steganography and steganalysis: Present status and future directions. Inform. Technol. J., 11: 566-576.

Amirtharajan, R. and J.B.B. Rayappan, 2012a. Brownian motion of binary and gray-binary and gray bits in image for stego. J. Applied Sci., 12: 428-439.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. Pixel authorized by pixel to trace with SFC on image to sabotage data mugger: A comparative study on PI stego. Res. J. Inform. Technol., 4: 124-139.

Amirtharajan, R. and J.B.B. Rayappan, 2013. Steganography-time to time: A review. Res. J. Inform. Technol., 5: 53-66.

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

Amirtharajan, R., G. Devipriya, V. Thanikaiselvan and J.B.B. Rayappan, 2013b. High capacity triple plane embedding: A colour stego. Res. J. Inform. Technol., 5: 373-382.

Amirtharajan, R., K. Karthikeyan, M. Malleswaran and J.B.B. Rayappan, 2013c. Kubera kolam: A way for random image steganography. Res. J. Inform. Technol., 5: 304-316.

Amirtharajan, R., K.M. Ashfaaq, A.K. Infant and J.B.B. Rayappan, 2013d. High performance pixel indicator for colour image steganography. Res. J. Inform. Technol., 5: 277-290.

Amirtharajan, R., M.V. Abhiram, G. Revathi, J.B. Reddy, V. Thanikaiselvan and J.B.B. Rayappan, 2013e. Rubik's cube: A way for random image steganography. Res. J. Inform. Technol., 5: 329-340.

Amirtharajan, R., P.S. Priya and J.B.B. Rayappan, 2013f. Pixel indicated user indicator: A muxed stego. Res. J. Inform. Technol., 5: 73-86.

Amirtharajan, R., R. Subrahmanyam, J.N. Teja, K.M. Reddy and J.B.B. Rayappan, 2013g. Pixel indicated triple layer: A way for random image steganography. Res. J. Inform. Technol., 5: 87-99.

Amirtharajan, R., S. Sulthana and J.B.B. Rayappan, 2013h. Seeing and believing is a threat: A visual cryptography schemes. Res. J. Inform. Technol., 5: 435-441.

Amirtharajan, R., S.D. Roy, N. Nesakumar, M. Chandrasekar, R. Sridevi and J.B.B. Rayappan, 2013i. Mind game for cover steganography: A refuge. Res. J. Inform. Technol., 5: 137-148.

Amirtharajan, R., V. Rajesh, P. Archana and J.B.B. Rayappan, 2013j. Pixel indicates, standard deviates: A way for random image steganography. Res. J. Inform. Technol., 5: 383-392.

Cheddad, A., J. Condell, K. Curran and P. Mc Kevitt, 2010. Digital image steganography: Survey and analysis of current methods. Signal Process., 90: 727-752.

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., Vol. 2013 10.1155/2013/848392.

Huang, F. and G. Zhang, 2013. A new image permutation approach using combinational chaotic maps. Inform. Technol. J., 12: 835-840.

Janakiraman, S., J. Chakravarthy, B. Radhakrishnan, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014a. Cover as key and key as data: An inborn stego. Inform. Technol. J., 13: 1969-1976.

Janakiraman, S., K.V.S.K. Kumar, R.R.K. Reddy, A. Srinivasulu, R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014b. Humming bird with coloured wings: A feedback security approach. Inform. Technol. J., 13: 2022-2026.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012a. Phase for face saving-a multicarrier stego. Proc. Eng., 30: 790-797.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2012b. Regulated OFDM-role of ECC and ANN: A review. J. Applied Sci., 12: 301-314.

Praveenkumar, P., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014a. Secret link through simulink: A stego on OFDM channel. Inform. Technol. J., 13: 1999-2004.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014b. Data puncturing in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2037-2041.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014c. Inserted embedding in OFDM channel: A multicarrier stego. Inform. Technol. J., 13: 2017-2021.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014d. Purposeful error on OFDM: A secret channel. Inform. Technol. J., 13: 1985-1991.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014e. Reversible steganography on OFDM channel-a role of RS coding. Inform. Technol. J., 13: 2052-2056.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014f. Spread and hide-a stego transceiver. Inform. Technol. J., 13: 2061-2064.

Praveenkumar, P., K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014g. Stego in multicarrier: A phase hidden communication. Inform. Technol. J., 13: 2011-2016.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014h. Coded crypted converted hiding (C^3H)-a stego channel. J. Applied Sci., 14: 1786-1797.

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

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2014j. Sub carriers carry secret: An absolute stego approach. J. Applied Sci., 14: 1728-1735.

Praveenkumar, P., R. Amirtharajan, R.S. Janani, K. Thenmozhi and J.B.B. Rayappan, 2014k. Multi (Carrier+Modulator) adaptive system: An anti fading stego approach. J. Applied Sci., 14: 1836-1843.

Praveenkumar, P., R. Deepak, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014l. Reversible steganography on OFDM channel: A role of cyclic codes. Inform. Technol. J., 13: 2047-2051.

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

Rajagopalan, S., H.N. Upadhyay, S. Varadarajan, J.B.B. Rayappan and R. Amirtharajan, 2014a. Gyratory assisted info hide-a nibble differencing for message embedding. Inform. Technol. J., 13: 2005-2010.

Rajagopalan, S., K. Pravallika, R. Radha, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014b. Stego on song-an amalgam of VI and FPGA for hardware info hide. Inform. Technol. J., 13: 1992-1998.

Rajagopalan, S., P.J.S. Prabhakar, M.S. Kumar, N.V.M. Nikhil, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014c. MSB based embedding with integrity: An adaptive RGB Stego on FPGA platform. Inform. Technol. J., 13: 1945-1952.

Rajagopalan, S., Y. Ravishankar, H.N. Upadhyay, J.B.B. Rayappan and R. Amirtharajan, 2014d. Modeling combo PR generator for Stego Storage Self Test (SSST). Inform. Technol. J., 13: 1936-1944.

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

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014a. LCC-LSB-FPGA stego-A reconfigurable security. J. Applied Sci., 14: 2139-2148.

Ramalingam, B., R. Amirtharajan and J.B.B. Rayappan, 2014b. Stego on FPGA: An IWT approach. Sci. World J. 10.1155/2014/192512

Thanikaiselvan, V., P. Arulmozhivarman, J.B.B. Rayappan and R. Amirtharajan, 2012a. Graceful graph for graceful security-towards a STE (G) Raph. Res. J. Inform. Technol., 4: 220-227.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012b. Horse riding and hiding in image for data guarding. Proc. Eng., 30: 36-44.

Thanikaiselvan, V., P. Arulmozhivarman, R. Amirtharajan and J.B.B. Rayappan, 2012c. Wavelet Pave the Trio travel for a secret mission: A stego vision. Global Trends Inform. Syst. Software Applic., 270: 212-221.

Thanikaiselvan, V., K. Santosh, D. Manikanta and R. Amirtharajan, 2013a. A new steganography algorithm against chi square attack. Res. J. Inform. Technol., 5: 363-372.

Thanikaiselvan, V., P. Arulmozhivarman, S. Subashanthini and R. Amirtharajan, 2013b. A graph theory practice on transformed image: A random image steganography. Sci. World J., Vol. 2013. 10.1155/2013/464107

Thanikaiselvan, V. , S. Subashanthini and R. Amirtharajan, 2014. PVD based steganography on scrambled RGB cover images with pixel indicator. J. Artif. Intell., 7: 54-68.

Thenmozhi, K., P. Praveenkumar, R. Amirtharajan, V. Prithiviraj, R. Varadarajan and J.B.B. Rayappan, 2012. OFDM+CDMA+Stego=Secure communication: A review. Res. J. Inform. Technol., 4: 31-46.

Wang, Y., K.W. Wong, X. Liao and G. Chen, 2011. A new chaos-based fast image encryption algorithm. Applied Soft Comput., 11: 514-522.

Xu, S.J., X.B. Chen, R. Zhang, Y.X. Yang and Y.C. Guo, 2012. An improved chaotic cryptosystem based on circular bit shift and XOR operations. Phys. Lett. A, 376: 1003-1010.

Yang, H., K.W. Wong, X. Liao, W. Zhang and P. Wei, 2010a. A fast image encryption and authentication scheme based on chaotic maps. Commun. Nonlinear Sci. Numer. Simul., 15: 3507-3517.

Yang, X., X. Yu, Q. Zou and J. Jia, 2010b. Image encryption algorithm based on universal modular transformation. Inform. Technol. J., 9: 680-685.

Ye, G., 2010. Image scrambling encryption algorithm of pixel bit based on chaos map. Pattern Recognit. Lett., 31: 347-354.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. Technol. J., 11: 209-216.