Research Journal of Information Technology

ISSN 1815-7432

Academic
Journals Inc.

www.academicjournals.com

Research Journal of Information Technology 5 (3): 341-351, 2013
ISSN 1815-7432 / DOI: 10.3923/rjit.2013.341.351

Why Image Encryption for Better Steganography

Rengarajan Amirtharajan, P. Archana and J.B.B. Rayappan
School of Electrical and Electronics Engineering, SASTRA University, India

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

ABSTRACT

In this study, declared a new fangled methodology for image encryption using one of the cryptographic modes. The need for protection rises phenomenally with greater than before custom of internet and online communication. It is challenging and crucial to safeguard the information be it any multimedia file online and to check illegal entrée'. Naturally images play a huge role in doing so in so called cryptographic and steganographic techniques. The former is very primeval but interestingly is still in use and lends a helping hand to realize secret sharing. Of the various fruits of cryptographic techniques, image encryption is awe-inspiring having multiple proficiencies possessing countless platforms to explore. This paper paints yet another advantageous model to image encryption where the image undergoes exceptional echelon of shuffling, scrambling and encrypting customs with Cipher Block Chaining (CBC) cryptographic mode as the brain. The analytical results demonstrate that this proposal is unsurpassed in the grounds of Correlation, BER, UACI, NPCR, PSNR and MSSIM. The encrypted images and their corresponding histograms are publicized to prove the paper's purpose creation.

Key words: Cryptography, image security, image encryption, cipher block chaining

INTRODUCTION

Rapid progress in use of digital information and its communication indeed demands for ideal security mechanisms. Moreover, images, being an integral part of online communication, need highest assiduity (Cheddad *et al*., 2010b; Hmood *et al*., 2010a, b). Not only just meant for recreation and sharing, images have now become a necessitated mode of apportioning in diverse domains, be it, engineering, medical, satellite communicating, geographical and oceanic applications and research, computer science etc. Having referred that, exploiting images for sharing and distributing secrets is not a big surprise (Amirtharajan *et al*., 2012a, b; Stefan and Fabin, 2000).

Okay that image is very helpful in communicating confidential information (Amirtharajan and Rayappan, 2012a-d; Cheddad *et al*., 2010a). But how? Just like that it would not accommodate any hush-hush data. Various researches had been and have been going on to make this a possibility. Legion methodologies and practices are invented to do so by taking 'Cryptography' as blood-line. It is an art, can also be entitled as science, by making use of which clandestine messages are shared between end to end users. Since present day technologies have a new facet with amalgamation of other horizons, Cryptography is not an elision (Salem *et al*., 2011; Schneier, 2007). It has spread its wings in many notable fields of study; to quote some computer science, information security, engineering, mathematics etc.

A few eminent cryptographic routines are DES, AES, IDEA, HASH, SHA, Block and Stream Ciphers, Cryptographic modes (ECB, CBC etc.), RSA, Pseudo random sequence generators and many more (Schneier, 2007). This encryption paper uses CBC (Amirtharajan *et al.*, 2012a) as backbone; it is for block ciphers where XOR operation is performed on plaintext with cipher text before getting encrypted. Feedback register is used to store the result; to make the message distinct from others, Initialization vector is used. Interesting fact here is that a single key can be used to encrypt surplus messages. Features of CBC like speed, cipher text is a block longer than that of plaintext, no pre-processing, un-parallelizable encryption, parallelizable decryption, fault-tolerance, unrecoverable synchronization error are worth mentioning (Stallings, 2010a, b). As a result, CBC finds its way in cryptographic mechanisms involving images that too mainly for image encryption. Encryption is one among a few modes that insures stability by inexplicably maximizing the probability of acknowledging that hush-hush information is truly enciphered (Schneier, 2007). Such encrypted images showing no sign of secret in it has jaw-dropped many. An interesting part here is that besides image, audio and video too can be taken advantage of and are in use at present (Zaidan *et al.*, 2010). Thus, image encryption has the power to hold out deliberate third party attacks while still maintaining haphazard arrangement on count. No doubt that image encryption has stretched its technical boundaries (Zhang and Liu, 2011; Zhu *et al.*, 2011).

Amin *et al.* (2010) proposed an image cryptosystems through chaotic block cipher algorithm for better security (Tong, 2013). Cheddad *et al.* (2010a) suggested a hash based image encryption for authentication. In addition there are several pixel based methods are reported in literature for image encryption (Hu and Han, 2009; Huang and Nien, 2009; Ye, 2010). Authentication based on image encryption reported by Yang *et al.* (2010). In image encryption, time taken to perform the process is reduced through fast image encryption algorithms (Wang *et al.*, 2011). Shyu (2009) suggested random grids based image encryption.

The cardinal maxims of encryption algorithms can be stated as mystification and dissemination. It can be said that the backbone of such algorithms is the key used in encryption in the source and decryption in the destination. So, it is vivid that the image encryption modus operandi is the blend of cryptography and steganography (Cheddad *et al.*, 2010b; Hmood *et al.*, 2010a, b). Having mentioned that, image encryption has pulled in numerous concepts in developing an algorithm. Above mentioned are inscrutable domains to explore. Image encryption is so vast that it is dug through versatile bailiwicks of engineering and mathematics. For instance, chaotic maps, permutation, correlation, statistical analysis, 3D baker maps, Phase and Magnitude manipulation, Matrix, SCAN patterns and many more (Amin *et al.*, 2010; Cheddad *et al.*, 2010b; Hu and Han, 2009; Huang and Nien, 2009; Shyu, 2009; Wang *et al.*, 2011; Yang *et al.*, 2010; Ye, 2010; Zhang and Liu, 2011; Zhu *et al.*, 2011).

There are other ways to preserve the confidential information, like image steganography (Amirtharajan and Rayappan, 2012a-d; Amirtharajan *et al.*, 2012a, b; Stefan and Fabin, 2000; Zhu *et al.*, 2011), watermarking (Stefan and Fabin, 2000; Zeki *et al.*, 2011; Zhang *et al.*, 2006) apart from Image encryption (Zhang and Liu, 2011; Zhu *et al.*, 2011). Image steganography is useful in hiding the confidential information of any digital media in spatial or transform domain co-efficient and watermarking is useful for copyright protection and authentication. But this paper deals only with image encryption.

PROPOSED METHOD

In the proposed algorithm of image encryption for a gray image, first we scramble the positions of the pixels in the plain image, then for this scrambled image we decompose pixel values into bits.

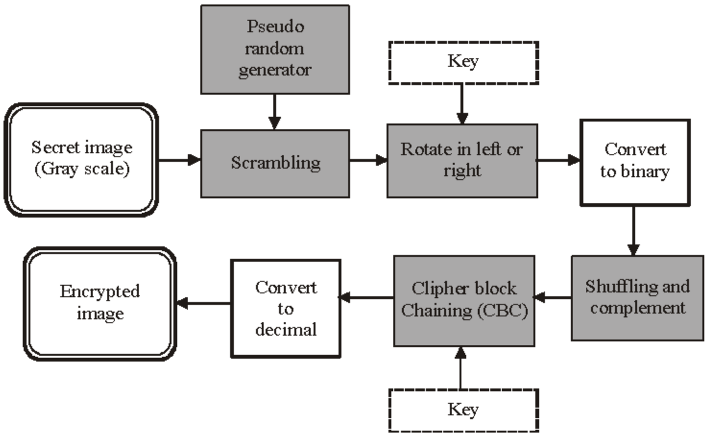

Fig. 1: Block diagram for proposed method

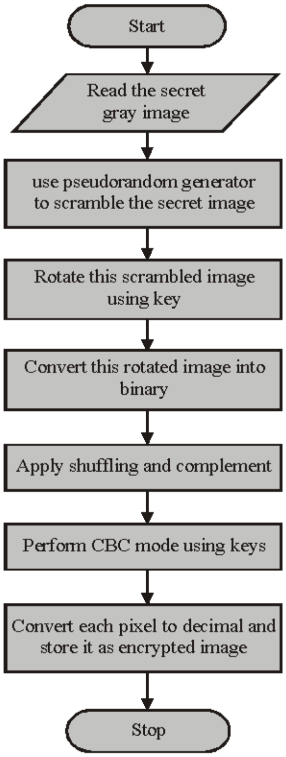
Start
Read the secret gray image
use pseudorandom generator to scramble the secret image
Rotate this scrambled image using key
Convert this rotated image into binary
Apply shuffling and complement
Perform CBC mode using keys
Convert each pixel to decimal and store it as encrypted image
Stop

Fig. 2: Flow chart for proposed method

For changing the intensity values we shuffle the bits in a particular order and convert to its respective decimal values. Then for this converted matrix we apply cipher block chain algorithm with a public key and a private key. To increase the complexity and security of the algorithm we also complement the intensity values. The algorithm is explained below in steps. The schematic diagram for this study is given in Fig. 1 and flowchart is given in Fig. 2.

Encryption algorithm

- Read the secret gray image of size 256×256
- Pseudorandom generator is initiated here to create the random sequence to scramble the secret image
- Rotate this scrambled image left or right key times, user only define this key
- Convert this rotated image into binary
- Then make a shuffle of each bit in every pixel of binary image and complement it
- Apply the most popular techniques in cryptography i.e., Cipher Block Chaining mode to the resultant shuffled image with their keys
- Then convert each pixel into decimal again
- Store the resultant image as encrypted image

Decryption algorithm

- Read the encrypted image
- Rotate the encrypted image in opposite direction to the direction which is rotated in encryption process
- Apply CBC with keys and convert it to binary
- Take complement to binary
- Shuffle the binary values as in encryption and convert it to decimal
- Using pseudorandom generator descramble the above values
- Store the resultant image as decrypted (original) image

RESULTS AND DISCUSSION

A perfect encryption algorithmic rule should stand for it in opposition to Cryptanalysis assails. Contrasting the conventional encryption methods, the requisites of digital encryption sound dissimilar. It does need cryptographic together with perceptual refuge. In this script, algorithm is run in MATLAB 7.1 with gray Lena as plain images which are of dimension 256×256 and their shuffled, encrypted versions and their corresponding histograms are shown in Fig. 3a-f, respectively. Tentative results for this study are depicted in Table 1.

In this script, algorithm is run in MATLAB 7.1 with gray Baboon as plain images which are of dimension 256×256 and their shuffled, encrypted versions and their corresponding histograms are shown in Fig. 4a-f, respectively.

In this script, algorithm is run in MATLAB 7.1 with gray Mahatma gandhi as plain images which are of dimension 256×256 and their shuffled, encrypted versions and their corresponding histograms are shown in Fig. 5a-f, respectively.

Table 1: Experimental results of image metrics obtained for image encryption

	Secret image			Encrypted image							
Secret image	Vertical correlation	Horizontal correlation	Diagonal correlation	Vertical correlation	Horizontal correlation	Diagonal correlation	BER	PSNR	MSSIM	NPCR image	UACI
Lena	0.9699	0.9413	0.9155	0.0160	-0.0086	0.0044	0.5002	9.2391	0.0103	99.5758	33.6274
Baboon	0.6337	0.7121	0.6230	0.0433	-0.0087	-0.0022	0.5011	9.4977	0.0108	99.6262	33.6629
Mahatma Gandhi	0.9767	0.9753	0.9526	0.0243	-0.0014	0.0016	0.5007	7.7745	0.0091	99.6033	33.6108
Kovil	0.8566	0.9113	0.8137	0.0247	-0.0039	-0.0091	0.4991	9.3307	0.0078	99.6002	33.6668

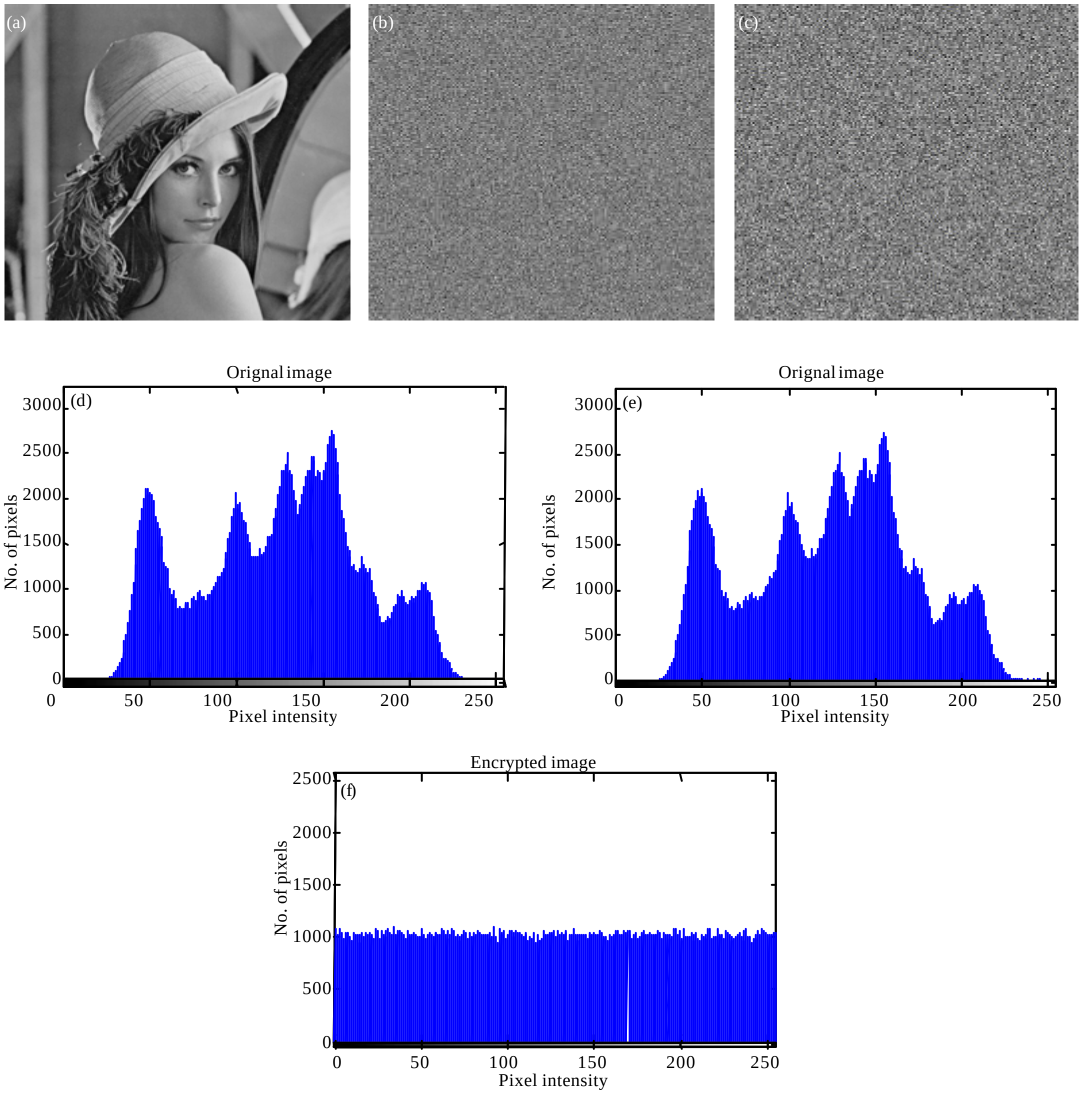

Fig. 3(a-f): (a) Lena, (b) Secret image shuffled image, (c) Encrypted image, Histogram of (d) Secret image, (e) Shuffled image and (f) Encrypted image

In this script, algorithm is run in MATLAB 7.1 with gray Kovil as plain images which are of dimension 256×256 and their shuffled, encrypted versions and their corresponding histograms are shown in Fig. 6a-f, respectively.

Stochasticity tests: Ergodic properties top the priorities of a consummate encryption model. Original and enciphered images are shown in figures which look absolutely absurd. Random literally mentions the processes bring forth identically detached and free-lance samples. The process is random if pragmatic value is determined through its position in sequence else through subsequent observations. Tentative outcomes suggest that this output produced in this paper is absolutely random giving no hint about the clandestine information.

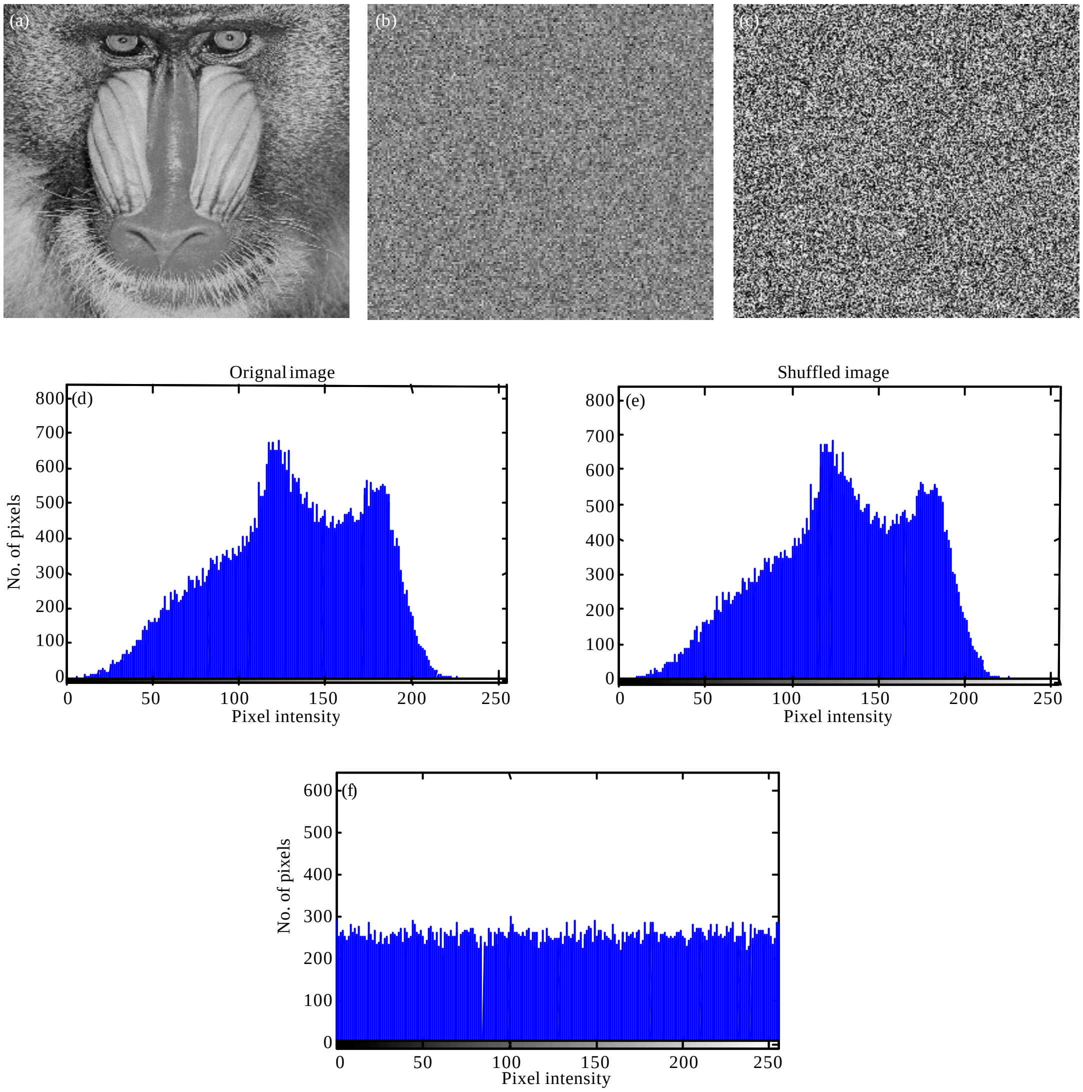

Fig. 4(a-f): Baboon (a) Secret image, (b) Shuffled image, (c) Encrypted image Histogram of (d) Secret image (e) Shuffled image (f) Encrypted image

Histogram tests: Histograms for pixels in all the four images are given. It is noticed that plain image histograms demonstrate a pattern whereas pixels distribution in encrypted version is flat. It signifies the fact that frequency investigation is unable to crack this algorithm. Also, in order to not letting the intruders to know about the covert information, it is mandatory that the histograms of original and end result remain statistically identical. Thus, in this paper encrypted histograms are appreciably unlike from their original ones. Plain histograms have huge cum spiky peaks trailed by jagged declines but the resultants comprise of homogenous variations.

Correlation of pixels: As the final outputs give the impression of being unsystematic, it is okay if third party expects zero correlation. As a matter of fact, pixel correlation is a key measure of performance in any image encryption algorithm. Here presented the values of all horizontal,

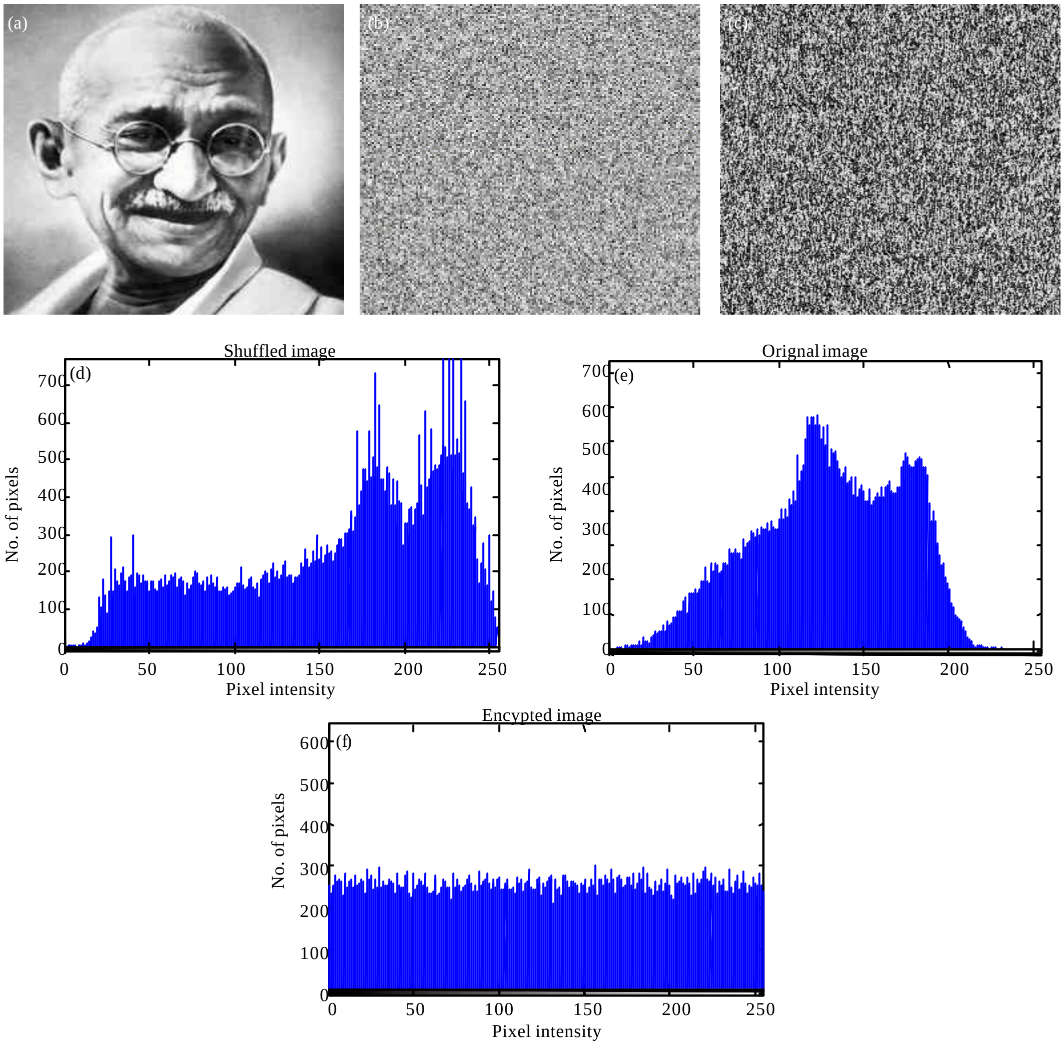

Fig. 5(a-f): Mahatma Gandhi, (a) secret image (b) shuffled image (c) encrypted image Histogram of (d) Secret image (e) Shuffled image and (f) Encrypted image

vertical and diagonal correlation among pixels in both plain and encrypted images. While for the former the correlation is nearly equal to 1 and almost 0 is the case for the latter. Thus plain images exhibit high correlation and encrypted images depict negligible correlation between adjacent pixel pairs in this study. The correlation coefficient is expressed by:

$$c = \frac{\text{cov}(i, j)}{\sigma_i \sigma_j}$$

where, σ = i and j's standard deviations, respectively cov(i, j) = Covariance of i and j.

Covariance is given as:

$$\text{cov}(i, j) = \frac{1}{N} \sum_{a=1}^{N} (i_a - \mu_i)(j_a - \mu_i)$$

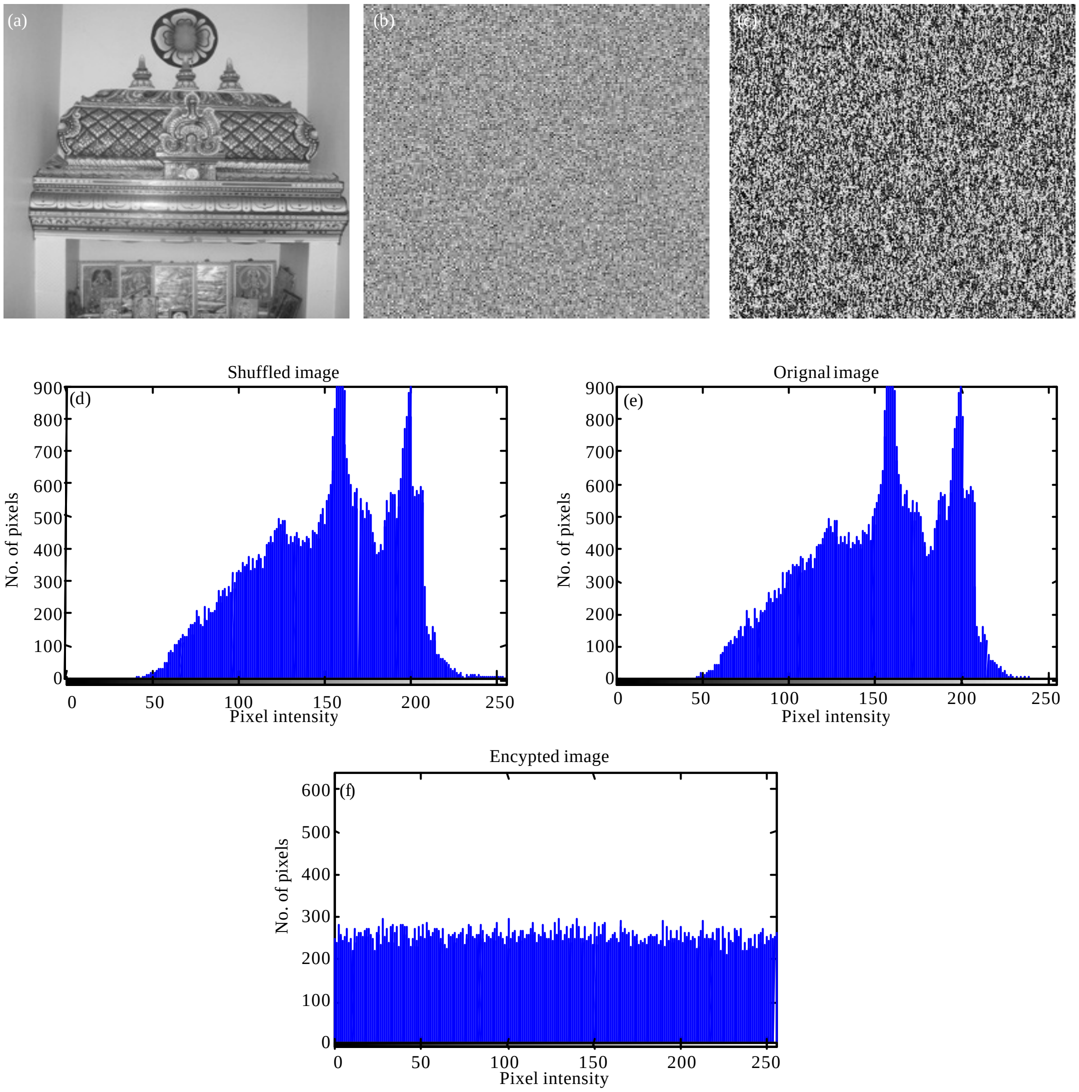

Fig. 6(a-f): Kovil: (a) Secret image (b) Shuffled image (c) Encrypted image Histogram of (d) Secret image (e) shuffled image (f) Encrypted image

Here, μ_i and μ_j are i and j's mean, respectively.

Differential attack: This index is to quantify the security of the algorithm. Here by altering a single pixel one can observe the subsequent resultant image. If there is any such change, then this run is said to be bungling and not viable. The two constraints involved in studying persuasion of a solitary pixel change are NPCR and UACI. Their expressions are given below:

$$\text{NPCR} = \frac{\sum i, j, k E(i, j, k)}{M \times N \times 3} \times 100\%$$

$$\text{UACI} = \frac{1}{M \times N \times 3} \frac{\left| E_1(i, j, k) E_2(i, j, k) \right|}{255} \times 100\%$$

This study is differential attack tested by exposing all the images which are of varying size. NPCR of approximately 99.6% and UACR of roughly 33.6% are witnessed in this paper which is fairly upright. Thus one cannot trace a small similarity between the original and resultant images. As a result, differential attack is not viable on this algorithm.

Image metrics: Making it ideal from the rest, this study is vindicated by BER, MSSIM and PSNR. These images have very less PSNR which signifies the fact that there is no relation between the original and the resultants. Moreover, the third party cannot predict that there is some confidential information contained in them. In simple, PSNR predicts the resemblance between two images which in this case is anticipated.

$$\text{PSNR} = 10\log_{10}\left(\frac{I_{\max}^2}{\text{MSE}}\right)\text{dB}$$

Mssim generally lies between -1 and 1; the nearer the value to 1 higher is the similarity between the images. The proposed model exhibits MSSIM of almost 0 that makes the paper take pride in security grounds. This means only trifling blunder is encountered by this algorithm which is for sure allowable and acceptable.

$$\text{MSSIM}(O,S) = \frac{1}{M}\sum\nolimits_{j=1}^{M}\text{SSIM}\left(O_j, S_j\right)$$

$$\text{SSIM}(X,Y) = \frac{(2\mu_O\mu_S + C1)(2\sigma_{OS} + C_2)}{\left(\mu_O^2 + \mu_S^2 + C_1\right)\left(\sigma_O^2 + \sigma_S^2 + C_2\right)}$$

Where:

$$C_1 = (K_1L)^2 L = 255$$

$$K_1 = 0.01C_2 = (K_1L)^2 L = 255K_2 = 0.03$$

$$\mu_O = \frac{1}{N}\sum\nolimits_{i=1}^{N} xi$$

μ_O is the estimate of the mean intensity of the cover (N = 255), σ_0 is the standard deviation

$$\sigma_O = \left(\frac{1}{N-1}\sum\nolimits_{i=1}^{N}(O_i - \mu_i)^2\right)\frac{1}{2}$$

$$\sigma_{OS} = \frac{1}{N-1}\sum\nolimits_{i=1}^{N}(O_i - \mu_O)(S_i - \mu_O)$$

Here σ_{OS} is correlation coefficient.

BER is also a performance criterion which tells about the error witnessed in the procedure. This proposal gives it approximately as 0.5 for all the images. It confirms there are almost 50% error rate.

CONCLUSION

This study introduces an inimitable image encryption model which takes Cipher Block Chaining Mode as the fundamental element and constructs further plots to achieve a secret sharing scheme. The algorithm takes advantage of dissemination and mystification via spoofing the secret image and with the help of keys and scrambling, the relation between the secret images and encrypted images is brought to zilch. The paper withstands some notable attacks namely differential, correlation, histograms to prove its creation for which simulation upshots are illustrated. It maximizes the efficiency by significantly improving the randomness among pixels and security as well. Experimental results confirm the practicality of this proposal. These features boost to put forward the paper as a pertinent and promising encryption algorithm. Since it is an image encryption routine, it does not bestow data expanding and thus is very much sensible to parameters having a good prognosis in information security.

REFERENCES

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

Amirtharajan, R. and J.B.B. Rayappan, 2012a. An intelligent chaotic embedding approach to enhance stego-image quality. Inform. Sci., 193: 115-124.

Amirtharajan, R. and J.B.B. Rayappan, 2012b. 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, 2012c. Inverted pattern in inverted time domain for icon steganography. Inform. Technol. J., 11: 587-595.

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

Amirtharajan, R., R. Anushiadevi, V. Meena, V. Kalpana and J.B.B. Rayappan, 2012b. Seeable visual but not sure of it. Proceedings of the IEEE-International Conference on Advances in Engineering, Science and Management, March 30-31, 2012, Nagapattinam, Tamil Nadu, India, pp: 388-393.

Cheddad, A., J. Condell, K. Curran and P.M. Kevitt, 2010a. A hash-based image encryption algorithm. Opt. Commun., 283: 879-893.

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

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010a. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hmood, A.K., H.A. Jalab, Z.M. Kasirun, B.B. Zaidan and A.A. Zaidan, 2010b. On the Capacity and security of steganography approaches: An overview. J. Applied Sci., 10: 1825-1833.

Hu, J. and F. Han, 2009. A pixel-based scrambling scheme for digital medical images protection. J. Network Comput. Appl., 32: 788-794.

Huang, C.K. and H.H. Nien, 2009. Multi chaotic systems based pixel shuffle for image encryption. Opt. Commun., 282: 2123-2127.

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inform. Technol., 3: 146-152.

Schneier, B., 2007. Applied Cryptography: Protocols, Algorithm and Source Code in C. 2nd Edn., Wiley, India.

Shyu, S.J., 2009. Image encryption by multiple random grids. Pattern Recognit., 42: 1582-1596.

Stallings, W., 2010a. Cryptography and Network Security: Principles and Practice. 5th Edn., Prentice Hall, USA.

Stallings, W., 2010b. Network Security Essentials: Applications and Standards. 4th Edn., Prentice Hall, USA.

Stefan, K. and A. Fabin, 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, London, UK.

Tong, X.J., 2013. Design of an image encryption scheme based on a multiple chaotic map. Commun. Nonlinear Sci. Numer. Simul., 18: 1725-1733.

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

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

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

Zaidan, B.B., A.A. Zaidan, A.K. Al-Frajat and H.A. Jalab, 2010. On the differences between hiding information and cryptography techniques: An overview. J. Applied Sci., 10: 1650-1655.

Zeki, A.M., A.A. Manaf and S.S. Mahmod, 2011. High watermarking capacity based on spatial domain technique. Inform. Technol. J., 10: 1367-1373.

Zhang, G. and Q. Liu, 2011. A novel image encryption method based on total shuffling scheme. Optics Commun., 284: 2775-2780.

Zhang, Y.H., B.S. Kang and X.F. Zhang, 2006. Image encryption algorithm based on chaotic sequence. Proceedings of the 16th International Conference on Artificial Reality and Telexistence-Workshops, November 29-December 1, 2006, Hangzhou, China, pp: 221-223.

Zhu, Z.L., W. Zhang, K.W. Wong and H. Yu, 2011. A chaos-based symmetric image encryption scheme using a bit-level permutation. Inf. Sci., 181: 1171-1186.