http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 13 (16): 2524-2533, 2014
ISSN 1812-5638 / DOI: 10.3923/itj.2014.2524.2533

Cryptic Cover for Covered Writing: A Pre-Layered Stego

Padmapriya Praveenkumar, K. Thenmozhi,
John Bosco Balaguru Rayappan and Rengarajan Amirtharajan
Department of Electronics and Communication Engineering,
School of Electrical and Electronics Engineering, SASTRA University, Thanjavur, Tamil Nadu, India

Abstract: Brobdingnagian may be the precise word for the usage of internet and advanced expertise in the globe in our day. Indeed, all sorts of this online communication go hand in hand with the so called major apprehension, information security. Since all kinds of digital files play an imperative role in internet operation, it is indispensable to defend the key features of private communication namely, seclusion, uprightness and legitimacy. This threat, in a roundabout way, has led to the breakthrough of information security rationales. Striking among these are Cryptography and Steganography, primordial skills pursued for the sake of secret sharing. The startling thing is that with the fruition of technology, these are giving prolific outcomes even now. Cryptography possesses such a litheness that its blend, in the company of other fields of study, facilitates offer much more options to explore security issues. This study envisions an inimitable approach to security in the context of encryption and embedding incorporating shuffling, chaotic equations in conjunction with Blowfish encryption algorithm. Here, encryption is performed on images followed by embedding secret data. The latter is done not literally but indirectly. This pitch endows with randomness and security with all the persuasive traits of encryption. Validation is given in terms of Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Relative Entropy (RE), entropy and correlation values. Experimental results are illustrated to vindicate the performance of this objective.

Key words: Cryptography, Steganography, image encryption, MSE, PSNR

INTRODUCTION

Riotous development in network communication and image processing lately has vastly increased handling of digital images online. Images, along with other digital files, have become an inherent part of computer communication which necessitate premier defense. It is said that they form the building block of various analyses in myriad domains, making most of them for secret sharing is definitely not unforeseen. They, at the present time, are of immense assistance in divvying off the record information.

To carry out the above and to make it a possibility, assortments of researches are being done with Cryptography as the lineage. Cryptography is an antique technique to share and communicate the hush-hush information without the knowledge and suspicion of others. It does not elision itself from updating itself with the help of up-to-the-minute know-how. Besides, it has extended horizons in some distinguished disciplines of study for instance mathematics, image processing, information and network security, computer science and so forth. Mentioned the key features of Cryptography, it is also noteworthy to mention the other approaches to defend the classified information (Praveenkumar *et al*., 2014a-n, 2013a-d, 2012a, b), such as image Steganography (Celik *et al*., 2005; Chang *et al*., 2008; Amirtharajan and Rayappan, 2012a-c, 2013; Amirtharajan *et al*., 2013a-j; Ni *et al*., 2006) and watermarking. While, the former focuses on masking the surreptitious message belonging to any digital medium within spatial or transform domain co-efficient (Ramalingam *et al*., 2014a, b; Rajagopalan *et al*., 2014a-d; Thanikaiselvan *et al*., 2012a-c, 2013a, b), the latter aims at copyright fortification and endorsement.

Encryption, by and large, is intended to indemnify stability as a result of enigmatically taking the full advantage of likelihood of conceding that furtive message is strictly enciphered (Encinas and Dominguez, 2006). As the so called encrypted messages or images do not give even a single inkling, this domain has caught the attention of many. Encrypted image differ from the plain image owing to elevated redundancy and bulk (data) capacity. Added gain in encryption is the fact that it supports all

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

sorts of digital files not particularly images. As a consequence, image encryption has got what it takes to proffer premeditated threats at the same time as upholding slapdash pact on count (Cheddad *et al*., 2010).

On account of custom, call for real-time inviolable transmission has been tremendously amplified for which loads of encryption plots are advised. To cite some unsurpassed examples, there are cryptosystems offering enhanced security via chaotic algorithms, promising authenticity with the help of hash-based encryption schemes (Norouzi *et al*., 2014; Seyedzade *et al*., 2010) myriad pixel-based techniques, hit and miss grid-based procedures, fast image encryption practices to decrease the computational time etc.

Of these, chaos based principles are evidence for a few remarkably sought-after properties in different grounds like security, efficiency, intricacy, viability etc. (Alvarez *et al*., 1999, 2000; Wei *et al*., 2012; Tong *et al*., 2009; Wang *et al*., 2011; Yen and Guo, 2000; Zhu, 2012). There already have been projected, for instance, Line map, DES etc., but having a drawback of their incongruity to practical encryption because of images' inherent features. One more concern in image encryption conniving is the algorithm's processing speed since it is quite hard for customary ones to promptly baffle and strew large magnitude of (image) data.

Chaos, a cogitation of non-linear dynamic system, pertains to fickleness whose underlying principle is to hobble the pixel positions in an image (Zhu, 2012; Kumar and Ghose, 2011; Li and Zheng, 2002; Belkhouche and Qidwai, 2003; Borujeni and Eshghi, 2013; Chen *et al*., 2004). It is of great help to image encryption since it is highly arbitrary, non-periodic and turbulent. Chaotic image encryption generally exercises pixel confusion and diffusion. Its ultimate motto is to perform image encryption through pixel (value) shuffling followed by grey scale value altering (Huang *et al*., 2013; Huang and Nien, 2009; Zhang and Liu, 2011). At the moment, chaotic schemes are used far and wide, thanks to their acute compassion even to petite changes. They promise speed, safe and sound encryption modes. In this study, a detailed discussion is done on the amalgamation of shuffling, chaotic perception, encryption and embedding. Blowfish, in general, (symmetric) block cipher works on an erratic length key. It is very fast, compact and simple as it is very undemanding, it is defiant to implementation blunders. Above it is a most secure routine than the rest. It is more suitable and competent for hardware implementation. Less memory space is an added advantage of Blowfish. Image quality metrics are used to support encryption schemes (Mayache *et al*., 1998; Wang and Bovik, 2002).

To achieve the same, there are different maps namely Arnold's cat, Ginger breadman, Henon, Polynomia and Zaslavskii, etc. Arnold's cat map, a discrete system, widens and folds its trails in phase space and is a chaotic map from torus onto itself. Ginger Bread Man is a type of 2D piecewise linear algorithm. Being a discrete-time dynamical system, it was originally established as simplified model of the Poincaré section. Among the most recognized form of complex dynamic families, the quadratic polynomials are the most recognized ones. The Zaslavskii Map, introduced in 1978, is unpredictable by its spread spectrum characteristic.

A detailed study is done on existing methods and this plot differs significantly from the rest as it aims at an image encryption model by means of seven methods. Validation is given by the widely accepted image metrics and comparison of this study with the previous ones implies that the former is found better.

MATERIALS AND METHODS

Algorithms used in the proposed methodology

Blowfish encryption: Blowfish, a symmetric block cipher, works on varying key length usually from 32-448 bits to encrypt data of a 64 bit block. Bruce Schneier designed this Blowfish algorithm in 1993 which is permit-free and non-proprietary. It entails Feistel network consisting 16 rounds to encrypt data. The XOR gates and modular addition are employed to carry out operation lookup table as they minimizes the computing time. Moreover, this is applicable to an involuntary file encrypted and communication links. Blowfish is a faster mean for encryption than the rest but is very hard to apply to a cryptanalytic method.

Blowfish algorithm for image encryption:

- Partition Y in to two 32 bit halves as Y_L and Y_R
- For j = 1-16, carryout the following sequences:

$$Y_L = Y_L \oplus P_i$$
$$Y_R = F(Y_L) \oplus Y_R$$

- Switch Y_L and Y_R and carry out the following sequences:

$$Y_R = Y_R \oplus P_{17}$$
$$Y_L = Y_L \oplus P_{18}$$

- Combine Y_L and Y_R
- Partition Y_L into four eight-bit quarters namely 1, 2, 3, and 4 and carryout the following sequences:

$F(Y_L) = ((S1, 1+S2, 2 \bmod 232) \oplus S3,3)+S4, 4 \bmod 232)$

Decryption algorithm: Decryption algorithm is almost same as that of encryption with the exception of P-array values get reversed. Here, cipher text's first leftmost 32 bits are XORed with P18. Contrarily, this is performed in the encryption process with P1. Decryption method takes place for 16 rounds.

Chaotic process: Chaos, a dynamic system, depends greatly on initial stipulations which are impulsive and arbitrary. It encrypts images through pixel values shuffling and grey values altering to form ciphered images. It is done so using the following equation:

$$X (i+1) = \bmod (y (i) +1-1.4\times x (i)\times x (i),256) +1$$
$$y(i+1) = \bmod (0.3\times x(i)+0.7\times y(i)\times x(i),256)+1$$

where, x, y is pixel location, X and Y represent row and column, respectively. The transformation function maps (X, y) is fresh location.

Chaotic algorithm:

- Generate random values ranging from 0-255
- XOR these values with that of the image pixels by the forthcoming equation:

$$x(i+1) = \bmod (y(i)+1-1.4\times x(i)\times x(i),256)+1$$
$$y(i+1) = \bmod (0.3\times x(i)+0.7\times y(i)\times x(i),256)+1$$

- This changes the grey scale entities. These equations generate recursive random numbers and user is free to give the key that sets the initial values

Hennon shuffling: Henon shuffling, a discrete-time dynamic system, is Poincare section's abridged model which is expressed by:

$$Xn+1 = Yn+1-ax2n$$
$$Yn+1 = bXn$$

It, in turn, is given by:

$$F: (X, Y)\rightarrow(Y+1-aX2, bXn)$$

where, (x, y) is pixel location, X is row, y is column of the pixel. The transformation function maps (X, y) to a different location.

Shuffling algorithm: Change the pixel location through the transformation function:

$$X\rightarrow(Y+1-X2)$$
$$Y\rightarrow(3X)$$

This is repeated till all pixels get mapped to their corresponding new location. Poincare Recurrence Theorem defines that after a long period of time, some systems will come back to state close to that of the original. To a maximum, image can be shuffled 3r times since at this stage, original image is obtained.

In the methodology, image gets shuffled for 3r times and the moment, at which maximum horizontal and vertical correlation values arrive, offers the original image. In method 2, pixel intensity is swapped by the total shuffling iterations which is helpful in de-shuffling the image.

Data embedding: The histogram of the encrypted image is uniform and the ASCII values of the message, to be embedded, uses 8 bits. These two facts are keys to this method. The ASCII value of the each character of the message is searched for the matching gray scale value in the encrypted image, which is the cover image. Suppose, if the ASCII value is 98, all the rows and columns with gray scale value 98 are stored in two different arrays. Using randperm function or any user defined function, one can select a pair of row and column values corresponding to grayscale value '98'. The process is repeated for the next three characters. All the 4 rows and 4 columns which constitute 64 bits are formed into a block and encrypted using blowfish algorithm and a secret key.

If the message has more than four characters, key expansion is done and the cipher of the first four characters serves as input to the encryption of the next four characters. The procedure is repeated till all characters are completed. In case the number of characters is not a multiple of four, some dummy values are used to make it a multiple of 4. The resulting cipher is sent to the mail of the person intended to receive message. Since, no bit is changed in the encrypted cover image, its decryption would give the exact original image. To extract the message, the receiver must decipher the cipher sent to his mail using the shared secret key. To further improve security, the message to be embedded can be encrypted. For the same message if one repeats the entire procedure, he or she won't get the same cipher to be sent to the mail as the previously sent one i.e., same message gives different ciphers each time as the row and column number are randomly selected.

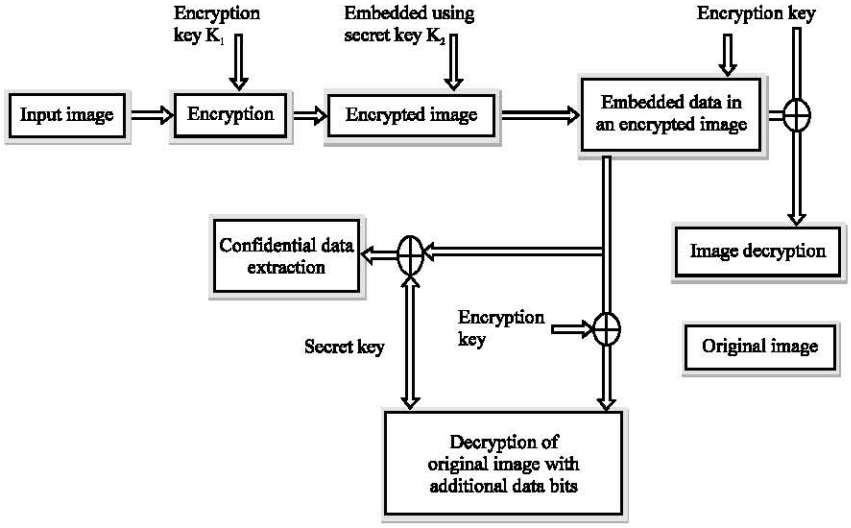

Fig. 1: Proposed methodology

Encryption and shuffling: In this methodology, image gets primarily shuffled by means of Hennon subsequently to chaos after which gets shuffled using Hennon once again. It is then lastly encrypted through Blowfish algorithm with the key value ('cxdsew4rtrtjh', 0.675, 0.9324).

The data is embedded into the encrypted image; here encryption and data hiding are separable. Separate keys are used for data hiding and encryption as shown in Fig. 1. Thus, data hiding key only retrieves the embedded data whereas the encryption only recovers the secret.

RESULTS AND DISCUSSION

An ideal encryption routine should put up with its antagonism to Cryptanalysis attack. Different from the rest of conventional encryption methods, the essentials of digital encryption are unalike. For experimental analysis, Lena image of dimension 256×256 are taken. The shuffling and encryption algorithms are simulated in MATLAB 7.1.

Histogram tests: Original test images, their encrypted images along with their corresponding histograms are depicted in Fig. 2a-h, respectively. As it is clear from the figures, histograms of the original images exhibit some pattern. But, encrypted images' histograms show no sign of such pattern but homogenous variation. It is undoubtedly dreadful to crack this routine. This study produces absolutely distinct histograms of plain and encrypted images which is very essential for any image encryption routine. By observing the same, one cannot come to a conclusion about what is being hidden in images.

Correlation of pixels: In plain images, there exists a strong relationship between pixels as there is high correlation. Correlation is a principal measure of performance of image encryption methods. All three horizontal, vertical and diagonal correlation values are computed for pixel pairs in all plain and encrypted images and the values are tabulated. In general, if it is 1, then there is high correlation among pixels, on the other hand if it is 0, then it signifies the fact that there is only obscurity and randomness among the pixels. Therefore, this study produces more than convincing results for correlation study as plain images have high correlation and encrypted upshots offer negligible correlation. The correlation coefficient is given by following:

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

where, σ_i, σ_j are i and j's standard deviations accordingly and cov (i, j) is Covariance of i and j.

Covariance is expressed as following equation:

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

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

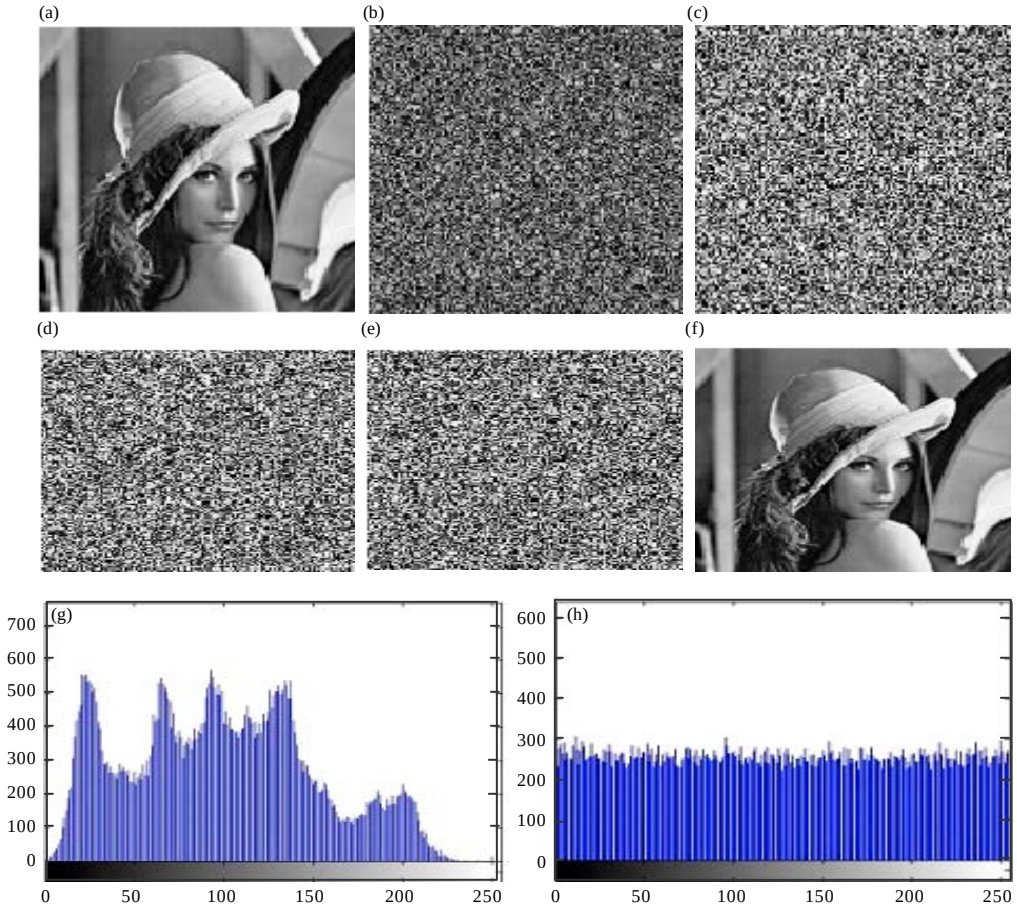

Fig. 2(a-h): (a-f) Original Lena image and its various encrypted and decrypted images, (g) Histogram of original Lena image and (h) Histogram after final encryption

Table 1: Comparison of metrics of the proposed scheme with the available literature

					Praveenkumar *et al.* (2014a, b)		
Method Metrics	Borujeni and Eshghi (2013)	Huang *et al.* (2013)	Kumar and Ghose (2011)	Norouzi *et al.* (2014)	Praveenkumar *et al.* (2014a)	Praveenkumar *et al.* (2014b)	Proposed method
HC	0.0041	-0.0025	0.0004992	0.0008213	0.0054	-0.0084647	-0.00060719
VC	0.0308	-0.0006	-0.001980	0.0008423	-0.0014	0.00292932	0.00042700
DC	0.0053	-0.0050	0.0008371	0.0005083	0.0024	0.00145603	-0.00013952
MSE	7510	–	–	9030	–	–	9096.70
PSNR	–	–	–	8.5740	–	–	8.5420
Entropy	–	–	–	7.9979	–	–	7.9971

Comparison of the proposed study and the existing method in references is given in Table 1. From the Table 1, it is clear that the method depict outstanding analytical results. If we take the horizontal correlation entries, the proposed methodology gives a very minimal value than the rest of the methods and is a remarkable measure of excellence. Not only horizontal but the corresponding vertical and diagonal correlation values also are very much minimized. When compared with referred existing methods, the proposed study offers greater than ever MSE of 9096.70 and lower than ever PSNR of 8.5420 promising a highly efficient technique for image encryption.

Differential attack: This measure is to reckon the algorithm's security. This is carried out by studying one-pixel-change in plain image and observing the successive resultant image. If this study shows any

changes, then the attack is rendered useless. Two major constraints of differential attack are Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) which are given by following equation:

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

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

This study is differential-attack free which is justified by disclosing the images of variable size. NPCR of around 99.6% and UACR of nearly 30.6% are produced in this study which is fairly honest. Therefore, one is unable to find even a small likeness between the original and encrypted images. So, differential attack fails on this method.

Image metrics: To justify this study, BER and PSNR values for the images are calculated and tabulated. Larger than ever MSE implies that the error in images is high and it declines the content in them. This, indeed, lowers the PSNR which is a quality measure for an image. This method offers most ergodic results to be analyzed which makes deliberate third party attacks frightful. The PSNR is computed by following equation:

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

Generally, MSSIM ranges in the interval [0, 1]. If it is close to 0, then there is no resemblance between images else if it is 1, the images have a striking resemblance. This study produces MSSIM of 0.0054 for method 1 which is almost equal to 0 signifying nil relationship between the pixel pairs thereby in images. This means, only slight error is witnessed by this routine which is for sure permissible and tolerable:

$$MSSIM\ (O, S) = \frac{1}{M} \sum_{j=1}^{M} SSIM\ (O_j, S_j)$$

$$SSIM\ (X, Y) = \frac{(2\mu_O\mu_S + C_1)(2\sigma_{OS} + C_2)}{(\mu_o^2 + \mu_S^2 + C_1)(\sigma_S^2 + \sigma_o^2 C_2)}$$

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

$$K_1 = 0.01\ C_2 = (K_2L)^2\ \ L = 255\ K_2 = 0.03$$

$$\mu_O = \frac{1}{N} \sum_{i=1}^{N} x_i$$

where, μ_O is the estimate of cover image's mean intensity (N = 255), σ_0 is the standard deviation:

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

$$\sigma_O = \left(\frac{1}{N-1} \sum_{i=1}^{N} (O_i - \mu_O)(S_i - \mu_O)\right)$$

where, σ_{OS} is correlation coefficient.

BER is a validation criterion which speaks about the error produced in this procedure. For this proposal, BER is approximately 0.5. It assures that almost 50% error rate, thereby declaring the encrypted output, is highly stochastic.

Other metrics for the proposed methodology are given as follows:

No. of errors	=	262216
Relative entropy	=	0.4271
SNR	=	2.8339
Bit_error_rate	=	0.5001
NPCR	=	99.6292
Quality	=	0.7654
MSSIM	=	0.0054
UACI	=	30.6905

The original Lena image and its various encrypted and decrypted images are given in Fig. 2a-f, respectively. The histogram of the original image and the histogram of the final encrypted image are given in Fig. 2g and h, respectively.

Figure 3a, 4a and 5a, respectively represents the horizontal, vertical and the diagonal pixel distribution of the original Lena image. From the figures, the pixel distribution are concentrated on a single area and was not uniformly distributed. Figure 3b, 4b and 5b represents the horizontal, vertical and the diagonal pixel distribution of the encrypted Lena image. From the figures, it is clear that, pixels are uniformly distributed after encryption.

Figure 6a represents the original Lena image and Fig. 6b represents the encrypted Lena image using the correct key and Fig. 6c represents the decrypted Lena using the correct key and Fig. 6d represents the decrypted image using the wrong key. From the results, it is clear the proposed algorithm was very sensitive to the key used even if a single bit change in the key value results in a totally unidentified image.

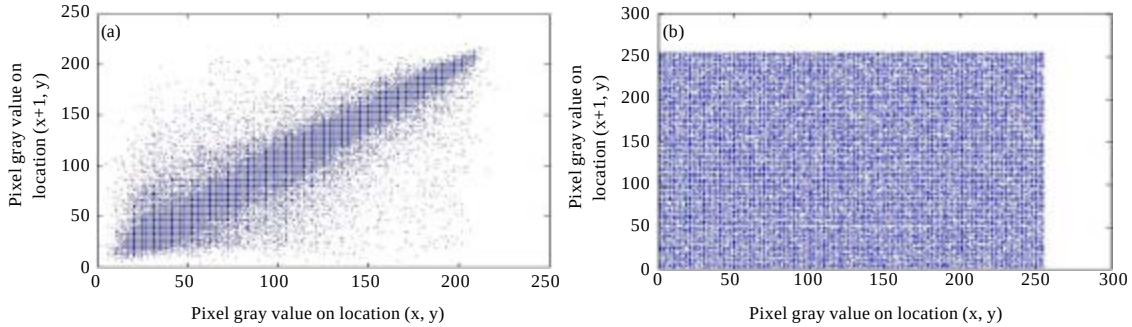

Fig. 3(a-b): Horizontal distribution of the pixels of (a) Original Lena image and (b) Encrypted image

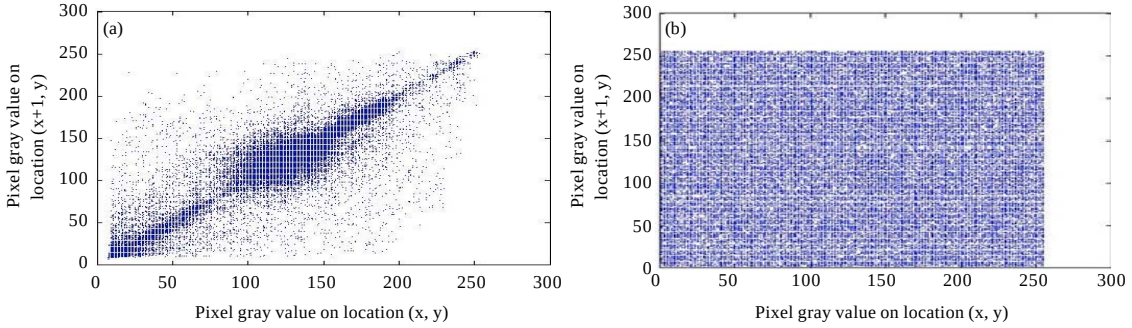

Fig. 4(a-b): Vertical distribution of the pixels of the (a) Original Lena image and (b) Encrypted image

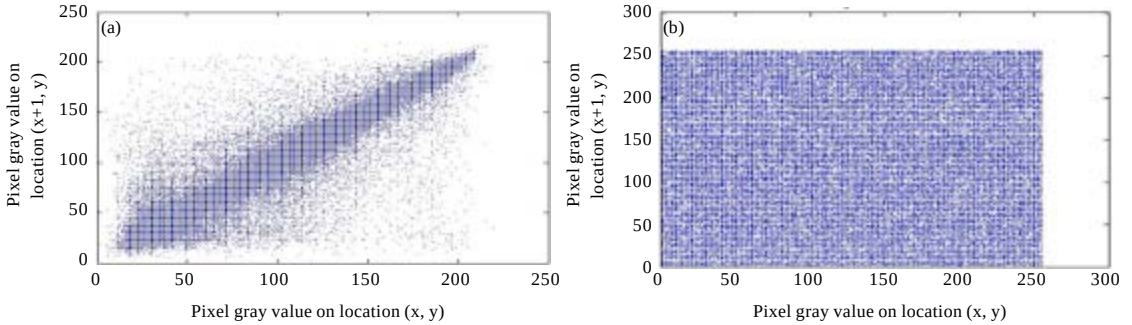

Fig. 5(a-b): Diagonal distribution of the pixels of the (a) Original Lena image and (b) Encrypted image

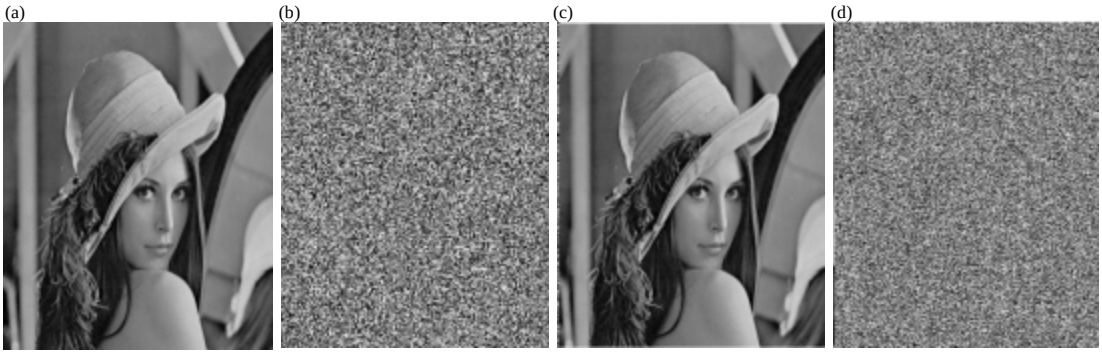

Fig. 6(a-d): (a) Original Lena image (b) Encrypted image of (a), (c) Decrypted image using the correct key and (d) Decrypted image using the wrong key

CONCLUSION

This study pioneers a peerless image encryption sculpt taking nonlinear dynamic system and Blowfish as elementary elements. The proposed schemes make use of the chaos maps for image encryption results in randomness. Blowfish cannot be broken until an attacker tries 28r+1 combinations where r indicates the number of rounds utilized. Hence, if the number of rounds are been increased then the Blowfish algorithm becomes stronger. Also combined with Chaotic, it provides a better and more secure encryption pattern. Correlation values are almost close to zero and entropy achieves value 8, both resemble the ideal values which forms the prime aspects of this study. On the whole, this encryption model promises security, effectiveness and robustness. Thereby it appreciably augments the confrontation to statistical and differential attacks. Analytical results justify that the algorithm is highly secure and practical.

REFERENCES

Alvarez, E., A. Fernandez, P. Garcia, J. Jimenez and A. Marcano, 1999. New approach to chaotic encryption. Phys. Lett. A, 263: 373-375.

Alvarez, G., F. Montoya, M. Romera and G. Pastor, 2000. Cryptanalysis of a chaotic encryption system. Phys. Lett. A, 276: 191-196.

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. 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., G. Devipriya, V. Thamkaiselvan and J.B.B. Rayappan, 2013a. 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, 2013b. 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, 2013c. 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, 2013d. Rubik's cube: A way for random image steganography. Res. J. Inform. Technol., 5: 329-340.

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

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.

Belkhouche, F. and U. Qidwai, 2003. Binary image encoding using 1D chaotic maps. Proceedings of the Annual Technical Conference on IEEE Region 5, April 11, 2003, New Orleans, LA., USA., pp: 39-42.

Borujeni, S.E. and M. Eshghi, 2013. Chaotic image encryption system using phase-magnitude transformation and pixel substitution. Telecommun. Syst., 52: 525-537.

Celik, M.U., G. Sharma, A.M. Tekalp and E. Saber, 2005. Lossless generalized-LSB data embedding. IEEE Trans. Image Process., 14: 253-266.

Chang, C.C., C.C. Lin and Y.H. Chen, 2008. Reversible data-embedding scheme using differences between original and predicted pixel values. IET Inform. Secur., 2: 35-46.

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

Chen, G., Y. Mao and C.K. Chui, 2004. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos Solitons Fractals, 21: 749-761.

Encinas, L.H. and A.P. Dominguez, 2006. Comment on A technique for image encryption using digital signature. Opt. Commun., 268: 261-265.

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

Huang, C.K., C.W. Liao, S.L. Hsu and Y.C. Jeng, 2013. Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system. Telecommun. Syst., 52: 563-571.

Kumar, A. and M.K. Ghose, 2011. Extended substitution-diffusion based image cipher using chaotic standard map. Commun. Nonlinear Sci. Numer. Simul., 16: 372-382.

Li, S. and X. Zheng, 2002. Cryptanalysis of a chaotic image encryption method. Proceedings of the IEEE International Symposium on Circuits and Systems, May 26 29, 2002, Phoenix-Scottsdale, AZ., USA., pp: 708-711.

Mayache, A., T. Eude and H. Cherifi, 1998. A comparison of image quality models and metrics based on human visual sensitivity. Proceedings of the International Conference on Image Processing, October 4-7, 1998, Chicago, IL., USA., pp: 409-413.

Ni, Z., Y.Q. Shi, N. Ansari and W. Su, 2006. Reversible data hiding. IEEE Trans. Circ. Syst. Video Technol., 16: 354-362.

Norouzi, B., S.M. Seyedzadeh, S. Mirzakuchaki and M.R. Mosavi, 2014. A novel image encryption based on hash function with only two-round diffusion process. Multimedia Syst., 20: 45-64.

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., K. Thenmozhi, M.N. Dinesh and R. Amirtharajan, 2013a. Fixing, padding and embedding: A modulated stego. Int. J. Eng. Technol., 5: 2257-2261.

Praveenkumar, P., M. Nagadinesh, P. Lakshmi, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2013b. Convolution and viterbi EN (DE) coders on OFDM hides, rides and conveys message-A neural STEGO. Proceedings of the International Conference on Computer Communication and Informatics, January 4-6, 2013, Coimbatore, pp: 1-5.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013c. Can we reduce PAPR? OFDM+PTS+SLM+STEGO: A novel approach. Asian J. Sci. Res., 6: 38-52.

Praveenkumar, P., R. Amirtharajan, K. Thenmozhi and J.B.B. Rayappan, 2013d. OFDM with low PAPR: A novel role of partial transmit sequence. Res. J. Inform. Technol., 5: 35-44.

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., G.S. Hemalatha, B. Reddy, K. Thenmozhi, J.B.B. Rayappan and R. Amirtharajan, 2014b. 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, 2014c. 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, 2014d. 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, 2014e. Purposeful error on OFDM: A secret channel. Inform. Technol. J., 13: 1985-1991.

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

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

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

Praveenkumar, P., R. Hemalatha, R. Uma, K. Madhunisha, K. Thenmozhi and R. Amirtharajan, 2014n. Image zoning? encryption. Res. J. Inform. Technol., 6: 368-378.

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.

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

Seyedzade, S.M., S. Mirzakuchaki and R.E. Atani, 2010. A novel image encryption algorithm based on hash function. Proceedings of the 6th Iranian Machine Vision and Image Processing, October 27-28, 2010, Isfahan, Iran, pp: 1-6.

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.

Tong, X., M. Cui and Z. Wang, 2009. A new feedback image encryption scheme based on perturbation with dynamical compound chaotic sequence cipher generator. Opt. Commun., 282: 2722-2728.

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.

Wang, Z. and A.C. Bovik, 2002. A universal image quality index. IEEE Signal Process. Lett., 9: 81-84.

Wei, X., L. Guo, Q. Zhang, J. Zhang and S. Lian, 2012. A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system. J. Syst. Software, 85: 290-299.

Yen, J.C. and J.I. Guo, 2000. A new chaotic key-based design for image encryption and decryption. Proceedings of the IEEE International Symposium on Circuits and Systems, Volume 4, May 28-31, 2000, Geneva, Switzerland, pp: 49-52.

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

Zhu, C., 2012. A novel image encryption scheme based on improved hyperchaotic sequences. Opt. Commun., 285: 29-37.