Received: July 28, 2017

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Image Encryption Method based on Hybrid Fractal-Chaos Algorithm

Sandhya Rani Malligere Halagowda[1]* **Sudha Kanakatti Lakshminarayana[2]**

[1]*Jain University, India*
[2]*Dayananda Sagar College of Engineering, India*
* Corresponding author's Email: sandhyarphd2017@gmail.com

Abstract: In recent years, there has been an increasing interest in the field of cryptography. Cryptography has applied in diverse applications and the researchers mainly concentrates on Image Encryption (IE) field. This paper proposes a hybrid encryption technique in order to provide high secure transmission. Here, an IE and decryption process is proposed by employing hybrid fractal-chaos technique. This proposed methodology consists of four modules like key generation, fractal encryption, chaos encryption and decryption. Initially, a key that is generated is utilized to encrypt and decrypt the image or data. Subsequently, fractal-IE is carried out by applying L-shaped tromino. Likewise, chaos encryption is carried by employing Discrete Cosine Transform (DCT), to have the final encrypted image. Whereas, the decryption process is carried out using chaos decryption and fractal decryption algorithms. Finally, the experimental outcome confirms that the projected technique delivers high security level network with low computational complexity.

Keywords: Discrete cosine transform, Image encryption, Key generation, L-shaped tromino.

1. Introduction

In the current scenario, information security is essential in various areas like internet communication, multimedia systems, medical imaging, tele-medicine, military communication, and so on, leading to an increasing interest in the field of cryptography [1, 2]. Cryptography is the progression of hiding information or try to keep the information safe and secure [3]. In cryptography, the image is one of the important tool for carrying information. By applying encryption process, the message or information is encoded by the authorized persons. IE schemes have been increasingly studied to meet the demand for real-time secure image transmission over private or public networks [4, 5]. Conventional-IE algorithms are not suitable for IE, because of the special storage characteristics of an image and weakness of low-level efficiency when the image is large [6]. In order to overcome these difficulties, two effective algorithms are combined for encryption and decryption process such as, fractal and chaos-based encryption algorithms [7].

Initially, the fractal based encryption algorithm encrypts the image by applying fractal key with the combination of L-shaped tromino method [8]. On the other hand, Chaos-based algorithm has found wide popularity among researchers, because of the inherent features of chaos systems, such as sensitivity to initial value and randomness, the chaos system-based IE method appears to be suitable for high-security encryption [9, 10]. This type of encryption typically requires two stages like permutation and diffusion. In the permutation step, image pixels are reallocated with the help of a chaotic map without changing the pixel's gray levels. Then, in the diffusion step, the value of each pixel is changed by applying a chaos sequence. Proposed chaos-based IE algorithm performs encryption using DCT algorithm. After encryption, the decryption procedure is performed by employing chaos and fractal based decryption methods. Finally, the experimental outcome shows that the projected hybrid technique delivers a high secure transmission with low computational complexity.

In this paper, a hybrid (fractal and chaos) based encryption techniques are proposed to provide a highly secure network with low computational complexity. At first, a key is generated that is utilized to encrypt and decrypt the image or data. Then, a fractal-IE algorithm is processed by applying L-shaped tromino. On the other hand, the chaos encryption algorithm is accomplished by employing DCT, to have the final encrypted image. Respective, encrypted image is decrypted by employing chaos and fractal decryption algorithm.

This literature is composed as follows. In Section 2, survey several IE and decryption strategies. In section 3, a hybrid (fractal and chaos) strategies are portrayed, to seek better security system. In Section 4, the execution of projected technique is assessed by simulation. The conclusion is made in Section 5.

2. Literature review

Numerous researches have been proposed by researchers in IE. In this section, a brief review of some important contributions to the existing literature is presented.

Mohammad Seyedzadeh [11] presented some chaos-based image cryptosystems. In this revision, the author proposed a chaos-based IE algorithm, to encrypt the color images by using Coupled Two-dimensional Piecewise Nonlinear Chaotic Map (CTPNCM). CTPNCM has some distinct characteristics like high security, high sensitivity and high speed that could be applied in encryption of color images. In order to generate the initial conditions and parameters of the CTPNCM, 256-bit long external secret key was employed. Computer simulations confirm that the proposed algorithm has high security compared to existing approaches. While employing 256-bit security key, the time consumption of encryption and decryption procedure was quite high and also CTPNCM performed poorly for encrypting the images with homogeneous background.

S.M. Seyedzadeh, and S. Mirzakuchaki [12] evaluated a technique named as chaos-based image cipher. In this literature, author improved the diffusion strategy for promoting the efficiency of permutation-diffusion type image cipher. To enhance the security of the cryptosystem, a plain-text related chaotic orbit turbulence mechanism was introduced in diffusion procedure by distressing the control parameter of the employed chaotic system according to the cipher-pixel. Extensive cryptanalysis has been performed on the proposed scheme using differential analysis, key space analysis, various statistical analysis and key sensitivity analysis. Analysed result indicates that the projected scheme has a satisfactory security level with low computational complexity. This plain-text related chaotic orbit turbulence mechanism contained more number of iterations, so that the computational time was quite high.

P. Li, and Y. Zhao [13] evaluated an encryption scheme for quantum colour image. Initially, a colour image was converted into a quantum superposition state by employing novel-Enhanced Quantum Representation (EQR), where the R, G, and B values of every pixel in a 24-bit RGB true colour image were symbolized by 24 single-qubit basic states, and each value have 8 qubits. Then, the 24 qubits were transformed from a basic state into a balanced superposition state by employing the controlled rotation gates. The gray-scale values of R, G, and B of every pixel were in a balanced superposition of 224 mutli-bits basic states. After measuring, the whole image was a uniform white noise that does not deliver any information. Whereas, decryption was the reverse procedure of encryption. Experimental outcomes showed that the proposed encryption approach has better security. But, this literature does not concentrate on the contrast of the reconstruction image, because it may lead to loss of information due to change in aspect ratio.

B. Norouzi, and S. Mirzakuchaki [14] illustrated a new IE algorithm based on Cellular Neural Network (CNN). In this literature, the projected scheme consists of three processes like bit-substitution, key stream generation process, and diffusion procedure. Hence, CNN systems were derived using a 256 bit-long external secret key by employing some algebraic transformations to the key. The original key stream was related to the plain-image, which increases the level of security and key sensitivity of the proposed algorithm. Finally, the experimental outcomes reveal that the new IE algorithm has the advantages of large key space, and high security. If the external key bit size was high, the performance of CNN method gets degrade.

To overcome the above mentioned drawbacks, a hybrid fractal-chaos technique is implemented that enhances the procedure acclimated in our anticipated strategy.

3. Proposed Methodology

This section evaluates, a hybrid IE algorithm that is based on fractal and chaos encryption in dual layers. The proposed technique overcomes the

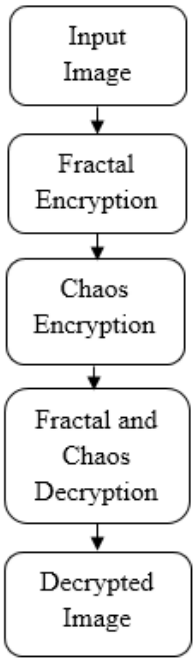


Figure.1 General block diagram of IE and decryption

drawback of existing techniques by the incorporation of fractal-chaos combination. Block diagram of the proposed technique is given in Fig.1.

In this scenario, the projected technique consists of four modules such as, key generation, fractal encryption, chaos encryption and decryption. In key generation, two keys are generated, key 1 is generated by utilizing random number (0 to 1).

$$\text{Key } 1 = \text{Random} \times 25 + 4 \quad (1)$$

In addition, key 2 is generated by employing the formula,

$$\text{Key } 2 = \text{Key } 1 \times 2 \quad (2)$$

These two keys (key 1, key 2) are utilized in encryption and decryption process of (Fractal and chaos) and the size of the key is 5 or 6 bit (based on random value).

3.1 Fractal Encryption Module

Fractal IE is employed to find the iterated contract transform of image pixels. Here, the generated keys are utilized as a key in the encryption and decryption procedure. Attributes like co-ordinates, iterations and zoom level are employed to generate the fractal image. In addition to this, L shaped tromino theorem is employed that makes the fractal encryption more effective in security. The architecture of the fractal-based image encryption is depicted in Fig.2.

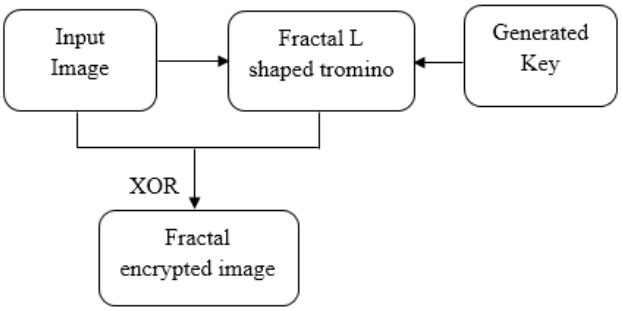


Figure.2 Fractal encryption stage

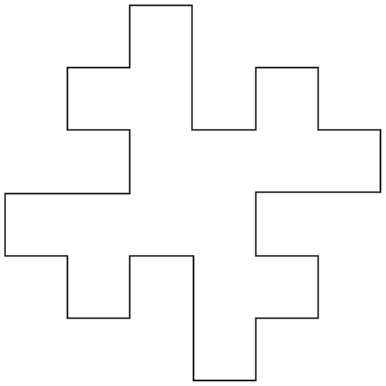


Figure.3 First iteration of L shaped tromino

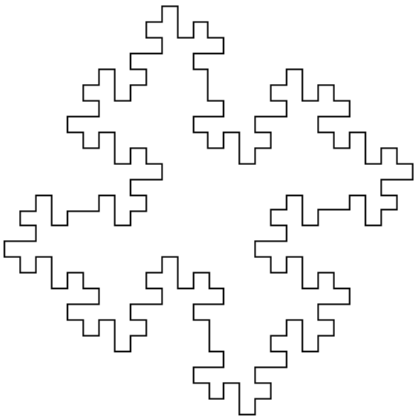


Figure.4 Second iteration of L shaped tromino

In this literature, the L shaped tromino can be dissected into smaller tromino of the same type, which is based on iteration. Number of iteration depends on image size $3 \times (512 \times 512 \times 3)$. The first iteration and second iteration images are stated in Figs.3 and 4. The L shaped tromino is performed based on two attributes $\theta = 90$ degree and L symbol '+' or '-'.

L shaped tromino images and the input images are combined by employing Exclusive-OR (XOR) operation with the help of generated keys. Basically, the fractal encryption algorithm depends on the modulo-operation and hence, it has an exact inverse.

Due to this property, it is a one-to-one encryption decryption algorithm, so the image cannot be corrupted during the decryption. The fractal encryption and decryption process can be done in two phases. The fractal encryption process works in pixel-by-pixel manner, each pixel contains three layers of colors represented as Red(R), Green(G) and Blue (B), where each falls in the interval [1,255].Let the keys involved are represented by $R_K, G_{K,} B_K$ and the layers of encrypted images are represented as$R_E, G_{E,} B_E$.

Phase 1:

$$\forall L \in R_K, G_{K,} B_K \quad (3)$$

$$\exists L'_{mxn}: \forall f \in [1, m], g \in [1, n] \quad (4)$$

$$l'_{fg} = \sum_{h=1}^{h_{max}} \sum_{k=1}^{k_{max}} p(f, g, h, k) X l_{H,K} \quad (5)$$

$$H_{max} = \left[\frac{f-1}{\delta+1}\right] + \left[\frac{m-f}{\delta+1}\right] + 1 \quad (6)$$

$$K_{max} = \left[\frac{g-1}{\delta+1}\right] + \left[\frac{n-g}{\delta+1}\right] + 1 \quad (7)$$

$$H = f - \left[\frac{f-1}{\delta+1}\right] \times (\delta + 1) + (h - 1) \times (\delta + 1) \quad (8)$$

$$K = g - \left[\frac{g-1}{\delta+1}\right] \times (\delta + 1) + (k - 1) \times (\delta + 1) \quad (9)$$

$$p(f, g, h, k) = \sqrt{[f - [\frac{f-1}{\delta+1}]} \times (\delta + 1) + (h - 1) \times (\delta + 1) - f]2 - \sqrt{[g - [\frac{g-1}{\delta+1}]} \times (\delta + 1) + (k - 1) \times (\delta + 1) - g]2 \quad (10)$$

For each pixel in the image, the grid is assumed to be built with spacing δ. Let $p(f, g, h, k)$ represented as the weight. Hence, the value of l'_{fg} every grid is different. It is also necessary to make sure of every element in L′is as unique as possible, which leads to strong key generation. H_{max} and K_{max} are stated as the maximum weight value.

Phase 2:

$$\forall R \in R, G, B; \exists R'_{mxm}: \forall f \epsilon [1, m], g \epsilon [1, n] \quad (11)$$

$$r'_{fg} = (r_{fg+l'_{fg}) mod 256} \quad (12)$$

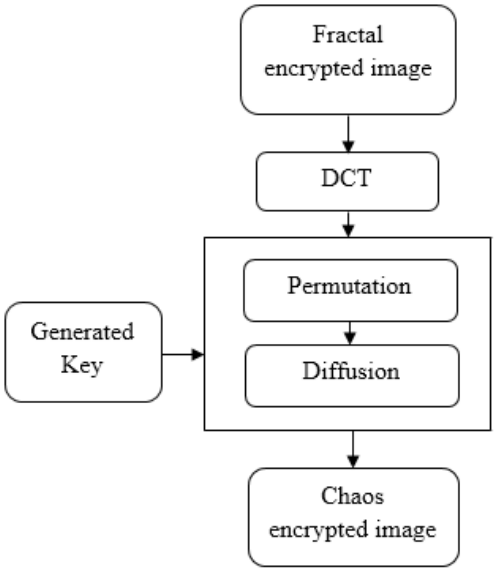


Figure.5 Chaos encryption stage

Here, one layer of encrypted image R, G and B is denoted as the matrix of R. After the encryption process the codebook is generated. The code book is generated by decomposing the encrypted image into non-overlapping blocks then select any N number of vectors randomly.

3.2 Chaos encryption module

Chaos encryption algorithm has extensive reputation among researchers, due to its inherent features of chaos systems. Whereas, chaos-based image cryptosystem mainly consists of two stages like permutation and diffusion. In permutation stage, the pixel permutation where the position of the pixels is scrambled over the entire image without disturbing the value of the pixels. Then, in the diffusion step, the value of each pixel is altered by employing a chaos sequence. In this module, DCT has been illustrated to increase the level of security and also improves the key space. The typical architecture of the chaos-based image cryptosystems is depicted in Fig.5.

Initially, the fractal encrypted images are converted into DCT. Here, the DCT transformation can be achieved by using 8×8 pixels block to sum of cosine signals weighted. These weights are represented by the matrix DCT coefficient. Mathematical equation of cosine transformation is given below.

$$y(k, l) = \frac{c(k)c(l)}{4}$$

$$\sum_{i=0}^{7}\sum_{j=0}^{7} i(x,y)\cos\left\{\frac{(2i+l)k\pi}{16}\right\}\cos\left\{\frac{(2i+l)\pi}{16}\right\} \quad (13)$$

Where,$k,l = 0,1 \ldots .7$, i (x, y) is the intensity of the pixel in row x and column y and Y (k, l) is the DCT coefficient in row k and column l of the DCT matrix.

After DCT transformation, the permutation and diffusion phases are carried by using generated keys (key 1 and key 2) and the value of logistic maps. In chaotic encryption module, one very simple chaotic map has been employed for cryptography application is named as logistic map. Mathematically, the logistic map is written as,

$$\text{Logistic}_i = rx_n(1 - x_n) \quad (14)$$

Where, x_n is represented as chaos sequence and r is stated as positive number (1 to 4).

Using generated keys and the value of logistic map as the parameter, iterating logistic maps for 5 times to get rid of the transient effect. Sorting the chaotic orbit obtained from previous step ascendingly, and permuting the diffused or plain-image by this order,

$$\text{Generated keys} = K_i \quad (15)$$

$$mim(i) = permut \oplus K_i(\text{logistic}_i p(i)) i = 1,2,3,..M \times N \quad (16)$$

Generating cipher key by permuted image and diffusing the permuted or plain-image by the logistic chaotic orbit from chaotic orbit. Output of diffusion stage is cipher-image.

$$c(i) = mim(i), i = 1,2,3, \ldots M \times N \quad (17)$$

Where, $p(i)$ is the original image pixel value, $mim(i)$ is the pixel value, which is permuted by the order or diffused by the orbit, $c(i)$ is the cipher-image. M and N are the width and height of the plain-image.

3.3 Decryption Module

Once the encryption process is over, decryption procedure is accomplished to retrieve the original image. Decryption section includes two stage process like chaos and fractal based decryption.

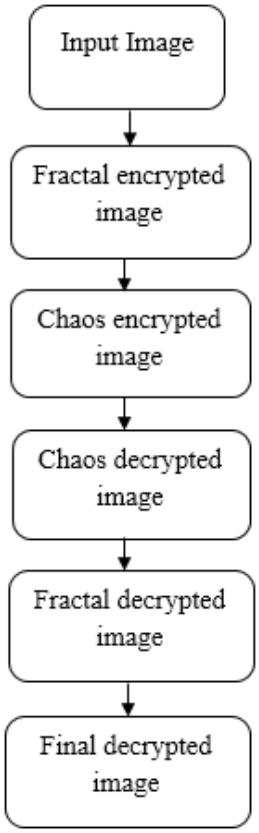


Figure.6 Block Diagram of Decryption Process

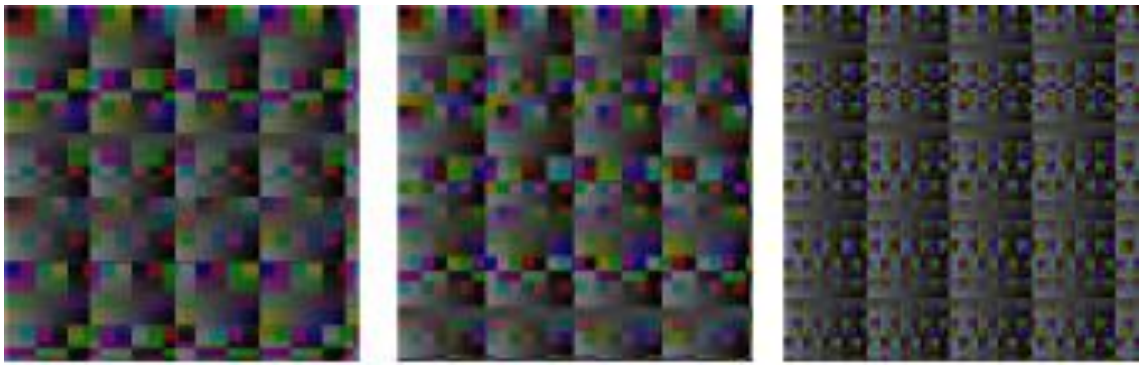
Initially, chaos based decryption is carried out on encrypted image, this process is opposite to chaos based encryption. Subsequently, the fractal based decryption is executed after chaos based decryption. The decrypted image should be the exact copy of original image. The block diagram of decryption module is given in Fig.6.

4. Result and discussion

In this section, the experimental results have been characterized in detailed. All experiments were implemented on PC with 1.8GHz Pentium IV processor by employing MATLAB (version 6.5). Here, color images of Lena, Baboon and Pepper were tested to demonstrate the speed uprate, bit rate and the quality of projected algorithm. Respective images were taken from USC veterbi database with the size of 512×512 that is displayed below.

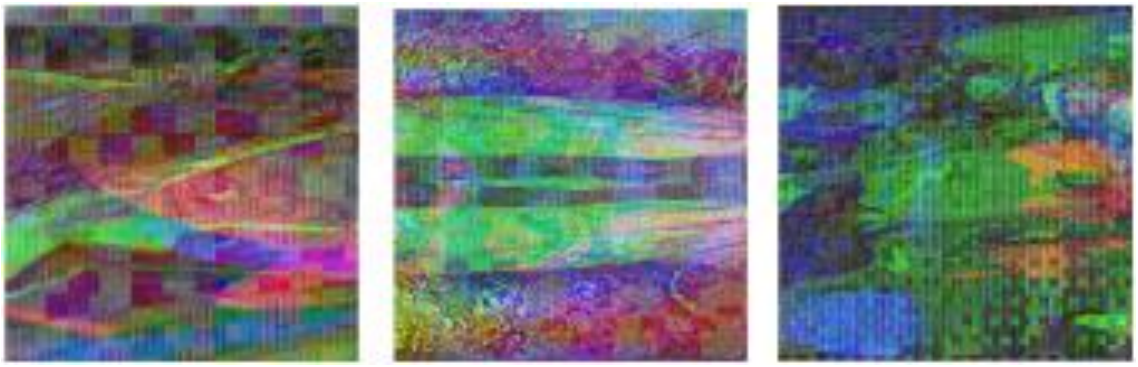
(a) (b) (c)

Figure.7 Input images: (a) Lena, (b) Baboon (c) pepper



(a) (b) (c)

Figure.8 Fractal tromino images

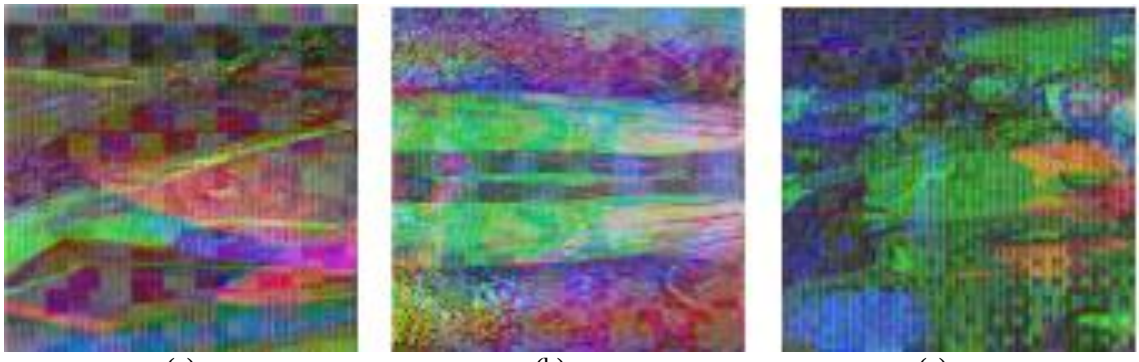


(a) (b) (c)

Figure.9 Fractal encrypted images

(a) (b) (c)

Figure.10 Chaos Encrypted images



(a) (b) (c)

Figure.11 Chaos decrypted images

(a) (b) (c)

Figure.12. Fractal decrypted images

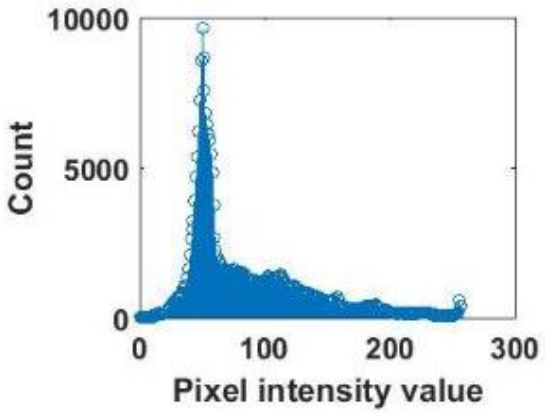


Figure.13 Input histogram of Lena image

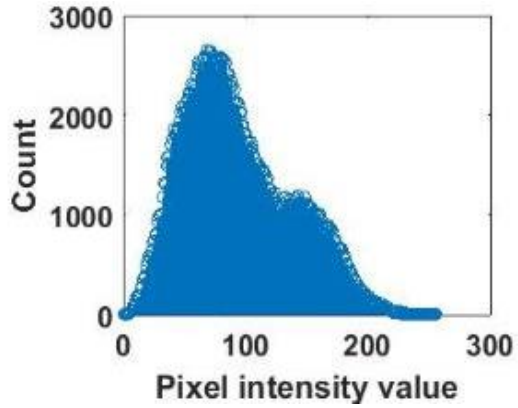


Figure.14 Fractal encryption histogram

Whereas, Fig.7 demonstrates the initial input images that are undertaken for image encryption and decryption process. Fig.8 illustrates the fractal L-shaped tromino images by employing L-shaped tromino theorem. This, L shaped tromino images are XOR with initial input images in order to deliver the fractal encrypted images that are symbolized in Fig.9. Likewise, the fractal encrypted images are further encrypted by employing chaos encryption method with the help of DCT, which is stated in Fig.10. Then, the chaos encrypted images are utilized to perform decryption process. Initially, the chaos decryption process is accomplished in chaos encrypted images, which is represented in Fig.11. Similarly, the chaos decrypted images are utilized to perform fractal decryption, the fractal decrypted images are demonstrated in Fig.12. Here, the histogram representations for Lena image is specified in Figs.13, 14, 15, 16, and 17.

In order to compare the performance evaluation of input and decrypted images, the Correlation Co-efficient (CC), entropy and Peak Signal-to-Noise Ratio (PSNR) parameters are employed. PSNR is most easily defined by Mean Squared Error (MSE), MSE is mathematically represented by,

$$\mathrm{MSE} = 1/\mathrm{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[\mathrm{I}(x-y)-\mathrm{k}(x,y)]^2 \quad (18)$$

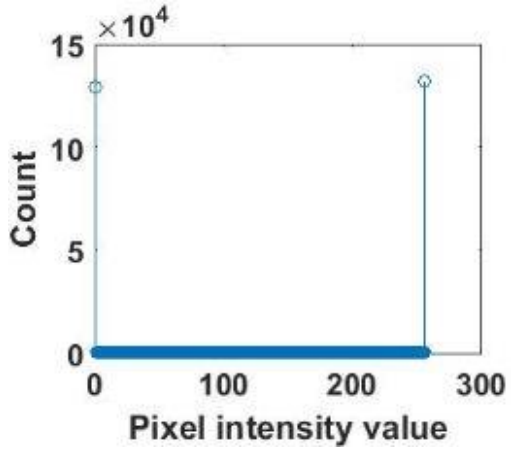


Figure.15 Chaos encryption histogram

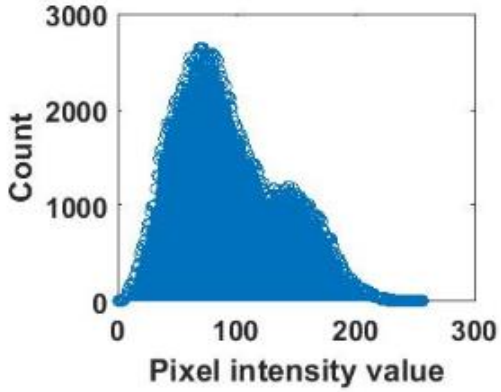


Figure.16 Chaos decryption histogram

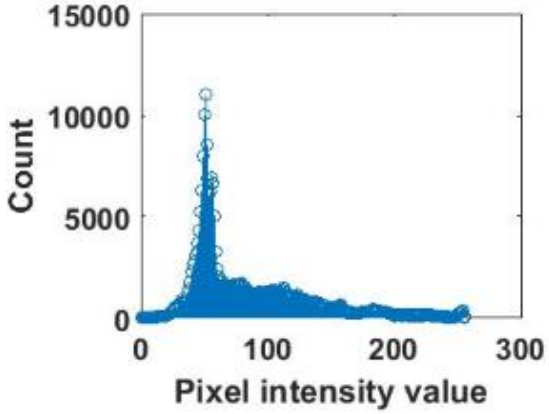


Figure.17 Fractal decryption histogram

Where, m and n are stated image and $I(x, y)$ is defined as input image, $k(x, y)$ is represented as decrypted image. CC is the useful measure to assess the encryption quality of any image cryptosystems. This metric can be calculated as follow,

$$\mathrm{E(x)} = 1/\mathrm{L}\sum_{\mathrm{l}=1}^{\mathrm{L}} \mathrm{x_l} \quad (19)$$

$$\mathrm{D(x)} = 1/\mathrm{L}\sum_{\mathrm{l}=1}^{\mathrm{L}} (\mathrm{x_l} - \mathrm{E(x)})^2 \quad (20)$$

Table 1. Performance evaluation of proposed method in terms of entropy

Image	Entropy	
Lena	Existing [15]	7.1062
	Proposed	7.5937
Baboon	Existing [15]	7.0932
	Proposed	7.6220
Pepper	Existing [15]	7.0289
	Proposed	7.5033

Table 2. Performance evaluation of proposed method by means of CC and PSNR

Image		Correlation Co-efficient			PSNR
		Vertical	Horizontal	Diagonal	
Lena	Pbest	-0.0013	0.0002	-0.0023	29.0363
	Pavg	-0.0036	-0.0012	-0.0031	29.0656
Baboon	Pbest	0.0020	0.0010	0.0028	20.9736
	Pavg	0.0003	-0.0001	0.0018	20.9799
Pepper	Pbest	-0.0003	-0.0007	-0.0008	35.4981
	Pavg	-0.0056	-0.0030	-0.0022	35.5793

$$\mathrm{Cov(x, y)} = 1/\mathrm{L}\sum_{\mathrm{l}=1}^{\mathrm{L}} (\mathrm{x_l} - \mathrm{E(x)})(\mathrm{y_l} - \mathrm{E(y)}))^2 \quad (21)$$

Where, L is the number of pixels involved in the calculations. The closer values of $\mathrm{x, y}$ are to be zero in order to attain better quality of encryption algorithm.

Tables 1 and 2 demonstrate the performance evaluation of hybrid encryption and decryption (fractal and chaos) algorithm. From the table 1 and 2, it can be inferred that the proposed algorithm is secure in transmission for any kind of color images.

K. Naik, and A.K. Pal [15] illustrated an image cryptosystem for uncompressed color image where the DCT is applied on each color components of the color image to select the superior coefficients and the respective coefficients are applied into encryption procedure for decreasing the computational overhead. Then, the selected coefficients are confused by utilizing Arnold transform followed by diffusion with keys. After completion of the encryption procedure, unencrypted coefficients are appended with encrypted components to form the uncompressed encrypted image. This scheme has been tested on a set of standard color test images and satisfactory results have been found with the entropy value up to 7.1. Compared to this existing scheme, our proposed

method works effectively in terms of CC and PSNR and entropy value.

5. Conclusion

This paper concentrates on developing a highly secured transmission of data by employing hybrid fractal and chaos IE algorithms for real time applications. In this scenario, the fractal encryption is performed with the combination of L-shaped tromino theorem that provides a number of security goals to ensure the privacy and integrity of data. On the other hand, the chaos encryption is accomplished by employing DCT algorithm, which has the ability to reduce the blocking artefact effect. Strong encryption and decryption makes the methodology very useful in applications such as medical imaging, multimedia applications, and military applications. The performance of the proposed hybrid algorithm is evaluated by utilizing the factors like PSNR, entropy and CC. While analyzing, the proposed hybrid algorithm shows a superior outcome in encrypted image that delivers a high secure transmission with low computational complexity. In future, we mainly focus on more secure transmission of data and the security can be increased by splitting the image into more number of sub-images and also different improved algorithms are applied in the images.

References

[1] H. Kashanian, M. Davoudi, and H. Khorramfar, "Image Encryption using chaos functions and fractal key", *International Journal of Computer Science and Network Security*, Vol.16, No.10, pp.87, 2016.

[2] Q.H. Alsafasfeh and A.A. Arfoa, "Image encryption based on the general approach for multiple chaotic systems", *Journal of Signal and Information Processing*, Vol.2, No.3, pp.238, 2011.

[3] G. Chen, Y. Mao, and C.K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", *Chaos, Solitons & Fractals*, Vol.21, No.3, pp.749-761, 2004.

[4] B. Murugan and A.G.N. Gounder, "Image encryption scheme based on block-based confusion and multiple levels of diffusion", *IET Computer Vision*, Vol.10, No.6, pp.593-602, 2016.

[5] F. Sun, S. Liu, Z. Li, and Z. Lü, "A novel image encryption scheme based on spatial chaos map," *Chaos, Solitons & Fractals*, Vol.38, pp.631-640, 2008.

[6] Z.L. Zhu, W. Zhang, K.W. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation", *Information Sciences*, Vol.181, No.6, pp.1171-1186, 2011.

[7] K.W. Wong, B.S.H. Kwok, and C.H. Yuen, "An efficient diffusion approach for chaos-based image encryption", *Chaos, Solitons & Fractals*, Vol.41, No.5, pp.2652-2663, 2009.

[8] S. Al-Maadeed, A. Al-Ali, and T. Abdalla, "A New Chaos-Based Image- Seyed Encryption and Compression Algorithm", *Journal of Electrical and Computer Engineering*, Vol.2012, pp.15, 2012.

[9] Y. Zhanga, C. Li, K.W. Wong, S. Shua, and G. Chen, "Cryptanalyzing a chaos-based image encryption algorithm using alternate structure", *Journal of Systems and Software*, Vol.85, No.9, pp.2077-2085, 2012.

[10] Q. Zhou, K.W. Wong, X. Liao, T. Xiang, and Y. Hu, "Parallel image encryption algorithm based on discretized chaotic map", *Chaos, Solitons & Fractals*, Vol. 38, No.4, pp.1081-1092, 2008.

[11] C. Fu, J. J. Chen, H. Zou, W.H. Menu, Y.F. Zhan, and Y. Wen, "A chaos-based digital image encryption scheme with an improved diffusion strategy", *Opt Express*, Vol.20, No.3, pp.2363-2378, 2012.

[12] S.M. Seyedzadeh and S. Mirzakuchaki, "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map", *Signal Processing*, Vol.92, No.5, pp.1202-1215, 2012.

[13] P. Li and Y. Zhao, "A Simple Encryption Algorithm for Quantum Color Image", *International Journal of Theoretical Physics*, Vol.56, No.6, pp.1961-1982, 2017.

[14] B. Norouzi and S. Mirzakuchaki, "An image encryption algorithm based on DNA sequence operations and cellular neural network", *Multimedia Tools and Applications*, Vol.76, No.11, pp.13681-13701, 2016.

[15] K. Naik and A.K. Pal, "A Partial Image Cryptosystem Based on Discrete Cosine Transform and Arnold Transform", In: *Proc. of International Conf. on Recent Advances in Information Technology*, New Delhi, India, pp.65-73, 2014.