International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 11, Issue 11 (November 2015), PP.08-16

A Novel Technique for Simultaneous Encryption of Multiple Images Using 3D Chaotic Permutation

Prabhudev Jagadeesh[1], P. Nagabhushan[2]
[1]*Department of Computer Science and Engineering, JSS Academy of Technical Education, Bengaluru, Affiliated to VTU, Belagavi*
[2]*Department of Studies in Computer Science, University of Mysore, Mysore*

Abstract:- With the swift increase of digital data exchange and increased usage of digital images, it is important to protect the confidential image data from illegitimate access. Digital image scrambling or encryption is the solution which transforms a meaningful image into a meaningless or disordered image in order to enhance the ability to tackle attack and in turn improve the security. However inherent features of image data such as bulky nature, high redundancy and high correlation among pixels demand the need to treat an image in a different way from text data regarding confidentiality. In this paper a novel scheme is proposed to simultaneously encrypt multiple images in an image database or image folder. Images are stacked and are viewed as a 3D block of images. Permutation of image pixels/blocks across the images is done using 3D chaotic permutation and pixel substitution using three-way grid based noise induction. 2D grid structure projected on each dimension of the 3D block of images defines the scrambling nature of pixels resulting in varied distortion of information. The proposed novel model of perceiving multiple images as 3D block of images and simultaneous scrambling provides an additional level of complexity for unauthorized access. The proposed scheme is more apt for secured storage of images. The experimental results demonstrate that the proposed algorithm can effectively and simultaneously scramble the images, and the security analysis of the algorithm also reveals that the proposed scheme can survive various attacks.

Keywords:- *Image Encryption, Scrambling, Image Entropy, Image correlation, Image histogram, chaotic map.*

I. INTRODUCTION

The security of multimedia data in digital distribution networks is generally provided by encryption. Classical and modern ciphers have all been developed for the simplest form of data i.e., text and thus are not apt for encrypting image data which has certain intrinsic properties like bulky nature, intractable high redundancy and higher correlation among pixels. There have been several image scrambling schemes for protecting confidentiality of sensitive images essentially through cryptographic and steganographic techniques [1-3]. Despite these efforts, analysis indicates that security level is still not strong for images and multimedia data in general [4-6]. Also these techniques hardly consider the important inherent properties of images. This indicates the need for content-based schemes which are simpler yet stronger for protecting confidentiality of digital images [2]. In the proposed work a novel scheme which is unique in its approach is proposed to simultaneously scramble multiple images in an image database or image folder.

The rest of this paper is organized as follows. Section 2 presents the related work found in literature with regard to image encryption. In Section 3, the proposed scheme for multiple image encryption based on 3D chaotic permutation is discussed. Section 4 contains the experiments carried out and the results obtained. Section 5 presents the detailed security analysis of the new proposed technique. Finally, Section 6 concludes the paper highlighting the research accomplishments and also proposing future directions.

II. RELATED WORK

Since Classical and modern cryptographic algorithms have been developed for basically text data and are not suitable for images, several image encryption schemes have been proposed[7-11] considering the intrinsic characteristics of images. Image encryption techniques can be categorized as spatial domain methods or frequency domain methods. Basically most encryption schemes are constructed using three methods namely permutation, substitution and combination of both. Algorithms which provide different levels of security ranging from degradation to strong encryption are categorized under scalable algorithms [12]. Permutation based techniques are based on bit, pixel or block permutation [13]. In [14] a random combinational Image encryption approach with bit, pixel and block permutations is proposed. There are approaches to scramble an image in a transformed domain by scrambling the transform coefficients. Methods for scrambling all the pixels and transform coefficients with multiplicative or additive matrices are proposed which are considered as a generalization of the permutation-only encryption. Some image encryption schemes are based on the multi-

round combination of secret permutations and pixel value substitutions [13]. Several chaos-based algorithms are also proposed for image encryption [15-16].

III. PROPOSED TECHNIQUE

A novel scheme is proposed to simultaneously scramble multiple images in an image database or image folder. Images are stacked and are viewed as a 3D block of images. Permutation of image pixels/blocks across the images is done using 3D chaotic permutation and pixel substitution using three-way grid based noise induction. 2D grid structure projected on each dimension of the 3D block of images defines the scrambling nature of pixels resulting in varied distortion of information. The proposed scheme is more suitable for secured storage of images.

The following sections provide the necessary background, 2D grid formation on images and the basics of 3D chaotic map.

3.1 2D grid structure

An image is first partitioned into several arbitrary grids of geometrical objects (in the present case into trapezoidal grids). For this the plain image is partitioned into several arbitrary trapezoidal grids by drawing: i) horizontal lines at regular intervals on the image and ii) lines with different slopes across the image such that they do not intersect within the image area. The lines are drawn with the above property to limit the grids formed to trapezoidal grids. This method of partitioning has a higher probability of image being partitioned into distinctive trapezoidal grids. To eliminate any chances of an attacker tracing out the grid formed on the image, pixels are considered in terms of p x q pixel blocks and are mapped to their respective trapezoidal grid. A p x q pixel block is mapped on to a grid where its center lies. Fig. 1 illustrates the formation of grids on an image. The keys for pixel substitutions are derived from the geometrical properties of the grids like the area or the perimeter of the grid. Using these keys the substitution process is carried out by adding noise to every pixel through simple substitution cipher. The slopes, intercept and interval of horizontal lines act as keys for pixel substitution. The same set of keys is used for decrypting the image.

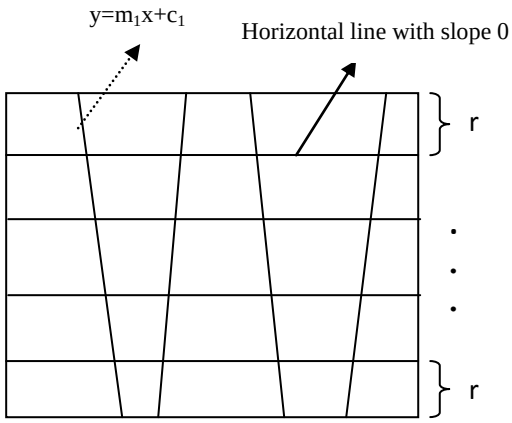


Fig. 1 Grid Formation on an Image

3.2 3D Chaotic Map

The simplicity of discrete chaotic maps and well established chaos theory make it possible to evolve prudently good solutions to image encryption. The classic Arnold cat map is a two-dimensional cat map. The extension of 2D map as 3D map for image encryption as proposed in [16] is described for the sake of clarity and completeness.

The classical Arnold cat map is a two-dimensional invertible chaotic map described in Eq.1 as:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \qquad (1)$$

In Eq.1 (x_n, y_n) are the original coordinates and (x_{n+1}, y_{n+1}) are the transformed coordinates. The generalized 2D cat map with two control parameters, a and b, is given in Eq.2 as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a \\ b & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod 1 \qquad (2)$$

Furthermore, the map in Eq.2 is extended to three-dimension by considering the following three maps [16].

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & a_z & 0 \\ b_z & a_z b_z + 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod 1 \quad (3)$$

i.e., by fixing z_n unchanged the 2D cat map is performed on the *x*–*y* plane.
In Eq.3 (x_n, y_n, z_n) are the original coordinates and $(x_{n+1}, y_{n+1}, z_{n+1})$ are the transformed coordinates.
The second one is similarly performed, but on the *y*–*z* plane while keeping x_n unchanged:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & a_x \\ 0 & b_x & a_x b_x + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod 1 \quad (4)$$

The last one is performed on the *x*–*z* plane:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & 0 & a_y \\ 0 & 1 & 0 \\ b_y & 0 & a_y b_y + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod 1 \quad (5)$$

Then, by combining these three maps together, a three-dimensional cat map is obtained as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \mathbf{A} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod 1 \quad (6)$$

Where

$$A = \begin{bmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix}$$

3.3 Discretization of the 3D cat map

Since encryption is a kind of transformation operated on a finite set, in order to incorporate a chaotic map into image encryption, it is discretized, while preserving some of its useful features such as the mixing property and the sensitivity to initial conditions and parameters.

The map in Eq.6 is discretized and extended to *N* x *N* x *N* 3D image blocks according to the following formula:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \\ z_{n+1} \end{bmatrix} = \mathbf{A} \begin{bmatrix} x_n \\ y_n \\ z_n \end{bmatrix} \bmod N \quad (7)$$

Where

$$A = \begin{bmatrix} 1 + a_x a_z b_y & a_z & a_y + a_x a_z + a_x a_y a_z b_y \\ b_z + a_x b_y + a_x a_z b_y b_z & a_z b_z + 1 & a_y a_z + a_x a_y a_z b_y b_z + a_x a_z b_z + a_x a_y b_y + a_x \\ a_x b_x b_y + b_y & b_x & a_x a_y b_x b_y + a_x b_x + a_y b_y + 1 \end{bmatrix}$$

(x_n, y_n, z_n) are the original coordinates and $(x_{n+1}, y_{n+1}, z_{n+1})$ are the transformed coordinates.
a_x, b_x, a_y , b_y , a_z, b_z are all positive integers.

The determinant of A is 1, which means that the discrete version of the 3D cat map is one to one, and that its mixing property and the sensitivity to initial conditions and parameters are kept unchanged.

3.4 Proposed Algorithm

The idea of the proposed approach is to simultaneously scramble a pool of images. The proposed encryption system is shown in Fig. 3. First, images are stacked to form 3D image block as shown in Fig 2. 3D blocks or cubes of specific size are formed. 2D trapezoidal grid structure generated from random slope lines are projected on each of the dimensions of 3D image block as shown in Fig. 2. Each cube is mapped onto appropriate trapezoidal grids in all the three dimensions depending on the position of the cube. A pixel's intensity value is altered using area parameter of the three trapezoidal grids onto which the cube containing the pixel is mapped. Permutation of pixels/cubes is carried out transforming pixels/cubes at one position to another position across images using 3D cat map presented above. The detailed algorithm is presented below.

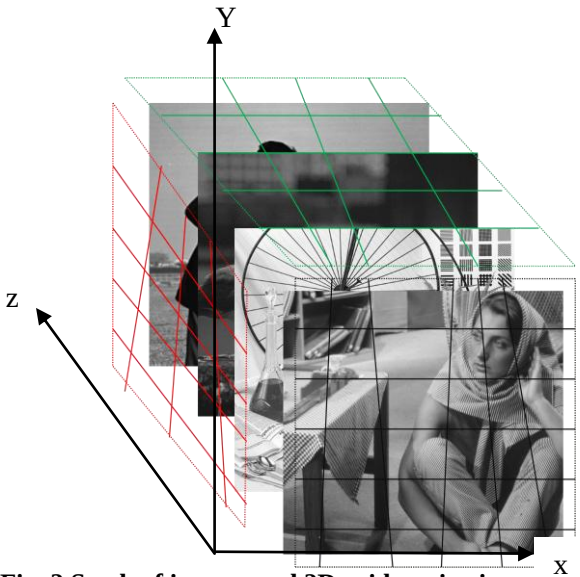


Fig. 2 Stack of images and 2D grid projection o ı plane.

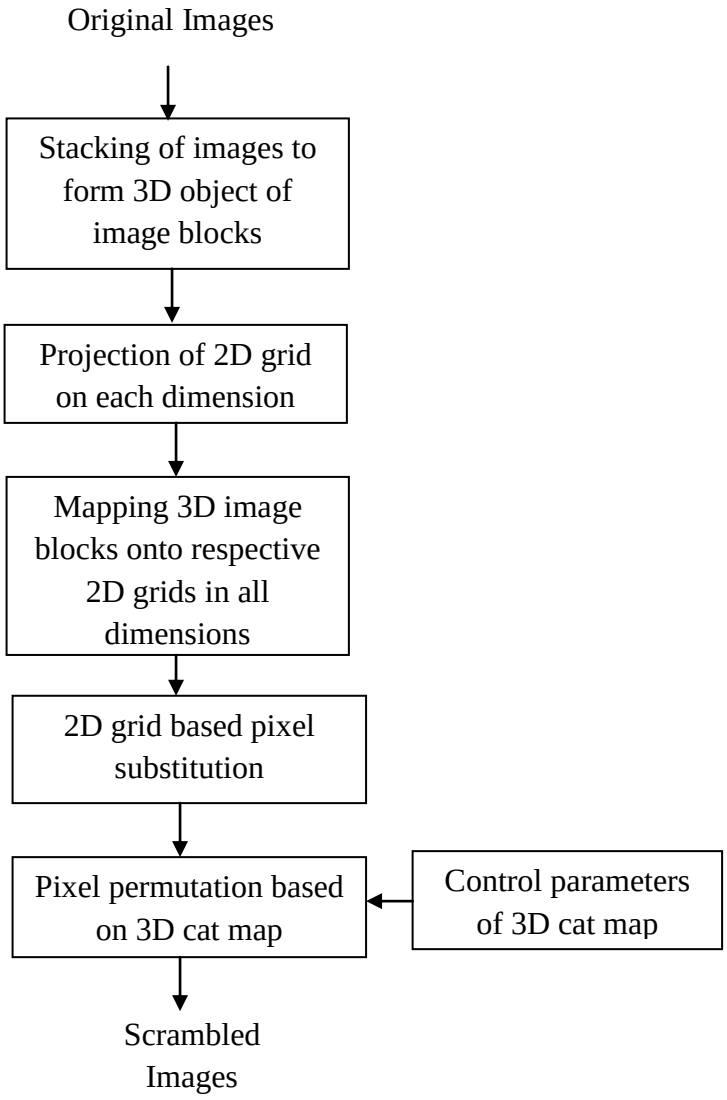


Fig. 3 Proposed Encryption Scheme

Algorithm

Step 1: Stack two-dimensional images as three-dimensional stack of images or cube.

Step 2: Project three randomly generated 2D trapezoidal grids one each on *x*-*y*, *y*-*z* and *z*-*x* plane of 3D image stack as shown in Fig. 2. Here *x* indicates the row position of pixel, *y* the column position and *z* indicates the image number in the image stack.

Step 3: Map 3D image blocks of size *p* x *p* x *p* onto the projected 2D trapezoidal grids separately for all the three projections.

The mapping is done such that a 3D image block is assigned to a grid if its center lies on that grid.

Step 4: Perform pixel substitution three times (for all three directions) using respective *Area* values of the trapezoidal grid to which the cube containing the pixel is mapped

$c = (p + Area) \bmod 256$

p is the original pixel and *c* is the transformed pixel and *Area* is the area of grid.

Step 5: Perform permutation of pixels/3D blocks using Arnold 3D cat map defined in Eq.7

Where (x_n,y_n,z_n) is the original position of pixel/3D blocks and $(x_{n+1},y_{n+1},z_{n+1})$ is the transformed position of the corresponding pixel/3D blocks. *N* x *N* is the size of each image in the set containing *N* images.

a_x, b_x, a_y , b_y , a_z, b_z are positive integers which can be viewed as keys for chaotic permutation.

Step 6: Repeat step 5 for required number of iterations.

For decryption and reconstruction of the original image, the above encryption process is reversed by using the same keys employed during encryption, by reversing first permutation and then the substitution in similar way done during encryption.

IV. EXPERIMENTAL RESULTS

The proposed algorithm was tested on the dataset of 100 images shown in Fig. 4 of size 100 x 100. Results of four images randomly selected are shown in Fig. 5. For results shown in Fig. 5, size of 3D image blocks for substitution process is 2 x 2 x 2. Permutation of these cubes is carried out across the planes using 3D map.

Fig. 4 Image dataset used for Encrypting Multiple Images

Sample Results

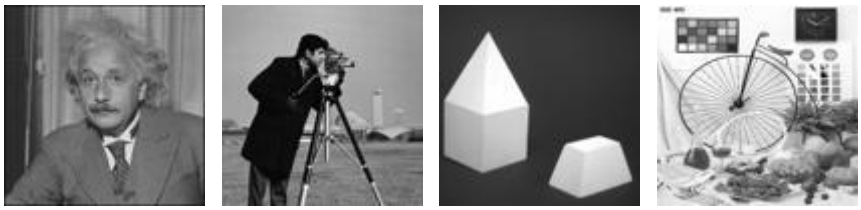
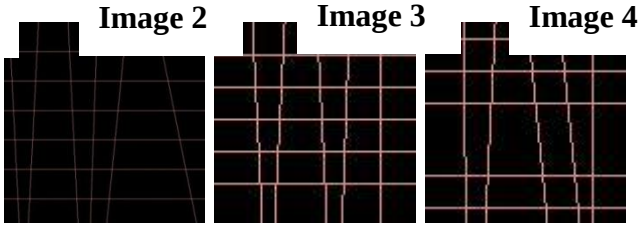
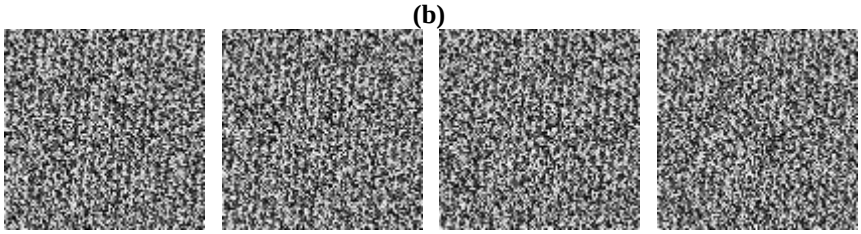


Image 1 **Image 2** **Image 3** **Image 4**



(b)



(c)

Fig. 5 (a) Original images (b) 2D grids used for encryption (c) Encrypted images

V. SECURITY ANALYSIS OF THE PROPOSED SYSTEM

An efficient image encryption algorithm should be robust against all kinds of statistical, cryptanalytic and brute-force attacks. To analyze the security of the proposed system, Entropy analysis, Histogram analysis and Correlation Coefficient analysis are carried out.

5.1 Entropy Analysis

The proposed technique is based on the principle of information entropy which intends to maximize the entropy thereby increasing the security. For a digital image, Image Entropy indicates the amount of information contained in an image. It can be chosen as a measure of the detail provided by an image. Higher the value of entropy less is the information revealed. The entropy E_n of a grayscale image is calculated as below:

$$E_n = \sum_{i=0}^{255}(p(i) * log_2(\frac{1}{p(i)}) \quad (8)$$

p(i) is the probability of occurrence of a pixel with grayscale value i. If each symbol has an equal probability then entropy of 8 would correspond to complete randomness, which is the ideal value expected in a scrambled image. The entropy of plain image and scrambled image are listed in Table. 1. The entropy values obtained for various scrambled image indicate that the proposed method results in a scrambled image that is more assorted thereby reducing the information revealed.

5.2 Histogram Analysis

Another Security analysis carried out is histogram analysis. An image histogram illustrates how pixels in an image are distributed by plotting the number of pixels at each intensity level. It is apparent from the results shown in Fig.6 that the histogram of the final encrypted image is comparatively uniform and is significantly different from that of the original image thus not revealing any hint for statistical attack.

5.3 Correlation Coefficient

To study the correlation property of horizontally adjacent pixels, vertically adjacent pixels and also diagonally adjacent pixels for the original image and scrambled image, 1000 pairs of adjacent pixels were selected randomly and the correlation coefficient of each pair is computed using Eq.9:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (9)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big) \quad (10)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (11)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (12)$$

Here *x* and *y* are grayscale values of two adjacent pixels in the image.

In Table 1, higher value of correlation coefficient of original image indicates pixels in original image are highly correlated, whereas the smaller value of correlation coefficient of encrypted image indicate lesser correlation between image pixels which is the property desired from any image encryption technique.

Table 1. Entropy and Correlation coefficients of original and scrambled image

		Horizontal correlation coefficient	Vertical correlation coefficient	Diagonal correlation coefficient	Entropy
Image 1	**Original image**	0.9745	0.9923	0.9804	3.8013
	Scrambled image	0.0173	0.0391	0.0063	7.9431
	Reduction(%)	98.21	96.05	99.35	
Image 2	**Original image**	0.9743	0.9841	0.9616	6.0707
	Scrambled image	0.0244	0.0152	0.0022	7.9391
	Reduction(%)	97.49	98.45	95.93	
Image 3	**Original image**	0.8863	0.8206	0.7487	6.5604
	Scrambled image	0.0710	0.0149	0.0228	7.9385
	Reduction(%)	91.99	98.18	92.20	
Image 4	**Original image**	0.9043	0.9111	0.8391	7.4672
	Scrambled image	0.0448	0.0636	0.0475	
	Reduction(%)	95.04	84.12	78.24	7.8338

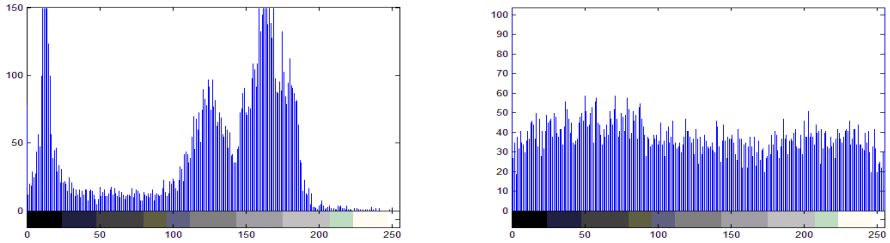


Image 1

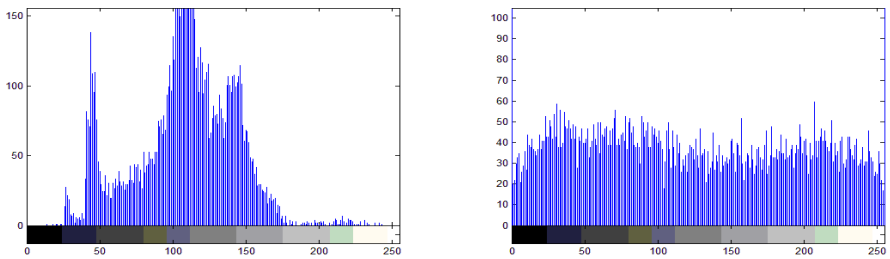


Image 2

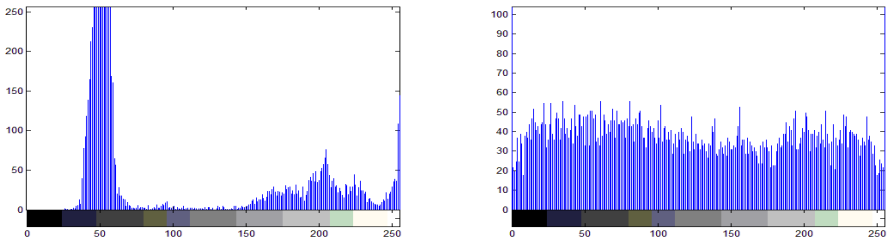


Image 3

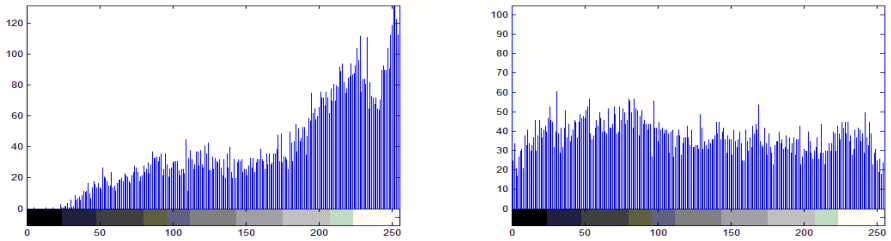


Image 4

(a) (b)

Fig. 6 (a) Histograms of original images (b) Histogram of Encrypted images

VI. CONCLUSION

A method proposed for simultaneously encrypting stack of images has produced promising results. A substitution process is proposed through which pixel intensity is altered using the property (area) of the 2D grid to which the pixel/pixel cube is mapped. A permutation method to shuffle pixels/pixel cube using 3D cat map was explored. Promising results are obtained for all the experimentations carried out. Encrypting multiple images simultaneously by considering them as 3D block of images, provides efficient results w.r.t statistical features, and also adds another dimension of complexity for various attacks. The model qualifies as an encryption technique more apt for storage security which has not been seriously addressed in separation with transmission security. The novel attempt to use 3D chaotic map for permuting pixels or block of pixels across multiple images is a noteworthy contribution. As future enhancement, the proposed work which employs simple substitution cipher and trapezoidal grids for exploratory purpose of 2D grid framework can also be explored with various other advanced substitution ciphers and chaotic maps.

REFERENCES

[1]. Yuan-Hui Yu, Chin-Chen Chang and Iuon-Chang Lin, A new steganographic method for color and grayscale image hiding, Computer Vision and Image Understanding, Volume 107, Issue 3, September 2007.

[2]. Furht B., D Kirovsk, Multimedia Security Handbook, 2005.

[3]. Shiguo Lian, Multimedia Content Encryption: Techniques and Applications, CRC Press, 2009.

[4]. I. Ozturk, I. Sogukpinar, "Analysis and comparison of image encryption algorithm," Journal of transactions on engineering, computing and technology December, vol. 3, 2004, pp. 38.

[5]. Qiudong Sun; Wenying Yan; Jiangwei Huang; Wenxin Ma, "Image encryption based on bit-plane decomposition and random scrambling", 2nd International Conference on Consumer Electronics, Communications and Networks, 2012, pp. 2630 – 2633.

[6]. A. Akhavan 1, A. Samsudin 1 and A. Akhshani, "On the Speed of Image Encryption with Chaotically Coupled Chaotic Maps", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 3, May 2012

[7]. Prabhudev Jagadeesh, Nagabhushan, Pradeep Kumar, "A Novel Image Scrambling Technique Based On Information Entropy And Quad Tree Decomposition", International Journal of Computer Science Issues ,Vol.10,Issue 2,No. 1, March 2013.

[8]. Alireza Jolfaei and Abdolrasoul Mirghadri, " Survey: Image Encryption Using Salsa20," IJCSI, Vol. 7, Issue 5, September 2010 pp 213-220.

[9]. Prabhudev Jagadeesh, P.Nagabhushan, R.Pradeep Kumar, "A Novel Color Image Scrambling Technique Based on Transposition of Image-Blocks between RGB Color Components", International Journal of Research in Engineering & Advanced Technology(IJREAT), Vol 1, Issue 2(2013).

[10]. Prabhudev Jagadeesh, P.Nagabhushan, R.Pradeep Kumar, "A Novel Perceptual Image Encryption Scheme Using Geometric Objects Based Kernel", International Journal of Computer Science and Information Technology (IJCSIT), Vol 5, No. 4(2013).

[11]. Prabhudev Jagadeesh, P.Nagabhushan, R.Pradeep Kumar, "A New Image Scrambling Scheme through Chaotic Permutation and Geometric Grid based Noise Induction", International Journal of Computer Applications(IJCA), Published by Foundation of Computer Science, New York, USA, Vol 78, No. 4, pp 38-35(2013).

[12]. Shengbing Che; Zuguo Che; Bin Ma, "An Improved Image Scrambling Algorithm", Second International Conference on Genetic and Evolutionary Computing, 2008, pp 495 – 499.

[13]. Mohammad Ali Bani Younes and Aman Jantan, "An Image Encryption Approach Using a Combination of Permutation Technique Followed by Encryption" IJCSNS, April 2008.
[14]. A. Mitra, Y V. Subba Rao, and S. R. M. Prasnna, "A new image encryption approach using combinational permutation techniques," Journal of computer Science, vol.1, no. 1, 2006, pp.127
[15]. Avasare M.G. Kelkar, V.V, "Image encryption using chaos theory", International Conference on Communication, Information & Computing Technology (ICCICT), 2015 pp. 1 – 6.
[16]. G. Chen, Y. Mao, C.K. Chui, A symmetric image encryption based on 3D chaotic maps, Chaos Solitons Fractals 21 , 2004, pp 749–761.