A New Image Scrambling Scheme through Chaotic Permutation and Geometric Grid based Noise Induction

Prabhudev Jagadeesh
Department of Studies in Computer Science
University of Mysore, India

P.Nagabhushan
Department of Studies in Computer Science
University of Mysore, India

R.Pradeep Kumar
Amphisoft Technologies Private Ltd.
Coimbatore, India

ABSTRACT
Digital images cover the major portion of data that is being exchanged over communication network. When digital images are personal or confidential a high level security has to be provided. Traditional Encryption which is normally used to disguise data making it unintelligible to unauthorized observers do not consider the inherent features of images and thus is not considered to be highly effective with regard to computational complexity and also the security level enforced on images. This paper presents a new concept for image scrambling by applying pixel permutation and pixel substitution on an image split into irregular trapezoidal grids. Pixel permutation is performed using Arnold's 2-D cat map which will disarray the pixels. Then substitution is performed employing a distinctive feature that the key for substitution process for pixels are derived from the properties of the trapezoidal grid to which the pixel belongs. Thus pixels mapped to various grids will have different noise induction thus providing high level security. The entire process of pixel permutation and substitution is repeated for several iterations to provide higher level security. The experimental results show that the proposed algorithm can successfully scramble the images, and the security analysis of the algorithm also demonstrates that the proposed scheme can withstand various cryptanalytic and statistical attacks.

General Terms
Security, Image Processing, Chaos Theory.

Keywords
Image Encryption, Scrambling, Chaotic map, 2-D cat map, Image histogram, Image correlation, Entropy.

1. INTRODUCTION
With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks where digital images constitute a major chunk. Many digital services such as pay-TV, confidential videoconferencing, medical and military imaging systems require reliable security in storage and transmission to enforce confidentiality of digital images and videos. Traditionally Encryption is used to disguise data making it incomprehensible to unauthorized observers. There have been several image scrambling schemes for protecting confidentiality of sensitive images basically through cryptographic and steganographic techniques [1]. An image scrambling scheme basically transforms an image into another unintelligible image. Traditional methods for image encryption based on cryptography concept such as Data Encryption Standard (DES) and Advanced Encryption Standard (AES) consider image or videos as a data stream and encrypt them block by block. However, their encryption and decryption processes have huge computation complexity. Intrinsic features of image such as bulky nature, high redundancy and high correlation among pixels call for the need to treat an image in a different way from text data with respect to confidentiality [1]. In spite of many efforts, analysis indicates that security level is still not strong for images and multimedia data in general [1,3]. Also these techniques hardly take into account the significant intrinsic properties of images. This indicates the need for content-based schemes which are simpler yet stronger for protecting confidentiality of digital images. In this direction the proposed approach is one such effort to construct simpler yet efficient security model for image confidentiality.

The rest of this paper is organized as followed. Section 2 provides the related work with regard to Image scrambling. Section 3 presents the basic concept of image encryption using chaotic maps. Section 4 presents the overall architecture and proposed algorithm. Section 5 illustrates the experimental results carried out on various images. Section 6 provides the various security analyses carried out on the proposed algorithm. Finally, Section 7 concludes the paper highlighting the accomplishments and scope for future work.

2. RELATED WORKS
The need to realize the security requirements of digital images have led to the development of several image scrambling techniques. Many efforts have been made to explore specific solutions to image scrambling. Numerous scrambling algorithms have been proposed in the literature based on different philosophy [2-7]. There are image scrambling methods that offer partial scrambling, while others offer strong form of encryption. Algorithms which provide different levels of security ranging from degradation to strong encryption are categorized under scalable algorithms. Permutation based techniques are based on bit, pixel or block permutation [4]. There are approaches to scramble an image in a transformed domain by scrambling the transform coefficients. Some image encryption schemes are based on the multi-round combination of secret permutations and pixel value substitutions. Due to the tight relationship between chaos theory and cryptography, chaotic cryptography has been extended to design image scrambling schemes. Some encryption algorithms have been presented recently which are based on different chaotic maps [7-11]. The encryption algorithms often use two different chaotic maps; one to change image pixel positions; the other is used for changing image pixel values. A chaotic map based block cipher is a

type of symmetric-key encryption algorithm that transforms a fixed-length group of plaintext bits into a group of ciphertext bits of the same length. Many symmetric block encryption techniques based on two-dimensional chaotic map, such as the standard map, cat map and baker map have been proposed [17-21]. A chaotic stream cipher is a pseudorandom cipher generated by a chaotic map, which is used to encrypt a plaintext by an XOR operation. All these techniques substantiate Chaos based encryption techniques as a good approach for realistic use since these methods provide a good combination of speed and high security at reasonable computational complexity.

3. IMAGE SCRAMBLING USING CHAOTIC MAPS

The simplicity of discrete chaotic maps and well established chaos theory makes it a viable technique for image and video encryption to produce practically good solutions. Basically there exists two typical ways to use chaos in image and video scrambling schemes. One approach is to make use of chaos as a source to generate pseudorandom bits with desired statistical properties to realize secret encryption. The other approach is to use 2-D chaotic maps to realize secret permutations of digital images. The latter has been specially employed for chaos-based image encryption. The idea of using 2-D chaotic maps to design image encryption schemes was primarily proposed in [12-15] and later standardized in [16-21]. Assuming that the size of the plain image is M x N, the scrambling procedure depicted in Fig 1 can be described as follows:

i) Define a discretized and invertible 2-D chaotic map on an M x N lattice. The discretized parameters act as the secret key.

ii) Apply the discretized 2-D chaotic map on the plain image to permute all pixels.

iii) Transform the values of all the pixels using a substitution algorithm resulting in a flattened histogram of the image, implying uniform distribution of pixels.

iv) Repeat the permutation and substitution process certain number of iterations to obtain the scrambled image.

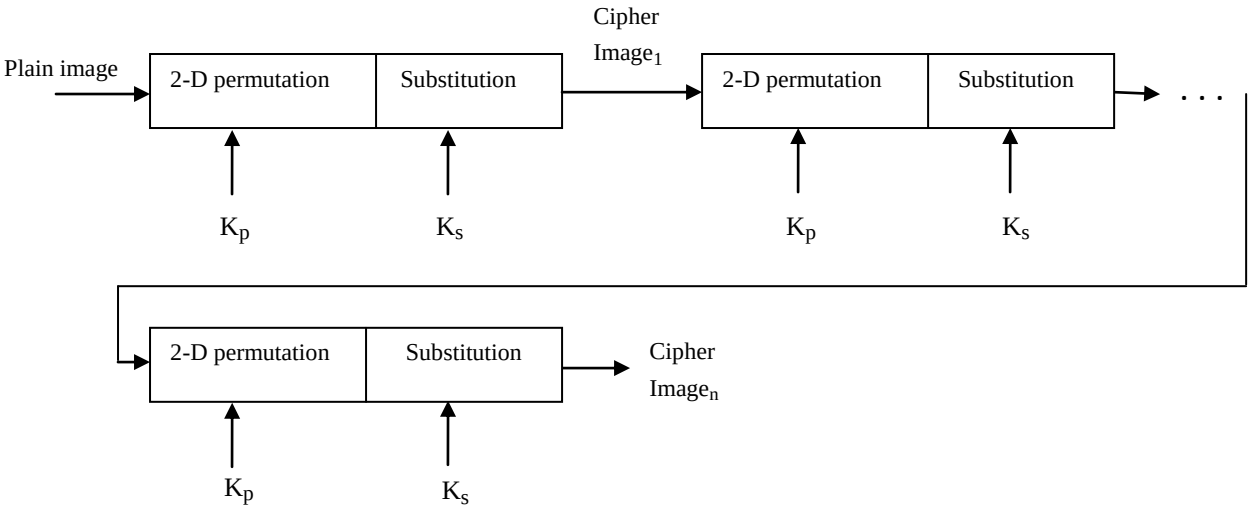


Fig 1: Image Encryption System based on chaotic permutations

4. PROPOSED TECHNIQUE

4.1 Methodology and Distinctive Features

The proposed approach is based on pixel permutation using 2-D cat map and pixel substitution employing a novel concept of geometrical grid based noise induction. The proposed scheme for scrambling is given in Fig 2. As per this scheme the 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 constrain the grids formed to trapezoidal grids. This method of partitioning has a higher probability of image being partitioned into unique 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. For this a p x q pixel block is mapped on to a grid where its center lies. Fig 3 illustrates the formation of grids on an image. Pixel permutation is carried out using Eq.(2).The keys for pixel substitution 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 process of pixel permutation and pixel substitution is repeated for n iterations to achieve the desired level of security. The parameters of the 2-D chaotic map and the number of iterations act as the key for realizing secret permutation of pixels while the slopes, intercept and interval of horizontal lines act as keys for pixel substitution. The same set of keys is used for descrambling the image.

For pixel permutation the 2-D invertible cat map introduced by Arnold and Avez [18-19] is used which is given as:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A \begin{pmatrix} x_n \\ y_n \end{pmatrix} (mod 1) \tag{1}$$

Where, $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$

In Eq. 1 (x_n, y_n) are the original coordinates and (x_{n+1}, y_{n+1}) are the transformed coordinates. The discretized version of generalized 2-D invertible cat map is obtained by changing the range of (x, y) from the unit square to the discrete lattice N × N as below:

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & ab+1 \end{pmatrix} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (mod N) \quad (2)$$

a and *b* are positive integers and determinant of *A* is 1.

The distinctive feature of the proposed approach is that unlike the traditional image scrambling techniques which employ the same key or keys derived from the primary secret key, the proposed method generates the keys for substitution process from the grid structure formed on the image. For this the various parameters of the lines constitute as input. The uniqueness of the proposed approach is that it can support fixed length key or variable length key by restricting the maximum number of lines or by allowing number of lines to be arbitrary respectively. Further the choice of trapezoid as the geometric grid makes the grid formation complexity simpler yet providing grids with varied dimensions resulting in assorted noise added to pixels. Also the choice of variable number of lines and slopes results in a large key space which is very much desired in an efficient encryption technique to prevail over any attempt of brute force attack. Since the key for substitution process is derived from only the geometrical properties of the image grids, even distortion or loss of some pixel values during transmission will have an effect limited to only those pixels during the decryption process thus making the proposed approach robust.

4.2 Algorithm

Step 1: Divide the image of size *N* x *N* into arbitrary sized trapezoidal grids.

This is done as follows:

ii) Draw horizontal straight lines on the image i.e., lines with zero slope at regular intervals of rows '*r*'.

ii) Draw straight lines L_i with slopes m_i and y-intercept c_i as shown in Fig. 3 between the first and last rows of the image. Further the slopes of the lines are chosen such that the straight lines do not intersect within the image area.

Step 2: Record the slope and y-intercept (m_i, c_i) for all the lines.

Horizontal line row interval 'r' and (m_i, c_i) are preserved as keys for computing the areas of various arbitrary sized trapezoidal grids formed on the image.

Step 3: Compute the area of the trapezoidal grids using Eq. (3) given below.

$$Area = ((s+t)*h)/2 \quad (3)$$

h is the height of the trapezoidal grid, *s* and *t* are the bases of the trapezoid. *s* and *t* are computed by finding the point of intersection of two straight lines using their slopes and intercepts. Here *h*=*r*.

Step 4: Divide the image into blocks of size *p* x *q* pixels.

Step 5: Map these image blocks of size *p* x *q* onto their respective trapezoidal grid.

The mapping is done such that an image block is assigned to a grid if the center of the image lies on that grid.

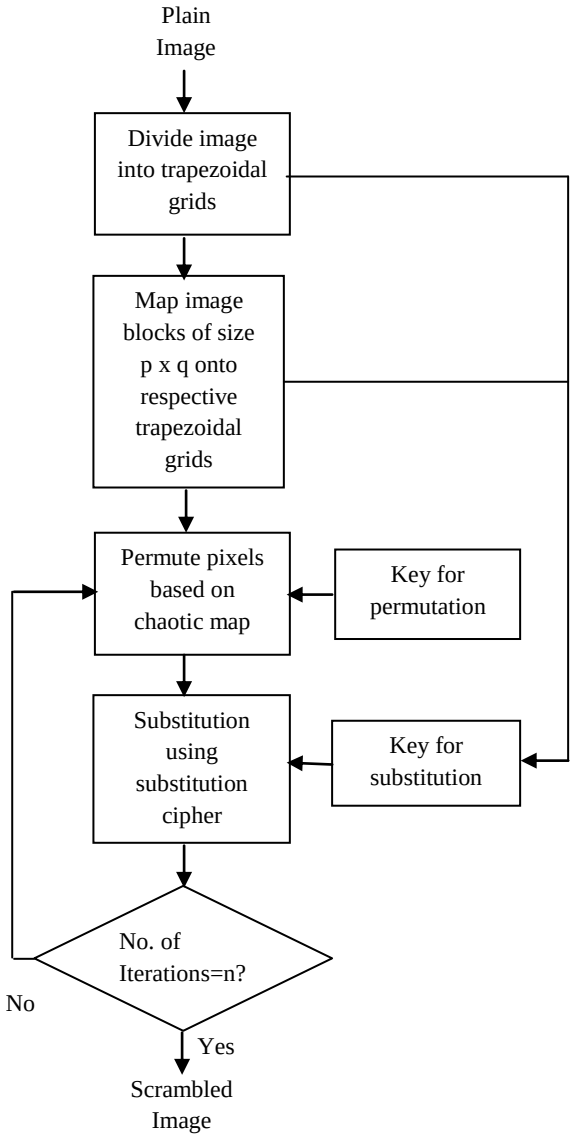


Fig 2: Proposed Scheme for Scrambling

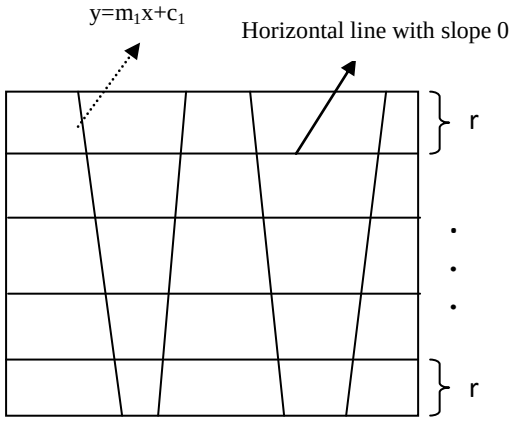


Fig 3: Grid Formation on an Image

Step 6: Perform permutation of pixels using Arnold 2-D chaotic map defined in Eq. (2).

i.e., translate the original coordinates (x, y) of the image into the new coordinate (x', y') as below:

$$x' = (x + a*y) \pmod N \quad (4)$$

$$y' = (b*x + (a*b + 1)*y) \pmod N \quad (5)$$

Step 7: Using *Area* as key perform substitution using a substitution cipher.

$$c = (p + Area) \bmod 256 \quad (6)$$

p is the original pixel and c is the transformed pixel.

Step 8: Repeat step 6 and step 7 n times.

For decryption and reconstruction of the original image, the above encryption process is reversed by using the same keys employed during encryption. Permutation of pixels is reversed using the inverse transformation given in Eq. (7).

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix} = A^{-1} \begin{pmatrix} x_n \\ y_n \end{pmatrix} (mod\ N) \quad (7)$$

$$A^{-1} = \begin{pmatrix} ab+1 & -a \\ -b & 1 \end{pmatrix}$$

5. EXPERIMENTAL RESULTS

Several images were tested using the proposed image scrambling scheme. The results for a grayscale image and a color image of sizes 512 x 512 are indicated in Fig 4 and Fig 7. For *Image 1* chaotic map parameters chosen are a=20, b=4 and number of iterations n=4. For *Image 2* chaotic map parameters chosen are a=40, b=8 and n=5.

6. SECURITY ANALYSIS

A good encryption procedure must be robust against all kinds of brute force, cryptanalytic and statistical attacks. To analyze the security of the proposed scheme, Entropy analysis, Histogram analysis and Correlation Coefficient analysis is carried out. Analysis of the proposed approach reveals that it is indeed strong against the most common attacks.

6.1 Histogram Analysis

An image histogram can be used to measure the statistical similarity between the original image and the scrambled image. Histograms demonstrate how pixels in an image are distributed by plotting the number of pixels at each intensity level. Histograms of several original images and corresponding encrypted images that have widely different content are analyzed. Histograms for the test images mentioned above are given in Fig 5 and Fig 8. It is evident from the results obtained that the histogram of the scrambled image compared to the original image is reasonably uniform and evenly spread across all possible intensity levels. Hence the scrambled image does not provide any clue for statistical attack.

6.2 Correlation Analysis

To examine the horizontal, vertical and diagonal correlation property among adjacent pixels, 1000 pairs of adjacent pixels were selected randomly and the correlation coefficient of each pair is computed using Eq.(8) for original image and scrambled image:

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (8)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\big(x_i - E(x)\big)\big(y_i - E(y)\big) \quad (9)$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (10)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (11)$$

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

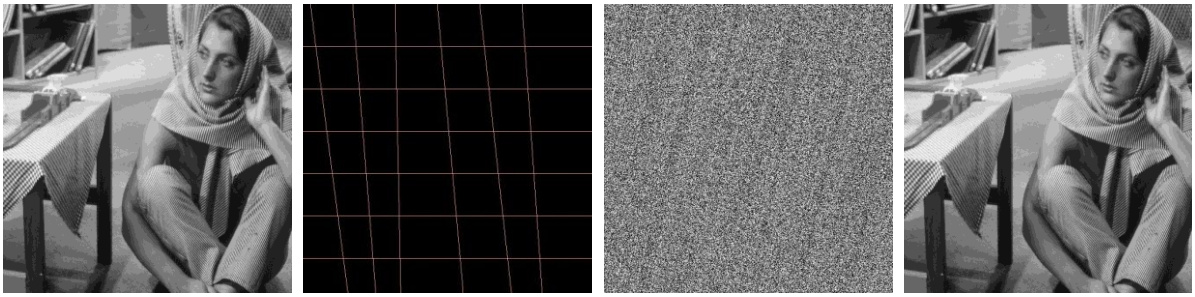
It can be observed from Fig 6 and Fig 9 that the adjacent pixels of original image are highly correlated with a larger correlation coefficient. In Table 1, higher value of correlation coefficient of original image indicates pixels in original image are highly correlated, whereas the smaller value of correlation coefficient of scrambled image indicate lesser correlation between image pixels which is the property desired from any image scrambling technique.

6.3 Entropy Analysis

Entropy, in an information sense is a measure of unpredictability. Entropy is proved to be a good method to express randomness or uncertainty of a random variable. 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:

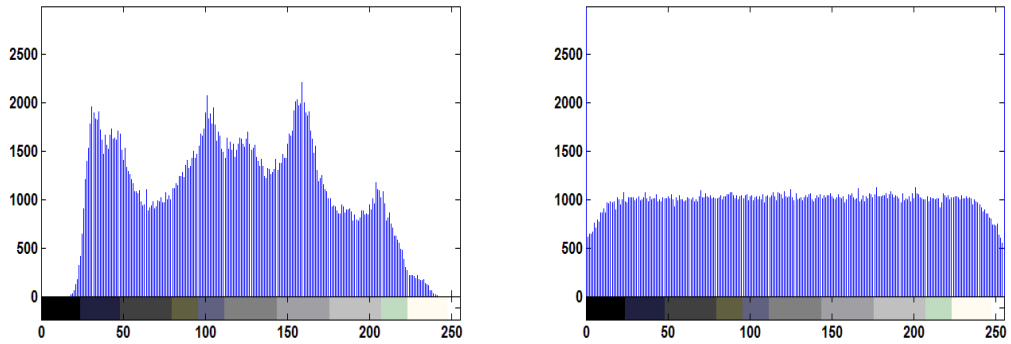
$$E_n = \sum_{i=0}^{255}(p(i) * log_2(\frac{1}{p(i)}) \quad (12)$$

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 values obtained for various scrambled image indicate that the proposed method results in a scrambled image that is more heterogeneous thereby reducing the information revealed. The entropy of plain image and scrambled image are listed in Table.1.



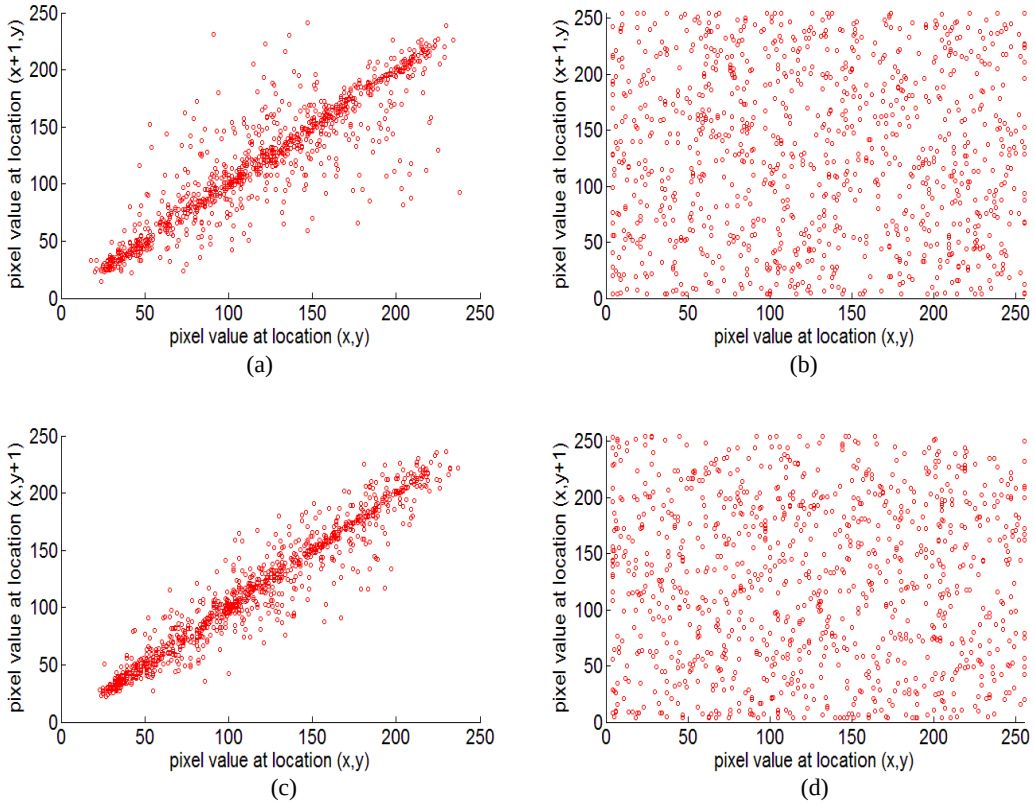
(a) (b) (c) (d)

Fig.4: *Image 1*. (a) original image (b) Grid used for scrambling (c) Scrambled image (d) Decrypted image.



(a) (b)

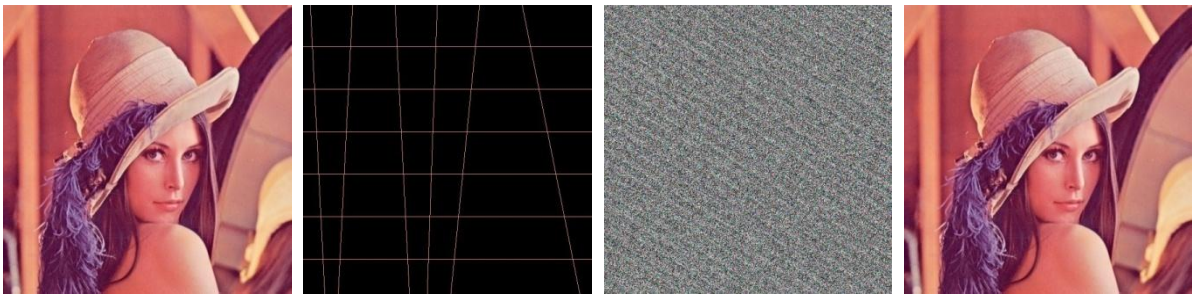
Fig 5: Histogram Analysis of Image *1*: (a) Histogram of orignal image. (b) Histogram of scrambled image.



(a) (b)

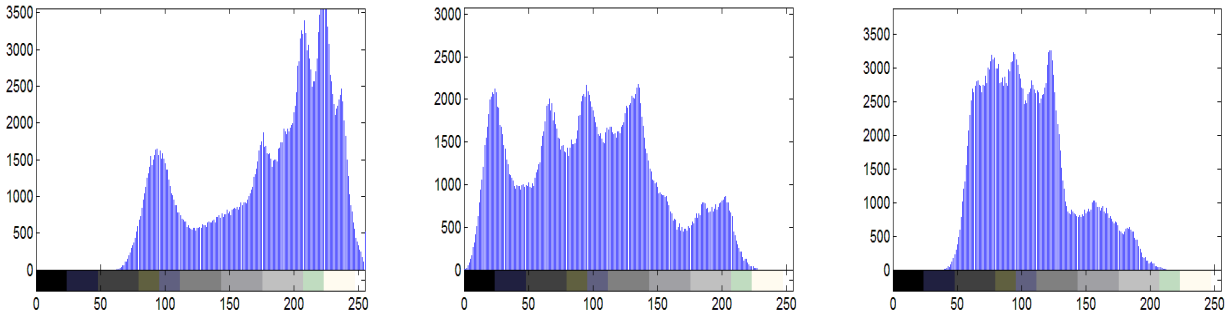
(c) (d)

Fig 6: Correlation Analysis of two adjacent pixels of *Image 1*: (a) Correlation of two horizontally adjacent pixels in original image. (b) Correlation of two horizontally adjacent pixels in scrambled image. (c) Correlation of two vertically adjacent pixels in original image. (d) Correlation of two vertically adjacent pixels in scrambled image.

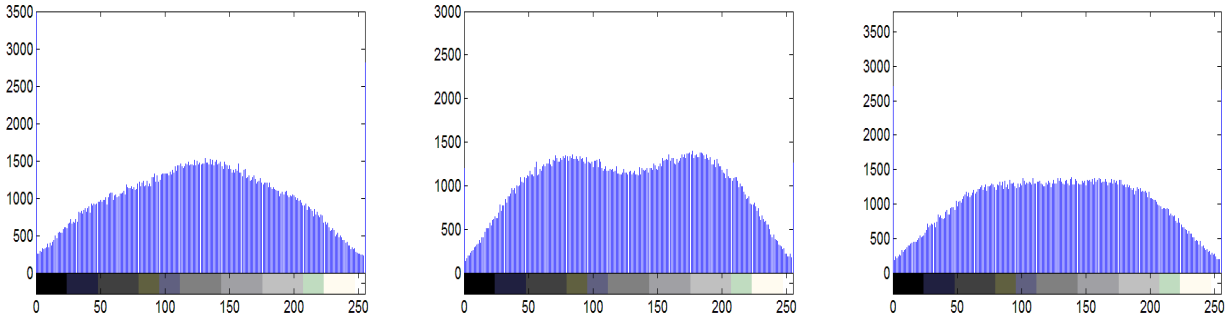


(a) (b) (c) (d)

Fig 7: *Image 2*: (a) Original image (b) Grid used for scrambling (c) Scrambled image (d) Decrypted image.



(a) (b) (c)



(d) (e) (f)

Fig 8: Histogram Analysis of *Image 2*: (a) to (c) Histograms of red, green and blue components of orignal image. (d) to (f) Histograms of red, green and blue components of scrambled image.

Table 1: Entropy and Correlation Coefficients of original image and scrambled image

		Image 1		*Image 2*	
		Original image	**Scrambled image**	**Original image**	**Scrambled image**
Correlation Coefficient	**Horizontal**	0.97135	0.00651	0.97963	0.03089
	Vertical	0.98425	0.01747	0.98355	0.01003
	Diagonal	0.94387	0.02016	0.94108	0.01194
Entropy		7.6321	7.9623	7.2665(Red) 7.5948(Green) 6.9816(Blue)	7.8636(Red) 7.8956(Green) 7.8797(Blue)

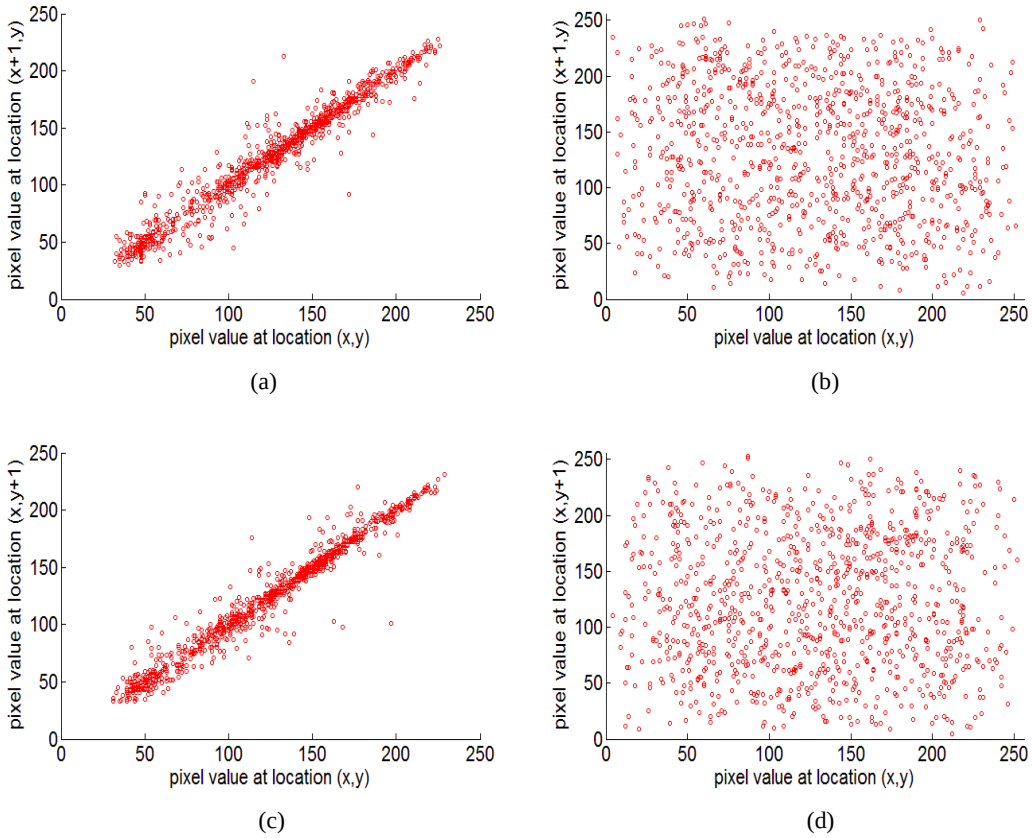


Fig 9: Correlation Analysis of two adjacent pixels of *Image 2*: (a) Correlation of two horizontally adjacent pixels in original image. (b) Correlation of two horizontally adjacent pixels in scrambled image. (c) Correlation of two vertically adjacent pixels in original image. (d) Correlation of two vertically adjacent pixels in scrambled image.

7. CONCLUSION

The proposed work is a novel scheme for image scrambling with the unique feature that the key for pixel substitution is derived from the assorted grids formed by partitioning the image. This result in varied noise induced onto pixels depending on the grid to which it is mapped. With this distinctive property employed for pixel substitution, together with efficient permutation of pixels using 2-D cat map, the proposed scheme qualifies as a strong image scrambling technique. The user has the flexibility to choose the number of iterations for applying the chaotic transform to achieve different levels of security. The parameters of the chaotic function, parameters of the image grids and the number of iteration acts as security keys and also together provide a key space large enough to make brute force attacks and other cryptanalytical attacks infeasible. As future enhancement, the proposed work which employs simple substitution cipher and trapezoidal grids for exploratory purpose of the geometric grid framework can also be explored with various other advanced substitution ciphers and chaotic maps alongside other geometric grids.

8. REFERENCES

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

[2] Furht, Kirovsk. 2005. Multimedia Security Handbook. CRC press.

[3] Alireza Jolfaei, Abdolrasoul Mirghadri. 2010. Survey: Image Encryption Using Salsa20. International Journal of Computer Science Issues, Vol. 7, Issue 5, 213-220.

[4] S. Li, C. Li, G. Chen, N. G. Bourbakis, and K. T. Lo. 2008. A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks. Signal Processing: Image Communication, vol. 23, no. 3, 212–223.

[5] T. Xiang, X. Liao, G. Tang, Y. Chen, and K. W. Wong. 2006. A novel block cryptosystem based on iterating a chaotic map. Physics Letters, Section A, vol. 349, 109–115.

[6] Prabhudev Jagadeesh, P. Nagabhushan, R. Pradeep Kumar. 2013. A Novel Image Scrambling Technique Based On Information Entropy And Quad Tree Decomposition. International Journal of Computer Science issues, Volume 10, Issue 2, No. 1.

[7] Ye Liu,, Junlei Lin, Jinghui Fan, Nanrun Zhou. 2012. Image Encryption Based on Cat Map and Fractional Fourier Transform, Journal of Computational Information Systems, 7485–7492.

[8] Qian Li, Yang Wang. 2011. The performance analysis of image encryption algorithm based on chaotic system. International conference on Electronic and Mechanical Engineering and Information, Volume 7, 3492-3494.

[9] G. Zhang and Q. Liu. 2011. A novel image encryption method based on total shuffling scheme, Optics Communications, vol. 284, no. 12, 2775–2780.

[10] Zhu, W. Zhang, K.-W. Wong, and H. Yu. 2011. A chaos-based symmetric image encryption scheme using a bit-level permutation. Information Sciences, vol. 181, no. 6, 1171–1186.

[11] Yicong Zhou, Karen Panetta, Sos Agaian. 2009. Image Encryption Based on Edge Information. Proceedings of SPIE-IS&T Electronic Imaging.

[12] Pichler, F and Scharinger, J. 1996. Finite dimensional generalized Baker dynamical systems for cryptographic applications. Proceedings of 5th International Workshop on Computer Aided Systems Theory, Lecture Notes in Computer Science, Vol. 1030, 465–476.

[13] Scharinger, J. 1997. Fast encryption of image data using chaotic Kolmogorov flows in Storage and Retrieval for Image and Video Databases. Proceeding SPIE, Vol. 3022, 278–289.

[14] Fridrich, J. 1997. Image encryption based on chaotic maps. In Proceedings of IEEE International Conference on Systems, Man and Cybernetics, Vol. 2, 1105–1110.

[15] Fridrich, J. 1997. Secure image ciphering based on chaos, Technical Report RL-TR-97-155, The Information Directorate of the Air Force Research Laboratory, New York.

[16] Fridrich J. 1998. Symmetric ciphers based on two dimension chaotic maps. International Journal of Bifurcation and Chaos, 1259 – 1284.

[17] Scharinger, J. 1998. Secure and fast encryption using chaotic Kolmogorov flows. In Proceedings of IEEE Information Theory Workshop, 124–125.

[18] N.K. Pareek, Vinod Patidar, K..K. Sud. 2006. Image encryption using chaotic logistic map. Image and Vision Computing 24, 926–934

[19] G. Chen, Y. Mao, C.K. Chui. 2004. A symmetric image encryption based on 3D chaotic maps, Chaos Solitons Fractals 21, 749–761.

[20] Lizhen Chen. 2012. A Novel Image Encryption Scheme Based on Hyperchaotic Sequences. Journal of Computational Information Systems. 4159 – 4167.

[21] H. Gao, Y. Zhang, S. Liang, and D. Li. 2006. A new chaotic algorithm for image encryption, Chaos. Solitons & Fractals, vol. 29, no. 2, 393–399.

[22] Gonzalez, R.C., R.E. Woods, S.L. Eddins. 2007. Digital Image Processing, Second Edition, Prentice Hall.

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