International Journal of Electrical and Computer Engineering (IJECE)
Vol. 10, No. 1, February 2020, pp. 786~800
ISSN: 2088-8708, DOI: 10.11591/ijece.v10i1.pp786-800

A new partial image encryption method for document images using variance based quad tree decomposition

C. R. Revanna[1], C. Keshavamurthy[2]
[1]Research Scholar at Jain University, Bangalore, India
[1]Faculty of ECE, Government Engineering College, Ramanagara, Karnataka, India
[2]Professor, Department of ECE, SRSIT, Bangalore, Karnataka, India

Article Info

Article history:

Received Feb 18, 2018
Revised Aug 21, 2019
Accepted Sep 27, 2019

Keywords:

MSE
NPCR
PSNR
SSIM
UACI

ABSTRACT

The proposed method partially and completely encrypts the gray scale Document images. The complete image encryption is also performed to compare the performance with the existing encryption methods. The partial encryption is carried out by segmenting the image using the Quad-tree decomposition method based on the variance of the image block. The image blocks with uniform pixel levels are considered insignificant blocks and others the significant blocks. The pixels in the significant blocks are permuted by using 1D Skew tent chaotic map. The partially encrypted image blocks are further permuted using 2D Henon map to increase the security level and fed as input to complete encryption. The complete encryption is carried out by diffusing the partially encrypted image. Two levels of diffusion are performed. The first level simply modifies the pixels in the partially encrypted image with the Bernoulli's chaotic map. The second level establishes the interdependency between rows and columns of the first level diffused image. The experiment is conducted for both partial and complete image encryption on the Document images. The proposed scheme yields better results for both partial and complete encryption on Speed, statistical and dynamical attacks. The results ensure better security when compared to existing encryption schemes.

Corresponding Author:

C. R. Revanna,
Research Scholar at Jain University, Bangalore, India
Faculty of ECE, Government Engineering College,
Ramanagara, Karnataka, India.
Email: revannacr2008@gmail.com

1. INTRODUCTION

The storage and exchange of images with high definition, redundancies and correlation of an important document at a higher rate of transmission itself takes a longer time and the encryption of such images takes additional computational time too. This requires a balance between security and synchronization for real time applications. In such situations, where high definition, low memory and low power are the limitations of the resources, partial encryption of the data is advantageous than encrypting an entire image. Partial encryption helps in reducing the computations and bandwidth. The document images consist of correlated and uncorrelated parts. Encryption of only the correlated part suffices than encrypting the complete image. The core idea of partial encryption is to first identify the significant pixels or region of pixels and then encrypt that region. Partial encryption also includes encryption of data with different security levels to suit end user customer requirement. A significant region from the complete image may be selected either statistically or dynamically for partial encryption to fulfill security and computational time for real time applications. So the partial encryption increases the efficacy of encryption by reducing computation size. To ensure a good security level a minimal data of 12.5% has to be encrypted [1].

In [2], the authors proposed a bit-level scrambling algorithms to scramble bit positions. It is also said that the proposed algorithm provides flexibility to select any image as the input source image, any decomposition technique for obtaining the bit plane, any decomposed bit plane as the security key bit plane and any scrambling technique for the bit-level permutation. In [3], a chaotic system based partial image encryption is proposed. The proposed scheme includes bit plane decomposition of source image. After decomposing, the significant bit plane are selected for encryption. Encryption is achieved by generating the pseudorandom number sequence using chaotic system.

In [4], a chaotic based partial grey sale image encryption is proposed. It is observed that the authors proposed a bit plane decomposing method for encryption. The various bit planes (significant and insignificant) are identified based on autocorrelation threshold of different binary planes. The key sequence obtained by chaotic map is used to encrypt the correlated bit planes. In [5], both selective and complete image encryption using the sequence of chaotic map. At first the chaotic map is used to generate a key to completely encrypt the plain image. Second, for the same input image selective portion is encrypted. Finally the complete and selective encrypted results are combined by XOR operation to achieve better security. A new technique called graph coloring problem (GCP) for partial encryption of medical image is proposed in [6]. The GCP technique is used to select the optimal positions of the pixels from the input medical image. In [7], researchers presented a partial image encryption technique based shuffling the pixels within a block. Pixels shuffling are achieved based on the sequence of chaotic map. By selecting varied block size, data encryption quantum can be varied.

In [8], a partial grayscale enciphering based on the chaotic map is proposed. The grayscale image is decomposed into eight binary planes. Scrambling is done for most significant bit planes. The Chaotic sequence generated by the Skew tent map is used to scramble the planes. The scrambled bit planes are encrypted to obtain cipher image. In [9], authors proposed a transform domain approach for partial image encryption. Four sub-bands are arrived at by applying DWT for the input plain image. The low frequency sub-band is encrypted by the sequence generated by the Logistic chaotic map. At last encrypted low frequency band and non-encrypted high frequency band are combined and inverse discrete wavelet transform is applied to obtain the cipher image. Discrete Cosine Transform (DCT) based partial encryption of color image is proposed in [10].

The DCT is applied for the input source image for all three planes. Then the encryption is performed by the sequence generated by the Logistic chaotic map. The encrypted planes are combined and inverse DCT is applied to obtain cipher image. In [11], the authors proposed an enciphering technique based on two levels of permutation and substitution. For every input source image, a dynamic key is generated which results in the basis of encryption processes. Then, a nonlinear S-box method is used for image substitution which is followed by a matrix multiplication which is performed for image diffusion. These two processes finally results in a cipher image. In [12], proposed a technique which combines both partial encryption and image compression. The compression is achieved by the quad tree and SPHIT image compression techniques. Only 13-27% of the quad tree compressed data and less than 2% of the SPHIT compressed data is partially encrypted for security. In [13] an efficient selective image encryption technique combining saw tooth filling, selected pixels, non-linear chaotic map and SVD(singular value decomposition) is proposed. Image scrambling is done using the saw tooth filling, whereas significant pixels are selected based on the pixels of interest. Finally, diffusion is performed on the more weighted pixels using chaotic map and singular value decomposition as the key. A substitution box [S-box] and linear fractional transform technique is proposed in [14] for partial image encryption. The proposed technique uses a lifting wavelet transform in frequency domain, which provides a sensitive information that can be encrypted by the sequence generated from chaotic map. The dual process of confusion and diffusion are carried out via permutation, diffusion and substitution process. In [15], a partial image encryption using DCT and light weight stream technique is proposed. By considering the basic fundamental attacks like statistical attack, replacement attack and differential attack, DCT Coefficients based transformation technique is proposed. In [16], a partial image encryption based on bit plane decomposition is proposed. The input source image is segmented into eight bit planes. Then the significant binary bit plane is considered for encryption. Using the tent chaotic map, a key sequence is obtained for encryption.

In [17], a non-adaptive partial encryption of grayscale image is performed using Chaotic map is proposed. The input source image is sub-divided into eight binary planes. By the Tent map method applying pseudorandom sequences, four significant bit planes are encrypted. The partial image encryption is obtained by scrambling using non sinusoidal wavelets is proposed in [18]. Kekre's Walsh Sequence procedure is used to scramble the image in the transform domain (wavelet). The transform domain helps in preventing the attacks by statistical means. In [19], a partial encryption technique is proposed. Encryption in both Spatial and transform domain has been deployed in this case. The bit plane decomposition technique is used for encrypting the image in spatial domain. At last, the ratio of encryption time and encoding time is calculated

to illustrate the speed performance. In [20], a DCT based partial color image encryption is presented. The DCT is used to select the significant regions in three different planes from the color image. Then the selected regions are encrypted or diffused using the Arnold chaotic map which results in cipher image.

From the literature review, there is a need to encrypt the Document images partially to synchronize with the real time applications and increase the security level for hand held devices and other less computationally capable gadgets. When an image is viewed as a whole with blocks, the blocks with uniform pixel intensity levels (Histogram) exhibit less meaningful information in the image but blocks with unequal pixel intensity levels exhibit more intelligent information and are referred to as significant regions. There is a need to identify blocks with unequal intensity levels. The proposed method uses a different approach to find the significant regions and encrypt only those regions. For identifying the significant regions, the image is segmented into blocks by taking variance as a parameter for Quad-tree Segmentation technique. This method decomposes an image into significant and insignificant blocks. It is enough to encrypt only the significant blocks to partially encrypt an image. The block size is a preset value, depending on the requirement based on the level of security. The partial encryption is performed using a chaotic system. The proposed work is also extended for complete encryption using mixed chaotic system.

2. RESEARCH METHOD

2.1. Quad tree segmentation

The Quad tree method is applied for the division of an image into blocks/regions by applying recursion [21]. The partitioned blocks are arranged in the form of hierarchal tree structure. The root block is called as parent block and the partitioned blocks are called as child blocks. The parent block is segmented into four (quad) equally sized sub-blocks and each sub-block is subjected to a test. A block is checked to see if the criterion for homogeneity is met, if it meets, then no further division is made and the node is left undivided and is called as a leaf node. If the criterion is not met, then divide the block into four sub blocks or regions and apply the test criteria again. The above procedure is performed until each sub-block obeys the criteria. Therefore each node/parent is either have no children or has four children. Hence the quad tree decomposing technique partitions the image into sub blocks or regions that are more homogeneous than the image itself. The least block size is variable one and depends on the requirements that suit the application. The decomposing lasts when Quad tree reaches its minimum size [22].

The quad tree decomposition is shown in the Figure 1 with a tree diagram. The root node indicates the whole image, this node is partitioned into equally sized four sub-blocks if it fails to satisfy the criteria of homogeneity. The leaf node indicates a block satisfies the homogeneity criteria.

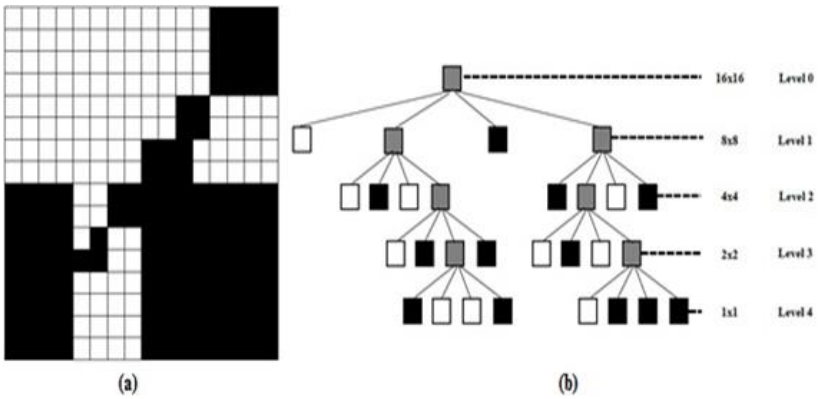

Figure 1. (a) Sample Image, (b) Quad Tree Decomposition Structure

2.2. Image Decomposition Criteria

The quad tree decomposition is made with variance of the image as the criteria. The variance of a block is calculated by computing the mean of the pixels in that block. The variance equation can be given as

$$V(x) = \frac{1}{n} \times \sum_{i=1}^{n} [x_i - \mu(x)]^2. \quad (1)$$

where $\mu(x)$ is the mean of that block.

$$\mu(x) = \frac{1}{n} \times [\sum_{i=1}^{n} x_i]. \quad (2)$$

The variance of the parent block calculated first and the variance of the partitioned children blocks are determined individually. Now check for the variance of the individual block, if it is greater than its parent block, then decompose the child block further. Otherwise the child block is left as a leaf block/node with no further division. This results in decomposing the image with unequal size partitioned blocks. Figure 2 is an example of a picture document which is decomposed into smaller blocks. A 4 × 4 decomposed Lena image is represented in Figure 2(a). Figure 2(b) represents the corresponding mapped blocks.

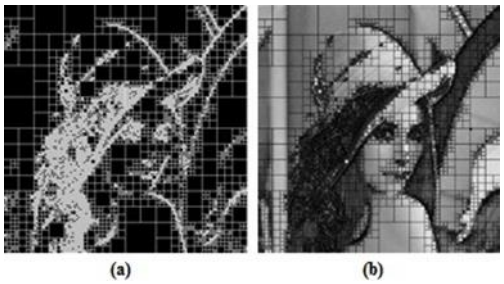

Figure 2. (a) Quad Tree Decomposition with Block Size 4 × 4,
(b) Decomposed Blocks mapped for Lena image

2.3. Chaotic Map

2.3.1. Skew tent map

This chaotic map is one dimensional in nature. It is also called as asymmetric tent map. Mathematically, it is given by

$$x_{n+1} = U(x_n) := \begin{cases} \frac{x_n}{a}, & If\ x_n \in [0, a], \\ \frac{1-x_n}{1-a}, & If\ x_n \in [a, 1]. \end{cases} \quad (3)$$

where a is control parameter ranges from [0, 1] and x_n is the state of system whose value ranges from [0, 1]. At a= 0.5, $U(x_n)$ becomes a regular tent map. Further details can be had on this map in [23].

2.3.2. Bernoulli map

This chaotic map is also one dimensional in nature. General formula for Bernoulli map can be written as follows

$$x_{k+1} = (b\ x_k) mod\ 1\ where\ x\ \in\ [0, 1]. \quad (4)$$

The control parameter of Bernoulli map (i.e., b) should be taken in the range of 1 to 5 to keep chaotic behavior [24, 25]. For $b = 2$, Equation (4) can be written as follows

$$x_{k+1} = (2\ x_k) mod\ 1 := \begin{cases} 2x_n, & If\ x_n \in [0, \frac{1}{2}], \\ 2x_n - 1, & If\ x_n \in \left[\frac{1}{2}, 1\right]. \end{cases} \quad (5)$$

where x_0 = 0.2709 is taken as the initial value. Further details can be had on this map in [26].

2.3.3. Henon map

In discrete time dynamic systems Henon map exhibit good chaotic behavior. It takes the point (X_k,Y_k) in the space and maps it to a new point.
Mathematically it can formulated as

$$x_{k+1} = y_k - 1 + ay_k^2, \quad (6)$$

$$y_{k+1} = bx_k. \quad (7)$$

The initial value $x_0 \in (0, 1)$ and $y_0 \in (0, 1)$ can be used as the key for the system (x_0, y_0). The Henon map mainly depends on two parameters a and b, the research results show that the value for a = 1.4 and b = 0.3, the Henon map exhibits chaotic nature [27].

2.4. Partial image encryption

The resultant decomposed image blocks of minimum size (variable) are scrambled using a Skew tent chaotic map. The partial encryption is performed detailed below.

1. Generate the chaotic sequences using the Skew tent map for each block size.
2. The chaotic sequence generated for a particular block size is used to confuse that block as follows.
   a. Convert the generated chaotic sequences for the block size into natural numbers by multiplying with a factor of 10^{15} (precision of real numbers) and obtain a unique index value whose range lies within the block size (Perform Modulus).
   b. Scramble/permute the various pixels within each block based on the index values generated in the previous step.
3. The steps 1 and 2 are repeated for all the block sizes generated.

The block diagram of the partial and complete encryption is shown in Figure 3 (a). The resultant partial encryption is referred as the first level confusion. The sequence of actions on the Document image is pictorially depicted in Figure 3 (b). The partially encrypted results for the Lena image with block sizes of 8 × 8, 16 × 16 and 32 × 32 are shown in Figure 4 (a), 4 (b) and 4 (c) respectively.

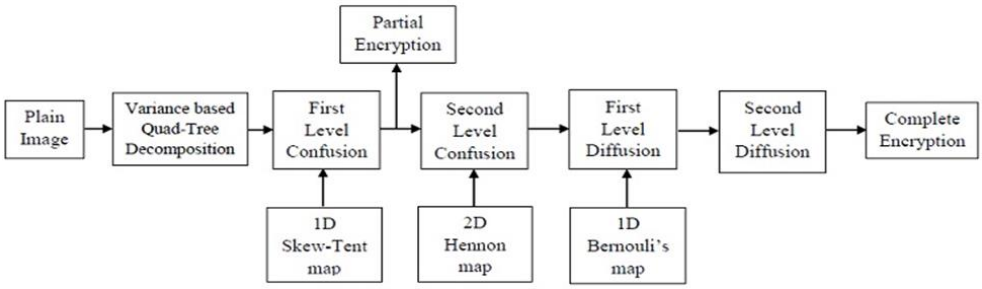

Figure 3 (a). Block diagram of proposed scheme

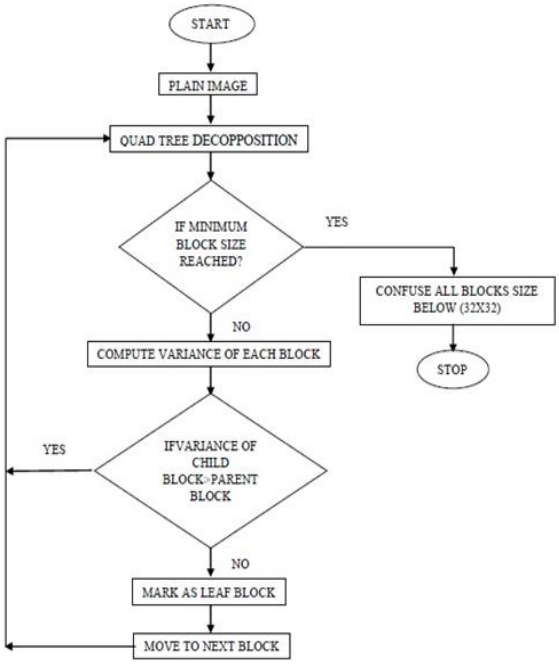

Figure 3 (b). Flow diagram of proposed document image segmentation using quad tree

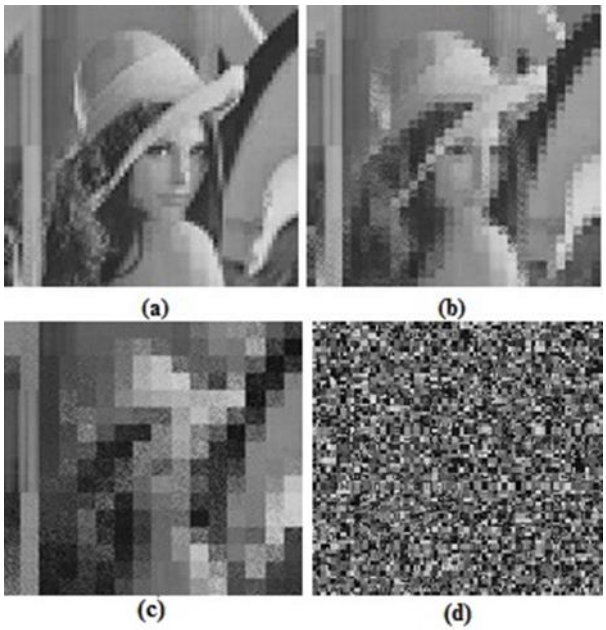

Figure 4. Partially Encrypted Lena images for (a) Block Size equal to 8 × 8, (b) Block Size equal to 16 × 16, (c) Block Size equal to 32 × 32, (d) Second level confused image

2.5. Complete image encryption

The proposed scheme can be further extended for complete image encryption by the addition of second level confusion and diffusion. In diffusion, where the pixel values are modified according to the sequence generated by the chaotic map including, establishing interdependency between the pixels. Diffusion is carried out at the first and second levels.

2.5.1. Second level confusion

1. Divide the partially encrypted image into non-overlapping blocks of size equal to the least level for which the partially encrypted block size is considered.
2. Generate chaotic sequence using 2D Henon map equal to number of blocks.
3. Permute the blocks according to sequence generated by Henon map. The resultant matrix is 'C'.

Figure 4 (d) depicts the second level confused image obtained after the partial encryption.

2.5.2. First level diffusion

1. Generate the chaotic sequence using the Bernoulli's map of size [1, M × N].
2. The generated sequence is converted into integer by multiplying with a factor of 10^{15} and modulus it with 255. Arrange this sequence of integers in order to obtain the matrix 'A' of size M × N.
3. The matrix 'B' which is the result of first level of diffusion is arrived by XORing the pixels of the partially encrypted image (from Section 2.4) with the corresponding pixels (elements) of the matrix 'A' obtained in the previous step.

2.5.3. Second level diffusion

To establish more interdependency between the neighboring pixels

1. Convert the input image matrix I of size M × N into an array X_n .Where n= 1, 2, 3……. M × N.
2. Establish forward row wise interdependency as shown Figure 5 such that

$$X'_n := \begin{cases} X_n, & for\ n = 0, \\ X_n \oplus X'_{n-1}, & for\ n = 1,2,3 \ldots\ldots M \times \mathrm{N}. \end{cases} \quad (8)$$

3. Establish backward row wise interdependency as shown Figure 5 such that

$$X''_K := \begin{cases} X'_K, & for\ K = M \times \mathrm{N}, \\ X'_K \oplus X''_{K+1}, & for\ 0 < K < M \times \mathrm{N}. \end{cases} \quad (9)$$

4. Arrange X_K'' into a matrix J of size M × N, arrange elements of J into an array X_l''' using column wise progressive scan method.
5. Establish column wise pixel inter dependency as shown Figure 5 such that

$$X_l''' := \begin{cases} X_l'', & for\ l = 0, \\ X_l'' \oplus X_{l-1}''', & for\ l = 1,2,3 \ldots\ldots M \times \mathrm{N}. \end{cases} \quad (10)$$

6. Arrange X_l''' into a matrix 'D' of size M × N.
7. The second level diffused image is the resultant matrix 'E' (Cipher Image as shown in Figure 6(b)) obtained by XORing the first level diffused image 'B' with matrix 'D' obtained in step 6.

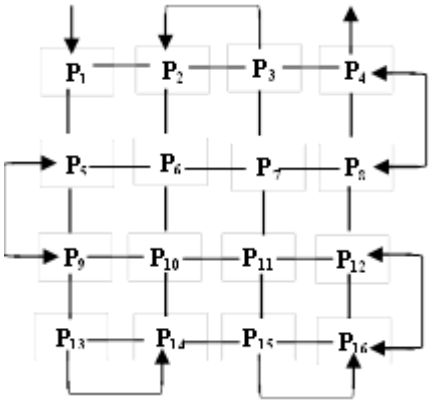

Figure 5. Interdependency matrix generation

Figure 6. (a) Input plain lena image, (b) Complete cipher image

2.6. Complete image decryption

The decryption is the reverse process of encryption. To decipher the encrypted image the following steps are followed.

1. The interdependency matrix 'D' which is shared (by sender) is XORed with the cipher image/matrix 'E' to obtain the first level diffused image 'B'.
2. Generate the matrix 'A' using Bernoulli's map with the same initial conditions and control parameters used in encryption (As in Step 1 and 2 of Section 2.5.2).
3. The second level confused image is obtained by performing XOR of matrix 'C' with 'B'.
4. Generate the Chaotic sequence using 2D Henon map with the same initial conditions and control parameters to permute the non-overlapping blocks obtained at the second level confused image and thus obtain the partially encrypted image.
5. Generate the chaotic sequence using Skew tent map with the same initial conditions and control parameters as in section 2.4 and permute the pixels within the blocks generated out of Quad Tree Decomposition. The resultant image obtained is the Original Plain image.

3. RESULTS AND ANALYSIS

To determine how much efficient the proposed encryption method to provide the security, the performance analysis was developed in MATALAB R2014a software using a Laptop having 4GB RAM and 80GB Hard disc. The simulation outputs of the proposed algorithm reveals that various gray scale images of different sizes (512 × 512 and 256 × 256) are fed as the input plain image. The initial conditions and the control parameters used are as shown in Table 1. The various block sizes used are 8×8, 16×16 and 32×32.

Table 1. Different maps with control parameters and initial conditions used as Keys

MAP	SUB KEYS	CONTROL PARAMETERS	INITIAL CONDITIONS
Skew Tent Map	k_1	a = 0.5	$x_0 = 0.1$
Bernoulli map	K_2	b = 2	$x_0 = 0.2705$
Henon Map	k_3	a = 1.4 b = 0.3	$x_0 = 0.6315477$ $y_0 = 0.18906343$

3.1. Mean square error and peak signal to noise ratio

The mean square error is nothing but the differences in intensity levels of pixels between input and output image representing the noise level. For an ideally completely encrypted cipher image, the MSE value is more but for the partially encrypted image, its value is moderate. MSE is calculated by using the equation

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[plain(i,j)-cipher(i,j)]^2}{M \times N}. \quad (11)$$

The partial encryption is always not secure because only the correlated part of the image is encrypted and the remaining part is left unencrypted. The amount of image encrypted determines the confidentiality level. A better confidentiality level is obtained when a minimum of 12.5% of data encrypted [1]. The proposed method yields 60% of encryption for a block size of 8×8.

$$\%\ \text{of encryption} = \frac{number\ of\ pixels\ encrypted}{total\ number\ of\ pixels}. \quad (12)$$

The PSNR of the encrypted document image should be less than 30dB in order to prevent the interceptor from extracting the plain image out of the noise present in the cipher image. Our method yields a PSNR of 8.8925dB. PSNR is given by

$$PSNR = 10log_{10}\left(\frac{255^2}{MSE}\right). \quad (13)$$

3.2. Histogram

Histogram is a pictorial way of depicting pixel distribution of varying intensity levels. It is plotted as, the total number of pixels with varying intensity along the y-axis and the different intensity levels along the x-axis. The histogram of plain and cipher image are shown in Figure 7. For a completely encrypted image the histogram is flat, but the partially encrypted image has spikes in it and is same as that of the plain image since, only the permutation of the pixels takes place. This depicts that any kind of statistical attack on the completely encrypted image is impossible but for the partially encrypted image it may be possible.

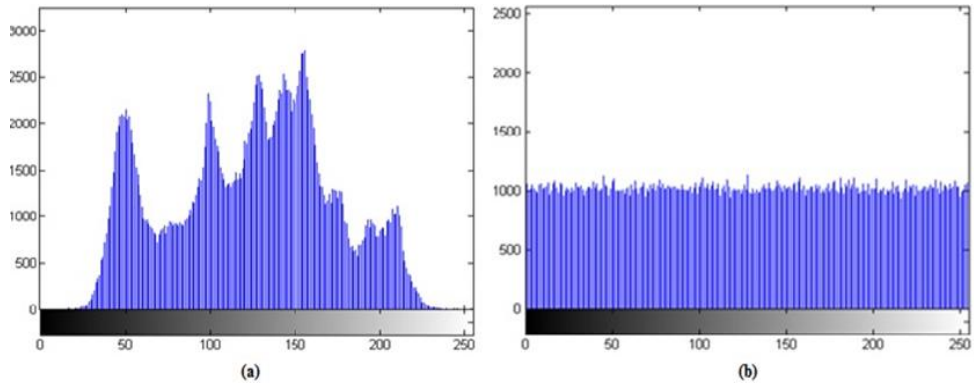

Figure 7. Histogram of (a) Plain image, (b) Cipher image (complete encryption)

3.3. Correlation

A clearly visible image with proper brightness has its correlation coefficient equal to one, but for the ciphered image it has a significantly reduced value (almost equal to zero). An encryption algorithm generates a ciphered image with randomly distributed pixels of different intensities and has its correlation coefficient between adjacent pixels close to zero. A set of 4000 pairs of two adjacent pixels in all directions (horizontal, vertical and diagonal) were randomly selected to determine the correlation coefficient from the plain and ciphered image. The correlation coefficient is given by

$$C_{xy} = \frac{COVR(x,y)}{\sqrt{V(x)}\sqrt{V(y)}}. \quad (14)$$

where $COVR(x, y)$ is the Covariance between x and y. it is given by

$$COVR(x, y) = \frac{1}{n} \times \sum_{i=1}^{n} E[(x_i - \mu(x))(y_i - \mu(y))]. \quad (15)$$

where x and y are two adjacent pixels values in the image, $V(x)$ is the variance of variable x and is given by

$$V(x) = \frac{1}{n} \times \sum_{i=1}^{n} [x_i - \mu(x)]^2. \quad (16)$$

$\mu(x)$ is the mean of variable x.

$$\mu(x) = \frac{1}{n} \times \sum_{i=1}^{n} x_i. \quad (17)$$

The correlation coefficient for the completely ciphered image was found close to zero in all the directions and a value between 0 and 1 for the partially encrypted image. This represents that the algorithm is resistant against statistical attacks. The correlation coefficients for Plain and cipher image in three different directions are shown in Figure 8.

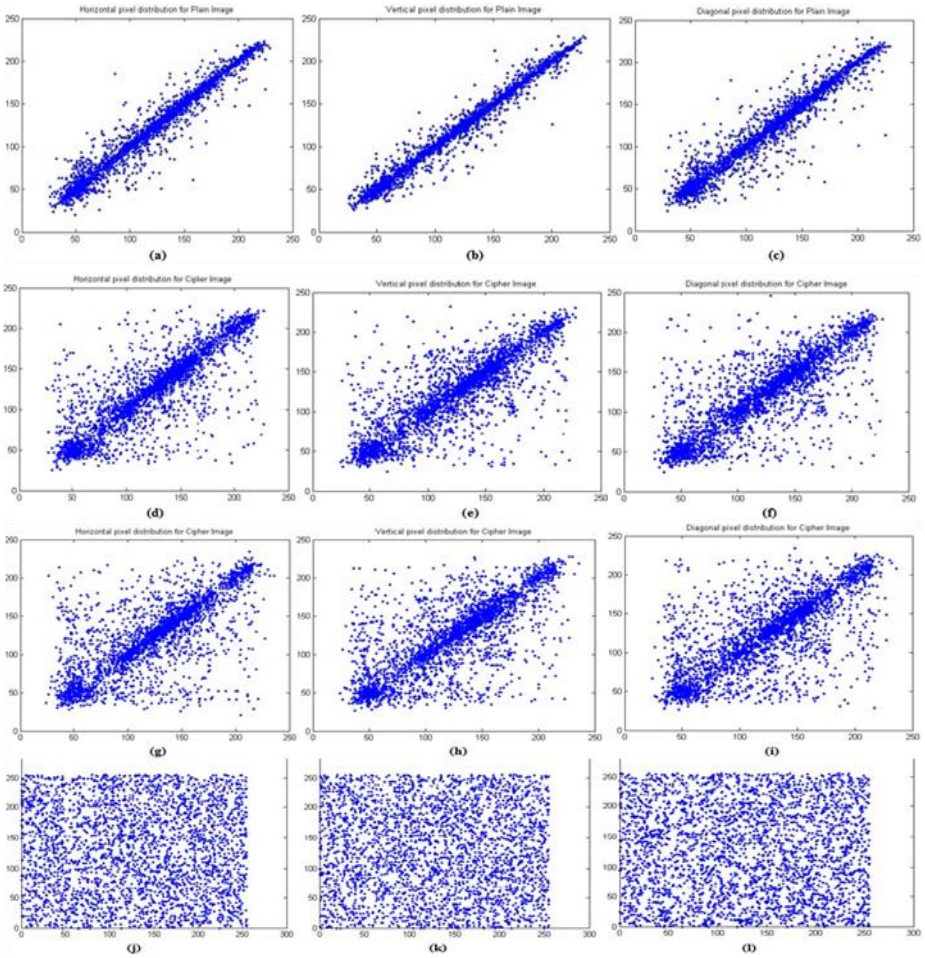

Figure 8. Correlation: (a-c) Correlation for Plain image in three different directions (Horizontal, Vertical and Diagonal), (d-f) Correlation for Cipher image block with size 8×8 in three different directions (Horizontal, Vertical and Diagonal), (g-i) Correlation for Cipher image block with size 16×16 in in three different directions (Horizontal, Vertical and Diagonal) and (j-l) Correlation for Complete Encrypted Cipher image in three different directions (Horizontal, Vertical and Diagonal)

3.4. Key space analysis

It's a measure of the total different keys that are used in the encryption and decryption process. The different secret key K is a combination of sub keys k_1, k_2 and k_3 which are taken from the various maps with their initial conditions and the system parameters used in the system as shown in the Table 1. The sub keys k_1, k_2 and k_3 are extracted from Skew Tent Map, Bernoulli's Map and Henon Map respectively. Consider the precision taken for the keys is of the order of 10^{-15}. Then the total key space used is $(10^{14})^{z}$, where z is the number of initial conditions and system parameters used in all the sub keys (z=8). This results in a very large key space and is sufficiently large to resist the attacks. For an encryption scheme based on chaos, the key space should be greater than the $2^{200} \approx 10^{30}$ [28] to withstand or resistant with the brute-force attack. The proposed method yields a key size of 10^{112} which is very much greater than 10^{30}.

3.5. Key sensitivity test

An encryption algorithm is said to be good if it produces a completely different plain image for a tiny change in the key K, without making any changes in the ciphered image. A plain image of size 512×512 is subjected to an encryption key K= $\{k_1, k_2, k_3\}$ where k_1, k_2 and k_3 are the sub keys. The correct key value K=K_1= {0.5, 0.1, 2, 0.2705, 1.4, 0.6315477, 0.3, 0.18906343} for which the decrypted image is as shown in Figure 9a. It is observed that the deciphered image is exactly same as that of the plain image. For a small change in the key K= K_2 = {0.5, 0.1, 2, 0.2705, 1.9, 0.6315477, 0.6, 0.18906343}, K = K_3 = {0.5, 0.1, 5, 0.1, 1.4, 0.6315477, 0.3, 0.18906343} and K= K_4 = {0.3, 0.2, 2, 0.2705, 1.4, 0.6315477, 0.3, 0.18906343} for which the decrypted images are entirely different from that of the plain image is shown in Figure 9b, 9c and 9d respectively. A tiny change in the value of key produces a completely different plain image for the same input cipher image. Hence the algorithm is key sensitive.

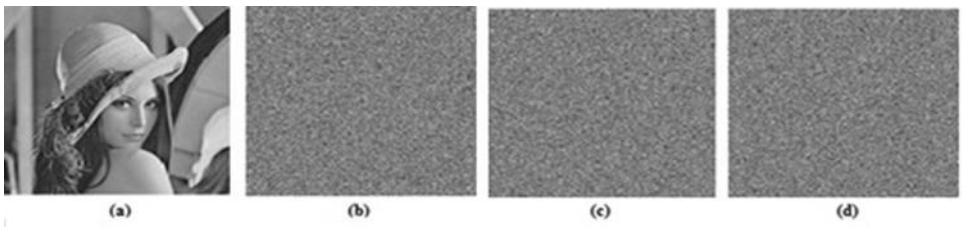

Figure 9. Decryption: (a) Cipher Image Decrypted with Correct Key K_1, (b-d) Decrypted using wrong Keys [(b) with K_2, (c) with K_3, and (d) with K_4]

3.6. NPCR AND UACI

An interceptor can make a tiny modification in the plain image and observe the changes in the output ciphered image. By doing so, the significant relationship between the input and output images can be observed. If it is observed that significant changes taken place in the ciphered image for a tiny change in the plain image, it means that the interceptor can extract the key used for the encryption and crack the algorithm. To check for the efficiency of this algorithm two parameters are calculated. They are NPCR and UACI. The ideal value for NPCR and UACI are 100 and 33.33 respectively [29].

$$\text{NPCR} = \frac{\sum_{i,j} W(i,j)}{M \times N} \times 100. \quad (18)$$

where M and N are the width and height of the image. $W(i,j)$ Can be defined as

$$W(i,j) := \begin{cases} 1, & If\ Cip1(i,j) \neq Cip2(i,j), \\ 0, & If\ Cip1(i,j) = Cip2(i,j). \end{cases}$$

where
$Cip1(i,j)$ Grey value of cipher image and
$Cip2(i,j)$ Grey value of new cipher image

$$\text{UACI} = \frac{1}{M \times N} \times \sum_{i,j} \frac{abs(Cip1(i,j) - Cip2(i,j))}{255} \times 100. \quad (19)$$

The results of the above tests for both partial and complete are shown in the Table 2 and Table 3. The results reveal that the algorithm is better than the existing methods.

3.7. Speed

The speed at which the encryption algorithm converts the plain image into a ciphered image is instrumental for real time applications. This algorithm is executed using a system with its specifications $k_1 = a$= 0.5 for skew tent map and $k_2 = x_0$ = 0.2709 for Bernoulli's map. It is found that the encryption speed is 133.723 m sec for partial and 622.517 m sec for complete encryption as in Table 2 and Table 3. It's compared with the other works in the Table 2 and found that this algorithm is more suitable for real time applications.

Table 2. Comparison of proposed partial encryption results with existing work

INPUT IMAGE [Reference]	PSNR	ENTROPY	ENCRYPTION (%)	EXECUTION TIME (m sec)	MSE
HAND [6]	19.6400	NA	18.7300	NA	NA
LENA [7]	29.8288	NA	NA	NA	67.6390
LENA [20]	10.1530	NA	NA	NA	NA
HAND [PROPOSED]	10.9811	7.1062	NA	NA	NA
LENA [PROPOSED]	16.3585	7.4458	18.5941	133.72	1.099×10^3

(Note: NA= Not Applicable)

Table 3. Comparison of complete encryption results with existing work

Reference	PSNR	NPCR	UACI	Correlation			EXECUTION TIME (m sec)	ENTROPY
				Horizontal	Vertical	Diagonal		
[2]	NA	96.4600	33.1000	0.0102	0.0053	0.0161	3500	NA
[14]	NA	99.6493	33.4305	NA	NA	NA	NA	NA
[17]	8.9055	97.2387	22.2154	NA	NA	NA	398	NA
[29]	8.3581	100.00	33.4657	0.0220	-0.0215	-0.0215	71.2	7.9993
[30]	NA	99.6390	27.7672	NA	NA	NA	7440	7.9978
[31]	NA	99.6108	33.4679	-0.00465	-0.051	-0.016	NA	7.9992
[32]	NA	99.6096	33.4595	-0.0127	0.0024	.0032	NA	7.9991
[33]	NA	99.6084	33.4719	0.0083	0.0041	0.04	NA	7.9991
[Proposed Paper]	8.3546	99.6487	33.4475	0.0218	0.0150	0.0197	622	7.9991

(Note: NA= Not Applicable)

3.8. Universal image quality index

Let x= $\{x_i | i = 1,2, \dots \dots . . M \times N\}$ and y= $\{y_i | i = 1,2, \dots \dots . . M \times N\}$ be the original and cipher images respectively, then the quality index can be defined as

$$UIQ = \frac{4\sigma_{x,y}xy}{(\sigma_x^2+\sigma_y^2)\times[(\bar{x})^2+(\bar{y})^2]}. \quad (20)$$

where

$$\bar{x} = \frac{1}{M\times N} \times \sum_{i=1}^{M\times N} x_i, \quad (21)$$

$$\bar{y} = \frac{1}{M \times N} \times \sum_{i=1}^{M \times N} y_i, \quad (22)$$

$$\sigma_x^2 = \frac{1}{M \times N} \times \sum_{i=1}^{M \times N} (x_i - \bar{x})^2, \quad (23)$$

$$\sigma_y^2 = \frac{1}{M \times N} \times \sum_{i=1}^{M \times N} (y_i - \bar{y})^2, \quad (24)$$

$$\sigma_{x,y} = \frac{1}{M \times N} \times \sum_{i=1}^{M \times N} (x_i - \bar{x}) \times (y_i - \bar{y}). \quad (25)$$

3.9. Structural Similarity Index Measure

SSIM is a measure of structural similarity between plain image and the encrypted image, mathematically it is represented as

$$SSIM = \frac{(2\bar{x}\bar{y}+c1) \times (2\sigma_{x,y}+c2)}{(\bar{x}^2+\bar{y}^2+c1) \times (\sigma_x^2+\sigma_y^2+c2)}. \quad (26)$$

where $c1$ and $c2$ are constants.

3.10. Entropy

Information entropy is a measure of randomness in the image. The randomness of the image is based on the probability of occurrence of the various gray levels in the image. An image with all pixels of equal gray levels are equally probable represents highest randomness. Randomness of an image says how much confidential the image is. It also represents the leakage of information. Entropy also finds the strength of the cryptosystem. Information entropy is calculated using the formula

$$\text{ET (m)} = - \sum_{i=0}^{L-1} p(m_i) \times log_2(p(m_i)). \quad (27)$$

Where ET is the entropy, L is the total number of grey level values and $p(m_i)$ is the probability of occurrence of pixel at each grey level m_i. A gray scale image with 256 levels to be random, the entropy should ideally be equal to 8. A ciphered image with its entropy value very close to 8 represents an extremely random image and the negligible leakage. An entropy value less than 8 represents a predictable image which threatens security. The proposed algorithm results in the entropy of 7.9991. This represents the uniformity of the document. Hence our algorithm is better with respect to certainty of the document. Therefore this scheme is capable of resisting the entropy base attacks.

3.11. Document image encryption

In the proposed encryption method the algorithm is subjected to different document images containing text, picture and text with picture. The results obtained for partial and complete encryption for all document types are shown in Figure 10. The security parameters obtained for all document types are tabulated in Table 4 and Table 5 for partial and complete encryption respectively.

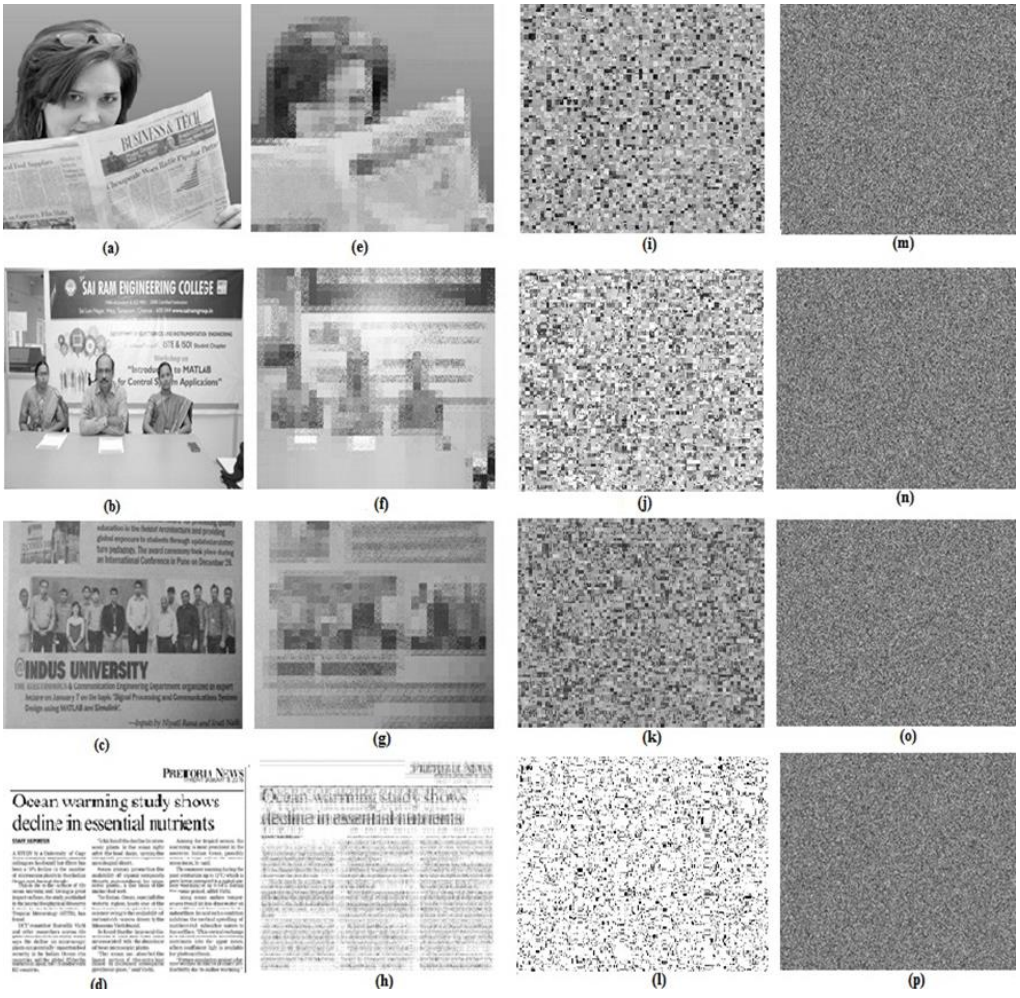

Figure 10. Encryption of Document Images: (a-d) Input Plain Document images, (e-h) Corresponding Partial Encryption results, (i -l) second level confused image and (m-p) Corresponding Complete Encryption results

Table 4. Partial encryption results for different document Images

INPUT IMAGE	MSE	PSNR	EXECUTION TIME (m sec)	SSIM	UIQ
DOC1	7.38155×10^{2}	19.3465	144.52	0.81468914	0.81468960
DOC2	1.7247×10^{3}	15.7636	134.08	0.6639804	0.66398114
DOC3	9.9899×10^{2}	16.8132	172.074	0.6363383	0.6363397
DOC4	5.9976×10^{3}	10.3509	170.34	0.00424	0.00423

Table 5. Complete encryption results for different document Images

INPUT IMAGE	MSE	PSNR	EXECUTION TIME (sec)	NPCR	UACI	ENTROPY	Correlation			SSIM	UIQ
							Horizontal	Vertical	Diagonal		
DOC1	8.465×10^{3}	8.7512	3.092	99.5304	33.4786	7.9992	-0.0513	-0.0160	-0.0227	0.002967	0.002966
DOC2	1.073×10^{4}	7.82	3.064	99.5338	33.3929	7.9994	0.0170	-0.0024	-0.0132	0.004679	0.004678
DOC3	7.03×10^{3}	8.33	3.054	99.5340	33.4050	7.9993	0.0142	0.0218	-0.0133	$-0.9.26\times10^{-4}$	$-0.9.27\times10^{-4}$
DOC4	1.814×10^{4}	5.543	3.067	99.4858	33.4304	7.9993	-0.0292	-1.0060×10^{-4}	0.0132	0.0003078	0.0003077

3.12. NIST test analysis

There are different complexity measurement techniques to measure the randomness of a given chaotic sequence. In this paper a NIST (National Institute of Standards and Technology) test Analysis has been conducted in WINDOWS (WIN 7 OS) environment to quantitatively estimate the complexity of different dimensional (2D and 1D) chaotic maps. The complexity of the proposed scheme can be assessed by making use of NIST special publication [34]. There are 16 different statistical test of special publication [35]. The different statistical methods are 1. Mono bit test, 2. Frequency test within block 3.Runs test, 4. Longest run ones test, 5. Binary matrix rank test, 6. Spectral test, 7. Non overlapping template matching test, 8. Overlapping template matching test, 9. Universal statistical test, 10. Lempel-Ziv compression test, 11. Linear Complexity test, 12. Serial test, 13. Approximate Entropy test, 14. Cumulative sums test, 15. Random excursion test and 16. Random excursion variant test.

For each of these tests the value of P is calculated from a binary sequences generated by the multi-dimensional chaotic maps (2D and 1D). Each P-value determines whether the produced sequence is random in nature or not. A P-value equals to 1 determines a perfect randomness. If P is in the range of 0.01 to 1, then the test indicates that the sequence produced in completely random in nature. The randomness of the sequence generated by the proposed algorithm can be evaluated by converting the encrypted pixels Pi to bit Pib. The NIST Test Analysis Table 6 shows that it is successful against statistical attacks and hence the proposed method is feasible for cryptography applications.

Table 6. NIST test analysis

	P-Value			
Statistical Analysis	2D Henon Map	Bernoulli map	1D Skew Tent Map	Status
Mono Bit Frequency Test	0.911722762	0.545081094	0.411058023	Success
Block Frequency Test	0.896651648	0.745444081	0.204953127	Success
Run Test	0.017473068	0.019475341	0.021192845	Success
Longest Run Ones	0.731976748	0.939505864	0.185557603	Success
Binary Matrix Rank Test	0.480372774	0.263197135	0.069933096	Success
Spectral Test	0.917508648	0.462602814	0.640251058	Success
No over Lapping Template Matching Test	0.981407246	0.594564267	0.397569266	Success
Overlapping Template Matching Test	0.835255129	0.241877465	0.473148082	Success
Universal Statistic Test	0.043523569	0.290658217	0.279569313	Success
Linear Complexity Test	0.790994918	0.394483897	0.904411584	Success
Serial Test	0.982153254	1.000000000	1.000000000	Success
Approx. Entropy Test	1.000000000	0.971174997	0.962333535	Success
Cumulative Sums Test Forward	0.966310137	0.932836878	0.521342232	Success
Cumulative Sums Test Reverse	0.979855053	0.600528263	0.532280136	Success
Random Excursion Test	0.453358511	0.708361415	0.746906358	Success
Random Excursions Variant Test	0.824497225	0.951898892	0.609856019	Success

4. CONCLUSION

The Proposed work presents a partial as well as complete image encryption scheme for document images. In the partial encryption, only the significant regions with a preset size are identified and are only permuted. The experimental results of the partial encryption are shown in the Table 2. In large size blocks, the pixels are scattered over a larger space and the partially encrypted document appears in less intelligent form and has lesser number of blocks permuted. Hence larger preset block sizes results in more security with less encryption time. For smaller block sizes the permutation takes place in smaller area and the document image appears with more correlation among pixels in the block and hence appears as original image. As the minimum block size is reduced the percentage of significant region increases hence it takes more encryption time. Table 2 reveals that the partial encryption is more secure as the Peak Signal to Noise Ratio is nearly equal to the ideal value of 8dB. Hence the proposed partial encryption scheme reduces the computational overhead and suits to real-time applications. Further the proposed scheme is extended for complete image encryption. The results of complete image encryption are shown in Table 3. The complete image encryption ensures more security since the input image being the partially encrypted one. The mixed chaotic system is used for permutation and substitution. The interdependency established between the pixels in an image, the row wise diffusion bi-directionally and the column wise diffusion unidirectional considerably reduces encryption time. The interdependency so established creates a non-linear relationship between the cipher image and the key and hence provides more security. The NIST ensures that the sequences generated by the chaotic systems are random and hence the system is more secure. The results shows that, the larger value of NPCR and UACI, a poor Correlation in Horizontal, Vertical and Diagonal directions, the Entropy close to ideal value, a flat Histogram and a small value of PSNR ensures that Encryption is resistant to dynamical and statistical attacks. The lesser encryption time shows that the algorithm is suitable for real time applications. Hence this scheme is efficient to completely encrypt the image and provide good security when compared to the existing methods. The experimental results for various Document images are tabulated in Table 4 and 5. The results reveals more security. The pictorial results for partial and complete encryption on document images are shown in Figure 10.

REFERENCES

[1] G. A. Spanos and T. B. Maples, "Performance study of a selective encryption scheme for the security of networked, real-time video," *Proceedings of 4th International Conference on Computer Communications and Networks*, pp. 20-23, 1995.

[2] Y. Zhou, et al., "Image encryption using Binary bit plane," *Signal Processing ELSEVIER Publications*, pp. 197-207, 2014.

[3] S. Som, et al., "Evaluating the Performance of a Chaos Based Partial Image Encryption Scheme," *Advanced Computing and Systems for Security, Advances in Intelligent Systems and Computing, Springer*, pp. 173-185, 2017.

[4] S. Som, et al., "A chaos based partial image encryption scheme," *2nd International conference on business and information management, IEEE*, 58-63, 2014.

[5] P. Praveenkumar, et al., "Chaotic and Partial Encrypted image on XOR Bus," *International conference on computer communication and informatics, IEEE*, 2016.

[6] A. Moumen, et al., "New Secure partial Encryption method for medical images using graph coloring problem," *Springer*, 2015.

[7] Panduranga H. T., et al., "Partial Image Encryption using block wise shuffling and chaotic map," *Proceedings of international conference on optical imaging sensor and security, IEEE*, 2013.

[8] J. K. Mandal, et al., "Adaptive Partial Image Encryption Technique based on Chaotic map," *4th International conference of Emerging applications of Information Technology, IEEE*, pp. 328-334, 2014.

[9] N. Hazarika, et al., "A Wavelet based partial image Encryption using Chaotic Logistic Map," *International Conference on Advanced Communication Control and Computing Technologies, IEEE*, pp. 1471-1475, 2014.

[10] N.i Hazarika and M. Saikia, "A novel Partial Image Encryption using Chaotic Logistic Map," *International Conference on Signal Processing and Integrated Networks, IEEE*, pp. 231-236, 2014.

[11] Z. Fawaz, et al., "An efficient and Secure Cipher scheme for images Confidentiality preservation," *Signal Processing: Image Communication*, vol. 42, pp. 90-108, 2016.

[12] H. Cheng and X. Li, "Partial Encryption of Compressed Images and Videos," *IEEE Transactions on Signal Processing, IEEE*, vol. 48, pp. 2439-2451, 2000.

[13] G. Bhatnagarand and Q. M. Jonathan W., "Selective Image Encryption based on pixels of Interest and Singular Value Decomposition," *Digital Signal Processing 22, ELSEVIER*, pp. 648-663, 2012.

[14] A. Belazi, et al., "Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms," *Optics and Lasers in Engineering, ELSEVIER*, pp. 37-50, 2017.

[15] S. Bahrami and M. Naderi, "Encryption of multimedia content in partial encryption scheme of DCT transform coefficients using a lightweight stream algorithm," *Optik, ELSEVIER*, pp. 3693-3700, 2013.

[16] Meghana H. K. and Prabhavathi K., "Chaos Based Partial Encryption Of Grayscale Image Using Couple Tent Map Based On Pseudo Random Number Generator," *International Journal for Technological Research in Engineering*, vol. 3, pp. 2850-2854, 2016.

[17] S. Som and S. Sen, "A non-Adaptive partial Encryption of Grayscale Images based on Chaos," *Science Direct, ELSEVIER*, pp. 663-671, 2013.
[18] T. S. P. N. Halarnakar, "Performance Evaluation of Non Sinusoidal Wavelets for Partial Image Scrambling Using Kekre's Walsh Sequency," *Science Direct, ELSEVIER*, pp. 755-762, 2015.
[19] S. Lian and X. Chen, "On the design of Partial Encryption Scheme for Multimedia Content," *Mathematical and Computer Modeling, ELSEVIER*, pp. 2613-2624, 2013.
[20] K. Naik and A. K. Pal, "A Partial Image Cryptosystem based on Discrete Cosine Transform and Arnold Transform," *Recent Advances in Information Technology, Advances in Intelligent Systems and Computing, Springer*, pp. 65-73, 2014.
[21] P. Jagadeesh, et al., "A novel Image Scrambling Technique based on Information Entropy and Quad Tree Decomposition," *International Journal of Computer Science Issues*, vol. 10, pp. 285-294, 2013.
[22] G. R. C. M´arquez, et al., "Simplified Quad tree Image Segmentation for Image Annotation," *Luis Enrique Sucar and Hugo Jair Escalante, Proceedings of the 1st Automatic Image Annotation and Retrieval Workshop*, vol. 1, pp. 24-34, 2010.
[23] Abid S. and Hasan H., "About asymmetric noisy chaotic maps," *Int J Basic Appl Sci*, vol. 3, pp. 62-73, 2014.
[24] R. Ye and Y. Ma, "A secure and robust image encryption scheme based on mixture of multiple generalized Bernoulli shift maps and Arnold maps," *International Journal of Computer Network and Information Security*, vol. 5, pp. 21, 2013.
[25] Schuster, et al., "Deterministic chaos: an introduction," John Wiley & Sons, 2006.
[26] D. J. Driebe, "The Bernoulli Map," *Fully Chaotic Maps and Broken Time Symmetry, Springer Science+Business Media Dordrecht*, pp. 19-43, 1999.
[27] S. H. Stogartz, "Non-linear dynamics and chaos," Addison-Wesley, 1994.
[28] IEEE Computer society, "IEEE standard for binary floating point arithmetic," *ANSI/IEEE std*, pp. 754, 1985.
[29] C. R. Revanna and C. Keshavamurthy, "A New Selective Document Image Encryption Using GMM-EM and Mixed Chaotic System," *International Journal of Applied Engineering Research*, vol. 12, pp. 8854-8865, 2017.
[30] A. M. Ayoup, et al., "Efficient selective image encryption," *Multimedia Tools Appl. Springer*, 2015.
[31] Y. Zhang, "A Chaotic system based image encryption algorithm using plaintext related confusion," *TELKOMNIKA, Indonesian Journal of Electrical Engineering*, vol. 12, pp. 7952-7962, 2014.
[32] Y. Zhang, "Plaintext related Image encryption scheme using chaotic map," *TELKOMNIKA, Indonesian Journal of Electrical Engineering*, vol. 12, pp. 635-643, 2014.
[33] Y. Zhang, "The Image Encryption algorithm with Plaintext related shuffling," *IETE Technical Review*, vol. 33, pp. 1-13, 2015.
[34] A. Melo, et al., "Priority QoE: a tool for Improving the QoE in Video Streaming," *Intelligent Multimedia Technologies for Networking Applications: Techniques and Tools*, chapter 11.
[35] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and High-dimension chaotic system," *Optical Communication*, vol. 284, pp. 3895-3903, 2011.

BIOGRAPHIES OF AUTHORS

DR C Keshavamurthy is B.E. and M.E. in Electronics and Communication Engineering and received his Ph. D in the area of C A N. His academic interests include Computer Communication Networks, Ad-hoc Wireless Networks and Multimedia Communication. He has a research experience of over 20 years. Served as the Principal at YDIT, Bangalore. Currently working as a Professor of Electronics and Communication Engineering at SRSIT, Bangalore.

Mr. C R Revanna is a B.E. in Electronics and Communication Engineering, M.E. in Electronics at UVCE from Bangalore University, Bangalore, India. His research interest includes Encryption, Image Processing and Cryptography. Currently working as Assistant Professor in Electronics and Communication Engineering at Government Engineering College, Ramanagaram, India. He is also pursuing his Ph. D. research work at Jain University, Bangalore, India.