Volume 3, Issue 5, May 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Image Encryption Using Bit-Level Sub Image Blocks Confusion and Circular Diffusion

Nandeesh G S
M.Tech Student(DECS)
Mce,Hassan
Karnataka, India.

Vijaya P A
Professor
BNMIT,Bangalore
Karnataka, India.

Sathyanarayana M V
Principal
Mce,Hassan
Karnataka, India.

Abstract—In recent years, Information security is a fast growing research field; image encryption is one of the important problems in the field of image information security. A number of Chaos based cryptosystem have been proposed, Most of them based on the traditional confusion-diffusion architecture. The draw backs of traditional architecture are Less sensitiveness in change of plain image and chosen/known plain-image attacks. In this paper, we propose A bit-level sub image blocks confusion and Circular Diffusion to provide the security of traditional architecture. Simulations have been carried out and the results demonstrate the superior security and high efficiency of the proposed scheme.

key words: Image information security, Image encryption, Chos, Bit level confusion.

I. Introduction

The development in the field of Computer Network technology and the evolution of several applications like military image databases, confidential video conferencing, medical imaging, cable TV, online personal photograph albums, etc. Needs fast, reliable and robust, security systems to store and transmit digital images. Image Encryption is different than text Encryption due to bulk data capacity, high correlation among pixels and High Redundancy, these intrinsic features are difficult to handle by traditional ciphers. Now days, Because of the development in theory and application of chaos, many chaos algorithms have been proposed. In1998, Fridrich[1] proposed a confusion diffusion architecture based on different chaotic systems. In this architecture, in first step the plain-image pixels are permuted by two-dimensional chaotic system which relocates the pixel value and reduce the correlation among adjacent pixels, where the pixel value cannot be influenced by external information, and in diffusion, the self-information is not sufficient and some external information should be introduced by one-dimensional chaotic map each pixel value is systematically changed. After both stage, the values of pixels, will be uniformly distributed. In recent years, chaos-based image cryptosystems have attracted increasing attentions and have been studied extensively. The existing systems classified into two categories. In first category, basic unit is pixels. Most of the image encryption schemes operate at the pixel level. In second category, pixel is divided into bits and confusion operation is applied on bit -planes and diffusion operation is applied on whole image. In[2], is a new block cipher which uses the modular multiplication in group and alternatively permutations are applied on plain text with the block length of multiple of 64-bits. In [3], a fast image encryption algorithm, here plain image pixels are partitioned as blocks and this blocks are shuffled by spatiotemporal chaos and change the pixel value by same. Spatiotemporal chaos is used to generate the pseudorandom numbers, which increases the encryption speed.

The drawback of Pixel level ciphers are diffusion dependent and diffusion phase requires more execution time than confusion. In [4], the permutation is employed to bit plane images which is obtained by converting plain image into bit plain image. Since the higher 4 bit-planes carry 94% of information a cat-map is employed to permute each bit-plane image, and lower 4 bit planes are permuted whole. Different strategies are employed to 8 bit plane images as they carry different information. The bit-level permutation changes pixel location and modifies the pixel value since different bit-planes are permuted in different methods. So diffusion operation requires to confusion stage due to bit-level permutation. In [5], is also the bit-level permutation it is called Two dimension Circulation Encryption Algorithm(TDCEA). In this encryption each bit-plane is considered as a block, every 8 pixels are treated as an encryption group in TDCEA. A 8 x 8 matrix is formed to form encryption group , Each column or row is shifted in cyclic manner by two kinds of bit rotation. The drawback of this scheme is Less sensitiveness in change of plain image and Confusion mechanism is not applied to whole image. As a result, this cipher has been broken in [6]. In[7], to solve the problems in the traditional architecture An encryption scheme with lightweight bit-level permutation and cascade circular diffusion is proposed. In this cipher confusion is done by bit-level permutation by applying cat map to higher bit-planes and light weight mapping technic with different conditions, in confusion stage changing the position and changing the pixel values are done at a time which save the execution time and reduce the computational redundancy . To avoid the stop point mechanism a cascade cross circular diffusion strategy is used. An encryption scheme with lightweight bit-level permutation and cascade circular diffusion avoids the stop point mechanism, which leads to insensitive to tiny modification of plain image. In the proposed

scheme, a light weight sub-image mapping is employed in the confusion phase to significantly reduce the correlation among the bit planes and uses the cat map for higher bit planes to provide the higher security .In diffusion phase, pixel values are systematically changed after permutation of whole bit-planes. This paper is organized as follows. In the next section, Confusion and Diffusion of different architecture are discussed .In section 3, the proposed image encryption scheme is described. In Section 4. Simulation results and performance analyses are reported. In section 5, Conclusion is discussed.

II. Confusion And Diffusion Operation

A. Confusion

The traditional chaos-based symmetric image encryption scheme, is an symmetric image encryption which uses the confusion and diffusion phase. Confusion phase is done by applying different chaotic maps, such as The cat map, standard map or baker map which is defined by Eqs. (1),(2) and (3), respectively.

Cat Map:

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} mod N, \tag{1}$$

Standard Map:

$$\begin{cases} X' = (X + y) mod N \\ Y' = \left(Y + k sin \dfrac{x'N}{2\pi}\right) mod N, \end{cases} \tag{2}$$

Baker Map:

$$B_d(X,Y) = \left[\frac{N}{n_i}(X - N_i) + y mod \frac{N}{n_i}, \frac{n_i}{N}\left(Y - Y_i mod \frac{N}{n_i}\right) + N_i\right] \tag{3}$$

Pseudorandom position of cipher image is calculated by two dimensional chaotic mapping rule, where for each pixel in the plain image needs to perform two kinds of operation first one new position calculation and second one changing the pixel position from original position to new position. The main aim of traditional architecture is to reduce the correlation of neighboring pixels. This is done by confusion stage, by relocating pixels in pseudorandom manner and Modification of pixels In the plain image to almost all pixels in the cipher image is done by diffusion stage. The confusion operation should be performed on a fullimage scale; otherwise, it not only results in a reduction in the correlation coefficients, but also leads to the other security problems. So the confusion operation should meet two basic requirements in Fridrich's structure. The first one is that the permutation should be performed in a full scale image, while the second one is that the correlation coefficients among the pixels should be reduced significantly after the confusion operation.

B. Diffusion operation

In a traditional architecture, an confusion operation is acts like substitution operation. which relocates the pixel value and reduce the correlation among adjacent pixels, here the pixel value cannot be influenced by external information, and in diffusion, the self-information is not sufficient and some external information should be introduced by one-dimensional chaotic map which systematically changes each pixel value. In diffusion operation, after confusion phase the two dimensional image is converted into a one-dimensional sequence then by, the initial condition of the chaotic system and previously processed pixel values cipher image pixels are calculated. The cipher image should be sensitive to change in bit in plain image.In traditional cipher The diffusion phase is governed by Eq. (4).

$$\begin{cases} C(i) = p(i) \oplus l(i) \\ t = 4 \square \left((c(i) + cs(i))/1000\right) \square \left(1 - \left((c(i) + cs(i))/1000\right)\right) \\ i(i+1) = (t \square 1000) mod\ 256 \end{cases} \tag{4}$$

Where,c(i) is the ith pixel in the cipher-image while p(i) is the corresponding pixel in the plain image. l(i) is a pseudorandom number sequence, which is determined by two factors: the value of the previously processed pixel and an independent pseudorandom sequence cs(i). In Eq.(4), c(1) = (4_keyd)_ 1000)mod256, where keyd is the diffusion key, arbitrarily set to 0.43524032254333. In Eq.(4), cs(i) = (logistic(2000 + i)_109)mod256, where the pseudorandom sequence logistic is obtained by iterating Eq.(5).

$$f(X_n) = \alpha X_{n-1}(1 - X_{n-1}) \tag{5}$$

In Eq.(5), and the initial value are set to 4 and 0.34552543678760,respectively. In[7],discussed the problem in the traditional architecture a stop point mechanism and this problem is solved with the help of cascaded circular diffusion,which results in the insensitivity to a tiny modification of the plain-image. Plaintext sensitivity Two images are used to test the sensitivity to the plain-image, one is the original plain-image while another is the modified plain-image which is obtained by changing a last of the pixel in the original plain-image from 0 to 1.Encrypt both plain image and bit changed image with the same parameter and keys. The number of different pixels between the two cipherimages is calculated. More different pixels indicate a higher sensitivity to the plain-image.

III. The Proposed Scheme

In the proposed scheme, a Bit-plane sub-image confusion scheme is employed which involves dividing Bit-plane image into 4 equal sub-images and applying mapping with five conditions to fulfil the basic requirement of confusion. The plain image is slice into eight bit planes. Fig. 1. Shows the original bit plane image is sliced to 8 bit plane images. The information contained in different bit planes can be calculated by Eq. (6).

$$p(i) = \frac{2^i}{\sum_{i=0}^{7} 2^i} \qquad (6)$$

In Eq. (6), p(n) indicates the percentage of plain-image information that the nth bit plane contains, n 2 [0; 7] . from Eq (6),The MSB contains large information, while the LSB only contributes less than 1% of the total information. Percentage of pixel information contributed by different bits are tabulated in Table. (I).

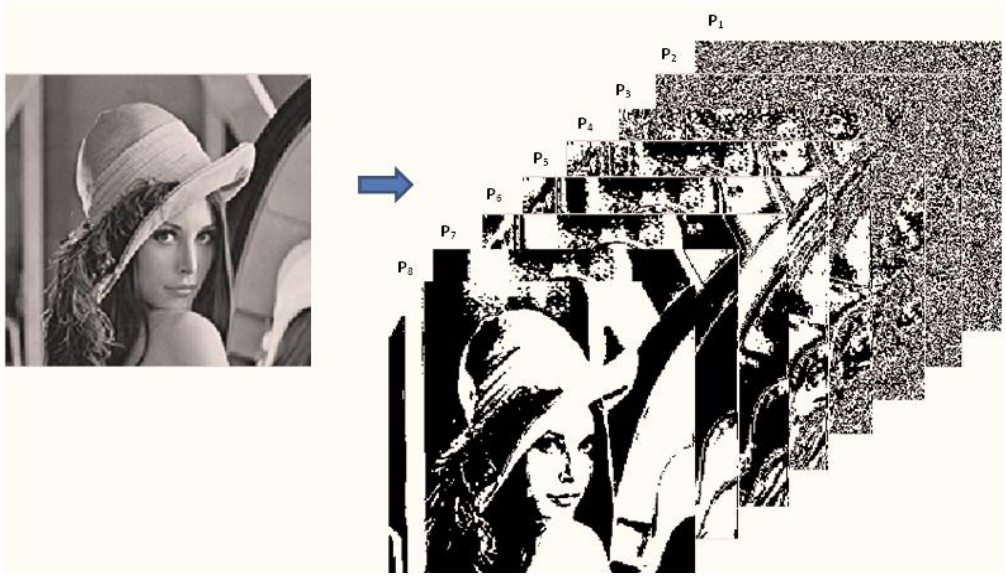

Fig. 1. Plain image to Bit-palne images

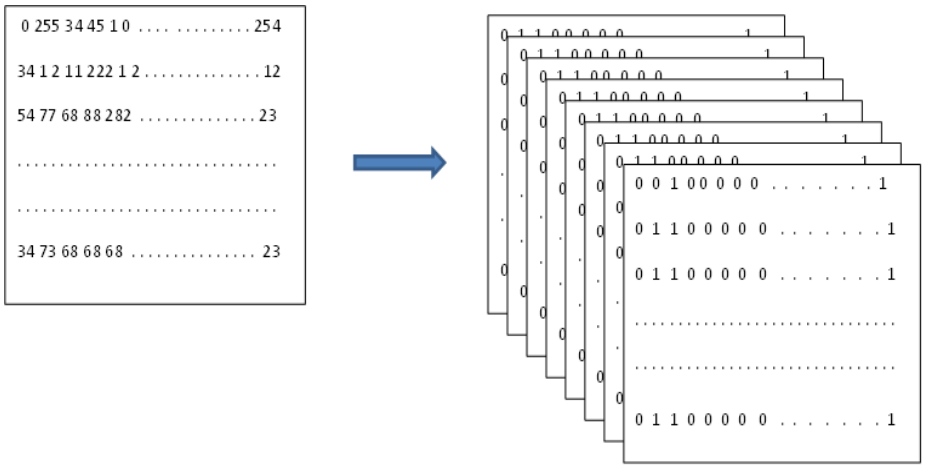

Fig. 2. Bit planes in pixel form

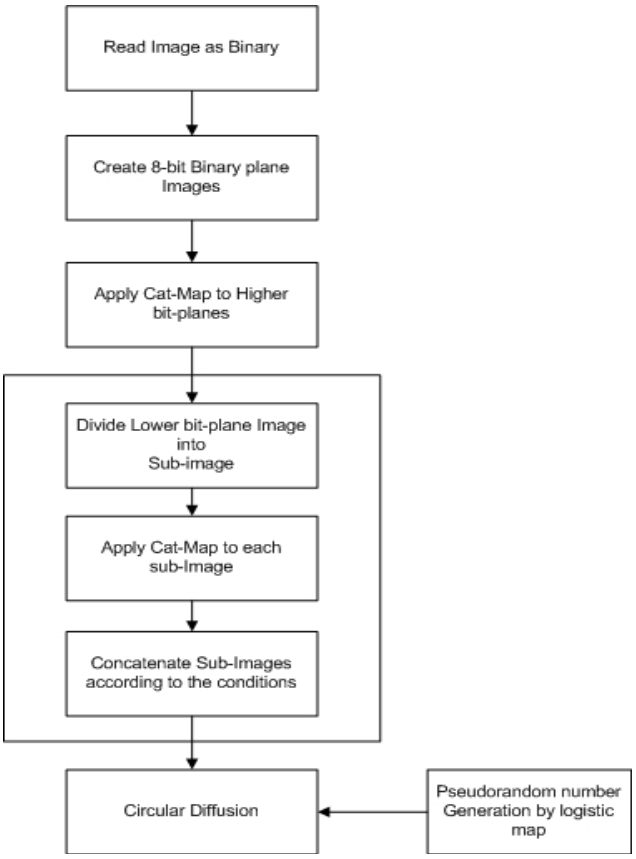

Fig. 3. Flowchart

TABLE I
Percentage Of Pixel Information Contributed By Different Bits

Bit position	Percentage
1	0.3922
2	0.8784
3	1.5686
4	3.1370
5	6.2750
6	12.550
7	25.10
8	50.20

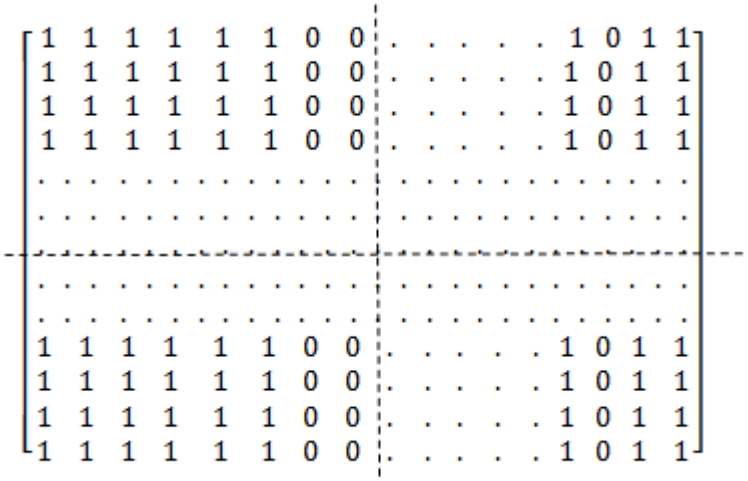

Fig. 4. Bit plane dividing to blocks

To apply the mapping rule to bit-panes first divide the bit plane image into 4 equal sub images. As shown in Fig. (3).

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$$

Where A11,A12,A21 and A22 are Sub-images with size M=2_ N=2. Let A be the bit-plane image with size M _ N then A11;A12;A21andA22 are four image blocks with size M=2_N=2 .The five kinds of mapping rules are given by the following five conditions, where

Conditionindex1

$$A = \begin{bmatrix} A_{11} & A_{11} \\ A_{21} & A_{21} \end{bmatrix}$$

Conditionindex2

$$A = \begin{bmatrix} A_{12} & A_{12} \\ A_{22} & A_{22} \end{bmatrix}$$

Conditionindex3

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{11} & A_{12} \end{bmatrix}$$

Conditionindex4

$$A = \begin{bmatrix} A_{22} & A_{21} \\ A_{12} & A_{11} \end{bmatrix}$$

Conditionindex5

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}$$

Conditioninedex indicates the mapping case for the k^{th} bit plane, k 2 [0; 7]. A(i, j) is the bit value after confusion at location (i, j) while A11;A12;A21andA22 are the image blocks original bit value. The value of indexk is governed by a logistic map, according to Eqs. (5) and (7).

$$Conditionindex_k = \left(X_{2000+k} * 10^9\right) mod\ 5 + 1 \qquad (7)$$

In Eq. (5), is the parameter of the logistic map. The output sequence is chaotic when 2 [3:57; 4] . In the proposed scheme, is set to 3.99999, the initial value x0 is set to 0.33284657332813, and indexk is calculated by Eq. (7). A cat map can be employed to permute each blocks in bit planes. In this case, the coefficients of the cat map are calculated by Eq. (8).

$$\begin{cases} p = (y_{2000+0} * 10^9) mod 512 \\ q = (y_{2000+1} * 10^9) mod 512 \end{cases} \qquad (8)$$

A .**Confusion phase step**

The confusion phase step

Step 1: For higher bit-planes apply cat map.

Step 2: The lower bit planes are divide into equal blocks and apply cat map to each blocks.

Step 3: Concatenate permuted blocks according to index value calculated by Eq. (7).

Step 4: For 8th bit plane apply lightweight bit-plane block confusion since it carries the 50% of information to provide higher security.

B. Diffusion phase

In diffusion phase, Two dimensional array is converted to one dimensional array by cascade circular method [lwt] two random positions, (rp_x; rp_y) and (rp''_x; rp''_y) , are firstly selected as the two random start pixels of the diffusion operations in two different directions.The two random positions are calculated by Eq. (9)[lwt].

$$\begin{cases} rp'_x = cs(2000) \times 10^9 mod 512 \\ rp'_y = cs(2001) \times 10^9 mod 512 \\ rp''_x = cs(2000) \times 10^9 mod 512 \\ rp''_y = cs(2001) \times 10^9 mod 512 \end{cases} \qquad (9)$$

then Eq. (9) is employed to diffuse.

$$\begin{cases} & t_2 = rand_1(t_1); \\ cipher(i) = & [ac(i) \otimes rand_2(t_2)] + rand_3; \\ & t_1 = cipher(i); \end{cases} \qquad (10)$$

In Eq. (10), the initial value of temp1 is set to by t = [4 *keyd (1 - keyd) *1000]mod256and rand1 and rand2 random number arrays with 512 elements Generated by the logistic map with the initial value k2 = 0:72345678912345 and k3 =

0:29837465123439. and rand3 is a chaotic sequence generated by Eq. (10). rand3(i) = (logistic(2000 + i) _ 109)mod256: (11)

where the random array logistic is obtained by iterating Eq. (5). After the first diffusion round, the one-dimensional array is transformed to a two-dimensional array.The location of the start pixel is determined by (rp"x; rp"y), and the two dimensional array is transformed to logical one-dimensional array with the start pixel (rp" x; rp"y) and the end pixel (rp"x1; rp"y1) diffusion round is employed with the Eq. (10).

$$rand_3(i) = (logistic(2000 + i) \times 10^5) mod 256 \qquad (11)$$

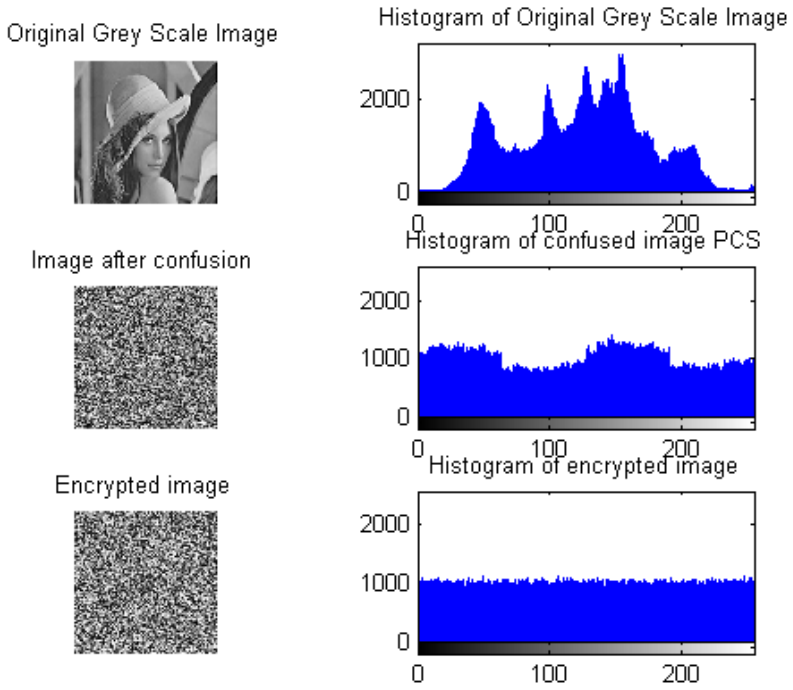

Fig. 5. Histogram analysis

IV. Simulation Results

In this section, simulation results and performance analysis for the proposed scheme and a comparable algorithm are reported. All the simulations were performed on a personal computer with Intel(R) Core(TM) i7-2670QM 2.26GHz CPU, 4 GB memory and 750 TB hard disk. The operating system is Windows 7 Enterprise, and the compile platform is Matlab 2012a.

A. Histogram analysis: The distribution information of pixel values are revealed by histogram. An ideal encrypted image should have a uniform and completely different histogram in comparison with that of the plain-image, to prevent the opponent from extracting any meaningful information from the fluctuating histogram of the cipher-image. In Fig. (5), plots the show the histogram of plain image, Histogram of confusion phase and histogram of encrypted image. The simulation results show that the histogram of the cipher image obtained by the proposed scheme is fairly uniform and is significantly different from that of the plain-image.

B. Correlation analysis: of two adjacent pixels We have analyzed the correlation between two vertically adjacent pixels, two horizontally adjacent pixels, and twodiagonally adjacent pixels in an image. 2000 pairs of two adjacent (in vertical, horizontal, and diagonal direction) pixels from plain-image and ciphered image were randomly selected and the correlation coefficients were calculated by using the following equations: x and y represent gray level values of two adjacent pixels. Table(II) is the horizontal, vertical and diagonal relevance of adjacent elements in image before and after encryption. Fig 8 shows the results of correlation analysis. Fig () show significant reduction in relevance of adjacent elements.

C. Differential attack analysis: The number of pixels change ratio (NPCR) and the unified average change in density (UACI) are two indicators to measure capability against differential attack. Differential analysis refers to the attacker changes arbitrarily a pixel value of encrypted image which he obtains to get a new image and then encrypts the image to observe the result. In this way, it is possible to find clear and meaningful relationship between plain and cipher images. If small changes in explicit can cause tremendous changes in cipher text, the differential attack is invalid and no practical significance.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (15)$$

Where, M stands for images width, N stands for images height and where D(i,j) defined as follows

$$D(i,j) = \begin{cases} 1 \; if \; C_1(i,j) \neq C_2(i,j) \\ 0 \; if \; C_1(i,j) = C_2(i,j). \end{cases} \quad (16)$$

Where c1 and c2 are the two cipher-images.

UACI is calculated by

$$UACI = \frac{1}{M+1} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \quad (17)$$

Two plain-images are used in this section. One is the original plain image, and the other one is obtained by changing the lower right pixel from 01010001 to 01010000. These two test images are encrypted using the same key for a few rounds to generate the corresponding cipher-images c1andc2:

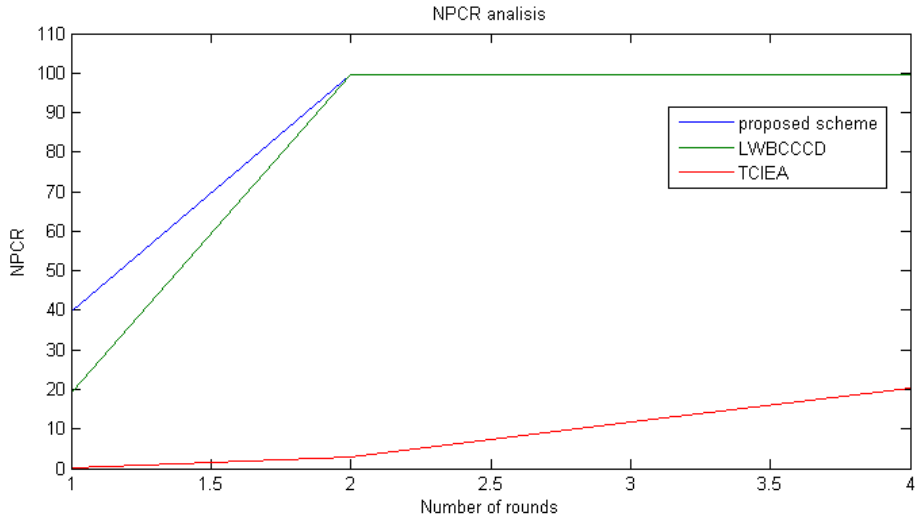

Fig. 7. NPCR analysis

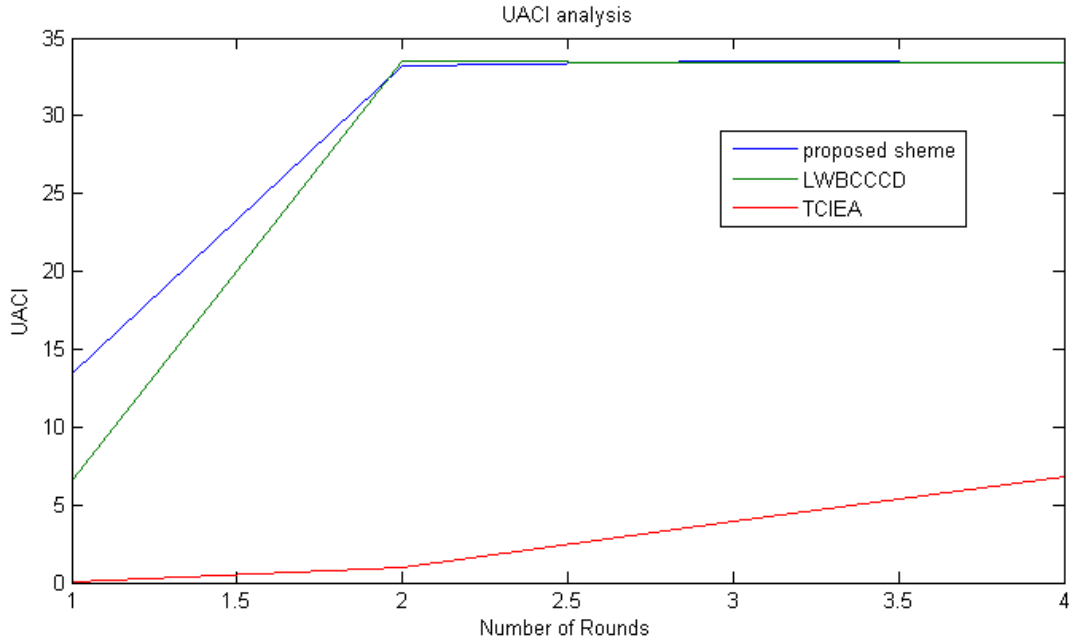

Fig. 8. UACI analysis

D. Information entropy analysis: The information entropy H(m) of a message source n is defined by Eq. (11).

$$H(m) = \sum_{i=1}^{2^N-1} p(m_i) \times log_2 \frac{1}{p(m_i)} \qquad (11)$$

Where p(mi) represents the probability of symbol mi and the entropy is expressed in bits. If the source m emits 28 symbols with equal probability, i.e.m = m1; m2; ; :::; m256, then the result of entropy is H(S) = 8, which corresponds to a true random source and represents the ideal value of entropy for message source S. Distribution of gray values in image encryption is showed by Information entropy. The more the distribution of gray value is uniform, the greater the information entropy. If encrypted image information entropy is less than the ideal value 8,then,there would be a possibility of predictability which threatens the image security. Table (ientro) shows the information entropy of plain and encrypted image.

V. Conclusions

In this paper, we studied the architecture and draw backs of traditional system, and proposed a new sub image block confusion and diffusion encryption scheme. A new confusion diffusion architecture is analyzed and is applied to gray scale image. Simulations have been carried out to compare its performance with that of An encryption scheme with lightweight bit-level permutation and cascade circular diffusion. The results show that the proposed scheme leads to a improved security level in terms of NPCR, UACI and entropy of the cipher-images.

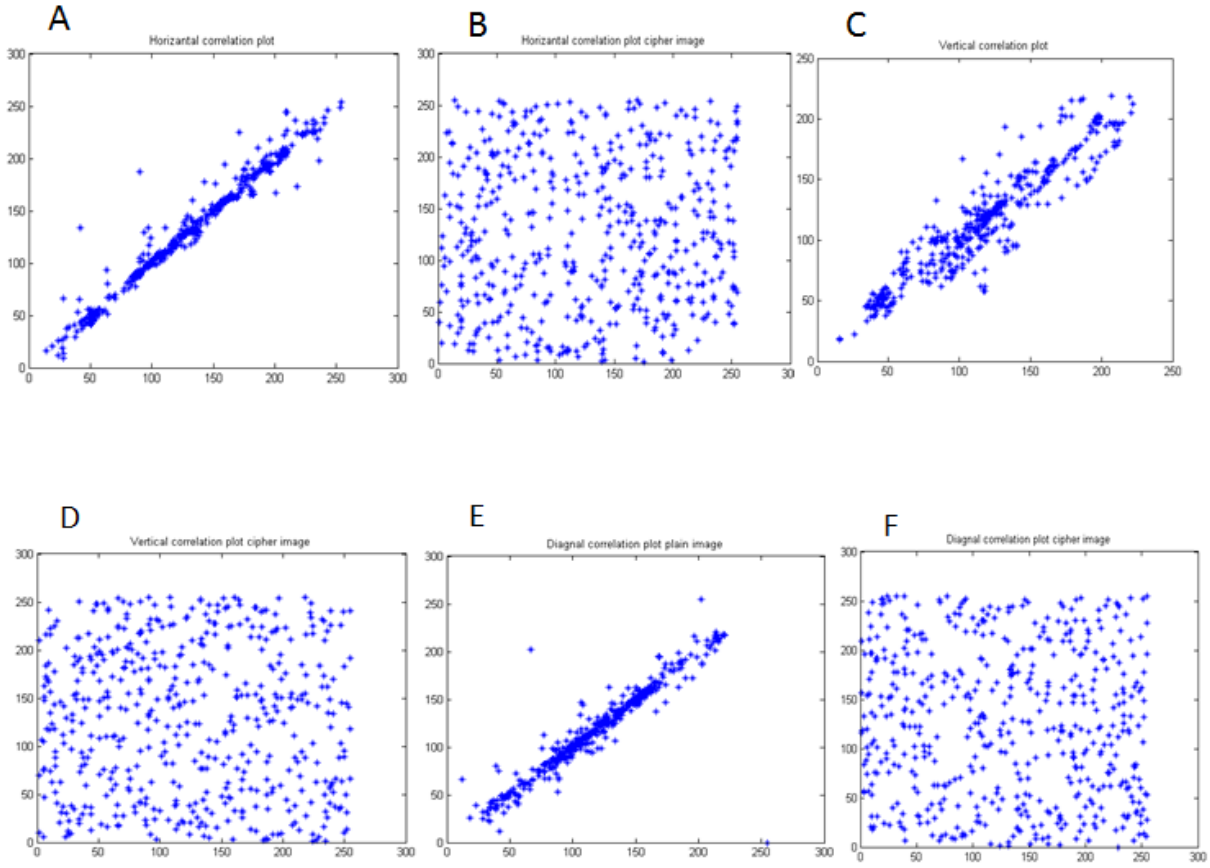

Fig. 6. Correlation plot of two adjacent plain-image pixels in (a) horizontal, (c) vertical, (e) diagonal directions. Correlation plot of two adjacent pixels of the cipher-image obtained by the proposed scheme in (b) horizontal, (d) vertical, (f) diagonal directions

References

[1] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," International Journal of Bifurcation and Chaos, vol. 08, no. 06, pp. 1259–1284, 1998. [Online]. Available: http://www.worldscientific.com/doi/abs/10.1142/S021812749800098X

[2] H. Yang, X. Liao, K. wo Wong, W. Zhang, and P. Wei, "A new block cipher based on chaotic map and group theory," Chaos, Solitons Fractals, vol. 40, no. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0960077907005322

[3] Y. Wang, K.-W. Wong, X. Liao, and G. Chen, "A new chaosbased fast image encryption algorithm," Applied Soft Computing, vol. 11, no. pp. 514 – 522, 2011. [Online]. Available:

http://www.sciencedirect.com/science/article/pii/S1568494609002658

[4] Z.-l. Zhu, W. Zhang, K.-w. Wong, and H. Yu, "A chaos-based symmetric image encryption scheme using a bit-level permutation," Inf. Sci., vol. 181, no. 6, pp. 1171–1186, Mar. 2011. [Online]. Available: http://dx.doi.org/10.1016/j.ins.2010.11.009

[5] H.-C. Chen, J.-I. Guo, L.-C. Huang, and J.-C. Yen, "Design and realization of a new signal security system for multimedia data transmission," EURASIP J. Appl. Signal Process., vol. 2003, pp. 1291–1305, Jan. 2003. [Online]. Available: http://dx.doi.org/10.1155/S1110865703309011

[6] C. Li, S. Li, G. Chen, G. Chen, and L. Hu, "Cryptanalysis of a new signal security system for multimedia data transmission," EURASIP Journal on Applied Signal Processing, vol. 8, pp. 1277 – 1288, May 2005. [Online]. Available: http://epubs.surrey.ac.uk/532628/

[7] W. Zhang, K.-w. Wong, H. Yu, and Z.-l. Zhu, "An image encryption scheme using lightweight bit-level confusion and cascade cross circular diffusion," Optics Communications, Jan. 2012. [Online]. Available: http://dx.doi.org/10.1016/j.optcom.2012.01.029

