Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 5, May 2013, pg.145 – 154

RESEARCH ARTICLE

AN IMAGE ENCRYPTION USING BIT LEVEL PERMUTATION AND DEPENDENT DIFFUSION

G.S. Nandeesh[1], P.A. Vijaya[2], M.V. Sathyanarayana[3]
[1]M. Tech Student (DECS) Mce, Hassan, Karnataka, India
[2]Professor BNMIT, Bangalore, Karnataka, India
[3]Principal Mce, Hassan, Karnataka, India

[1] nandi.kit@gmail.com; [2] pavmkv@gmail.com; [3] principal@mcehassan.ac.in

Abstract— Chaos-based cryptosystems have been studied extensively due to their superior properties in security and complexity. Recently, quite a lot of chaos-based image encryption schemes have been proposed. Most of them adopt the traditional permutation and diffusion operations. The drawbacks are: the architecture is not sensitive to changes in the plain-image and they are insecure upon chosen/known plain-image attack. Due to the favourable properties of bit-level permutation, we propose a bit-level confusion and dependent diffusion to enhance the security of the cryptosystem and to reduce the computation redundancy in traditional architectures. Simulations have been carried out and the results demonstrate the superior security and high efficiency of the proposed scheme.

Key Terms: - Encryption; image; Bit level permutation; confusion; Chaos; Cryptography; Image encryption; information security

I. INTRODUCTION

With the rapid development of computer network technology, a lot of sensitive information is transmitted over the network. Hence information security becomes more and more important. Image information transmission has increased rapidly and hence image encryption technology has drawn more attention. Nowadays, image encryption schemes include two processes: substitution and diffusion. The substitution stage permutes all the pixels as a whole, without changing their values. In the diffusion stage, the pixel values are modified sequentially so that a tiny change in a pixel spreads to as many pixels in the cipher-image as possible. The two processes can achieve a satisfactory level of security. Image encryption is different from text encryption due to some inherent features such as bulk data capacity and high correlation among pixels.

Therefore, traditional cryptographic techniques such as DES, IDES and RSA are no longer suitable for image encryption. The properties of chaotic maps such as sensitivity to initial conditions and random-like behaviour have attracted attention to develop image encryption algorithms. In recent years, some chaos based image encryption algorithms have been developed [2, 3, 4, 5]. chong FU et.al presented a novel chaos based bit level permutation scheme for digital image encryption and provides a fast and high security to overcome the drawbacks of conventional algorithms they propose significant diffusion effect in permutation procedure through a two stage bit level shuffling algorithm. Arnald cat map and chaotic sequence are used for shuffle all bit planes. This method decreases computational complexity and real time image communication applications[6].Yue Wu et.al have presented image encryption using the Sudoku matrix. Sudoku matrix defines as no two digits in the same block can be aligned in the same row, column or box.

Encryption of the image consists of three stages. In first stage, a reference Sudoku matrix is generated and it is used for scrambling process. The image pixels intensities are then changed by using the reference Sudoku matrix values, and then the pixels positions are shuffled using the Sudoku matrix as a mapping process. so using this matrix we can encrypt any digital images such as binary images, gray and RGB images. logistic map used for control the size of Sudoku matrix[7]. Yue Wu.et al has proposed a novel Latin square image cipher. provides a 256 bit key length for generating s Latin square and generates 256 x256 square image and it looks like Sudoku matrix that is no two digit in the same block can be aligned in the same row, column or box .LSIC achieve many desired properties of a secure cipher including a large key space, high key sensitivities, uniformly distributed cipher text, excellent confusion and diffusion properties, semantically secure, and robustness against channel noise [8]. Yue Wu.et.al have presented Sudoku associated two dimensional bijections for image Scrambling.

Sudoku configuration provides us a new alternative way of matrix element representation by using block-grid pair besides the conventional row-column pair and also discovers six more representations by using row digit pair, digit row pair, column digit pair, digit column pair, digit block pair, block digit pair associated with a Sudoku matrix. Sudoku Associated Image Scrambler only using Sudoku associated two dimensional bijections for image scrambling without bandwidth expansion[9].It has been also observed that, usage of Sudoku, Latin Square in Steganography and also in image encryption. The Duc Kieu et .al [10] have proposed a Sudoku based wet paper hiding scheme in which a secret key has been used to randomly select a subset of pixels from a cover image as dry pixels. Then a total automorphism is applied to the cover image to maximize the number of dry pixel pairs and each secret digit in the base-9 numeral system is embedded into one dry pixel pair.

Chin-Chen Chang et.al [11] has presented a Sudoku based secret image sharing scheme to lossless reveal of secret image. And also their approach derives the secret shadows and generates the meaningful shadow images by adopting the Sudoku. Roshan Shetty B et.al [12] have proposed a information scheme using Sudoku puzzle in which they used Sudoku solutions to guide cover pixels to modify pixel values so that secret messages can be embedded. Hill cipher is a type of mono alphabetic poly graphic substitution cipher. A novel method of generating self-invertible matrix is proposed which can be used in Hill cipher algorithm [15]. In this paper they try to overcome the drawback of using a random key matrix in Hill cipher algorithm for encryption, where we may not be able to decrypt the encrypted message, if the matrix is not invertible. Also the computational complexity can be reduced by avoiding the process of finding inverse of the matrix at the time of decryption, as we use self-invertible key matrix for encryption [16].

II. CHAOTIC MAP

In this section, the chaotic map will be described brief.

A. Bit level image

In a gray-level image, the brightness between black and white is quantized into an integer number of levels ranging from 0 to 255. The value of the pixel at coordinate (x,y) is denoted as f(x,y). Each pixel can transform to an 8 bit binary value, given by

$$f(x,y) = P(8)P(7)P(6)P(5)P(4)P(3)P(2)P(1) \tag{1}$$

So, the image can be divide into binary images according to the bit location within a pixel. Select the sample image Lena of size 256 x 256 and with 256 gray levels (Figure 1), divide it into 8 binary image (Table 2) according to the bit location within a pixel. In table 2 bit-plane(i) represents the binary image obtained by collecting the ith bits of all the plain-image pixels. A bit can be containing different amount of information depending on its position in the pixel. For example the 8th bit of a pixel represents128 (2^7), but it only represents 1 (2^0) at the first bit. The higher 4 bits (8th, 7th, 6th and 5th) carry 94.125% of the total information of the image. On the other hand, the lower 4 bits (4th, 3rd, 2nd and 1st) carry less than 6% of the image information, according to Eq.2. The percentage of the pixel information is shown in Table 1.

TABLE 1
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**

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

B. Chaotic map

An important step in any digital chaotic encryption is the selection of the map. Chaotic maps have different behaviour regarding complexity, chaotic properties cycle length, chaotic interval, periodic windows, etc., sensitivity to initial conditions and reaction to trajectory perturbations, etc., that influence the structure or behaviour of the chaotic encryption system. In fact, some systems have been broken for not considering the weaknesses of the chosen chaotic map and efficiency; it is desirable to provide some independency between the cryptosystem and the chaotic map under consideration. This independency means that, a full knowledge of the selected chaotic map is not needed to fulfil the security and efficiency requirements of a good cryptosystem.

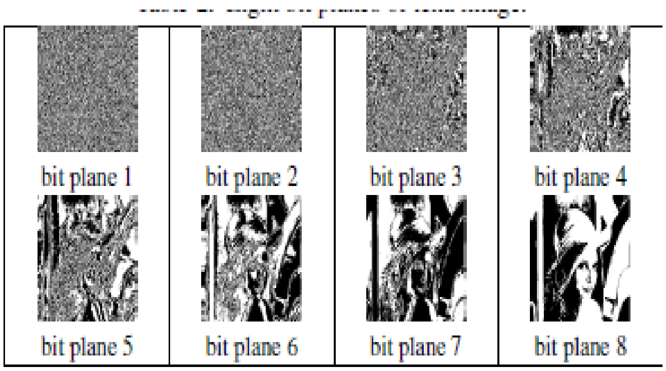
For their mathematical simplicity there are two options: logistic map and tent map. The logistic map is represented by

$$X_{n+1} = rX_n(1 - X_n) \qquad (3)$$

The logistic map chaotic signal used has primary values of X0 ϵ[0; 1] and r ϵ [3:57; 4].

Fig.1. Plain lena image of size 256 _ 256

TABLE 2
Eight bit planes of lena image.



III. Traditional Confusion Operation

Two-dimensional chaotic map is usually employed to permute the pixels. The cat map, standard map or ker map defined by Eqs.(4) to (6), respectively, suit this purpose.

$$\begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} modN, \tag{4}$$

$$\begin{cases} X' = (X+y) modN \\ Y' = \left(Y + ksin\dfrac{x'N}{2\pi}\right) modN, \end{cases} \tag{5}$$

$$B_d(X,Y) = \left[\frac{N}{n_i}(X - N_i) + ymod\frac{N}{n_i}, \frac{n_i}{N}\left(Y - Y_i mod\frac{N}{n_i}\right) + N_i\right] \tag{6}$$

A two-dimensional chaotic map defines a mapping rule from a regular position in the plain-image to a pseudorandom position in the cipher image. For each pixel in the plain-image, two kinds of operations need to be performed: calculate the new position of the pixel and then move the pixel from the original position to the new position. In general, the former computation needs more execution time than the latter one.

Consider the confusion process for an image with size 512**X**512, totally 262,144 pixels, using a cat map or a standard map. The first kind of operation computes 262,144 locations

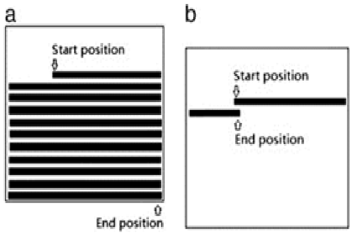


Fig.2. (a) The ideal situation, and (b) the actual situation, in plaintext sensitivity test

Since each location contains two coordinates (x,y), we need to calculate 2621442=524288 pseudorandom numbers, and the computation of each such number includes multiple complicated floating point operations. However, in the second kind of operation, we just need to move a byte from a memory address to another. These drawbacks are illustrated using TDCEA [2] as an example. TDCEA is a typical permutation-only cipher with the confusion operation not operating on the full-image. The basic confusion unit is a group of 8 pixels, and there is no confusion strategy among all the pixels in the plain-image. A diffusion phase is added to the TDCEA to form an enhanced version called ETDCEA.

IV. TRADITIONAL DIFFUSION OPERATION

In a traditional cryptosystem, an effect of the confusion operation is to determine the order of diffusion. All the pixel values are systematically modified in the diffusion phase. On the contrary, we just change the pixel locations in the confusion phase while the statistical information of the permuted image is not changed at all. In conventional diffusion operations, the two dimensional image is transformed to a one-dimensional sequence. The value of the ciphered pixel is governed by two factors, the previously processed pixel values and the initial condition of the chaotic system. The order of process is always from the upper left corner to the lower right corner. The original and the modified plain images are permuted in the same way in which the modified pixel is relocated to a random position referred to as the start position. At last, the two permuted images are diffused using the same key to obtain two cipher-images.

The number of different pixels between the two cipher-images is calculated. More different pixels indicate a higher sensitivity to the plain-image. As illustrated in Fig 2. However, in the actual situation, the modified pixel sequence is not as long as expected, as shown in Fig 2(b) Fig 2(a) and (b), the black pixels, from the start position to the end position, indicate the unequal pixels between the original and the modified cipher-images after one round of confusion and diffusion. However, the modified cipher image deviates the original orbit from the textitstart position where the modified pixel locates. As Fig 2(b) illustrates. Some intrinsic features or mechanisms stop the deviation of the orbit, and drive it back to the original one.

V. THE PROPOSED SCHEME

The confusion phase In [1], a new cryptosystem using a bit-level permutation (abbreviated as BLP) was proposed, in which a pixel is further divided into 8 bits. Since different bit locations in an 8- bit plane carry different amount of information, two strategies are employed in the confusion phase. The higher four bits, which contain 94.125 of the total information, are permuted independently with different parameters of the chaotic map. The lower four bits, which contain 5.875 of the total information, are permuted as a whole. In traditional encryption schemes, permutation-only ciphers fail to provide sufficient security and almost all of them have been cryptanalyzed by known/chosen plaintext attacks. Therefore, we can conclude that in Fridrich's architecture, the confusion operation is a necessary part and can be treated as a preparation for the diffusion phase in which most of the masking or encryption tasks are achieved. In Section II, we have discussed the two basic requirements of confusion. Firstly, the range of confusion should be at the full-image scale; otherwise, a modification in the plain-image can only spread over a limited area in the cipher-image (like TDCEA). Secondly, the correlation coefficients of the image should be significantly reduced after confusion. Furthermore, the processing order of the diffusion operation is governed by the confusion round.

$$case \quad index = \begin{cases} ac(i,j) = C_{scan}, index_k = 1 \\ ac(i,j) = D_{scan}, index_k = 2 \\ ac(i,j) - O_{scan}, index_k - 3 \\ ac(i,j) = S_{scan}, index_k = 4 \\ ac(i,j) = Z_{scan}, index_k = 5 \end{cases} \qquad (7)$$

In the proposed scheme, a bit level permutation scheme is employed which involves the five kinds scan patterns shown in Fig. 3. Some simple mappings among different bit planes are performed to achieve a higher operating efficiency and to fulfil the basic requirements of confusion. Different mapping cases are employed for different bit planes. Therefore, the bit-constitution of each original pixel is modified, which leads to a new pixel value.

The proposed confusion scheme simultaneously changes the pixel locations and modifies their values. A pseudorandom number determines the kind of mapping employed in each bit plane. To permute a basic image unit (pixel or bit) using conventional confusion, two pseudorandom numbers should be generated to determine the new position of that basic unit. After that, the unit is relocated from the original memory address to the new memory address. The execution time consumed in the first calculation varies according to different two-dimensional mapping rule. The mean time is 28.03 ms in each confusion round for a 512**X**512 plain image. However, the time needed for the relocation is only 3.1 ms for all mappings since just 512**X**512 units are moved from a memory location to another. Since the relocation process is necessary for confusion, it is suggested to reduce the execution time of the first calculation as much as possible. In the lightweight confusion the proposed confusion makes best efforts to reduce the calculation redundancy in traditional confusion, and simultaneously reduces the correlation coefficients of the image significantly. If the entire eight bit planes are permuted by two-dimensional chaotic maps, the execution time is much longer than the proposed lightweight confusion operation.

To permute them, 24.8 ms is required by the proposed scheme while 49.6 ms and 424.8 ms are needed using cat map and standard map confusion, respectively. Furthermore, since the 8th bit plane carries more than 50 of the total information of the plain-image, a cat map can be employed to permute it. In this case, another 3.1ms is needed. Otherwise, the eight bit planes are all permuted by bit level permutation using different mapping cases, and the performance is still satisfactory. In the confusion phase, the permutation of each bit plane is governed by Eq. (6) where N be both the width and the height of the image.

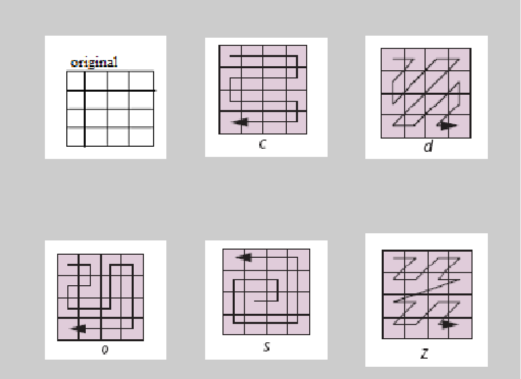


Fig. 3. Five kinds of Scan patterns in the proposed lightweight confusion

In Eq. (6), index k indicates the mapping case for the kth bit plane,k[0; 7]. ac(i, j) is the bit value after confusion at location (i, j) while arr(i, j) is the original bit value. The value of indexk is governed by a logistic map, according to Eqs. (5) and (6).

$$index_k = (X_{2000+k} * 10^9)mod\ 5 + 1 \tag{8}$$

In Eq. (5), r is the parameter of the logistic map. The output sequences chaotic when [3.57, 4]. In the proposed scheme, is set to 3.99999, the initial value x0 is set to 0.33284657332813, and index$_k$ is calculated by Eq. (8). A cat map can be employed optionally to permute some significant bit planes for a better performance, with an additional 3.1 ms required. In this case, the coefficients of the cat map are calculated by Eq. (9).

$$P = (y(2000+0) \times (10^9)modNq) = (y(2000+1) \times (10^9)modNq) \tag{9}$$

In Eq. (9), y is the output sequence of the logistic map with coefficient=3.99999 and initial value 0.67215678912329.

VI. The Diffusion Phase of the Proposed Scheme

The process of dependent diffusion is governed by Eq. (10)

$$\begin{gathered} Ciph(x,y) = conf(x,y) \oplus ([t \times (t/1000) \times [1 \quad (t/1000)] \times 1000]mod256) \\ t = Ciph(x,y) \end{gathered} \tag{10}$$

In Eq. (10), conf is represents confused image and t is a temporary variable storing the value of the previous ciphered pixel. Its initial value is defined by t = [4 *keyd (1 - keyd) *1000]mod256, N is the width (or height) of the test image, x[0;N1],y[0;N1]. keyd is set to 0.33456434300001.

VII. Experimental Results and Performance Analysis

Statistical analysis: In the proposed encryption algorithm, the diffused image is randomly distributed. This is shown by a test on the histograms of the cipher-images in Section i, the information entropy of the cipher-image in Section ii, the correlations of adjacent pixels in the plain-image and cipher image in Section iii, Analysis of differential attack in section iv. Analysis of key sensitivity in section v.

i. Histogram analysis. An image histogram illustrates that how pixels in an image are distributed by plotting the number of pixels at each gray scale level. The distribution of cipher-text is of much importance. More specifically, it should hide the redundancy of plain-text and should not leak any information about the plaintext or the relationship between plain-text and cipher-text.Table 4 shows the histograms of plain-images and its ciphered images generated by the proposed scheme respectively. It's clear from that the histograms of the cipher-images are fairly uniform and significantly different from that of the plain image and hence do not provide any clue to employ statistical attack.

ii. Information entropy analysis. In information theory, entropy is the most significant feature of disorder, or more precisely unpredictability. To calculate the entropy H(X) of a source x, we have:

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

TABLE 3
Entropy

Input images	Size	Plain image entropy	Encrypted image entropy
Lena	512x512	7.4451	7.9993
Peppers	512x512	7.5937	7.9992
Cameraman	512x512	6.971	7.9965
Babon	512x512	7.3583	7.9993
Elaine	512x512	7.5060	7.9992

If the output of a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. The entropies for plain image and ciphered images using various images are calculated in Table 3. Apparently, the proposed algorithm is much closer to the ideal situation. This means that information leakage in the encryption process is negligible and the cryptosystem is secure against entropy attack. Analysis of correlation of adjacent pixels. For an ordinary image having definite visual content, each pixel is highly correlated with its adjacent pixels either in horizontal, vertical or diagonal direction. However, an efficient image cryptosystem should produce the cipher image with sufficiently low correlation in the adjacent pixels.

The visual testing of the correlation of adjacent pixels can be done by plotting the distribution of the adjacent pixels in the plain image and its corresponding cipher image. The correlation distribution of two horizontally adjacent pixels, two vertically adjacent pixels and two diagonally adjacent pixels of the plain image and the cipher image produced by the proposed scheme is shown in fig 4, respectively. It is clear that the strong correlation between adjacent pixels in plain image is greatly reduced in the cipher image produced by the proposed scheme. To quantify and compare the correlations of adjacent pixels in the plain and cipher image, the following procedure is carried out. First, randomly select 1000 pairs of adjacent pixels in each direction from the plain image and its ciphered image. Then, calculate the correlation coefficient rx;y of each pair by using the following four formulas:

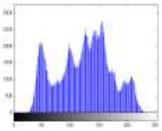
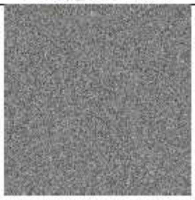
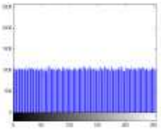
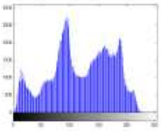
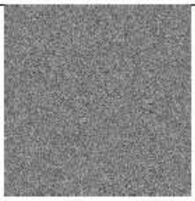
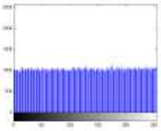
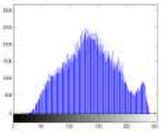
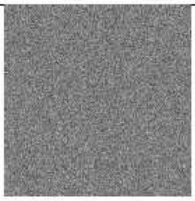
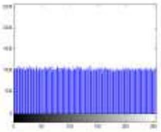
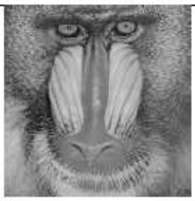
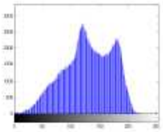
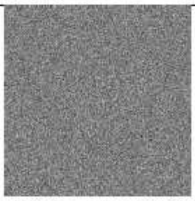
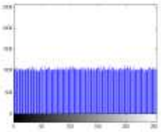
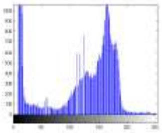
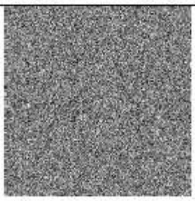
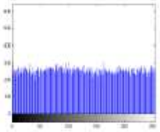
$$Cov(x, y) = E\big(x - E(x)\big)\big(v - E(v)\big) \tag{12}$$

$$E(x) = \tfrac{1}{N}\textstyle\sum_{i=1}^{N} X_i \tag{13}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\big(X_i - E(X_i)\big)^2 \tag{14}$$

where x and y are grayscale values of two adjacent pixels in the image and N denotes the total number of samples, Cov(x, y) is covariance, D(x) is variance, E(x) is mean

TABLE 4
Resultant Encrypted Images and its histogram of proposed method

Input Image	Histogram	Encrypted Image	Histogram
			
			
			
			
			

.

iii Analysis of differential attack. A well-designed encryption algorithm should be highly sensitive to plain-image and keys, so a slight change in plain-image or keys will make the cipher-image quite different. If an encryption scheme contains no confusion or diffusion stage, it would easily be destroyed by differential attacks. In order to confirm whether the proposed encryption algorithm is sensitive to plain image and keys, this paper brings out two tests: Number of pixels change rate (NPCR) and Unified average changing intensity (UACI) [21]. The equation to calculate UACI is Eq. 15

$$UACI = \frac{1}{M+1}\sum_{i,j}\frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \qquad (15)$$

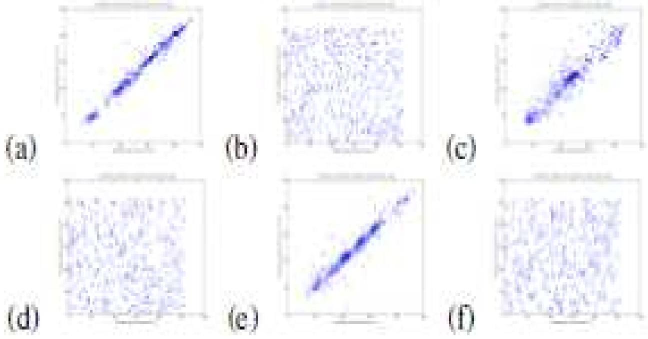


Fig. 4. Correlations of two adjacent pixels for lena image of size 512_512(a) horizontal direction of the plain image, (b) horizontal direction of the cipher image, (c) vertical direction of the plain image, (d) vertical direction ofthe cipher image, (e) diagonal direction of the plain image, and (f) diagonaldirection of the cipher image

C1(i,j) means the gray-scale value of cipher-image in position (i,j), and C2(i,j) means the gray-scale value of the new cipher-image which is the encryption result of modified plain image that has just one different pixel to the original plain-image. NPCR can be calculated by Eq. 16

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \qquad (16)$$

TABLE 5
Correlation coefficients of two adjacent pixels in plain-image and ciphered-images of proposed method

	Plain image			**Encrypted image**		
Image	**Horizontal**	**Vertical**	**Diagonal**	**Horizontal**	**Vertical**	**Diagonal**
Lena	0.9691	0.9841	0.9842	0.0051	-0.0005	0.0013
Peppers	0.9733	0.9764	0.9809	0.0200	0.0027	0.0049
Baboon	0.8652	0.7524	0.7567	-0.0051	-0.0037	-0.0021
Camaramen	0.9333	0.9565	0.9564	-0.0129	-0.0081	-0.0045
Elaine	0.9738	0.9695	0.9697	-0.0386	0.0007	0.0030

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

$$D(i,j) = \begin{cases} 1 \; if \; C_1(i,j) \neq C_2(i,j) \\ 0 \; if \, C_1(i,j) = C_2(i,j). \end{cases} \qquad (17)$$

When one bit of a pixels gray-scale value in the plain image is changed, then a new plain image is generated from the original one. Encrypt the two images with the same secret keys, then take cipher images into Eqs. 15 and 16 and results are shown in Table 6. From the Table results we can find that our algorithm is very sensitive to tiny changes in the plain image, even if there is only one bit difference between two plain images, the decrypted images will be completely different.

TABLE 6
NPCR and UACI of Proposed method

Image	**NPCR%**	**UACI%**
Lena	99.56	28.60
Peppers	99.60	29.69
Camaraman	99.60	31.09
Baboon	99.62	27.75
Elaine	99.61	28.49

VIII. CONCLUSION

The conventional architecture of chaos-based image encryption has been investigated in detail. The drawbacks of the confusion and diffusion operations are described. An encryption scheme with lightweight bit-level permutation and dependent diffusion is proposed to solve the problems encountered in the traditional architecture. In the confusion stage, bit level permutation not only changes the locations of the image pixels, but also modifies their values. Furthermore, the lightweight bit confusion operation reduces the computation redundancy in this stage. In the dependent diffusion phase, chaotic map based equation employed to get encrypted image. Simulation results show that the NPCR, UACI, and information entropy of the proposed schemes are better than those of a comparable cryptosystem, BLP. All these results justify the superior security and computational efficiency of our cryptosystems.

REFERENCES

[1] S.H. Wang, J.Y. Kuang, J.H. Li, Y.L. Luo, H.P. Lu, G. Hu, Physical Reviews E 66 (6) (2002)

[2] H.J. Liu, X.Y. Wang, Optics Communications 284 (2011) 3895.

[3] Y. Wang, K.W. Wong, X.F. Liao, G.R. Chen, Applied Soft Computing 11 (2011) 514.

[4] X.Y. Wang, J.F. Zhao, H.J. Liu, Optics Communications 285 (2012) 562.

[5] A. Kumar, M.K. Ghose, Communications in Nonlinear Science and Numerical Simulation 16 (2011) 372.

[6] Chong Fu , Bin-bin Lin , Yu-sheng Miao , Xiao Liu , Jun-jie Chen. A novel

[7] Chaos-based bit-level permutation scheme for digital image encryption. Optics Communications 284 (2011) 54155423. doi:10.1016/j.optcom.2011.08.013.

[8] Yue Wu ,Yicong Zhou, Joseph P. Noonan, Karen Panetta, Sos Agaian. Image Encryption using the Sudoku Matrix. Proc. of SPIE Vol. 7708, 77080P 2010 SPIE CCC code: 0277- 786X/10/18 doi: 10.1117/12.853197.

[9] Yue Wu, Yicong Zhou, Joseph P. Noonan, Sos Agaian and C. L. Philip Chen. A Novel Latin Square Image Cipher. IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. arXiv:1204.2310v1 [cs.CR] 11 Apr 2012.

[10] Yue Wu, Sos Agaian and Joseph P. Noonan. Sudoku Associated Two Dimensional Bijections for Image Scrambling. arXiv:1207.5856v1 [cs.CR] 25 Jul 2012.

[11] The Duc Kieu, Zhi-Hui Wang, Chin-Chen Chang, and Ming- Chu Li, A Sudoku Based Wet Pa-per Hiding Scheme, International Journal of Smart Home, 2009, 1 12.

[12] Chin-Chen Chang, Pei-Yu Lin, Zhi Hui Wang and Ming Chu Li, A Sudoku-based Secret Image Sharing Scheme with Reversibility, Journal Of Communications, Vol. 5, No. 1, January 2010, 5-12.

[13] Roshan Shetty B R, Rohith J, Mukund V, Rohan Honwade, Shanta Rangaswamy, International Conference on Advances in Recent Technologies in Communication and Computing, 2009.

[14] Zhengjun Liu et al. Double image encryption by using Arnold transform and discrete fractional angular transform, Optics and Lasers in Engineering 50 (2012) 248255.

[15] Zhenjun Tang and Xianquan Zhang, Secure Image Encryption without Size Limitation Using Arnold Transform and Random Strategies, Journal of Multimedia, VOL. 6, NO. 2, APRIL 2011, 202-206.

[16] BibhudendraAcharya, GirijaSankarRath, Sarat Kumar Patra, Saroj Kumar Panigrahy. Novel Methods of Generating Self- Invertible Matrix for Hill Cipher Algorithm, International Journal of Security, Vol 1, Issue 1, pp. 14-21, 2007. 6 International Journal of Computer Applications (0975 8887) Volume * - No. *, ——— 2012

[17] BibhudendraAcharyaet. al, Involutory, permuted and reiterative key matrix generation method for hill cipher system, International journal of recent trends in engineering, Vol. 1, No. 4, pp. 106-108, May 2009.

[18] Zhang, L. Guo, X.P. Wei, Image encryption using DNA addition combining with chaotic maps, Mathematical and Computer Modeling 52 (1112) (2010) 20282035.

[19] Q. Zhang, Q. Wang, X.P. Wei, A novel image encryption scheme based on DNA coding and multi-chaotic maps, Advanced Science Letters 3 (4) (2010) 447451(Cuba, Logistic).

[20] Hongjun Liua,b, Xingyuan Wanga, Abdurahman kadirc, Image encryption using DNA complementary rule and chaotic maps. Applied Soft Computing 12 (2012) 14571466.

[21] N.K. Pareek et al.,Diffusion-substitution based gray image encryption scheme Digital Signal Process. (2013).