Image Encryption using Chaos and Parity based Pixel Modification in Permutation

T.Gopalakrishnan
Assistant Professor
Dept. of EEE
Dr.Mahalingam college of Engineering and Technology
Pollachi, India

S.Ramakrishnan
Professor & Head
Dept. of IT
Dr.Mahalingam college of Engineering and Technology
Pollachi, India

M.Balakumar
PG Scholar
Dept. of EEE
Dr.Mahalingam college of Engineering and Technology
Pollachi, India

ABSTRACT
This paper introduces a chaos based image encryption with parity based pixel value modification in the permutation stage. The encryption algorithm consists of two stages permutation-diffusion. Permutation stage original image pixels are scrambled and diffusion stage masks the original image pixel with the pseudo random binary sequence. Parity based pixel modification in permutation gives maximum security level in minimum rounds. The 1D chaotic maps logistic map, sine map and cubic map employed to permute and diffuse image pixels.

Keywords
Chaotic map, Image encryption, Odd or even parity, Random binary sequence, Security analysis.

1. INTRODUCTION
Cryptosystem has grown over recent years particularly gained much attention for its potential role in information safety. Chaotic systems have good features such as sensitivity to initial conditions, ergodicity, mixing property and parameters, which have granted chaotic cryptosystems a promising alternative for the traditional cryptography algorithms. To attain a great demand for protected image communications through public channels, a variety of chaos-based image encryption schemes have been proposed [1]-[14]. In 1989, Matthews first proposed the chaos-based encryption algorithm [2], and Fridrich first adopted chaotic systems into image encryption in 1997 [3]. Fridrich's scheme consists of substitution and diffusion in spatial domain. The substitution is attained by shuffling all the pixels as a whole using a 2D chaotic map. The current pixel is moved to calculated new position using 2D chaotic map. In the diffusion process, the pixel values are changed consecutively and the change made to a particular pixel depends on the accumulated effect of all the previous pixel values. This substitution–diffusion style forms the basic structure for many following chaos based image encryption algorithms.

The main characteristics of these schemes consist of one or several chaotic maps serving the purpose of either just scrambling the pixels or consequently masking the resulting shuffled image. A 2D chaotic map is generalized to 3D standard map to shuffle the positions of the image pixels and another chaotic map is used to confuse the relation between the encrypted and its original image in [4]. The similar idea is used with the 3D chaotic baker's map at the substitution stage instead of the 3D standard map [5].In [6], the 2D cat map is used to shuffle the position of the image pixels and the output of a discretized Chen's system is used to mask the pixel values. After shortly encryption scheme in [6] proposed, it is exposed that there are some weak keys present, and the key space of the chaotic baker's and cat maps is not as large as that of the chaotic standard map [7]. Then, the chaotic standard map is used for the confusion or substitution along with a new diffusion function having high diffusion speed based on the quantized chaotic logistic map and a key stream generator based on the chaotic skew polynomial map. It is also recommended that at least four rounds of the substitution and diffusion are essential for security performance. Again, [8] showed that the diffusion effect in [7] is not necessarily contributed solely by the diffusion process. Instead, it is introduced in the substitution stage to achieve security performance in less number of rounds than the one suggested in [7].The image encryption schemes are cryptanalyzed due to weakness in key stream or in its architecture. To avoid the chosen-plaintext attack for every round of image encryption the permutation and diffusion bits needs to be updated. In this proposed method in the permutation stage the image pixels are scrambled and the pixel values are also modified based on the parity of the chaotic map generated pseudo random sequence. In the diffusion stage different random sequence are generated for each round to avoid different attacks. The rest of the paper is organized as follows; section II explains the proposed encryption scheme. Section III shows the experimental analysis and also different visual effect analysis and in the last section conclusion is given.

2. PROPOSED METHOD
In this section a chaotic image encryption using permutation-diffusion structure shown in Fig.1. In permutation process the original image pixels are scrambled in spatial domain and diffusion process the original image pixel bits are masked with the randomly generated binary sequence. The main aim of the encryption algorithm should resist the cipher image from various attacks and also the speed of the algorithm is one of the important constraints in the real time processes. In this proposed method chaotic maps are used to generate the pseudo random sequence to permute and diffuse the image pixels. In the permutation process original image pixels locations are modified and also the pixels values are modified. Logistic map Eq. 1 is one of the popular chaotic maps in the chaos based image encryption algorithm and it is given by following relation,

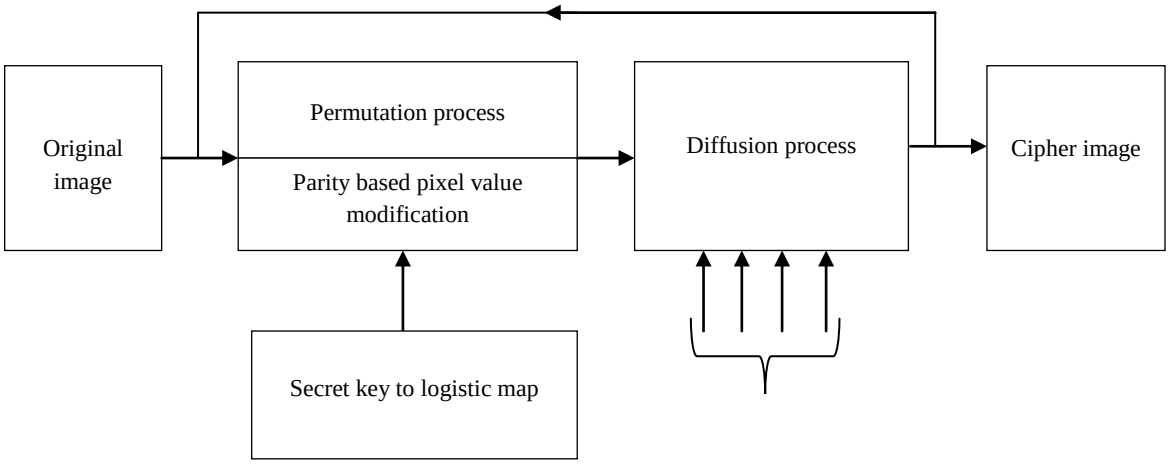

Fig 1: Proposed Encryption Structure

$$z_{n+1} = rz_n(1-z_n) \quad (1)$$

where r is the parameter and it ranges from 0 to 4. When r is greater than the 3.57 it possesses the chaotic behavior. Permutation process the logistic map which is used to generate the random sequence with non-repeated values. The outcome of the map is (0.2, 0.9, 0.3, 0.8, 0.7, 0.1, 0.5, 0.6) and sorted sequence is in random (6, 1, 3, 7, 8, 5, 4, 2). Using this random sequence the original image pixels are altered and also by using Eq. 2 random integers are generated.

$$rand\_seq_i = (x(\mathrm{i}) * 2^{32}) \bmod 256 \quad (2)$$

The generated random integers are converted in to binary of 8 bits each and based on the 1's parity the scrambled pixel bits are shifted using Eq. 3. The parity of the random values is determined by the number of 1's present in the binary form of the random value and the number of bit shifting determined by number of 1's present in the random value. If the random integer value of 1's parity is odd then the pixel bits shift towards right and if the 1's parity is even, then the pixel bits are shifted towards left side. The shifting is performed sequentially up to all pixels gets over.

$$parity\_output = \begin{cases} odd, right\,shift \\ even, left\,shift \end{cases} \quad (3)$$

This simple pixel value changes directly the encryption technique in the reduction of number of rounds required to achieve the maximum security. In the diffusion process random binary sequence is generated as shown in Fig. 2. The diffusion keys are fed as initial condition for the sine map Eq. 4 and cubic map Eq. 5; it is iterated for the length of the binary sequence of the shuffled image pixel bits.

$$x_{n+1} = a\sin(\pi x_n) \quad (4)$$

$$y_{n+1} = by_n(1-y_n^2) \quad (5)$$

where a and b are the control parameters of the sine and cubic map is in the range of [0,1] and [0,3]. Both maps possess chaotic behavior in the range of sine map 0.76 to 0.99 and for cubic map 2.59 to 3.

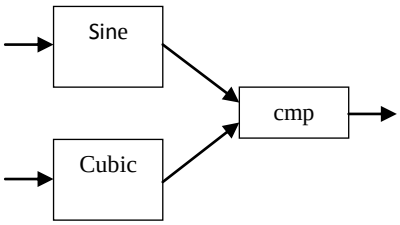

Fig 2: Random Binary Sequence Generator

K is the diffusion keys for round 1 the first two keys are fed as initial condition for sine and cubic map. For second round other two keys act as an initial condition to both maps. The sine and cubic map values are compared (cmp) and if sine is greater than cubic value the random binary value is 0 otherwise it produces 1. This sequence is generated up to total length of shuffled image pixel bits. This random binary sequence generator produces the different sequence for every round though the ciphered image at every round is different from previous one. Employing of two chaotic systems improves the chaotic behavior and randomness of the random binary sequence. The generated random binary sequence is masked with image binary sequence and produces the binary cipher image. Then the binary sequence is converted to integer sequence to produce the cipher image.

2.1 Encryption Algorithm

The chaotic based spatial domain encryption techniques should resist the different cryptanalysis attacks and also differential attacks and statistical attacks. The effective permutation-diffusion gives efficient cipher image.

Step1: Original image pixels are scrambled based on the random sequence generated by logistic map.

Step2: Based on parity of the random integer sequence the shuffled image pixel bits are shifted either right side or left side.

Step3: Random binary sequence is generated as shown in Fig. 2. The generated sequence is manipulated with the shuffled image pixel bits.

Step4: The binary sequence is converted into integer sequence to produce the cipher image. This process is repeated for two rounds.

2.2 Decryption Algorithm

Decryption is the reverse of the encryption process. It is a symmetric key encryption algorithm in which the same keys are used in the retrieval process. The use of chaos provides the lossless encryption and decryption.

3. EXPERIMENTAL ANALYSIS

To demonstrate the cipher image security and the encryption architecture performance analysis are performed like statistical analysis, differential analysis, and entropy analysis. The simulated resultant outputs are shown in Fig. 3. The Lena gray scale image is encrypted using this encryption algorithm. Figure 3 shows the ciphered image for two rounds. The pixel intensity value modification in permutation process improves the encryption quality in minimum rounds. The proposed encryption algorithm in the first round attains encryption criteria's NPCR, UACI, Correlation coefficient and it is performed for maximum two rounds to produce complex computations.

3.1 Secret Key and Key Space Analysis

The symmetric keys are used in the both encryption and decryption side. The use of chaotic map and its main and very effective property of being sensitive to initial condition provides good security to encryption algorithm. The secret keys are given in floating numbers, The MATLAB can perform up to 14 bits maximum length (i.e) 10^{14}. Sine and cubic map parameters a, b, four diffusion keys and logistic map parameter r and its initial condition. The total key space is 1084 and it is greater than the minimum required level of key space to avoid brute force attack.

3.2 Key Sensitivity Analysis

The image is encrypted with initial set of diffusion keys and the four diffusion keys are slightly modified the resultant image and its histogram is shown in the Fig.3.The histogram variation shows that the encryption algorithm is very sensitive to its initial condition (i.e) symmetric encryption keys. The slight variation in the key gives drastic variation in its cipher image.

3.3 Histogram Analysis

A histogram of an image shows how pixels are distributed in that image. The graph shows the pixel values in x-axis and number of occurrence in y-axis. The histogram of several encrypted and original images of widely different content are calculated and analyzed. It is clear that the histograms of encrypted images are flat and has no clue about the original histogram of the image. The results of histogram analysis are in Figure 3 (a) and 3(b) shows the original and encrypted images of size 256x256 Fig. 3 (e) and Fig. 3 (f) shows the original and encrypted images histograms respectively. From these results Fig. 3 (f) is completely flat and has no clue about the histograms of Fig 3 (a).

3.4 Correlation Coefficient Analysis

The noticeable characteristic of visually meaningful images is redundancy. There are high correlations between pixels and their adjacent pixels at horizontal, vertical and diagonal directions. The image encryption algorithm aims to break these pixel correlations in the original images with little or no correlations. This analysis shows the correlation between the randomly selected pairs of both original image and cipher image. This analysis carried out by following the procedures, Randomly 5,000 pairs horizontally, vertically and diagonally adjacent. The correlation is calculated by the following equations,

$$r_{xy} = \frac{E\left\{\left|x - E(\mathrm{x})\right|\left|y - E(\mathrm{y})\right|\right\}}{\sqrt{D(\mathrm{x})}\sqrt{D(\mathrm{y})}} \tag{6}$$

$$E(\mathrm{x}) = \frac{1}{s}\sum_{i=1}^{s} x_i \tag{7}$$

$$D(\mathrm{x}) = \frac{1}{s}\sum_{i=1}^{s}\left[x_i - E(\mathrm{x})\right]^2 \tag{8}$$

where x and y are the gray level values of the two adjacent pixels in the image, E(x) and D(x) are the mean and standard deviation of the corresponding gray level values. rxy is the correlation between the adjacent pixels. If the correlation co-efficient value is 1 means the image is original and the correlation between the adjacent pixels is not broken. If the value is -1 means that the image is the exact negative of the original image. The Table 1 shows the correlation coefficients of the original and encrypted images when compared with wong k et al. algorithm in horizontal, vertical and diagonal direction. The original image values are nearly equal to 1 because the correlation between the adjacent pixels is high. The encrypted image values are approximately 0. Figure 4 shows the horizontal direction correlation plot. Figure 5 shows vertical direction correlation plot and Figure 6 shows diagonal correlation plots of original and encrypted image.

Table 1. Correlation coefficients

Direction	Original image	Proposed	Wong k [8]
Horizontal	0.9432	0.0007	0.0026
Vertical	0.9699	0.0086	0.0091
Diagonal	0.9218	-0.0057	0.0034

3.5 Differential Attack

In order to avoid differential attack, a minor change of original image should cause a substantial change in the cipher image. The common measures used to measure this sensitivity are NPCR (Number of pixel change rate) and UACI (unified average changing intensity) proposed by NIST. They are given by the following equations,

$$NPCR = \frac{\sum_{i,j} D(\mathrm{i},\mathrm{j})}{W \times H} \times 100\% \tag{9}$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j}\frac{\left|c_1(\mathrm{i},\mathrm{j}) - c_2(\mathrm{i},\mathrm{j})\right|}{255}\right] \times 100\% \tag{10}$$

where C1 and C2 are the cipher images whose original images have a slight difference in one pixel.

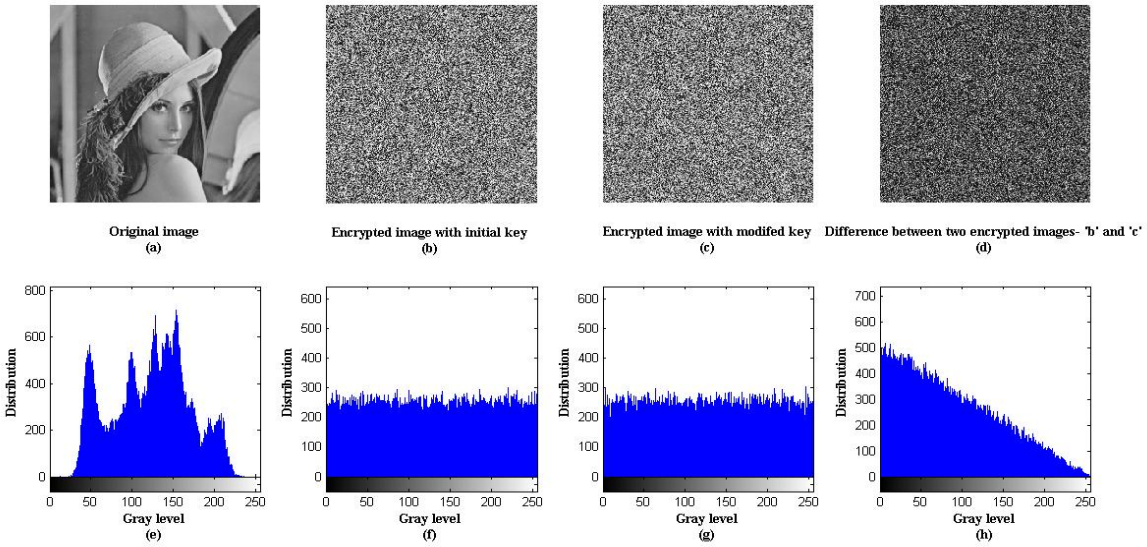

Fig 3:a) Original image b) Encrypted image with initial key c) Encrypted image with modified key d) Difference between two encrypted images e) Histogram of original image f) Histogram of Encrypted image with initial key g) Histogram of Encrypted image with modified key h) Histogram of Difference between two encrypted image

C1 (i, j) denotes the position of pixel in C1.W and H are width and height of the cipher image. D(i, j) is determined as1,if C1(i, j)=C2(i, j) otherwise D(i, j)=0. The resulting NPCR and UACI values are tabulated in Table 2. NPCR is greater than or equal to 0.995 and UACI is greater than or equal to 0.333. From Table 3 it clearly shows that the proposed method has NPCR and UACI values average of 0.9962 and 0.3346 and also compared with wong k et al. method. For the security purpose maximum 2 rounds of the proposed algorithm performed. The NPCR of our scheme can reach 99.61% in the first round. That indicate the cryptosystem is very sensitive to even a 1-bit modification. The Table III shows the NPCR and UACI for different images. For various images the proposed method satisfies the NPCR and UACI criteria.

Table 2. NPCR and UACI analysis

Round	Proposed		Wong k [8]	
	NPCR	UACI	NPCR	UACI
1	0.9961	0.3340	0.9959	0.3343
2	0.9964	0.3362	0.9962	0.3342

Table 3. NPCR and UACI analysis of various images

Images	NPCR	UACI
Lena	0.9965	0.3355
Baboon	0.9967	0.3362
House	0.9962	0.3354
Camera man	0.9959	0.3357
Boat	0.9956	0.3352
Barbara	0.9968	0.3350

3.6 Randomness Test

The randomness test is performed to check the encrypted image randomness. This test is performed using sp800-22 test suite developed by NIST [12]. The Table 4 shows that the encrypted image has the randomness quality and it succeeds in the all above tabulated tests.

Table 4. Randomness test

Statistical test	P value	Result
Frequency	0.8391	Success
Block frequency	0.2460	Success
Runs	0.6990	Success
Binary Matrix Rank	1.0000	Success
Cumulative sums	0.7598	Success

3.7 Information Entropy Analysis

The entropy of a message source can be measured by,

$$H(m) = \sum_{i=0}^{M-1} p(m_i) \log \frac{1}{p(m_i)} \qquad (11)$$

where m is total number of symbols, p(mi) represents the probability of occurrence of symbol mi, and log denotes the base 2 logarithm so that the entropy is expressed in bits. The entropy can be used for evaluating the randomness of an image. If an entropy score of an image is close to the maximum entropy value it shows the excellent random property. Table 5 shows the information entropy comparison of proposed and Wong et al. algorithm. For a gray scale image with a data range of 0 to 255, its maximum entropy is 8. The cipher image entropy value is nearly equal to 8 bits. Hence the proposed algorithm is robust against entropy attacks. Table 6 shows the entropies of various images. The entropy

determines the randomness of the encrypted image. In our algorithm the entropy value is approximately (entropy=7.9972) equal to 8.

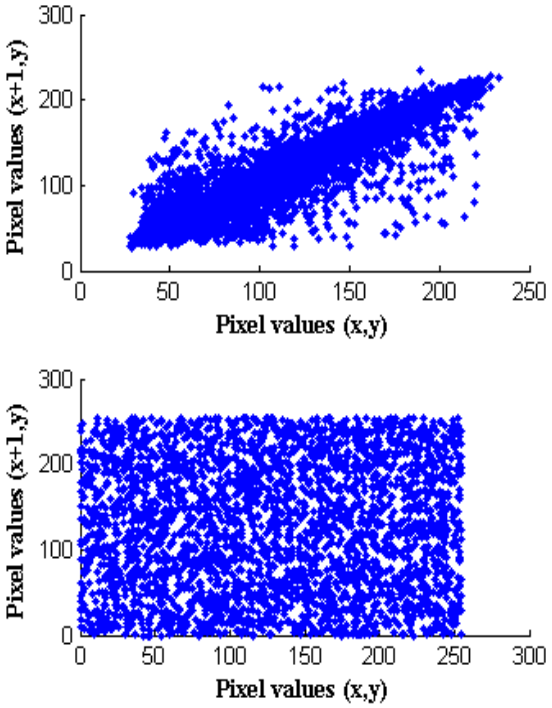

Fig 4: Horizontal Direction Correlation Plot

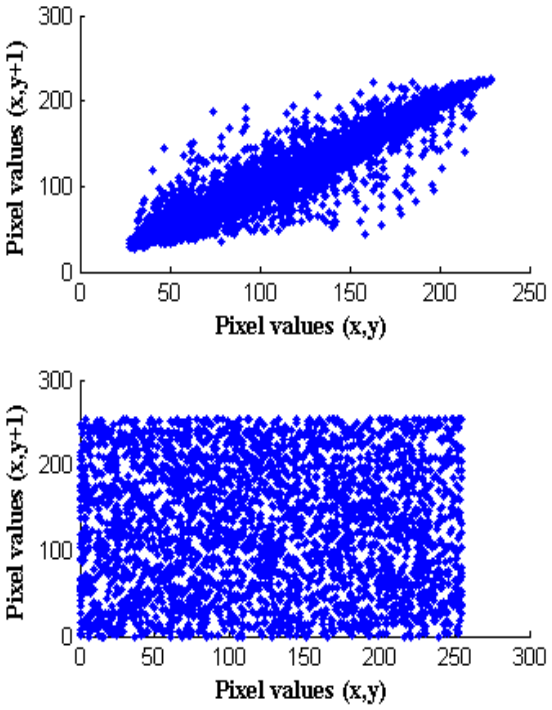

Fig 5: Vertical Direction Correlation Plot

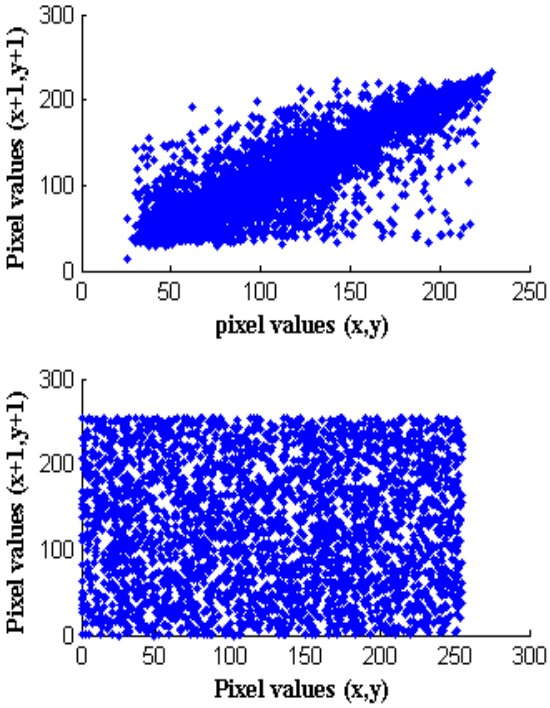

Fig 6: Diagonal Direction Correlation Plot

Table 5. Entropy comparison

Lena Image	Entropy
Wong et al. method	7.9965
Proposed method	7.9972

Table 6. Entropy analysis

Images	Entropy
Lena	7.9972
Baboon	7.9994
House	7.9998
Peppers	7.9978
Camera man	7.9982
Boat	7.9985

4. CONCLUSION

In this paper, permutation process scrambles the image pixels and also parity based simple pixel modification introduced in the permutation stage. This parity based shuffling proves that the encryption algorithm needs only very less number of rounds (Rounds=2) to achieve highly uncorrelated cipher image. Employing different chaotic maps in the encryption algorithm increases the randomness of the cipher image that can be proved by NIST tests. In the diffusion process the random binary values are masked with the permuted image pixel bits. The diffusion bit updation in each round provides different ciphered image for every round of encryption this process can resist the chosen plaintext attack. Mainly, encrypted images of the proposed encryption algorithm are random, non- repeated and unpredictable, even using same set

of keys and the same original image. The algorithm can also withstand various different attacks such as statistical, differential and security. Further extension of this work is introducing compression and employment of multidimensional chaotic maps which give more security. The compression provides small bandwidth for large image data transmission through network.

5. REFERENCES

[1] G. Alvarez, S. Li, "Some basic cryptographic requirements for chaos based cryptosystems", International Journal of Bifurcation and Chaos, vol. 16, pp. 2129–2151, 2006.

[2] R. Matthews, "On the derivation of a chaotic encryption algorithm", Cryptologia, vol. 13, pp. 29–42, 1989.

[3] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps", International Journal of Bifurcation and Chaos, vol. 8, pp. 1259–1284, 1998.

[4] G.R. Chen, Y. B. Mao, C. K. Chui, "Asymmetric image encryption scheme based on 3D chaotic standard maps", Chaos Solitons and Fractals, vol. 21, pp. 749–761, 2004.

[5] Y. B. Mao, G. R. Chen, S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps", International Journal of Bifurcation and Chaos, vol. 14, pp. 3613–3624, 2004.

[6] Z. H. Guan, F. Huang, W Guan, "Chaos based image encryption algorithm", Physics Letters A, vol. 346, pp. 153–157, 2005.

[7] S. Lian, J. Sun, Z. Wang, "A block cipher based on a suitable use of chaotic standard map", Chaos Solitons and Fractals, vol. 26, pp. 117–129, 2005.

[8] K. W. Wong, B. S. H. Kwok, W. S. Law, "A fast image encryption scheme based on chaotic standard map", Physics Letters A, vol. 372, pp. 2645–2652, 2008.

[9] R. Rhouma, E. Solak, S. Belghith, "Cryptanalysis of a new substitution– diffusion based image cipher", Communications in Nonlinear Science and Numerical Simulation, vol. 15, pp. 1887–1892, 2010.

[10] C. Li, S. Li, K. T. Lo, "Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps", Communications in Nonlinear Science and Numerical Simulation, vol. 16, pp. 837–843, 2011.

[11] Ahmed A. Abd El-Latif, Li Li, Ning Wang, Qi Han, Xiamu Niu, "A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces", Signal Processing, vol. 93 pp. 2986–3000, 2013.

[12] The NIST website. http://www.itl.nist.gov/div893/staff/soto/ jshome.html.

[13] Yang Liu, Xiaojun Tong, Shicheng Hu, " A family of new complex number chaotic maps based image encryption algorithm", Signal Processing: Image Communication, vol. 28, pp. 1548-1559, 2013.

[14] Yicong Zhou, Long Bao, C.L. Philip Chen, "Image encryption using a new parametric switching chaotic system", Signal Processing, Vol. 93, pp. 3039-3052, 2013.