Chaotic Image Encryption using Modular Addition and Combinatorial Techniques

Sathishkumar Arthanari[1], Mohamedmoideen Mastan[1] and Boopathy Bagank[2]
[1] Department of Electronics and Communication Engineering,
Sri Venkateswara College of Engineering, India
[2]Department of Electronics, Anna University Chennai, India

Abstract: *The image encryption is widely used to secure transmission of data in an open internet and internet works. For image based cryptosystems chaotic maps can be used as a key because of its nonlinear component. Due to sensitivity to initial conditions, chaotic maps have best alternative for designing dynamic permutation of the image based cryptosystem. A chaotic map is used to generate permutation matrix. An external secret key is used to derive the initial conditions for chaotic map. A pixel shuffling is used to expand diffusion property in the image and dissipate the high correlation among image pixels. The proposed algorithm is basically consisting of a pixel shuffling and modular addition plus permutation, which is a combination of block permutation, pixel permutation and value transformation. In general, diffusion and permutation is performed in a concurrent manner. These two methods are opened and operated alternatively in every round of encryption process at least four such chaotic sub keys are employed in every round of primitive encryption process. Decryption has the same structure, which operates in reverse order. Results of the various types of analysis are encouraging and imply that the proposed approach is able to adeptly trade off between the speed and protection. Hence, it is suitable for the secure transmission of image, video and multi-media in real-time. The proposed algorithm is tested for different types of statistical analysis by examining their autocorrelation, Cross Correlation (CC) performance, measuring the histogram of the cipher image and the bit error probability for the received data in a communication system.*

Keywords: *Image encryption, modular addition, chaotic maps, logistic map, socek, grp, cross, block cipher.*

Received September 5, 2012; accepted January 20, 2013; published online April 23, 2014

1. Introduction

Today, the use of computers and networks has grown tremendously and this growth is unavoidable. However, all computers and networks are being installed, interconnected, to form a global network and internet. In recent years, more and more information has been pumped into wired and wireless transmission media over the internet. The information transferred is not only text but also images, audio and multimedia. Recent years, images have been widely used and this growth is unavoidable. However, the more extensive use of the mages, the more security risk such as eaves-dropping and tampering. It is highly important to protect the military related documents, the most precise data captured by military satellites and the diagrams of bank building. Recently, image security has become a hot topic. Many crypto systems have been proposed in literature and the most common way to protect large multimedia files is by using conventional cryptographic techniques. The software or hardware implementations of popular public key crypto systems, such as RSA or El-Gamal cannot support fast and high speed encryption rates. While security of these algorithms relies on the difficulty of quickly factorizing large numbers or solving the discrete logarithm, these topics are challenged by recent advances in number theory and distributed computing. On the other hand, symmetric key bulk crypto algorithms, such as Triple DES or blowfish are suitable for transmission of large amounts of information or data. However, they are not fast in terms of their execution speed and cannot be clearly explained, so that the detection of flaws and crypt analysis can be easily drawn. In contrast, chaos-based crypto schemes Abir *et al.* [3, 4, 5, 8, 18, 19, 20, 22, 23] are fast and easily realized in both hardware and software, which makes it more suitable for multimedia content rich data encryption.

The two fundamental properties of chaotic systems Parker and Chua [16] are the sensitivity to initial conditions and mixing. Sensitivity to initial conditions means that when a chaotic map is iteratively applied to two initially close points, their iteration quickly diverges and they bear no correlation after a few iterations. Sensitivity to parameters causes the properties of the map to change quickly when the parameters on which the map depends are mildly disturbed. Mixing is the tendency of the system to quickly confuse small portions of the state space into an intricate network, so that two nearby points in the system totally lose the correlation they once shared and get scattered all over the state space. The chaotic behaviour produced by the random property of the nonlinear definite systems, which is a pseudo-random

and looks like random process. In the chaotic maps, the logistic map is a popular and generalizations of the logistic map to generate pseudo-random bits with desired statistical properties to realize secret encryption operations.

The two fundamental properties of chaotic systems [16] are the sensitivity to initial conditions and mixing. Sensitivity to initial conditions means that when a chaotic map is iteratively applied to two initially close points, their iteration quickly diverges and they bear no correlation after few iteration. Sensitivity to parameters causes the properties of the map to change quickly when the parameters on which the map depends are mildly disturbed. Mixing is the tendency of the system to quickly confuse small portions of the state space into an intricate network, so that two nearby points in the system totally lose the correlation they once shared and get scattered all over the state space. The chaotic behaviour produced by the random property of the nonlinear definite systems, which is a pseudo-random and looks like random process. In the chaotic maps, the logistic map is a popular and generalizations of the logistic map to generate pseudo-random bits with desired statistical properties to realize secret encryption operations.

The rest of the paper is organized as follows: The next section gives a brief description the previous work, section 3 discussed chaotic map, section 4 discussed about the proposed encryption and decryption of image. Section 5, we test the new algorithm and show the high level security. Section 6 concludes the paper.

2. Previous Research

2.1. Image Encryption

For still images, the security is often achieved by using the naive approach to completely encrypt the entire image. However, there are number of applications for which naive encryption is not suitable. For example, a limited bandwidth and processing power in small mobile devices calls for different approaches. Each type of data has its own unique features; different approaches should be used to protect confidential still image data from unauthorized attacks. It is well known that images are different from texts in many aspects, such as high redundancy and correlation. However, due to large data size and real time requirement, the techniques that are appropriate for textual data may not be suitable for multimedia data. The major problem in designing an effective image based encryption algorithms is the difficulty of pixel shuffling and diffusing such image data by traditional cryptosystems techniques. In general, the real time images have the value of any given pixel can be reasonably predicted from the values of its neighbours.

2.2. Related Work

The chaotic maps are suitable for image encryption systems, since it has desirable properties of ergodicity, high sensitivity to initial conditions and control parameters. Chaotic image encryption systems have high speed with low cost, which makes them better candidates than many traditional cryptosystem for multimedia data encryption. Many researcher contributed to the growth of image based cryptosystem, basically image encryption is achieved by permutation, diffusion, pixel scrambling and XOR'ing, modulo addition and permutation of selective part of the image.

Xiangdong *et al.* [22] have presented an image scrambling technique based on chaos theory and sorting transformation. Jiankun and Fengling [12] have presented, a pixel-based scrambling approach for digital medical images protection.

Etemadi and Mohammad [8] have presented a permutation-substitution based image encryption using chaotic maps and Tompkins-Paige algorithm. Xiaojun and Minggen [23] have presented an image encryption using compound chaotic sequence cipher shifting dynamically. Shubo *et al.* [20] have presented an improved image encryption technique based on chaotic system. Patidar *et al.* [17] have presented a substitution-diffusion based image encryption using chaotic standard and logistic maps. Abdulkarim *et al.* [2] have presented a Modified Advanced Encryption Standard (MAES) adaptable for image based cryptosystems. Sathishkumar *et al.* [18, 19] have presented image encryption by scrambling approach and diffusion and multiple chaotic maps.

2.3. Limitations of the Existing Work

Many algorithms were proposed to protect confidential information such as data and images but memory space, speed and efficiency plays a crucial role that was not addressed. Also, the image based cryptosystem must satisfy avalanche effect, diffusion effect, randomness and sensitivity issues. Also, the completeness effect and key space analysis are an important parameter for any security algorithms. Most of the algorithm satisfies few parameters and lacks in the other parameter that leads to information leakage. Also, level security plays a vital role that decides how many parameters must be satisfied by the algorithms. Comparing with the previous work our algorithm reduces these problems and the performance is considerably increased.

3. Piecewise Linear Chaotic Map

A Piecewise Linear Chaotic Map (PWLCM) is a map composed of multiple linear segments as given below.

$$X_{(N)} = F\left[X_{(N-1)}\right] = \begin{cases} X_{(N-1)} \times 1/p & \text{if } 0 < X_{(N-1)} < p \\ X_{(N-1-p)} \times 1/(0.5 - p) & \text{if } p < X_{(N-1)} < 0.5 \\ F_{\left[1-X_{(N-1)}\right]} & \text{if } 0.5 < X_{(N-1)} < 1 \end{cases} \quad (1)$$

Where, the positive control parameter and the initial condition are respectively $p \in [0: 0.5]$ and $x(i) \in [0: 1]$. Compared to the Logistic map [16, 21] situation, we have a wider range of control parameter choices when using the PWLCM because the Logistic map is ergodic in (0, 1) only when r approaches 4. The PWLCM has a better balance property and uniform invariant density function. A perturbation algorithm [7] is used to improve the dynamic statistical properties of PWLCM. It can be achieved by expanding the cycle length such that good statistical properties are reached.

3.1. The Proposed Key Generation Method

The key stream is generated using 2 perturbed PWLCM as shown in Figure 1 [3, 5]. The output of a 32 bit LFSR tapped at 10th and 20th bits is XOR'ed with the last 32 bits of the PWLCM at intervals of length Δ. Here, Δ is 16. The perturbation starts from the first iteration. However, in order to remove weak keys the first 140 iterations are not included in the key stream.

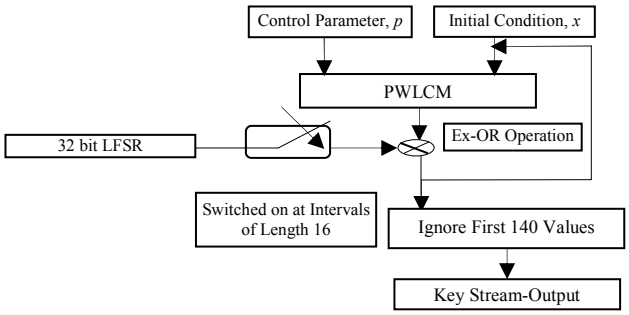


Figure 1. The Proposed perturbed PWLCM as key generation-Keygen (p, x) [3, 5].

4. The Proposed Algorithm

In this paper, we have considered an 8 bit gray scale image of r rows and c columns with p as the total number of pixels as shown in Figure 2. Let $PI(i)$ be the i^{th} pixel's intensity and n be the total number of values PI can have. We use linear indexing of image pixels where, $PI(1, 1)=PI(1)$, $PI(2, 1)=PI(2)$ and so on. Hence, $p=rxc$, $PI \in Z_n\{0, 1, ..., 255\}$ and $i \in U=\{1, 2, ..., P\}$.

PI: Plain Image.
I: Cipher Image.
Block=128 bits (16 pixels); Sub Block=32 bits (4 pixels).

Thus, $K \in V=\{1, 2, ..., 255\}$, $\oplus$ represents bitwise XOR operation. $x \leftarrow y$ means y is assigned to x.

- *Step 1*: Reading of (plain) original image (PI), the plain image is converted to gray scale if it is color image.

$$PI_{256\times256} \leftarrow \{PI_{ij}\} \quad 1 \le i \le H \text{ and } 1 \le j \le W$$

Here, H and W respectively, are height and width of the original image in pixels and resized to 256×256.

- *Step 2*: Divide the image to two sub blocks PI_1 and PI_2 of size 128×128 bit.
- *Step 3*: For each sub-block whitening is performed by XOR'ing with key, $i \leftarrow k$.

$$PI_{1(i:128)} \leftarrow (PI_{1(i:128)} \oplus K_{11})$$

$$PI_{2(i:128)} \leftarrow (PI_{2(i:128)} \oplus K_{22})$$

- *Step 4*: For each sub-block intra block modulo 256 Addition is performed.

$$PI_{1(i:128)} \leftarrow (PI_{1(i:128)} \oplus K_{12})_{mod\ 256}$$

$$PI_{2(i:128)} \leftarrow (PI_{2(i:128)} \oplus K_{22})_{mod\ 256}$$

- *Step 5*: Further each sub block is divided in to four Sub sub blocks of size of 32 bits.

$$PI_{1(i:128)} \rightarrow PI_{11(i:32)}, PI_{12(i:32)}, PI_{13(i:32)}, PI_{14(i:32)}$$

And:

$$PI_{2(i:128)} \text{®} PI_{21(i:32)}, PI_{22(i:32)}, PI_{23(i:32)}, PI_{24(i:32)}$$

- *Step 6*: Here, alternately two key XOR'ing, two permutations scoek and cross [3, 5, 9] method is performed.

$$PI_{11(i:32)} \leftarrow (PI_{11(i:32)} \oplus K_{31})$$

$$PI_{12(i:32)} \leftarrow (PI_{12(i:32)})_{SOCKEPERM}$$

$$PI_{13(i:32)} \leftarrow (PI_{13(i:32)} \oplus K_{32})$$

$$PI_{14(i:32)} \leftarrow (PI_{14(i:32)})_{CROSSPERM}$$

$$PI_{1(i:128)} \rightarrow (PI_{11(i:32)} \mid PI_{12(i:32)} \mid PI_{13(i:32)} \mid PI_{14(i:32)})$$

$$PI_{21(i:32)} \leftarrow (PI_{21(i:32)} \oplus K_{41})$$

$$PI_{22(i:32)} \leftarrow (PI_{22(i:32)})_{SOCKEPERM}$$

$$PI_{23(i:32)} \leftarrow (PI_{23(i:32)} \oplus K_{42})$$

$$PI_{24(i:32)} \leftarrow (PI_{24(i:32)})_{CROSSPERM}$$

$$PI_{2(i:128)} \rightarrow (PI_{21(i:32)} \mid PI_{22(i:32)} \mid PI_{23(i:32)} \mid PI_{24(i:32)})$$

- *Step 7*: Intra blocks are XOR'ed on all sub sub blocks. This creates a good diffusion effect.

$$PI_{2(i:128)} \rightarrow (PI_{21(i:32)} \oplus PI_{22(i:32)} \oplus PI_{23(i:32)} \oplus PI_{24(i:32)} .. PI_{n(i:32)})$$

- *Step 8*: Again divide the intermediate image to two sub blocks of size 128 bit.

$$CI_{b(i:256)} \leftarrow CI_{b1(i:128)}, CI_{b2(i:128)}$$

- *Step 9*: For each sub block whitening is performed by XOR'ing with key.

$$CI_{b1(i:128)} \leftarrow (CI_{b1(i:128)} \oplus K_5)$$

- *Step 10*: For each sub block intra block modulo 256 Additions is performed.

$$CI_{b1(i:128)} \leftarrow (CI_{b1(i:128)} + K_6)_{\text{mod}\,256}$$

- *Step 11*: Further each sub block is divided in to four sub sub blocks of size of 32 bit.

$$CI_{b1(i:128)} \rightarrow CI_{b11(i:32)}, CI_{b12(i:32)}, CI_{b13(i:32)}, CI_{b14(i:32)}$$

And:

$$CI_{b2(i:128)} \rightarrow CI_{b21(i:32)}, CI_{b22(i:32)}, CI_{b23(i:32)}, CI_{b24(i:32)}$$

- *Step 12*: Here, alternately four key xor'ing, two permutations *scoek* and *grp* [3, 5, 9] method is performed.

$$CI_{b11(i:32)} \leftarrow (CI_{b11(i:32)} \oplus K_{71})$$

$$CI_{b12(i:32)} \leftarrow (CI_{b12(i:32)})_{SOCKPERM}$$

$$CI_{b13(i:32)} \leftarrow (CI_{b13(i:32)} \oplus K_{72})$$

$$CI_{b14(i:32)} \leftarrow (CI_{b14(i:32)})_{GRPpermu}$$

$$CI_{b21(i:32)} \leftarrow (CI_{b21(i:32)} \oplus K_{91})$$

$$CI_{b22(i:32)} \leftarrow (CI_{b22(i:32)})_{SOCKPERM}$$

$$CI_{b23(i:32)} \leftarrow (CI_{b23(i:32)} \oplus K_{92})$$

$$CI_{b24(i:32)} \leftarrow (CI_{b24(i:32)})_{GRPpermu}$$

- *Step 13*: After step 12, four such sub sub blocks of size 32 bits are combined to form cipher 1, similarly other four sub sub blocks of size 32×32 bits are combined to form cipher 2.

$$CI_{b1(i:128)} \leftarrow CI_{b11(i:32)} \,|\, CI_{b12(i:32)} \,|\, CI_{b13(i:32)} \,|\, CI_{b14(i:32)}$$

And:

$$CI_{b2(i:128)} \leftarrow CI_{b21(i:32)} \,|\, CI_{b22(i:32)} \,|\, CI_{b23(i:32)} \,|\, CI_{b24(i:32)}$$

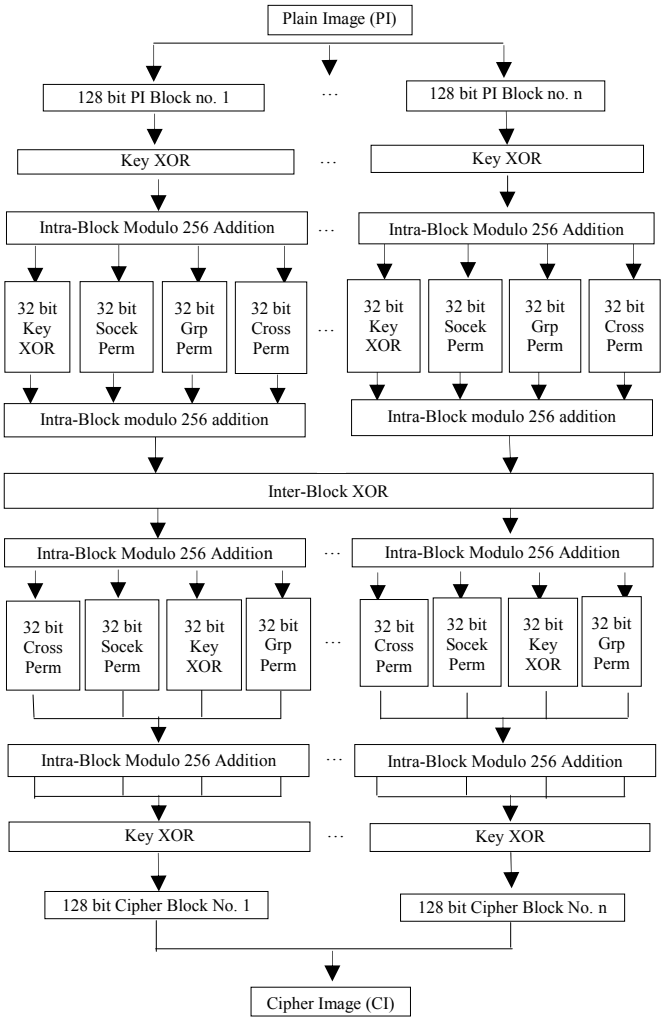


Figure 2. The Proposed model.

- *Step 14*: Finally, ciphers 1 and 2 are concatenated to form a cipher image.

$$CI_{(i:256)} \leftarrow CI_{b1(i:128)} \,||\, CI_{b2(i:128)}$$

- *Step 15*: $i \leftarrow i+1$ Repeat Step 2 to step 13 *r-1* times.

5. Statistical Analysis

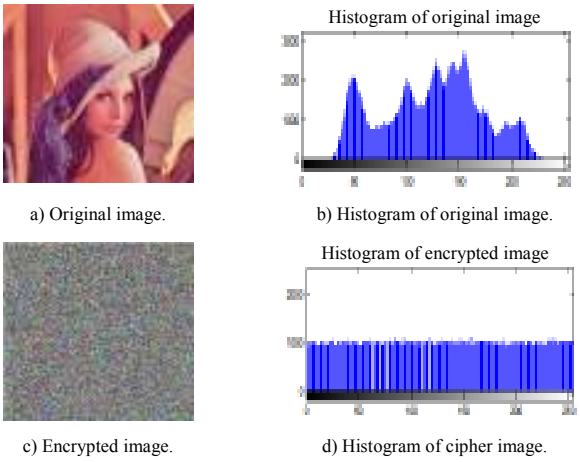
Factors to measure quality of image encryption:

5.1. Histograms Analysis

To prevent the leakage of information to an opponent, it is also advantageous that if the cipher image bears no statistical similarity of the plain image. An image histogram [2, 4, 5, 6, 8, 17, 18, 19, 22, 24] illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level.

We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. One typical example among them is shown in Figure 3-b. The histogram of a plain image contains large spikes. These spikes correspond to gray values that appear more often in the plain image. The histogram of the cipher image as shown in Figure 3-d, is uniform, significantly different from that of the original image, and bears no statistical resemblance of the plain image.

It is clear that the histogram of the encrypted image gives no information about the original image hence, it does not provide any clue to employ any statistical attack on the proposed image encryption algorithm.



a) Original image. b) Histogram of original image.

c) Encrypted image. d) Histogram of cipher image.

Figure 3. Histogram analysis of LENA image.

Key x_0=0.7239, y_0=0.5672 used throughout this paper α=0.35899926, β=0.25899926. The same key used in [3, 5]. For comparison we have considered the CBC mode of CBCSTI-A since, it is most secure.

5.2. Correlation Co-Efficient Analysis

For a plain image having definite visual scene, each pixel is highly correlated with its adjacent pixels either in horizontal, vertical direction and diagonal direction. In ideal case an image encryption scheme should

produce a cipher image with no such correlation in the adjacent pixels. In Table 1 shows that, we have given the horizontal, vertical and diagonal correlations of the adjacent pixels in cipher images [1, 2, 3, 4, 5, 6, 8, 11, 12, 15, 17, 18, 19, 20, 21, 22, 23, 24]. In Table 2 [4], we have given the mean intra-component correlation coefficients of various channels of color images. In Table 3, we have given the mean intra-component correlation coefficients of original and color images. It is clear that the two adjacent pixels in the original image are highly correlated, but there is negligible correlation between the two adjacent pixels in the encrypted image. For this purpose, we use the following formula:

$$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \quad (2)$$

$$r_{xy} = \frac{Cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (3)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \quad (4)$$

N.R=Not Reported.
CC=Cross Correlation. R=Red component. G=Green component. B=Blue component.

Table 1. Mean* absolute values** of the correlation coefficients of adjacent pixels.

Image	Lena			Mandrill		
Resolution	512×512	512×512×3		512×512	512×512×3	
Technique	CBCSTI-A in [3]	[5]	Proposed	CBCSTI-A in [3]	[5]	Proposed
Horizontal Correlation	0.0127	0.0377	0.0029	0.0092**	0.0282	0.0026
Vertical Correlation	0.0093	0.0107	0.0044	0.0096	0.0022	0.002
Diagonal Correlation	0.0059**	0.0119	0.0047	0.0083**	0.0193	0.0013

Table 2. Mean intra-component correlation coefficients.

Image	Lena			Mandrill		
Resolution	512×512×3					
Technique	CBCSTI-A in [3]	[5]	Proposed	CBCSTI-A in [3]	[5]	Proposed
Red (R)	N.R.	0.0035	0.0054	N.R.	0.0155	0.0024
Green (G)	N.R.	0.0025	0.0024	N.R.	0.0055	0.0014
Blue (B)	N.R.	0.0046	0.0042	N.R.	0.0138	0.002

Table 3. Inter-components correlation coefficients of original and permuted images.

Image	Lena			Mandrill		
Resolution	512×512×3					
Technique	CBCSTI-A in [3]	[5]	Proposed	CBCSTI-A in [3]	[5]	Proposed
CC_{RG}	N.R.	0.00615	-0.0015	N.R.	0.0703	0.0017
CC_{GB}	N.R.	0.0381	-0.0012	N.R.	0.0591	0.00017
CC_{BR}	N.R.	0.0120	0.0025	N.R.	0.0088	0.00084

5.3. Information Entropy

The Entropy is defined as follows [15]:

$$H_e = -\sum_{k=0}^{G-1} P(k) \times l \quad (5)$$

G: *Gray level of input image* (*0*, *…*, *255*).
P(*k*): *Is the probability of the occurrence of symbol k.*

In Table 4 compares CC and Entropy for various images, it shows that the proposed model is highly secure.

Table 4. Entropy of the original images and their encrypted forms.

Image	Original	Encrypted by CBCSTI-A in [3]	Encrypted by [5]	Encrypted by Proposed Algorithm
Lena (512×512×3)	7.7502	N.R.	N.R.	7.9998
Mandrill (512×512×3)	7.7624	7.9999	≈7.9993	7.9998
Lena (512×512)	7.4456	N.R.	N.R.	7.9998
Mandrill (512×512)	7.3579	N.R.	N.R.	7.9993

5.4. Differential Cryptanalysis

In general, a desirable property for an encrypted image is being sensitive to the small changes in plain-image (e.g., modifying only one pixel). Opponent can create a small change in the input image to observe changes in the result. By this method, the meaningful relationship between original image and encrypted image can be found. If one small change in the plain-image can cause a significant change in the cipher-image, with respect to diffusion and confusion, then the differential attack actually loses its efficiency and becomes practically useless. Three common measures were used for differential analysis: NPCR and Unified Average Changing Intensity (UACI) [17]. NPCR means the number of pixels change rate of ciphered image while one pixel of plain-image is changed. UACI which is the unified average changing intensity, measures the average intensity of the differences between the plain-image and ciphered image.

The larger NPCR is the higher sensitivity in the plain image has and the more difficult the system's security against differential attack. Let two ciphered images, whose corresponding plain images have only one pixel difference; be denoted by *CI1* and *CI2*. *Label* the grayscale values of the pixels at *grid* (*i, j*) in *CI1* and *CI2* by *CI*(*i, j*) and *CI*(*i, j*), respectively. Define a bipolar array *D*, with the same size as images *CI1* and *CI2*. Then, *Diff*(*i, j*) is determined by *CI1*(*i, j*) and *CI2*(*i, j*), namely, if *CI1*(*i, j*)=*CI2*(*i, j*) then *Diff*(*i, j*)=*1*; otherwise, *Diff*(*i, j*)=*0*. The NPCR [11, 17, 20, 23] is defined as:

$$NPCR = \frac{\sum_{i,k} Diff(i, j)}{W \times H} \times 100\% \quad (6)$$

UACI means changing intensity of the corresponding pixels of the plain image and cipher image. The larger the UACI is the more resistant to the differential attack the encryption scheme. The UACI [17] is defined by:

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j}\frac{CI_1(i, j) - CI_2(i, j)}{255} \times 100\%\right] \quad (7)$$

In Table 5 shows that CC, NPCR and UACI between the original image lena and mandrill and cipher image.

Table 5. Mean of parameters to quantitatively measure encryption.

Parameter	Cross-Correlation			NPCR(%)			UACI(%)		
Technique	**[3]**	**[5]**	**Proposed**	**[3]**	**[5]**	**Proposed**	**[3]**	**[5]**	**Proposed**
Lena (512×512×3)	0.0014	-0.0022	0.0014	99.62	99.6246	99.6029	30.42	29.9932	30.4909
Mandrill (512×512×3)	0.0019	-0.0028	0.0022	99.61	99.6235	99.6043	29.94	33.0823	29.9407

5.5. Sensitivity Test Results

The image encryption scheme has to be more secure and key sensitive [6, 11, 17], means that a small tiny changes in the key leads to significant change in the cipher. To determine the key sensitive the following key values are used. Key used in this paper is x_0=0.7239, y_0=0.5672, α=0.35899926, β=0.25899926 Alpha changed to 0.35899926000001, the 10^{-15th} of the key value is changed. (In [3] 10^{-8th} of the key has been changed) and NPCR, UACI and CC are tabulated in Table 6 and the results shows that our proposed algorithm is highly sensitive to key.

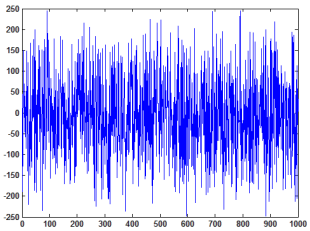
Also, the plain text sensitivity is measured by taking two plain images with one bit difference. The results show that our proposed algorithm is secure against differential and plain text attack.

Table 6. Sensitive analysis.

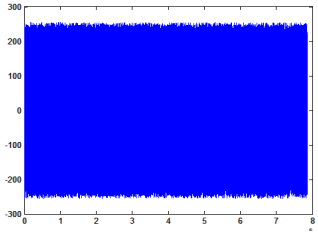
Parameter	Cross-correlation			NPCR (%)			UACI (%)		
Technique	**CBCSTI-A in [3]**	**[5]**	**Proposed**	**CBCSTI-A in [3]**	**[5]**	**Proposed**	**CBCSTI-A in [3]**	**[5]**	**Proposed**
Key sensitivity	N.R.	0.0029	0.0023	71	99.6128	99.611	24	33.4420	33.4687
Plaintext sensitivity	N.R.	N.R.	0.036	100	78	99.2055	27	N.R.	30.5843

5.6. Key Space Analysis

Each PWLCM employs a 53 bit control parameter $p \in [0: 0.5]$, a 53 bit initial condition and $x_i \in [0: 1]$ and a 32 bit LFSR without the seed as zero. Moreover, 2 PWLCMs are used as shown in Figure 4. Hence, the key space is $[(2^{53}/2)\times 2^{53}\times (2^{32}\text{-}1)]^2 \approx 2^{274}$.



a) Plot of difference between first 1000 pixels and all pixels of images ciphered by two adjacent keys.



b) Second image may conceal any regularity in the pattern hence the first image is essential to show the irregularity.

Figure 4. Histogram of cipher image.

5.7. Statistical NIST Test Suite

Among the numerous tests for measuring pseudo-randomness, best way to measure the randomness of the produced sequence by NIST test suite. To validate our results we have tested 100 encrypted images of size 512×512. In Table 7 shows the comparative results of the proposed technique and [5] for a number of tests. Note that the cipher images generated with randomly selected PWLCM secret keys.

Table 7. Nist test suite for 100 cipher images.

Statistical Test	[5]	Proposed technique
Run Test	97	97
Serial Test	98	97
DFT Test	97	97
Frequency Test	100	100
Block Frequency Test	97	96
Longest Run Test	98	94
Rank Test	98	98
Cumulative Sum	100	100
Approximate Entropy	98	94
Universal	97	97
Linear Complexity	100	100
Template Test	98	98

5.8. Error Propagation

In general when information is transmitted [3] over a channel, definitely there is a noise and channel interference that deteriorates reconstruction of information. The error in the transmission will be propagated to the receiver. If the cipher has small error then it will be propagated to the plain image while decrypting the cipher image Table 8.

*1 corrupted block in transmitted image leads to maximum of 3 corrupted blocks in decrypted image.

1. Error in 1st block leads to error in 1st and 2nd block.
2. Error in last block leads to error in last and penultimate block.
3. Error in n^{th} block leads to error in $n\text{-}1^{th}$, n and $n+1^{th}$ blocks.

Table 8. Error propagation.

No. of Erroneous Blocks in Received Encrypted Image	No. of Erroneous Blocks in Decrypted Image		
	CBC Mode of CBCSTI-A [3]	**CBC Mod in [5]**	**Proposed**
1	2	2	3*

5.9. Speed Performance Evaluation and PSNR

Apart from the security consideration, running time and speed [3, 5, 17] is also an important issue on image encryption. We have implemented the technique in MATLAB 7.6 using a PC equipped with 2.2 GHz Pentium IV with 4 GB of RAM running Windows XP.

Table 9 shows the performance evaluation of the proposed scheme. The analysis has been done on an 8 bit image of dimension 512×512×3.

Table 9. Comparison of performance analysis results.

Technique	Time Taken For Encryption In Seconds
CBCSTI-A in [3] in CBC mode	545
[5]	N.R.
Proposed	45

PSNR [14] of encrypted image and original image is computed. We can see that the higher the visual quality of the encrypted image is the less the number of changed pixels will be and the larger the value of PSNR will be and the time cost will be less too. The proposed method gives typical values of 9.25 DB.

6. Conclusions and Future Work

The security of an image data is different from that of a text file. Because of its intrinsic characteristics, the encryption speed and algorithm simplicity are usually considered to be more important than the absolute security. Chaos theory has already proved that it is an excellent alternative to provide a fast, simple, and reliable image encryption scheme and has a high degree of security. In this paper, an image encryption scheme is proposed based on combined diffusion and permutation technique using two chaotic maps have been described. The system is block cipher based architecture and its effectiveness is tested in MATLAB 7.6 version. A detailed statistical analysis is given above and the experimental results shows, that it outperforms the existing techniques, both in terms of speed and security. From an engineer's perspective, chaos-based image encryption technology is very promising for real-time security of a still image and video communications in military, industrial and commercial applications. In future, the proposed method can be tested in real-time applications like wireless communication, Ad-Hoc networks.

References

[1] Abdelfatah Y. and Ayman A., "A Shuffle Image-Encryption Algorithm," *the Journal of Computer Science*, vol. 4, no. 12, pp. 999-1002, 2008.

[2] Abdulkarim S., Bahaa Eldin H., and Abd El Fatah H., "An Efficient Modified Advanced Encryption Standard Adapted for Image Cryptosystems," *the International Journal of Computer Science and Network Security*, vol. 10, no. 2, pp. 226-232, 2010.

[3] Abir A. and Abdelhakim S., "New Chaotic Permutation Methods for Image Encryption," *the International Journal of Computer Science*, vol. 37, no. 4, pp. 9, 2010.

[4] Abir A. and Dounia A., "Efficient Image Chaotic Encryption Algorithm with No Propagation Error," *ETRI Journal*, vol. 32, no. 5, pp. 774-783, 2010.

[5] Abir A., "A New Chaos-Based Cryptosystem for Secure Transmitted Images," *IEEE Transaction on Computers*, vol. 1, no. 3, pp. 252-262, 2011.

[6] Ahmed H., Kalash M., and Farag Allah S., "An Efficient Chaos-Based Feedback Stream Cipher for Image Encryption and Decryption," *the International Journal Informatica*, vol. 31, no. 1, pp.121-129, 2007.

[7] Chen G., Mou X., and Li S., "On the Dynamical Degradation of Digital Piecewise Linear Chaotic Maps," *the International Journal of Bifurcation and Chaos*, vol. 15, no. 10, pp. 3119-3151, 2005.

[8] Etemadi S. and Mohammad E., "Chaotic Image Encryption Design using Tompkins-Paige Algorithm," *the Hindawi Journal of Mathematical Problems in Engineering*, vol. 2009, pp. 1-22, 2009.

[9] Furht B., Muharemagic E., and Socek D., "Enhanced 1-D Chaotic Key-Based Algorithm for Image Encryption," *in Proceedings of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks*, Athens, Greece, pp. 406-407, 2005.

[10] Hilewitz Y., Shi J., and Lee B., "Comparing Fast Implementations of Bit Permutation Instructions," *in Proceeding of the 38th Asilomar Conference on Signals, Systems and Computers*, California, USA, pp. 1856-1863, 2004.

[11] Ismail A., Mohammed A., and Hossam D., "An Efficient Image Encryption Scheme Based Chaotic Logistic Map," *the International Journal of Soft Computing*, vol. 2, no. 2, pp. 285-291, 2007.

[12] Jiankun H. and Fengling H., "A Pixel-Based Scrambling Scheme for Digital Medical Images Protection," *the Elsevier Journal of Network and Computer Applications*, vol. 32, no. 4, pp. 788-794, 2009.

[13] Lee B., Shi J., and Yang X., "Efficient Permutation Instructions for Fast Software Cryptography," *the IEEE Micro*, vol. 21, no. 6, pp. 56- 69, 2001.

[14] Lip P., Delina B., Tan A., and Sim O., "An Enhanced Mechanism for Image Steganography using Sequential Colour Cycle Algorithm," *the International Arab Journal of Information Technology*, vol. 10, no. 1, pp. 51-60, 2013.

[15] Mohammad Y. and Jantan A., "Image Encryption using Block-Based Transformation Algorithm," *the International Journal of Computer Science*, vol. 35, no. 1, pp. 15-23, 2003.

[16] Parker S. and Chua O., "Chaos: A Tutorial for Engineers," *in Proceedings of the IEEE*, Washington, USA, pp. 982-1008, 1995.

[17] Patidar V., Pareek K., and Sud K., "A New Substitution-Diffusion Based Image Cipher using Chaotic Standard and Logistic Maps," *the Elsevier Communications in Nonlinear Science and Numerical Simulations*, vol. 14, no. 7, pp. 3056-3075, 2009.

[18] Sathishkumar A., Bhoopathy K., and Sriraam N., "Image Encryption Based on Diffusion and Multiple Chaotic Maps," *the International*

Journal of Network Security and Its Applications, vol. 3, no. 2, pp. 181-194, 2011.

[19] Sathishkumar A., Bhoopathy K., and Vivekanand V., "A Novel Algorithm for Image Encryption by Integrated Pixel Scrambling Plus Diffusion Utilizing Duo Chaos Mapping Applicability in Wireless Systems," *the Elsevier Journal of Proceedia of Computer Science*, vol. 3, pp. 378-387, 2011.

[20] Shubo L., Jing S., and Zhengquan X., "An Improved Image Encryption Algorithm Based on Chaotic System," *the Journal of Computers*, vol. 4, no. 11, pp. 1091-1100, 2009.

[21] Wu W. and Rulkov F., "Studying Chaos Via 1-D Maps-A Tutorial," *the IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications Journal*, vol. 40, no. 10, pp. 707-721, 1993.

[22] Xiangdong L., Junxing Z., Jinhai Z., and Xiqin H., "Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation" *the International Journal of Computer Science and Network Security*, vol. 8, no. 1, pp. 64-68, 2008.

[23] Xiaojun T. and Minggen C., "Image Encryption with Compound Chaotic Sequence Cipher Shifting Dynamically," *Elsevier Image and Vision Computing*, vol. 26, no. 6, pp. 843-850, 2008.

[24] Zhang Y., Wang Y., and Shen X., "A Chaos-Based Image Encryption Algorithm using Alternate Structure," *Springer-Verlag, Science in China Series F: Information Sciences*, vol. 50, no. 3, pp. 334-341, 2007.

Sathishkumar Arthanari received his PhD degree from Anna University, Chennai and ME degree from PSG College of Technology, India. He is a faculty member in the Department of Electronics and Communication Engineering, Sri Venakesateswara College of Engineering, Sriperumbudur. His research areas include network security, VLSI and signal processing algorithms.

Mohamedmoideen Mastan graduated from Crescent Engineering College, India. He received his ME degree. Communication systems from Sri Venkateswara College of Engineering, India.

Bhoopathy Bagank completed his doctoral degree from IIT Madras. He is presently working as Professor, ECE Department in Anna University, MIT Chrompet campus, Chennai. His areas of interest include signal processing, image processing and network security.