A Novel Image Encryption Algorithm Using Pixel Shuffling and BASE 64 Encoding Based Chaotic Block Cipher (IMPSBEC)

G.A.SATHISHKUMAR and Dr.K.BHOOPATHY BAGAN
Department of ECE ,Department of Electronics
Sri Venkateswara College of Engineering ,MIT, Anna University Campus, Chrompet
Sriperumbudur,Tamil nadu, Chennai, Tamil Nadu
INDIA
sathish@svce.ac.in ,kbhoopathy02@yahoomail.com , http://www.svce.ac.in/~sathish

Abstract: - The image encryption is widely used to secure transmission of data in an open internet and internet works. Each type of data has its own unique features; therefore different data requires a different type of encryption algorithm. Most of the present day techniques are suitable for textual data and they are not suitable for multi- media content rich data such as images. Combined with nonlinear dynamic (chaotic) maps, a new algorithm is developed and applied to image based cryptosystems. In this proposed algorithm, we propose a pixel shuffling, base 64 encoding based algorithm, which is a combination of block permutation, pixel permutation and value transformation. In general, diffusion and permutation is performed in an iterative fashion. 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. The statistical analysis shows that the proposed algorithm has good immunity to various attacks and it is suitable for various software and hardware applications. A new approach is proposed to generate a random-bit sequence with a high degree of randomness. The proposed algorithm is a better alternative to satisfy the need for information security services. The performance analysis of the proposed new approach is tested for randomness by carrying out various testing rules and statistical test. Results of the various types of analysis are encouraging and imply that the proposed approach is very successfully able to adeptly trade offs between the speed and protection. Hence it is suitable for the real-time transmission of image and wireless communication applications.

Key-Words Image encryption, Base 64 encoding, chaotic maps, logistic map and block cipher

1 Introduction

Currently, 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 days more and more information has been pumped into wired and wireless media over the internet. The information transferred is not only text, but also multimedia, audio, video and other images. Today, images have been widely used and this growth is unabated. However, the more extensively we use the images, the more risk in security vulnerabilities, eaves dropping, and tampering. It is very essential to protect the military related documents, the diagrams of bank building, and the most precise data captured by military satellites. Recently, image security has become a hot topic. Many crypto system and encryption/decryption techniques have been proposed in literature, and the most common way to protect large multimedia files is by using conventional classical 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 [1-8] are fast and easily realized in both hardware and software, which makes it more suitable for multi media content rich data encryption.

The two fundamental properties of chaotic systems [9] 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 pseudorandom 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 about the chaotic map, Section 3 discussed about the proposed encryption and decryption of image. Section 4, we test the new algorithm and show the high level security. Section 5 is a conclusion.

2. CHAOTIC MAPS

Chaos is a definite pseudo-random [9-10] process produced in nonlinear dynamical systems. It is non-periodic, non convergent and extremely sensitive to the initial condition. In general, the chaotic system model is given as

$$x(n) = f(x(n-1)) \qquad (2.1)$$

$$x_{n+1} = \mu x_n (1 - x_n) - - - - (2.2)$$

Where $x(n)$ is a chaotic sequence generated by the nonlinear map $f(.)$, $x(0)$ is the initial condition. Where $x \in (0,1)$. The research result shows that the system is in chaos under the condition that 3.569 >X<4

In order to keep its chaotic property, we present a new algorithm to rearrange the image position. The new algorithm can facilitates the choice of chaotic systems and reduces the time complexity of traversing the images scrambling quantified by chaos. Because of the strong irregularity of the new algorithm, the encrypted image possesses high-level security. In section 3, we will describe the image encryption algorithm in detail.

3. THE PROPOSED METHOD

3.1. Key stream generator

Generate a random sequence from the logistic map with secret key

$$x_{n+1} = \mu x_n (1 - x_n) - - - - - 3.1$$

For $x_n \in (0,1)$ and $\mu(3.9876543210001,4)$, μ and x_n are the system control parameter and initial condition. A secret key value is x_0 its typical value is 0.9876543219991.Depending on the value of μ, the dynamics of the system can change dramatically. The choice of μ in the equation above guarantees the system is in chaotic state and output chaotic sequences x_n have perfect randomness [21, 22].Then the value generated by both the chaotic maps are converted it in to decimal.

Key Generation: Initially 2x 256 bit keys are generated for each round; each key is circular shifted by 6 times. The key1 & key2 are splitted into 4 parts (k11,k12, k21, k22) and (k31,k32, k41, k42) each of 64 bits.

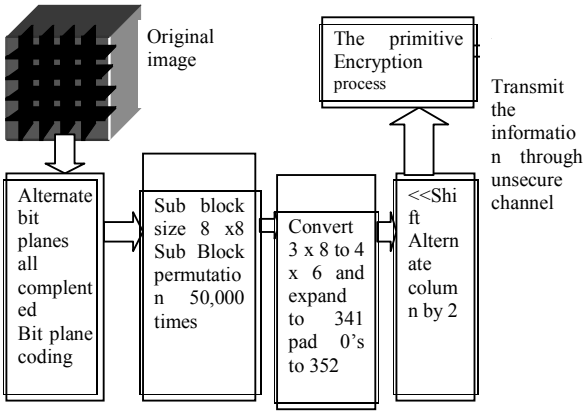


Figure.1: The Proposed Encryption model

3.2. The proposed Algorithm

Strep1: First the image is divided to blocks and they pass through bit plane coding.

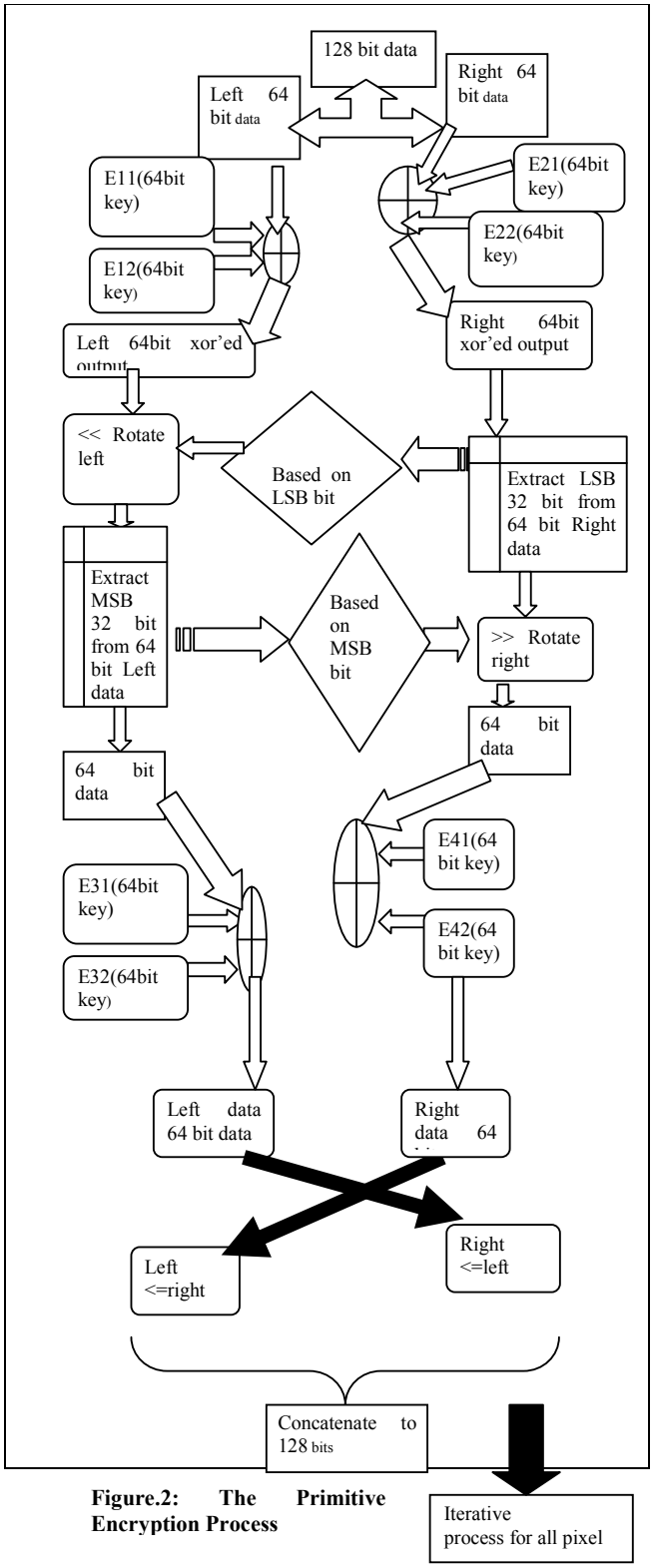


Figure.2: The Primitive Encryption Process

Alternate bit planes are complemented amongst adjacent pixels xor'ed to reduce the correlation of the cipher image.

Step2: In each block select three pixels (size 3x8= 24 bits), which are combined and split into four pixel values (4x6 =24bits) resulting in extra no. of column's, this will change the image size which makes it difficult to identify the original image.
Step3: Alternate columns are shifted left by two bits, when combined into four values each pixel will be a 6 bit data, i.e. '00' followed by 6 bits of data.
Step4: This is followed by the primitive encryption algorithm. This algorithm is iterated for 5 rounds.

3.2.1. The primitive encryption process

Step1: First 128 bit pixel information is divided in to 2 x 64 bit pixel information.

$$IM[1.....128] = R[1\ldots64]L[1....64]$$

Step 2: $L_k[1\ldots64] = L[1....64] \oplus E_{11} \oplus E_{12}$

Step 3: $R_k[1\ldots64] = R[1....64] \oplus E_{21} \oplus E_{22}$

Step 5: If ($R_{[lsb]} = Extract(R_k 1...64])$

$L_{k1}[1\ldots64] = <<< L[1....64]$

Step 6: $L_{k2}[1\ldots64] = L_{k1}[1....64] \oplus E_{31} \oplus E_{32}$

Step 7: If ($L_{[lsb]} = Extract(L_k 1...64])$

Step 8: $R_{k1}[1\ldots64] = <<< R[1....64]$

Step 9: $R_{k2}[1\ldots64] = R_{k1}[1....64] \oplus E_{41} \oplus E_{42}$

Step 10: $R_{k2}[1\ldots64] = L_{k2}[1....64]$

Step 11: $L_{k2}[1\ldots64] = R_{k2}[1....64]$

Step 12: $\mathrm{IM}[1.....128] = R_{k2}[1\ldots64] || L_{k2}[1....64]$

Step 13: Iteratively repeat step 1to 12.

4. Experimental Results

4.1. Histogram analysis

To prevent the leakage of information to an opponent, it is also advantageous if the cipher image bears little or no statistical similarity to the plain image. An image histogram [11],[12],[13] and [14] illustrates how pixels in an image are distributed by graphing the number of pixels at each color intensity level.

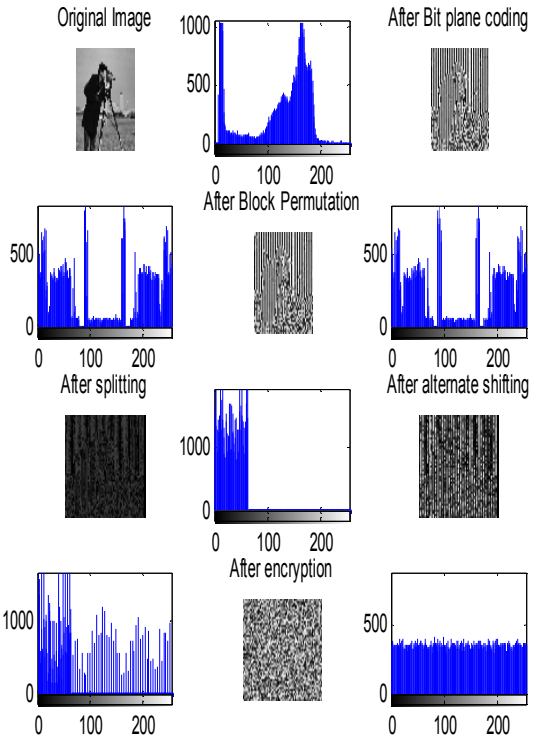


Figure 3 Plain image, Histogram of plain and Cipher image

We have calculated and analyzed the histograms of the several encrypted images as well as its original images that have widely different content. The histogram of a plain image contains large spikes (see Fig.3). These spikes correspond to gray values that appear more often in the plain image. The histogram of the cipher image (see Figure.4.b), is uniform, significantly different from that of the original image, and bears no statistical resemblance to the plain image. It is clear that the histogram of the encrypted image is fairly uniform and significantly different from the respective histograms of the original image and hence does not provide any clue to employ any statistical attack on the proposed image encryption procedure.

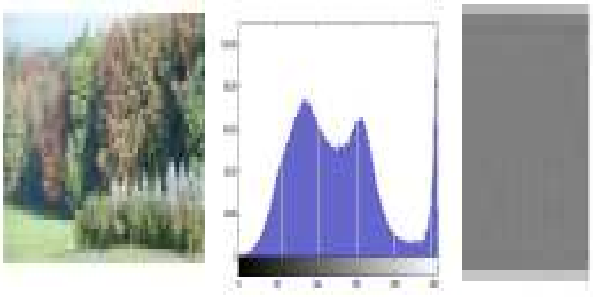
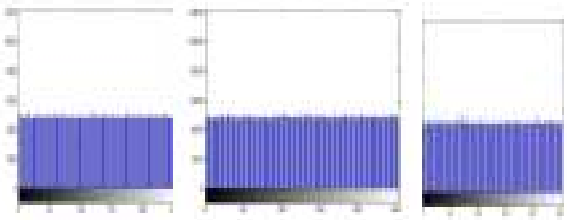


Fig. 4 a) Swiss lake image and histogram of plain image



b)Cipher image and histogram of cipher image(Red, Green and Blue channel)

4.2. 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 I, show that, we have given the horizontal, vertical and diagonal correlations of adjacent pixels in the cipher images [11-17]. In Table 3 [15], we have given the correlation coefficients for the original and encrypted 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:

$$\mathrm{cov}(x, y) = E(x - E(x))(y - E(y)) - -4.2.1$$

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} - - - 4.2.2$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 - - - - 4.2.3$$

Table 1.Correlation of cipher image

Image	Out of 10 runs for each image			
	Over all Correlation	Vertical Correlation	Horizontal Correlation	Diagonal Correlation
cameraman	-1.05E-06	0.0054	-0.010385649	0.010321951
peppers	-0.000193991	0.0083	0.000429663	0.003964922
man	1.57E-05	0.0034	0.00176834	0.011426897
john hall mri	-0.001040605	-0.012695568	-0.004890521	0.001779142
lena	-0.000145044	0.006232844	-0.002818791	0.005763352
barbara	-0.000255068	0.007051571	0.002490855	0.012825531
goldhill	-0.000850963	0.009	-0.005313267	0.013333272
ship	-7.20E-05	0.0047	0.003430977	0.007672764
crowd	-0.000191431	0.0043	0.004014324	0.003002649
Penguin	5.02E-05	0.0061	0.004934336	0.014064123

Table 2.Corrleation of ten images with various channels

Color Image		Cbr		cbg		cbb	
	Size	Min	Mean	Min	Mean	Min	Mean
Car	340*640	0.0015	0.0195	0.012	0.011	0.004	0.00214
aegerilake swiss	778*1199	2.24E-04	-1.78E-04	1.11E-05	-4.55E-04	3.44E-07	-2.89E-05
flowers-image-small	100*150	3.08E-04	-7.30E-04	3.94E-05	-1.98E-04	1.92E-04	4.43E-04
forest_wood	778*1199	6.58E-04	-2.84E-04	1.38E-04	0.002	3.92E-04	1.61E-04
fruits picture	742*1160	8.62E-05	-3.22E-04	2.85E-04	-4.45E-04	1.78E-04	-2.23E-04

Table 3 Correlation of the Cipher Image for encryption quality [15]

S. No	Image	AES[18]	Ismail' etal	Gun etal	Chen etal	Proposed method (IMPSBEC)
1	Lena	0.002904848	-0.0001046	0.0090000	0.0089000	-0.000145044
2	Ship	0.004904848	0.0000425	0.0042000	0.0022000	-7.20E-05
3	Penguin	0.009904848	0.0005917	0.0114000	0.0100000	5.02E-05

4.3. Entropy

The Entropy is defined as follows [18]

$$H_e = -\sum_{k=0}^{G-1} P(k)\log_2(P(k)) \qquad 4.3.1$$

G : gray level of input image (0…255);

P(k):is the probability of the occurrence of symbol k.

In Figure 6, compares Entropy after encryption and before encryption for various images, it shows that the proposed model is highly secured.

Table 4.Entropy of Plain image before and after encryption

Image	Size	Entropy	
		Before	After
car	340*640	6.7401	7.8101
aegeri lake swiss	778*1199	7.7412	8.00E+00
flowers-image-small	100*150	7.6519	8.00E+00
forest_wood	778*1199	7.8075	7.9999
fruits picture	742*1160	7.4004	7.9999

4.4. Sensitivity analysis

The influence of one-pixel change on the Plain image, encrypted by the proposed method [19] is measured using Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) parameters. For the proposed (IMPSBEC), the typical values of NPCR is 99.92% and typical value of UACI is 12-20%

Table 5.Sensitive Analysis of cipher image

Image	NPCR	UACI
cameraman.tif	99.61492365	13.83499227
peppers	99.59716797	13.31389782
man	99.61825284	11.2753149
lena	99.62158203	13.57299152
goldhill	99.60160689	11.45083504
elaine	99.61603338	15.97203219
bridge	99.58829013	12.03061463

4.5. Testing rules

Various statistical tests [21-22] can be carried out on the generated bit sequence to compare and evaluate the sequence to be truly random bit sequences. Randomness is a probabilistic property, it is characterized and described in terms of probability. The likely outcome of statistical tests, when applied to a truly random sequence, is known a priori and can be described in probabilistic terms. There are various statistical tests, each assessing the presence or absence of a "pattern" which, if detected, would indicate that the sequence is non-random.

After a key is generated, its randomness it tested by some of the important statistical tests. Now consider the key as a binary sequence and test for random-bit sequence or not.

A statistical test [23] is formulated to test a specific null hypothesis (H0). For the purpose of this document, the null hypothesis under test is that the sequence being tested for random. Associated with this null hypothesis is the alternative hypothesis (Ha) which, for this document, is that the sequence is not random. For applied test a decision or conclusion is derived that accepts or rejects the null hypothesis, i.e., whether the generator is (or is not) producing random values, based on the sequence that was produced. For each test, a relevant randomness statistic must be chosen and used to determine the acceptance or rejection of the null hypothesis. Under an assumption of randomness, such a statistic has a distribution of possible values.

4.5.1. Testing rule 1:

H0: The binary bit-sequence generated is not a random sequence.

HA: The binary bit-sequence generated is a random sequence.

4.5.2. Testing rule 2:

Next important thing is to test the security level of the generated keys. We have to test the relationship between the security level of the generated key and its randomness level.

H0: No, relationship between randomness level and security level.

HA: Yes .There is a relationship between randomness level and security level.

4.6. Methods for testing rules

To test all rules stated above, we have to calculate the randomness level of each key. This will be performed by testing the statistical tests [1][15].

Randomness level

Let the binary sequence S = S0, S1, S2. . . Sn_1 of a length of a. The basic statistical tests are:

4.6.1 Frequency (Mono bit) Test

The objective of the test is the proportion of zeroes and ones for the entire sequence. The focus of this test is to determine whether the number of 0's and 1's are approximately the same. The test assesses the closeness of the fraction of ones to ½, that is, the number of ones and zeroes in a sequence should be about the same. This test is accomplished as follows:

$$X1 = (a0 - a1)2/a \quad (4.5.1)$$

Where: a0; the number of 0's a1; the number of 1's; a: the sequence length (a = a0+ a1)

In fact, X1 is approximately follows a chi-square $\chi 2$ reference distribution with 1 degree of freedom if a ≥ 10.

$$\text{Compute the test statistic } Sobs = |Sn|/\sqrt{n} \quad (4.5.2)$$

Sobs: The absolute value of the sum of the Xi (where, $Xi = 2e - 1 = |1|$) in the sequence divided by the square root of the length of the sequence.

$$\text{Compute P-value} = \text{erfc}(Sobs/\sqrt{2}) \quad (4.5.3)$$

Where erfc is the complementary error function.

If the computed P-value is < 0.01, then conclude that the sequence is non-random. Otherwise, conclude that the sequence is random.

4.6.2 Run test

This test runs up and down or the runs above and below the mean by comparing the actual values to expected values. The statistics for comparison the

'chi-square' test is carried out. It is to find whether the number of zeros or ones of various lengths 'i' in the sequence S is as expected for a random sequence which is:

U i = (a-i+3)/2 i+2

$$X_2 = \sum_{i=}^{n} \frac{(Ci-Ui)^2}{Ui} + \sum_{i=1}^{n} \frac{(Di-Ui)^2}{Ui} \qquad 4.5.4$$

where ;

Ci; the number of blocks of length i in S

Di; the number of gaps of length i in S

where $1 \le i \le n$ and n is the largest integer i.

In fact,X2 approximately follows a chi-square $\chi 2$ distribution with 2n - 2 degrees of freedom.

4.6.3 Autocorrelation test

Test the correlation between numbers and compare the sample correlation to the expected correlation of zero. The main focus of this test is to determine correlations between the sequence S and the shifted versions of it.

$$B(k) = \sum_{j=0}^{n-k-1} S_j \oplus S_{j+k} \qquad 4.5.5$$

Where; k; any fixed integer, $1 \le k \le \lfloor n/2 \rfloor$,

$\oplus$; XOR operator.

$$X_3 = 2\left(B(k) - \frac{n-k}{2} \right) / \sqrt{n-k} \qquad 4.5.6$$

In fact, X3 approximately follows an N (0, 1) distribution if n-k ≥ 10.

4.6.4 Serial test (Gap test)

Count the number of digits that appear between repetitions of a particular digit and then use the Kolmogorov-Smirnov test to compare with the expected number of gaps. The focus of this test is the frequency of all possible overlapping m-bit patterns across the entire sequence.

The focus of this test is to determine whether the number of occurrences of the 2m m-bit overlapping patterns is approximately the same as would be expected for a random sequence. This test is used to determine whether the number of occurrences of 00, 01, 10, and 11 are approximately the same by using:

$$X_4 = \frac{4}{(a-1)^2}(a^2_{00} + a^2_{01} + a^2_{10} + a^2_{11}) - \frac{2}{a}(a_0^2 + a_1^2) + 1 \qquad 4.5.7$$

where :

a00; the number of occurrences of 00

a01; the number of occurrences of 01

a10; the number of occurrences of 10

a11; the number of occurrences of 11

In fact, X4 approximately follows a chi-square $\chi 2$ distribution with 2 degrees of freedom if a >= 21.

4.6.5 Poker test

It treats numbers grouped together as a poker hand. Then the hands obtained are compared to what is expected by using the 'chi-square' test. It determines whether the occurrences of each part of the length m are approximately the same.

$$X_5 = \frac{2^l}{p}\left(\sum_{i=1}^{2^l} O_i^2 \right) - p \qquad 4.5.8$$

where;

l; the length of each part (bits)

P; the number of non-overlapping parts of length l

Oi; the number of occurrences of the ith part

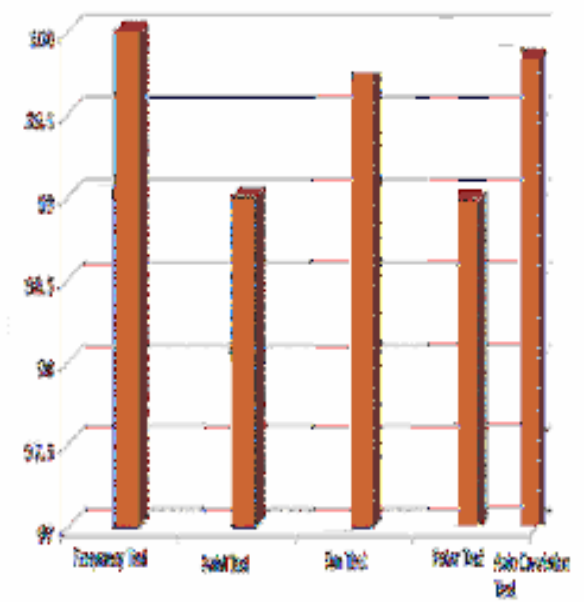


Fig.4 Randomness test results of proposed methods

In practice, X5 is approximately follows a chi-square $\chi 2$ distribution with 2l -1 degrees of freedom. We have tested our proposed technique to see how arbitrary [18-20] their output sequence. In figure 4 we see the average test results for 1000 test runs on each method with a bit length of 256 bits.By using a significance level of $\alpha = 0.05$, then the threshold values for X1,X2, X3,X4, and X5 becomes 3.9, 9.349,1.89, 5.09 and 14.507 respectively. For each generated random bit-sequence value the X1, X2 , X3, X4, and X5 are calculated. Each computed value is individually compared with the threshold value, the results for method - 1 were 98.9,97.5,99.9,99.9 and 99.8 for method - 2 were 99.9,98.9 and 99.9,98.8 and 99.8.The histogram of the test values of each statistical test follows the expected distribution.

5. Conclusion

The proposed crypto system has a simple chaotic map for key generation. A logistic map was used to generate a pseudo random bit sequence, which was in turn used to shift to generate random number for each process. In this algorithm, pixels are transformed by simple diffusion processes. The security of the algorithm needs 2 x 256 different keys is required for each round. The total key length is 512 bits for each round and about ten rounds. Therefore, the key space is approximately 2512, which was large enough to protect the system against any brute-force attacks. The image was a 2-D array of pixels, each with 256 gray scales. To improve security of the proposed encryption system, the histogram needed to become uniform.

All parts of the proposed (IMPSBEC) chaotic encryption system were simulated using a MATLAB 7.6 version. The histogram of the encrypted image was approximated a uniform distribution. Therefore, the proposed encryption (IMPSBEC) system was resistant against any statistical attack. To quantify the difference between encrypted image and corresponding plain-image, three measures were used: Correlation and key space analysis is performed. It was concluded that the correlation and KSA criteria of the proposed system were satisfactory when compared to other research results as against the security performance of the proposed system.

References:

[1]. LIU Xiangdong, Zhang Junxing, Zhang Jinhai, He Xiqin," Image Scrambling Algorithm Based on Chaos Theory and Sorting Transformation", International Journal of Computer Science and Network Security, VOL.8 No.1, January 2008

[2]. Shahram Etemadi Borujeni1, 2, Mohammad Eshghi1 "Chaotic Image Encryption Design Using Tompkins-Paige Algorithm ",Hidawi Journalof Mathematical Problems in Engineering Volume 2009 (2009), Article ID 762652, 22 pages doi:10.1155/2009/762652

[3]. Xiaojun Tong a, Minggen Cui b ,"Image encryption with compound chaotic sequence cipher shifting dynamically" ,ELSEVIER , Image and Vision Computing 26 (2008) 843–850

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

[5] G. R. Chen, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos Solitons & Fractals, vol. 21, pp. 749-761, 2004.

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

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

[8]. Shiguo Lian, Jinsheng Sun, Zhiquan Wang, "Security Analysis of A Chaos-based Image Encryption Algorithm ", PhisicaA, Elsevier Science,2005

[9].T. S. Parker and L. O. Chua, , Chaos: a tutorial for engineers, Proceedings of the IEEE, vol. 75, no. 8, pp. 982–1008 (1995)

[10].C.W.Wu and N. F. Rulkov, Studying chaos via 1-Dmaps—a tutorial, IEEE Trans. on Circuits and Systems I: Fundamental Theory and Applications, vol. 40, no. 10, pp. 707–721 (1993)

[11]. Shubo Liu1,2, Jing Sun1,2, Zhengquan Xu1,"An Improved Image Encryption Algorithm

based on Chaotic System" Journal of Computers, Vol. 4, No. 11, November 2009

[12]. Vinod Patidar a, N.K. Pareek b, K.K. Sud a ,"A new substitution–diffusion based image cipher using chaotic standard and logistic maps "ELSEVIER , Communications in Nonlinear Science and Numerical Simulations 14 (2009) 3056–3075

[13]. Jiankun Hu _, FenglingHan , "A pixel-based scrambling scheme for digital medical images protection" ,ELSEVIER, Journal of Network and Computer Applications 32 (2009) 788–794

[14]. Nawal El-Fishawy1 and Osama M. Abu Zaid2 , Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms , International Journal of Network Security, Vol.5, No.3, PP.241–251, Nov. 2007

[15]. R. Krishnamoorthi† and P. D. Sheba Kezia Malarchelvi††,"Selective Combinational Encryption of Gray Scale Images using Orthogonal Polynomials based Transformation", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.5, May 2008

[16]. ZHANG YiWei1†, WANG YuMin2 & SHEN XuBang1 "A chaos-based image encryption algorithm using alternate structure "Springer-Verlag, Science in China Series F: Information Sciences 2007

[17].I.A.Ismail,Mohammed Amin and Hossam Diab ,"An Efficient Image Encryption Scheme Based chaotic Logistic Map", International .Journal of Soft Computing 285-291,2007.

[18].Mohammad Ali Bani Younes and Aman Jantan ," Image Encryption Using Block-Based Transformation Algorithm ",IAENG International Journal of Computer Science, 35:1, IJCS_35_1_03

[19]. Hossam El-din H. Ahmed, Hamdy M. Kalash, and Osama S. Farag Allah ," An Efficient Chaos-Based Feedback Stream Cipher (ECBFSC) for Image Encryption and Decryption", Informatica 31 (2007) 121–129

[20].Marwa Abd El-Wahed, Saleh Mesbah, and A.min Shoukry ," Efficiency and Security of Some Image Encryption Algorithms", Proceedings of the World Congress on Engineering 2008 Volume I WCE 2008, July 2 - 4, 2008, London, U.K.

[21]. Abdulkarim Amer Shtewi†, Bahaa Eldin M. Hasan, Abd El Fatah .A. Hegazy,"An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems". IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.2, February 2010

[22].Scott Raynel , Anthony McGregor, Murray Jorgensen," Using the IEEE 802.11 frame check sequence as a pseudo random number for packet sampling in wireless networks" Proceedings of the 7th international conference on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks ,Seoul, Korea ,Pages: 552-557, 2009

[23].csrc.nist.gov/groups/ST/toolkit/rng/documents/SP800-22b.pdf

Sathishkumar.G.A obtained his M.E from PSG college of Technology, Coimbatore, India. He is currently perusing PhD from Anna University, Chennai and Faculty member in the Electronics and Communication Engineering Department of Sri Venakesateswara College of Engineering, Sriperumbudur. His research interest is Network Security, VLSI & Signal processing Algorithms.

Dr.K.Bhoopathy Bagan completed his doctoral degree from IIT Madras. He is presently working as Professor & Head, ECE dept, in Anna University, MIT Chrompet campus, Chennai. His areas of interest include Signal processing, Image Processing and Network Security.

ACKOWLEDGEMENT: The part of coding has been done by Mr.S.Sathya Narayanan, who is a under graduate student , Sri Venakesateswara College of Engineering, Sriperumbudur.This work is dedicated to my beloved teachers and my family.