View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Elsevier - Publisher Connector

Available online at www.sciencedirect.com

ScienceDirect

Procedia Technology 10 (2013) 663 – 671

Procedia Technology

First International Conference on Computational Intelligence: Modelling, Techniques and Applications(CIMTA-2013)

A Non-adaptive Partial Encryption of Grayscale Images Based on Chaos

Sukalyan Som[a], Sayani Sen[b]

[a] *Department of Computer Science, Barrackpore Rastraguru Surendranath College*
85, Middle Road & 6, Riverside Road, Barrackpore, Kolkata – 120, West Bengal, India
sukalyan.s@gmail.com

[b] *Department of Computer Science, St. Xavier's College (Autonomous)*
30 Park Street, Mother Teresa Sarani, Kolkata-700016, West Bengal, India
sayani.sen@gmail.com

Abstract

Research papers published in recent times have focused towards different kinds of image encryption techniques. Image encryption based on Chaos became very popular for cryptography since properties of Chaos are related to two basic properties of good cipher-Confusion and Diffusion. In this paper, A Non-adaptive Partial Encryption of Grayscale Images Based on Chaoshas been proposed. In Partial encryption speed and time is the main factor. We decompose the original grayscale image into its corresponding binary eight bit planes then encrypted using couple tent map based pseudorandom binary number generator (PRBNG). The four significant bit planes, determined by 5% level of significance on contribution of a bit-plane in determination of a pixel value, are encrypted using keys which are obtained by applying the recurrence relation of tent map based PRBNG. Then the four insignificant bit planes along with encrypted significant bit planes are combined to form the final cipher image. In order to evaluate performance, the proposed algorithm was measured through a series of tests to measure the security and effectiveness of the proposed algorithm. These tests includes visual test through histogram analysis, measures of central tendency and dispersion, correlation-coefficient analysis, key sensitivity test, key space analysis, information entropy test, Measurement of Encryption Quality – MSE, PSNR, NPCR, UACI. Experimental results show that the new cipher has satisfactory security and efficient.

© 2013 The Authors. Published by Elsevier Ltd. Open access under CC BY-NC-ND license.

Selection and peer-review under responsibility of the University of Kalyani, Department of Computer Science & Engineering

Keywords: Partial Image Encryption; Chaos; Cryptography; Tent Map; Pseudo Random Binary Number Generator; Information Entropy.

1. Introduction

Cryptography deals with protecting the privacy of information during communication. Visual information through images plays an important role in all aspects of our lives. In recent days, the increasing use of computers leads to an increasing tendency to security and image fidelity verification. Transmitted images may have different applications, such as commercial, military and medical applications. So it is necessary to encrypt image data before transmission over the network to preserve its security and prevent unauthorized access. However, compared to text, much more processing power and bandwidth for processing is required. In recent years number of different image encryption schemes has been proposed in order to overcome image encryption problems. The chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption [1]-[9]. Chaos is one of the possible behaviours associated with evolution of a nonlinear dynamic

* Corresponding author. Tel.: +91-9830814843;
E-mail address: sukalyan.s@gmail.com

2212-0173 © 2013 The Authors. Published by Elsevier Ltd. Open access under CC BY-NC-ND license.
Selection and peer-review under responsibility of the University of Kalyani, Department of Computer Science & Engineering
doi:10.1016/j.protcy.2013.12.408

system and occurs for specific values of system parameters. The chaotic behaviour of a non-linear system apparently looks random. The chaotic state can be observed by the existence of a chaotic attractor in which all the system trajectories evolve following a certain pattern but are never the same. Existing techniques consume enough computational time for encryption due to its bulk size. Since an image can be considered as a combination of correlated and uncorrelated data wherein most of the information found to be present in the correlated part rather than the uncorrelated part, thus it would be sufficient to encrypt the correlated bit planes instead of encrypting the entire image in order to speed up the entire process and save time too. In partial encryption techniques usually the significant information has to be encrypted leaving insignificant information unencrypted. Considerable amount of recent research papers have focused towards different kinds of partial encryption techniques in image processing. In this research we have tried to find a simple, fast and secure algorithm for partial image encryption using the characteristics of chaotic functions. Finally, this algorithm is very sensitive to small changes in key so even with the knowledge of the key approximate values; there least possibility for the attacker to break the cipher.

The rest of the paper is organized as follows: In Section 2, we review some of the existing image encryption techniques followed by the background of proposed scheme which is described in Section 3. In Section 4, we introduce the proposed scheme for encryption and decryption used in this paper. In section 5, we analyse the security of the proposed image cipher and evaluate its performance through various tests such as statistical analysis, key sensitivity test, key space analysis, information entropy test etc. and compare the results. Finally, conclusions are drawn in Section 6 with future directions of work.

2. Related Works

In recent years, a number of chaos based partial image encryption schemes have been proposed. In [10] the partial image encryption has been described in two ways using hill cipher technique. First encryption technique uses two slightly different keys to construct two self-invertible matrices, which are used in two different stages to get partially encrypted image. Second encryption technique use one key to construct one self-invertible matrix and it is used in first stage. In second stage same key matrix along with few modification in diagonal values are used to construct another self-invertible matrix which leads to partial image encryption. In [11] a simultaneous image compression and encryption scheme is discussed. The order of the two processes viz. compression and encryption is EC i.e. image encryption is performed first then the image compression is applied. For image encryption a symmetric key cryptography multiplicative cipher is used. Similarly for compression Discrete Cosine Transform is used. In the proposed approach a private key cryptography is used for encryption without sharing the secret key. But image transmission is required two times. Therefore to save the bandwidth partial encryption is carried out. In [12] two contributions are made using partial image encryption techniques. One is to scrambling the pixel position and other second is by using SCAN mapping method. In [13] a novel concept of combined partial image encryption using phase manipulation and sign encryption has been proposed. Entire encryption process involves two stages where image to be encrypted are applied to phase manipulation block. In first stage Fourier Transform (FT) is applied to get phase and magnitude of the input image. Phase of the image are scrambled to get modified image after applying Inverse Fourier Transform. In second stage the modified image is partially encrypted by using sign encryption. Sign Encryption finally gives resultant partially encrypted image by extracting the sign bits of modified image. In [14] new partial encryption schemes are present, in which a secure encryption algorithm is used to encrypt only part of the images. Only part of the original data is encrypted for two different grayscale images resulting in a significant reduction in encryption and decryption time.

3. Background

3.1. Bit-plane decomposition

In a gray-level image, the pixel intensity 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 be decomposed into an 8 bit binary value, given by

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

So, the input image can be divided into 8 binary images according to the bit locations within a pixel. In Fig 1 Original grayscale image Elaine of size 512×512 and the binary images obtained by collecting the ith bits of all the plain-image pixels has been presented.

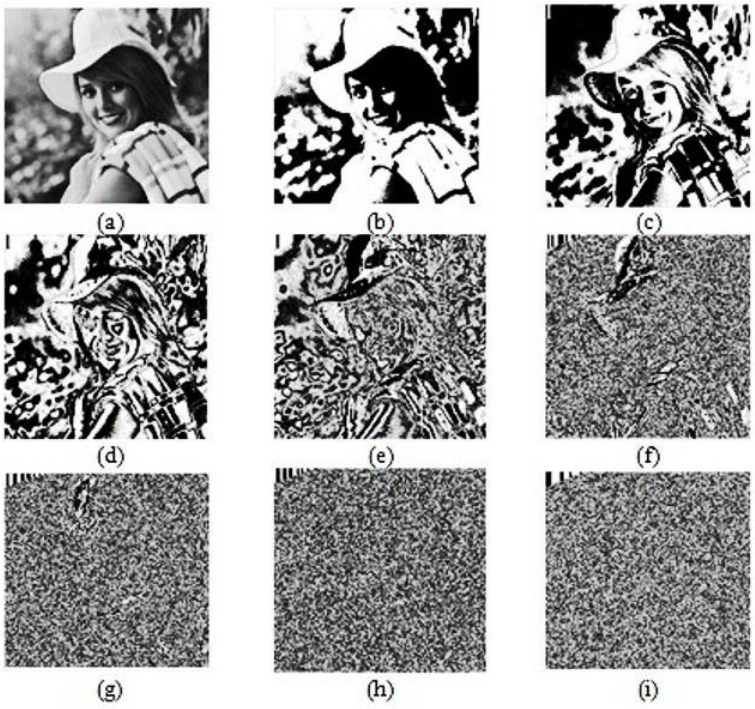

Fig 1 Bit plane decomposition of a grayscale image (a) Plain image Elaine of size 512 × 512(b) – (i) Bitplane slicing of plain image(512×512).The corresponding Bitplanes are (b) Bitplane8, (c) Bitplane7, (d) Bitplane6, (e)Bitplane5, (f) Bitplane4, (g) Bitplane3, (h) Bitplane2 and (i) Bitplane1

3.2. Significant bit-plane determination

A bit can carry different amount of information depending on its position in an 8 bit binary number i.e. if there exists a 1 at the 8th position (MSB) of a 8 bit binary number then its contribution towards the formation of corresponding decimal number is 127 where as it contributes only 1 if it is present at the 1st position (LSB). Percentage of contribution of different bit positions in the formation of a pixel of intensity 255 is shown in Table I that can be derived by the formula as stated in [15].

$$p(i) = \frac{2^i}{\sum_{i=0}^{7} 2^i} \quad (1)$$

TABLE I PERCENTAGE OF CONTRIBUTION IN THE FORMATION OF PIXEL INTENSITY

Bit position	Percentage of contribution in the formation of a pixel intensity
1	0.392156
2	0.784313
3	1.568627
4	3.137254
5	6.274509
6	12.549019
7	25.098039
8	50.196083

To determine whether a bit-plane is significant or not we frame the null hypothesis as $\mathcal{H}_0$: i^{th} bitplane is significant against the alternative hypothesis$\mathcal{H}_1$: i^{th} bitplane is not significant. Considering level α critical region at $\alpha = 0.05$ i.e. 5% level of significance from Table I we consider the first four bit-planes to be insignificant in terms of their percentage contribution.

3.3. Chaos based Pseudorandom Binary Number Generator

A Pseudo random bit generator (PRBG) based on two one-dimensional tent maps proposed by K. K. Sud et al. [16] running side-by-side and starting from random independent initial conditions has been used in the literature. The pseudorandom bit sequence is generated by comparing the outputs of both the chaotic logistic maps. The pseudo random bit generator (PRBG) is based on two tent maps stated as

$$x_{n+1} = f_\mu(x_n) = \begin{cases} \mu_2 x_n \text{for } x_n < \frac{1}{2} \\ \mu_2(1-x_n) \text{for } \frac{1}{2} \le x_n \end{cases} \text{ and } y_{n+1} = f_\mu(y_n) = \begin{cases} \mu_2 y_n \text{for } y_n < \frac{1}{2} \\ \mu_2(1-y_n) \text{for } \frac{1}{2} \le y_n \end{cases} \quad (2)$$

The bit sequence is generated by comparing the outputs of both the tent maps as

$$g(x_{n+1}, y_{n+1}) = \begin{cases} 1 & \text{If } x_{n+1} > y_{n+1} \\ 0 & \text{If } x_{n+1} \le y_{n+1} \end{cases} \quad (3)$$

4. Proposed scheme

4.1. Method of Encryption

Step 1: Consider the plain image to be $I_{original}(x,y)$ of size $M \times N$ where $x = 0,1,2,..,M-1$ and $y = 0,1,2,...,N-1$.

Step 2: Each pixel value $P_i(x,y)$in $I_{original}(x,y)$ is decomposed into its corresponding 8 bit binary equivalent and thus 8 bit-planes $BP_i(x,y)\ \forall\ i = 1,2,..,8$ are formed.

Step 3: Significant bit planes are determined by the level α critical region from the hypothesis $\mathcal{H}_0$: i^{th} bitplane is significant against the alternative hypothesis $\mathcal{H}_1$: i^{th} bitplane is not significant where the test statistics is the percentage contribution of a bit plane in formation of a pixel.

Step 4: Keys for diffusing the significant bitplanes are generated using Tent Map based PRNG stated in (2) – (4), with chosen values of the triplet (x_0, y_0, μ). The final iterated values of (x_{n+1}, y_{n+1}) for highest significant bitplane become the initial values (x_0, y_0) for generating the next key and so on.

Step 5: The significant bitplanes, determined by α% (0.05) level of significance, are ciphered as $CBP_j = BP_j \oplus K_j\ \forall\ j = 1,..,4$.

Step 6: The cipher bit planes CBP_j and the unencrypted bitplanes BP_i are combined together to form cipher image as$C_i(x,y) = CBP_j + BP_k\ \forall i = 1,2,..,8,\ j = 1,..4$ and $k = 5,..,8$ where $'+'$ is used to denote combining process.

4.2. Method of Decryption

Step 1: Consider the cipher image to be $I_{Cipher}(x,y)$ of size $M \times N$ where $x = 0,1,2,..,M-1$ and $y = 0,1,2,...,N-1$.

Step 2: Each pixel value $P_i(x,y)$in $I_{Cipher}(x,y)$ is decomposed into its corresponding 8 bit binary equivalent and thus 8 bit-planes $BP_i(x,y)\ \forall\ i = 1,2,..,8$ are formed.

Step 3: Significant bit planes are determined by the level α critical region from the hypothesis $\mathcal{H}_0$: i^{th} bitplane is significant against the alternative hypothesis $\mathcal{H}_1$: i^{th} bitplane is not significant where the test statistics is the percentage contribution of a bit plane in formation of a pixel.

Step 4: upon receiving the triplet (x_0, y_0, μ) Keys for diffusing the significant bitplanes are generated using Tent Map based PRNG stated in (2) – (4). The final iterated values of (x_{n+1}, y_{n+1}) for highest significant bitplane become the initial values (x_0, y_0) for generating the next key and so on.

Step 5: The significant cipher bitplanes, determined by α% level of significance, are deciphered as $BP_j = CBP_j \oplus K_j\ \forall\ j = 1,..,4$.

Step 6: The decipher bit planes BP_j and the insignificant bitplanes BP_i are combined together to form original image as $P_i(x,y) = BP_j + BP_k\ \forall i = 1,2,..,8,\ j = 1,..4$ and $k = 5,..,8$ where $'+'$ is used to denote combining process.

5. Security Test and Analysis

An extensive study of the proposed algorithm has been performed using the CVG image database [17] which is collections of digitized images available and maintained by University of Granada primarily to support research in

image processing, image analysis and machine vision. Currently, two volumes available at CVG are—Gray level images and Color images. We have chosen miscellaneous volume of Gray level image database. The miscellaneous volume of 512 sizes consists of 96 images and the miscellaneous volume of 256 sizes consists of 68 images.

5.1. Statistical test

1) Visual Test through Histogram Analysis

An image histogram demonstrates how pixels in an image are distributed by graphing the number of pixelsat intensity level. In order to have a perfect ciphered image the histogram of the image mustexhibit uniformity of distribution of pixels against the intensity values. The histograms of original as wellas encrypted images have been analysed. In Figure 2 the histograms of the originalimage of Elaine of size 512×512 and the histograms of corresponding Cipher Image has been presentedwhich depicts that the histograms of plain image has certain pattern where as that of the Cipher image areuniformly distributed.

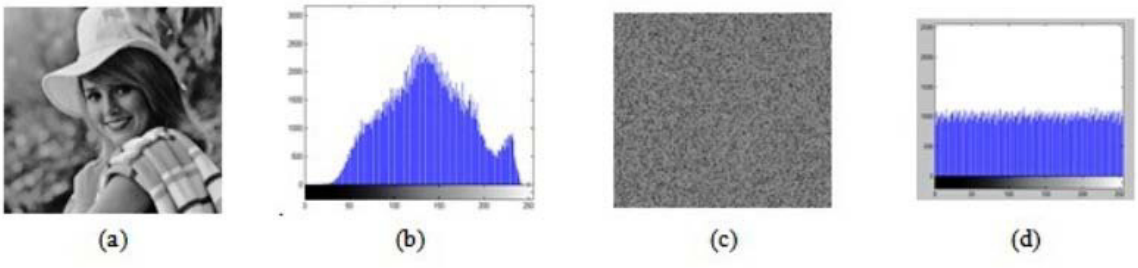

Fig 2 Visual Test and Histogram Analysis (a) Plain Image, (b) Histogram of Plain Image (c) Cipher Image (d) Histogram of Cipher Image.

2) *Measures of Central Tendency and Dispersion*

Measures of Central Tendency and Dispersion have been used as a measure of homogeneity. The comparative analysis as presented inTable II depicts that the measures are different in original image and encrypted image. The measuresin Cipher Images are uniform which shows that cipher images have uniform mean, median pixel intensities.

TABLE II MEASURES OF CENTRAL TENDENCY AND DISPERSION

Image Name	Mean		Median		Standard Deviation	
	Plain Image	Cipher Image	Plain Image	Cipher Image	Plain Image	Cipher Image
Boat	129.7	127.7	143.0	127.0	46.7	73.8
Elaine	136.4	127.4	135.0	127.0	46.1	73.9
Baboon	126.6	127.4	130.0	127.0	69.7	73.8
Map	180.6	127.2	192.0	127.0	39.4	74.0

3) Correlation Coefficient Analysis

In most of the plain images, there exists high correlation among adjacent pixels whereas poor correlation between the neighbouring pixels of corresponding cipher image is observed. Karl Pearson's Product Moment correlation coefficient, stated as follows, is used as a measure to find the correlation of horizontally, vertically and diagonally adjacent pixels of both the plain and cipher image and the correlation between the plain image and cipher image pixels.

$$r_{xy} = \frac{cov(x,y)}{\sigma_x \sigma_y} \text{where } cov(x,y) = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})(y_i - \bar{y}) \tag{4}$$

$$\sigma_x = \frac{1}{n}\sum_{i=1}^{n}(x_i - \bar{x})^2 \text{ and } \sigma_y = \frac{1}{n}\sum_{i=1}^{n}(y_i - \bar{y})^2 \text{ with} \sigma_x \neq 0 \text{ and } \sigma_y \neq 0 \tag{5}$$

Image Name	Horizontal Pixels		Vertical Pixels		Correlation between pixels of Original and Cipher Image	Information Entropy	
	Plain Image	Cipher Image	Plain Image	Cipher Image		Original Image	Cipher Image
Boat	0.9400	0.0045	0.9704	-0.0015	-0.0014	7.1914	7.9835
Elaine	0.9757	0.0026	0.9730	-0.0020	-0.0019	7.5060	7.9971
Baboon	0.9409	0.0016	0.9275	0.0013	0.0050	7.8282	7.9967
Map	0.9804	-0.0020	0.9930	0.0036	0.0002	6.9940	7.9985

In Table III correlation coefficient between two vertically, and horizontallyadjacent pixels of four sample original images and corresponding encrypted images are presented from which it can be concludedthat there is negligible correlation between the twovertically and horizontallyadjacent pixels inencrypted image but high correlation in original image. Table III also presents the correlation coefficient between the original image and the cipher image.

5.2. Key Sensitivity test

A good cryptosystem should be sensitive to a small change in secret keys i.e. a small change in secretkeys in encryption process results into a completely different encrypted image. Our proposed encryptionalgorithm is sensitive to a tiny change in the secret keys.As an example plain image of Elaine of size 512×512 is encrypted with$x_0 = 0.45001, y_0 = 0.54001,\ \mu_1 = \mu_2 = 1.97$. In Fig 2 different cipher images of Elaine with minor changes in secret keys has been presented.

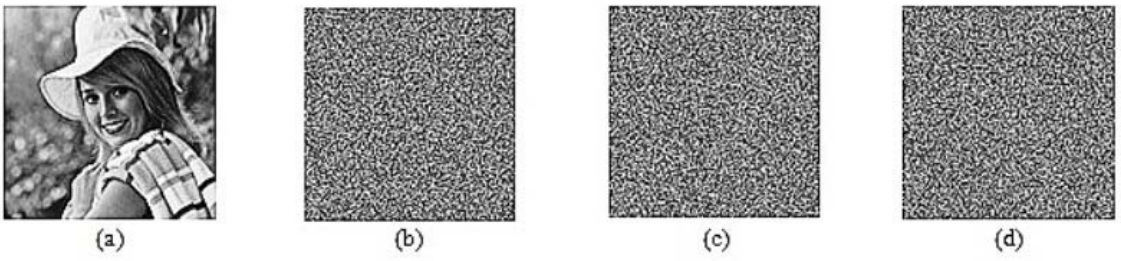

Fig 2 Key Sensitivity test (a) Plain Image Elaine (b) Cipher image with chosen secret key (c) Cipher image with change in $x_0 = 0.45002$(d) Cipher Image with change in $y_0 = 0.54002$

5.3. Key Space Analysis

A good encryption scheme should be sensitive to the secret keys and the key space should be large enough to make brute force attack infeasible. In the proposed CBPIE algorithm, the initial conditions and the system parameters of the chaotic maps i.e. the triplet (x_0, y_0, μ) forms the symmetric key. Considering the precision of calculation as $10^{-14}$the key space for the proposed scheme is $10^{14} \times 10^{14} \times 10^{14} = 10^{42}$which is reasonably large enough to resist the exhaustive attack.

5.4. Information Entropy Test

It is well known that the entropy H(s) of a message source s can be calculated as:

$$H(s) = \sum_{i=0}^{2^N-1} p(S_i).\log_2 \frac{1}{p(S_i)} \tag{6}$$

Where, (S_i) represents the probability of symbol Si and the entropy is expressed in bits. Let us suppose that the source emits 2^8symbols with equal probability, i.e.$S = \{S_1, S_2, S_3, \ldots, S_{2^8}\}$. Afterevaluating the above equation, we obtain the entropy H(S) = 8, corresponding to a truly random source. Actually, given that a practical information source seldom generates random messages, in general its entropy value is smaller than the ideal one. However, when the messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security.Information entropy of

some sample images and their corresponding cipher images is shown in Table III which are very close to the theoretical limit signifying that the proposed scheme is robust against entropy attack.

5.5. Measurement of Encryption Quality – MSE, PSNR, NPCR, UACI

A very useful measure of the performance of the decryption procedure is the Peak Signal-to-Noise Ratio (PSNR). Greater PSNR value (>30dB) reveals better image quality. For encrypted image, smaller value of PSNR is expected.

Let,$C(i,j)$and $P(i,j), i = 0,1,2,\dots,M-1\ and\ j = 0,1,2,\dots,N-1$be the gray level of the pixels of a cipher and original image respectively. The MSE between these two images is defined as

$$\mathrm{MSE} = \frac{1}{\mathrm{M}\times\mathrm{N}}\sum_{\mathrm{i}=0}^{\mathrm{M}-1}\sum_{\mathrm{j}=0}^{\mathrm{N}-1}|\,\mathrm{C(i,j)}-\mathrm{P(i,j)}|^2 \tag{7}$$

$$\mathrm{PSNR} = 20\ \times\ \log_{10}\left(\frac{255}{\sqrt{\mathrm{MSE}}}\right) \tag{8}$$

PNSR for the cipher images with respect to their plain images for several images have been calculated. In all test cases, it was found to be small (<10dB). The computed results of PSNR for four sample images are presented in Table IV. 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 then the differential attack actually loses its efficiency and becomes useless. To test the effect of one-pixel change on the image encrypted by the proposed algorithm, two common measures were used – Number of Pixel Change Rate (NPCR) and Unified Average Change in Intensity (UACI) [18][19]. Consider two cipher-images, $\mathrm{C_1(i,j)}$and$\mathrm{C_2(i,j)}$ wherei $= 0,1,2,\dots,\mathrm{M}-1$ and $\mathrm{j} = 0,1,2,\dots,\mathrm{N}-1$, whose corresponding plain-images have only one pixel difference. Then NPCR and UACI are defined as

$$\mathrm{NPCR} = \frac{\sum_{\mathrm{i,j}}\mathrm{D(i,j)}}{\mathrm{M}\times\mathrm{N}}\ where D(i,j) = \begin{cases}0\ , if C_1(i,j) = C_2(i,j)\\ 1\ , if C_1(i,j) \neq C_2(i,j)\end{cases} \tag{9}$$

$$UACI = \frac{1}{M\ \times N}\sum_{i,j}\frac{|\,C_1(i,j) - C_2(i,j)|}{255}\times 100\% \tag{10}$$

Tests have been performed on the proposed scheme about the one-pixel change influence on 256 grayscale image of different size and results on four sample images is presented in Table IV.

TABLE IVMEASUREMENT OF ENCRYPTION QUALITY AND ENCRYPTION AND DECRYPTION TIME COMPARISON

Image Name	MSE	PSNR	NPCR	UACI	Encryption (in S)	Decryption (in S)
Boat	7.7495e+003	9.2721	98.6953	18.2354%	0.9235	0.6341
Elaine	7.2443e+003	9.5649	98.2354	28.1145%	0.9397	0.7120
Baboon	8.4319e+003	8.9055	97.2387	22.2154%	0.3985	0.2960
Map	7.2240e+004	7.2871	98.2584	19.5403%	0.9150	0.8148

5.6. Comparison of encryption and decryption time

For images of different size the timetaken by the proposed algorithm to perform determination of bit plane to encrypt, key generation, encryption and decryption is presented in Table IV.

6. Comparison with existing techniques

In order to compare the novelty of the proposed scheme security and encryption and decryption time has been considered. It is shown that the key space and the information entropy of our proposed algorithm are reasonable compared to others. Test of homogeneity of the cipher images is carried out in our communication which is not available in all the references. Our approach has achieved best information entropy among the

others.Computationally the proposed scheme is faster than the existing methods for encrypting the entire image as a whole and a partial encryption method.

TABLE VCOMPARISON WITH EXISTING METHODS

Parameter of comparison	Proposed method	L Liu et al [20]	Som et al [9]	Rao et al[14]
Key space	10^{42}	10^{52}	NA	NA
Key sensitivity	Yes	Yes	Yes	NA
Entropy (average)	7.9940	7.9890	7.9968	NA
Cross correlation (average)	-0.00275	0.00936	0.00225	0.0016
Average encryption time (in s)	0.59375	0.97530	1.0825	NA
Average decryption time (in s)	0.06253	0.6082	1.975	NA
Test homogeneity	Yes	NA	Yes	NA

7. Conclusion

This communication puts forward a non-adaptive partial encryption of grayscale images based on chaos. The proposed algorithm effectively determines significant bit planes on the basis of contribution made by them to form a pixel. The significant bit planes are encrypted by the key steam generated on the basis of a chaos based pseudorandom binary number generator where the insignificant bit planes are left over to reduce the computational time. Thesimulation experiment and results show that the encryption algorithm is effective, simple to implement, itssecret key space is reasonably large and can effectively resists exhaustive attack, statistical attack and so on. To prove the superiority of the proposed scheme comparisons are madewithexiting algorithms for encrypting the image entirely and partially. An image can be classified in three categories images (i) where only a single bit plane contains the entire information, (III) images where all the bit planes contain significant information, and, (IV) images where some bit planes are significant and some other are not. Our interest mainly lies with the third category as encrypting the other categories is easier. Once we classify an image into the third category, a threshold is defined through which we evaluate the importance of the individual bit planes before encrypting them. Designing an adaptive algorithm to detect the significant bit planes and thereafter encrypting them by chaos based PN sequence would be of future concern.

References

1. N. Pisarchik, N. J. Flores-Carmona, M. Carpio-Valadez, “Encryption and decryption of images with chaotic map lattices”, CHAOS Journal, American Institute of Physics, vol. 16, 2006.
2. C. Dongming, Z. Zhiliang, Y. Guangming, "An Improved Image Encryption Algorithm Based on Chaos." in Proceedings of IEEE International Conference for Young Computer Scientists, 2008.
3. N. K. Pareek, V. Patidar, K. K. Sud, “Image encryption using chaotic logistic map.” Image and Vision Computing, vol.24, no.9, pp. 926–934, 2006.
4. N.K. Pareek, VinodPatidar, K.K. Sud, Cryptography using Multiple one-dimensional chaotic maps, Communications in Nonlinear Science and Numerical Simulation, 2005.
5. N.K. Pareek., VinodPatidar., K.K. Sud,Image encryption usingchaotic logistic map, Image and Vision Computing, 2006.
6. Schneier B. Applied cryptography: protocols, algorithms and source code in C. New York: John Wiley and Sons; 1996.
7. Shubo Liu, Jing Sun, ZhengquanXu,An Improved Image Encryption Algorithm based on Chaotic System. Journal of Computers, vol. 4, no. 11 (2009).
8. J. Fridrich, “Symmetric ciphers based on two-dimensional chaotic maps.” International Journal of Bifurcation and Chaos, vol.8, no.6, pp.1259-1284, 1998.
9. S. Som, A. Kotal, “Confusion and diffusion of grayscale images using multiple chaotic maps,” in Proc. NCCCS 2012, Durgapur, Dr. B. C. Roy Engineering College, ISBN: 978-1-4673-1952-2, INSPEC Accession Number: 13246202, DOI:10.1109/NCCCS.2012.6412989, pp.1 – 5.
10. H. T. Panduranga, S. K. Naveen Kumar, “Advanced Partial Image Encryption using Two-Stage Hill Cipher Technique”, International Journal of Computer Applications (0975 – 8887) ,vol. 60 no.16, December 2012.
11. A. Razzaque, Dr.N.V.Thakur, “An Approach to Image Compression with Partial Encryption without sharing the Secret Key”, IJCSNS International Journal of Computer Science and Network Security, vol. 12 no.7, July 2012.
12. B. D. Parameshachari, Dr. K M S Soyjaudah, “A Study of Binary Image Encryption Using Partial Image Encryption Technique”, International Journal of Modern Engineering Research (IJMER), vol.2, Issue.3, pp. 955-959, ISSN: 2249-6645, May-June 2012.

13. B. D. Parameshachari, K M Sunjiv Soyjaudah, Sumitrha Devi K A, "Secure Transmission of an Image using Partial Encryption based Algorithm", International Journal of Computer Applications (0975 – 8887), vol. 63, no.16, February 2013.
14. Y. V. SubhaRao, Abhijit Mitra, S. R. MahadevaPrasanna, "A Partial Image Encryption Method with Pseudo Random Sequences", in: Proceedings of ICISS 2006, LNCS 4332, pp. 315 325, 2006.
15. Lin Teng, Xingyuan Wang, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive", Optics Communication, 285, pp 4048 – 54, 2012.
16. Narendra K Pareek, Vinod Patidar, Krishan K Sud, "A Random Bit Generator Using Chaotic Maps", International Journal of Network Security, Vol.10, No.1, PP.32 {38, Jan. 2010.
17. CVG Image Database, Computer Vision Group, University of Granada http://decsai.ugr.es/cvg (accessed on Jan 12, 2013).
18. G. Chen, Y. Mao, and C.K. Chui, "A Symmetric Encryption Scheme Based on 3D Chaotic Cat Map," Chaos, Solitons & Fractals, 21, 749-761, 2004.
19. G. Alvarez, and S. Li, "Breaking an Encryption Scheme Based on Chaotic Baker Map," Phys. Lett. A, 352(1-2), 78-82, 2006.
20. L. Liu, Q. Zhang, X. Wei, "A RGB image encryption algorithm based on DNA encoding and Chaos map," Computers and Electrical Engineering, vol. 38, 1240-1248.