ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Robust Image Encryption Technique using Fusion of Chaotic maps

Priya R Sankpal [1], P. A. Vijaya [2]

Assistant Professor, Department of ECE, B.N.M. Institute of Technology, Bangalore, India[1]

Professor & HOD, Department of ECE, B.N.M. Institute of Technology, Bengaluru, India[2]

ABSTRACT: Information transmitted over the Internet includes text, audio, image, and other multimedia files. In daily chores of life, images are used for varied purposes and as a result, the security of image data is a major concern. The proposed approach of encrypting images is based on chaotic maps. Every minute deviation in the initial condition will result in a totally different sequence. Chaos is a deterministic process but it appears to be random in nature. The unique characteristics like sensitivity to initial conditions and unpredictability make them suitable for designing encryption algorithms. In the proposed method, image encryption is based on the use of multiple chaotic maps, in order to meet the requirements of secured image transmission. Chaotic maps implemented are logistic map and skew tent map. The image encryption scheme uses an external secret key of 80-bit for logistic map and 128 bit for skew tent map. To make the cipher more robust against attacks, the fusion or combinations of logistic and skew tent maps have been implemented. Statistical analysis and key sensitivity tests were done for different methods to validate the proposed method.

KEYWORDS: Chaotic system, Logistic map, Skew tent map, Fusion map.

I. INTRODUCTION

In the present age of advanced digital technology, information is a very important asset that has to be safeguarded and secured from all kinds of possible attacks. For information to be secured, it has to be hidden from unauthorized access and protected from unauthorized change. Also the secured information must be available to an authorized entity whenever needed/required. All these issues are the major security goals. In this age of universal electronic property, of viruses and hackers, of electronic eavesdropping and electronic fraud, there is no time at that security doesn't matter. Hence, cryptography is one of the efficient approaches in providing data security. There are many traditional encryption–decryption algorithms that have been developed; which provide enhanced security. With growing threat of piracy within the net and infringement of copyright cases, image encryption is employed to assure confidentiality, integrity and legitimacy of the digital images. Image encryption is a technique that provides security to images by converting the original image into an image which is difficult to understand. Applications of image encryption can be extended to medical science, telemedicine, internet communication, military communication, multimedia systems, etc. Many works have been done in the field of chaos based image encryption. The proposed methodology aims at achieving image encryption based on Chaos Theory using Logistic and Skew Tent maps.

II. CHAOS THEORY

Chaos theory studies the behavior of ever changing systems that are highly sensitive to initial conditions: an effect that is popularly cited as the butterfly effect. Little variations in initial conditions (such as those due to misreckoning errors in numerical computation) yield widely oblique outcomes for chaotic systems and this happens although these systems are deterministic. Chaotic systems Behavior is determined by their initial conditions.This behavior is known as deterministic chaos, or simply chaos [1-2]. In this paper, chaotic maps are used to produce the chaotic sequence which is used to control the encryption process. The chaotic sequence is generated using the logistic map and the skew tent map.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

II.1 Logistic map

A simple and well-studied example of a one dimensional map that exhibits complicated behaviour is the logistic map [3 - 5]. It is defined as

$$x_{n+1} = r\, x_n(1-x_n) \qquad (1)$$

Where $x_n \in (0, 1)$ and 'r' is the control parameter $[0 \leq r \leq 4]$. x_n is n^{th} value in the sequence and x_{n+1} is $(n+1)^{th}$ value in the sequence.

II.2 Skew Tent map

Skew Tent map [7-9] is mathematically defined as

$$x(n+1) = \begin{cases} \frac{x(n)}{a}, & 0 < x \leq a \\ \frac{1-x(n)}{x(n)-a}, & a \leq x < 1 \end{cases} \qquad (2)$$

Where $x(n+1) \in (0, 1)$ and $0 < a < 1$. x_n is n^{th} value in the Sequence and x_{n+1} is (n+1) value in the sequence.

III. IMPLEMENTATION OF PROPOSED IMAGE ENCRYPTION SCHEME

The proposed Image encryption scheme is implemented in three stages i.e. single map implementation, double map implementation and fusion of the two chaotic maps. The single map implementation does not produce good quality of encryption and therefore we go for a double map (i.e. using the same map twice) implementation. This conclusion is arrived at, after comparisons of the various analysis parameters and simulation results. To enhance the security level of the encryption scheme, the logistic and skew tent maps were fused (combine) in different combinations. In the fusion implementation, the bit XOR operation is performed on various combinations of fused ciphers, so that the histogram of the cipher-image is significantly different (uniform) from that of the plain-image and therefore enhancing the resistance to statistical attack as well as differential attack greatly. The decryption algorithm is same as the encryption.

III.1 Single map implementation

1. Logistic Map

a) Usage of an 80-bit key to generate the initial condition X0 for the chaotic Logistic map.
   - o User input in hexadecimal(hex) format is converted to binary(B) and select few bits(Bi) to calculate a unique real number, as given below:
     - X01 = (B1)10/(2^24)
     - X02 = ($\sum_{i=13}^{18}(hex)_{10}$)/96
     - X0 = (X01 + X02) mod 1
   - o Reading and storing of the plain grayscale image of different sizes (MxN).

b) Implementation of the Logistic equation using the above calculated initial condition X0.

c) Iteration of the map't = MN' times where (MxN) is the size of the image to generate the chaotic sequence x (m).

d) Generation of chaotic image 'n' of size (MxN) using the above chaotic sequence x (m).

e) Exclusive OR operation performed on the plain and chaotic images to obtain the ciphered image.

2. Skew Tent Map

a) Usage of an 80-bit key to generate the initial condition X_0 for the chaotic Logistic map.
   - o User input in hexadecimal(*hex*) format is converted to binary(B) and select few bits(B_i) to calculate a unique real number, as given below:
     - $X_{01} = B_1$ xor B_3
     - $X_{02} = (\sum_{i=1}^{8}(hex)_{10})/128$
     - $X_0 = (X_{01} + X_{02})$ mod 1

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

- Reading and storing of the plain grayscale image of different sizes (MxN).

b) Implementation of the Skew Tent map equation using the above calculated initial condition X_0.
c) Iteration of the map't = MN' times where (MxN) is the size of the image to generate the chaotic sequence x (m).
d) Generation of chaotic image 'n' of size (MxN) using the above chaotic sequence x (m).
e) Exclusive OR operation performed on the plain and chaotic images to obtain the ciphered image.

III.2 Double map implementation

1. Logistic Map

a) Usage of an 80-bit key to generate the initial conditions X_0 and Y_0 for the double chaotic Logistic map.

- User input in hexadecimal(*hex*) format is converted to binary(B) and select few bits(B_i) to calculate a unique real number X_0 for the first map as given below:
  - $X_{01} = (B_1)_{10}/(2^{\wedge 24})$
  - $X_{02} = (\sum_{i=13}^{18}(hex)_{10})/96$
  - $X_0 = (X_{01} + X_{02}) \bmod 1$
- Iterate the Logistic map desired times using the above initial condition X_0.
- Generate a sequence of 24 real numbers '*f*(*k*)' in the range (0.1, 0.9) and convert it to integers using the formula

$$P_k = int\ (23 * (f_k - 0.1)/0.8) + 1, \text{ where } k = 1,2, \ldots, 24$$

- Select few bits(B_i) to calculate a unique real number Y0 for the second map, is as given below:

  - Y01 = (B2)10/(2^24)
  - Y02 = $(\sum_{k=1}^{24} B_2[P_k] * 2^{k-1})/2^{24}$
  - Y0 = (Y01 + Y02) mod 1
- Reading and storing of the plain grayscale image of different sizes (MxN).

b) Implementation of the Logistic map equation using the above calculated initial conditions X_0 and Y_0.
c) Iteration of the two maps 't = MN' times, where (MxN) is the size of the image, to generate the chaotic sequences x (m) and y (m).
d) Generation of two chaotic images 'n1' and 'n2' of sizes (MxN) using the above chaotic sequences x (m) and y (m).
e) Exclusive OR operation is performed on the plain and two chaotic images in sequence to obtain the ciphered image.

2. Skew Tent Map

a) Usage of an 128-bit key to generate the initial conditions X_0 and Y_0 for the double chaotic Logistic and Skew Tent maps respectively.

- User input in hexadecimal(*hex*) format is converted to binary(B) and select few bits(B_i) to calculate a unique real number X_0 for the first map as given below:
  - $X_{01} = B_1 \text{ xor } B_3$
  - $X_{02} = (\sum_{i=1}^{8}(hex)_{10})/128$
  - $X_0 = (X_{01} + X_{02}) \bmod 1$

Select few bits(B_i) chosen to calculate a unique real number Y_0 for the second map as given below:

- $Y_{01} = B_2 \text{ xor } B_4$
- $Y_{02} = (\sum_{i=9}^{16}(hex)_{10})/128$
- $Y_0 = (Y_{01} + Y_{02}) \bmod 1$

- Reading and storing of the plain grayscale image of different sizes (MxN).

b) Implementation of the Skew Tent map equation using the above calculated initial conditions X_0 and Y_0.
c) Iteration of the two Skew Tent maps't = MN' times, where (MxN) is the size of the image, to generate the chaotic sequences x(n) and y(n).

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

d) Generation of two chaotic images 'n1' and 'n2' of sizes (MxN) using the above chaotic sequences x(n) and y(n).

e) Exclusive OR operation is performed on the plain and two chaotic images in sequence to obtain the ciphered image.

III.3 Fusion Map Implementation

1. *Single Map Fusions*

a. Logistic Cipher with Skew Tent Cipher (Fusion1)

- Single maps of Logistic and Skew Tent were used to generate separate chaotic images that were XOR'ed with the plain image separately to obtain two intermediate cipher images.
- These intermediate cipher images were XOR' ed with each other to obtain the final ciphered image.

b. Logistic Cipher with Skew Tent Chaotic Image (Fusion2)

- Single Logistic map generated-chaotic image is XOR'ed with the plain image to get the intermediate cipher image.
- Intermediate cipher image is XOR'ed with the single Skew Tent map generated chaotic image to get the final cipher image.

c. Skew Tent Cipher with Logistic Chaotic Image(Fusion3)

- Single Skew Tent map generated-chaotic image is XOR'ed with the plain image to get the intermediate cipher image.
- Intermediate cipher image is XOR'ed with the single Logistic map generated chaotic image to get the final cipher image.

2. *Double Map Fusions*

a) Double Logistic Cipher with Double Skew Tent Cipher(Fusion4)

- Double maps of Logistic and Skew Tent were used to generate separate chaotic images that were XOR'ed with the plain image separately to obtain two intermediate cipher images.
- These intermediate cipher images were XOR'ed with each other to obtain the final ciphered image.

b) Double Logistic Cipher with two Skew Tent Chaotic Images(Fusion5)

- Double Logistic map generated-chaotic images are XOR'ed with the plain image to get the intermediate cipher image.
- Intermediate cipher image is XOR'ed with the double Skew Tent map generated-(two) chaotic images in sequence to get the final cipher image.

c) Double Skew Tent Cipher with two Logistic Chaotic Images (Fusion6)

- Double Skew Tent map generated-chaotic images are XOR'ed with the plain image to get the intermediate cipher image.
- Intermediate cipher image is XOR'ed with the double Logistic map generated-(two) chaotic images in sequence to get the final cipher image.

3. *Mixed Fusion*

Double Logistic Cipher with Single Skew Tent Cipher (Fusion7)

- Double Logistic map generated-chaotic images are XOR'ed with the plain image to get the intermediate cipher image (1).
- Single Skew Tent map generated-chaotic image is XOR'ed with the plain image to get the intermediate cipher

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

image (2).

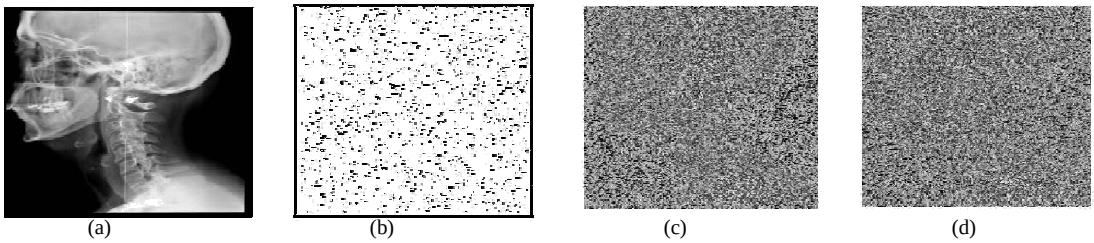
- These two intermediate cipher images (1) and (2) are XOR'ed with each other to obtain the final cipher image.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

In this section, proposed image encryption methodology experimental results are presented. The work is accomplished with a computer having specification, Intel(R) Core(TM) i3-3120M, 2.50GHz CPU, and running Windows 7. Also the encryption algorithm is analysed for different security aspects like key sensitivity, key space, histogram and correlation coefficient analysis. The encryption algorithm is analysed for all the three implementation i.e. single map implementation, double map implementation and fusion map implementation.

IV.1 Logistic Map- Encryption

In the single map implementation, plain image as in fig1(a) is XORed with the logistic chaotic map as in fig1(b).The cipher image obtained fig1(c) reveals certain amount of information about the plain image. This can be overcome by using double logistic maps as shown in fig. 1(d).

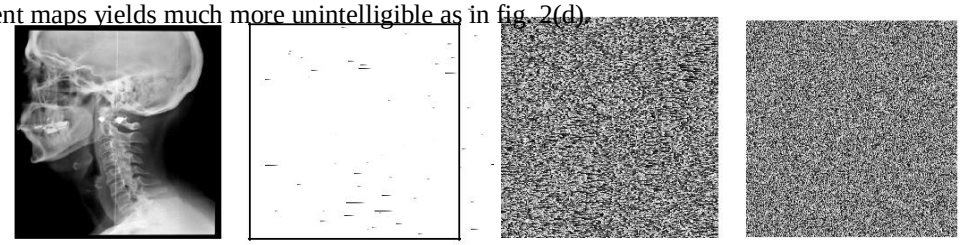


(a) (b) (c) (d)

Figure 1(a): Plain Image (b) Chaotic Image for 1 D Logistic map (c) Cipher Image obtained using single Logistic map and (d) Cipher Image obtained using double Logistic map

IV.2 Skew Tent Map- Encryption

In the single map implementation using Skew tent map, the plain image as in fig 2(a) is XORed with the Skew tent chaotic map as in fig2 (b). The resultant cipher image is as shown in fig2(c). The encryption results obtained using single Skew Tent map fig2(c) is better than single logistic map as seen in fig. 1(c). The cipher image obtained using double Skew Tent maps yields much more unintelligible as in fig. 2(d).



(a) (b) (c) (d)

Figure 2(a): Plain Image (b) Chaotic Image for skew tent map (c) Cipher Image obtained using single skew tent map and (d) Cipher Image obtained using double skew tent map.

IV.3 Fusion of Maps – Encryption

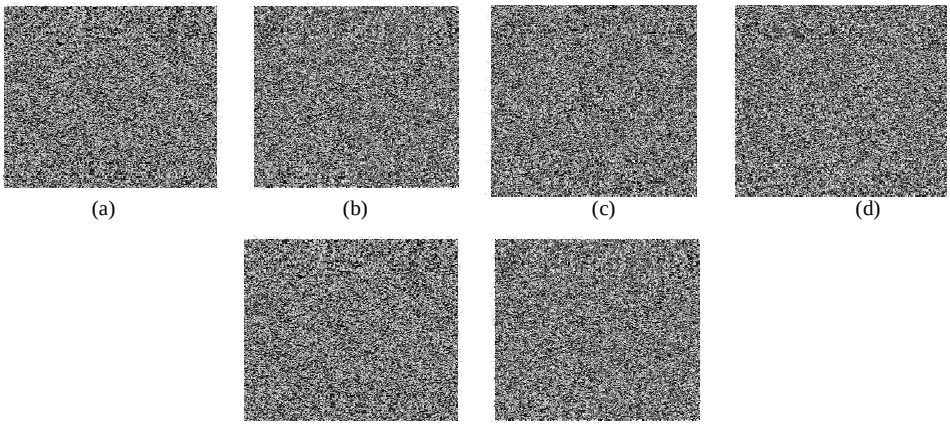
To enhance the security level, encryption is performed by using different combinations of Logistic and Skew Tent map (Fusion 1-Fusion 7). Cipher image obtained using single map implementation of Logistic map and Skew tent map is as shown in fig3 (a) and fig3 (b). The cipher image in fig3(c) is obtained by fusing single Logistic map and Skew tent map. The cipher image in fig3 (d) and fig3 (e) is result of using double map implementation of Logistic and Skew tent maps respectively. The cipher image in fig3 (f) is obtained as a result of fusion of double map implementation of Logistic and Skew tent maps. In all the various cases, the cipher image obtained doesn't reveal any information regarding the plain image.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016



(a) (b) (c) (d)

(e) (f)

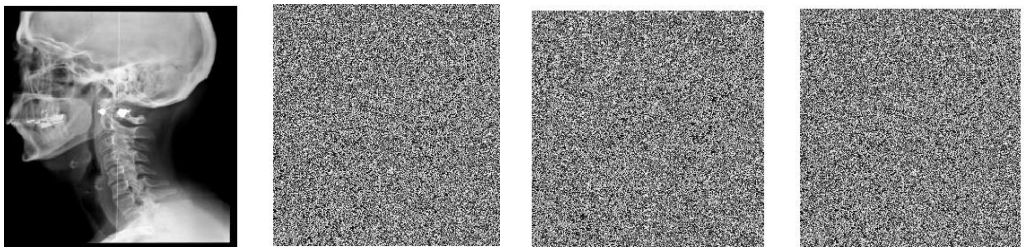
Figure 3 Cipher Image obtained using (a) single logistic map (b) Single Skew Tent map (c) Fused Cipher Image using single logistic and skew tent, d) double logistic maps, (e) double skew Tent maps (f) Fused cipher image of (d) and (e)

IV.4 Key Space

Key space size is the total number of different keys that can be used in the encryption. Security issue is that the size of the key area/space. If it's not giant enough, the attackers could guess the image with brute-force attack. The key space for logistic map is 2^{80} and that of skew tent map is 2^{128}. Therefore, the size of key space for initial conditions and control parameters of the proposed scheme is 2^{208} ($2^{80} * 2^{128} = 2^{208}$). This size is large enough to defeat brute-force attack by any computer today.

IV.5 Sensitivity Analysis

Sensitivity Analysis is the study of however the variation (uncertainty) within the output of a mathematical model may be distributed, qualitatively or quantitatively, to totally different sources of variation within the input of the model. An ideal image encryption procedure should be sensitive with respect to the secret key i.e. the modification of one bit within the secret key ought to turn out a totally different encrypted image. Encryption of the original image is done using the hexadecimal secret key1. The resultant image is shown in fig 4(b) for Logistic map and in fig.5 (b) for Skew Tent map. A slight modification is made in the secret key i.e. the most significant bit is changed in the secret key, key 2 and the resultant encrypted image obtained is as in fig. 4(c) for logistic map and in fig5(c) for Skew Tent map. Again, the original image is encrypted by making the slight modification in the secret key i.e. the LSB is changed in the secret key3.The resultant encrypted image is as shown in Fig. 4(d) for logistic map and in fig.5(d) for Skew Tent map. The three encrypted images fig.4 and 5(b) – (c) are compared. It is not easy to compare the encrypted images by simply observing these images. So for comparison, we've got calculated the correlation between the corresponding pixels of the three encrypted images.



(a) (b) (c) (d)

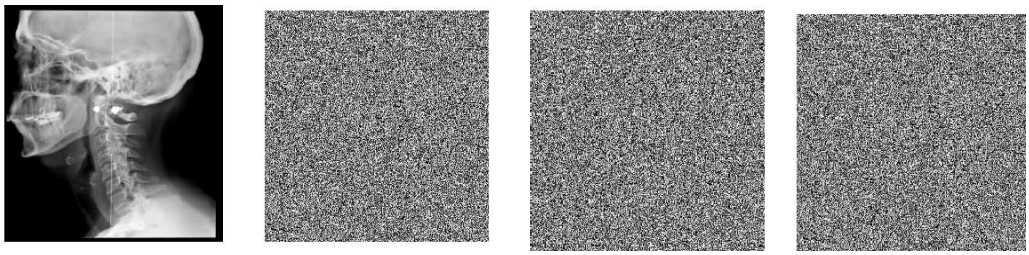
Figure 4(a) Plain Image, (b –d) Cipher Image obtained using Logistic map with different keys. (b)Key 1: ABCDEF0123456789FF05, (d) Key 2: BBCDEF0123456789FF05, (d) Key 3: ABCDEF0123456789FF06

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

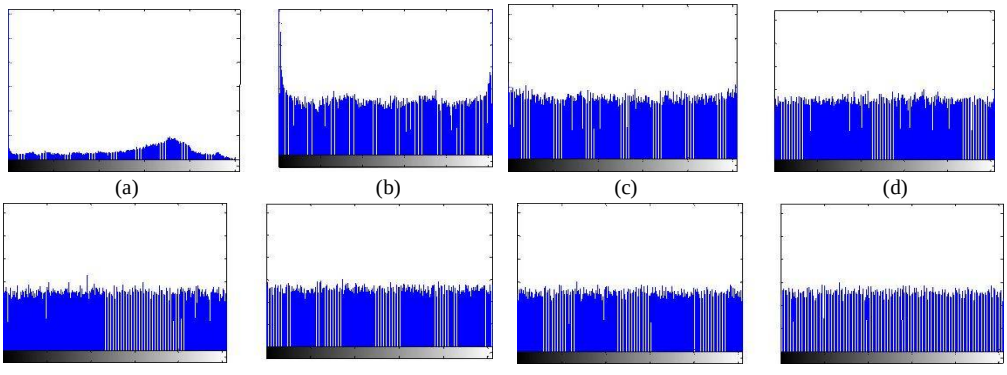


(a) (b) (c) (d)

Figure 5(a): Plain image, (b – d) Cipher image obtained using Skew Tent map with (b) Key 1: 8D6CFB3A538F493DAEDCFD2CFA87A5E6, (c) Key 2: AD6CFB3A538F493DAEDCFD2CFA87A5E6, (d) Key 3: 8D6CFB3A538F493DAEDCFD2CFA87A5E8.

IV.6 Histogram

To prevent the escape of data to attackers, it's necessary to confirm that encrypted and original images don't have any applied mathematical similarities. According to statistical analysis, the representation of number of pixels in an image as a function of their intensity is termed as histogram. The cryptanalyst can get very useful information from the cipher image by analysing the image histogram. The histogram analysis can clarify how pixels in an image are distributed by plotting the number of pixels at each intensity level. If the distribution in the cipher image is close to a uniform distribution, no information can be derived from its histogram and hence, will result in better data security. The histogram of the plain image i.e. X-ray is as seen in fig.6 (a). The histogram of the cipher image obtained using single Logistic map reveals certain amount of information, particularly at the edges as in fig.6 (b). This drawback is overcome by using double Logistic map which is evident from fig. 6(c). The performance of skew Tent map is much better than the Logistic map. Both single and double skew Tent map have uniformly distributed histograms as shown in fig6 (d) and (e). The fusion map implementation, single, double and mixed all are resistive against the statically attack that is evident from the uniform histogram in fig. 6(f), (g) and (h).



(a) (b) (c) (d)

(e) (f) (g) (h)

Figure 6. Histogram of the (a) Plain Image (b) Single Logistic map (c) Double Logistic map (d) Single Skew Tent Map (e) Double Skew Tent Map, (f) Single map Fusion (g) Double map Fusion and (h) Mixed Fusion .

IV.7 Correlation Coefficient Analysis

In statistical analysis, Correlation coefficient is defined as the relationship between two adjacent pixels in vertical, horizontal and diagonal sets. For higher resistance of an image encryption system against the applied mathematical or statistical attacks, correlation coefficients of pixels within the encrypted image ought to have low values. In plain images, the correlation coefficients are close to 1, but in cipher images the coefficients should be as low as possible. The correlation coefficient of each pair is calculated by using the following formulae.

$$\mathrm{Cov}(x, y) = E(x - E(x))\, E(y - E(y)) \quad (3)$$

$$r = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)}\ \sqrt{D(y)}} \quad (4)$$

Where x and y are grey-scale values of two adjacent pixels in the image. Here E(x) is the expected value of x, D(x) is the variance of x and cov(x, y) is the covariance of x and y. The correlation coefficients are shown in Table 1. An

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

image size of 256 * 256 is considered as original (plain) image. The correlation co-efficient analysis of the cipher images obtained using various fusion implementations are listed in table 1. In fusion implementation, the correlation coefficient values were found to be very low, when compared with the existing methods [3 – 9]. Fusion implementation, correlation co-efficient analysis is much better than individual Logistic or Skew Tent map implementation.

Table 1: Correlation coefficient Analysis of all Implementations.

Image / Method	Horizontal	Vertical	Diagonal	Image / Method	Horizontal	Vertical	Diagonal
Plain Image	0.9933	0.9820	0.9758	Fusion1	0.4582	-0.0112	-0.0034
Logistic 1 map	0.0027	0.00044909	-0.00010032	Fusion2	0.0024	0.0025	-0.0021
Logistic 2 maps	-0.0040	-0.0045	0.0019	Fusion3	-0.0047	-0.0051	-0.0012
Skew Tent 1 map	0.4587	0.0029	-0.00017086	Fusion4	-0.0043	0.000052111	0.00072631
				Fusion5	-0.0043	0.000052111	0.00072631
Skew Tent 2 maps	-0.1086	-0.0036	-0.00067177	Fusion6	0.00016165	0.00075973	-0.00053909
				Fusion7	0.0024	0.0025	-0.0021

V. CONCLUSION

The proposed image encryption scheme utilizes double chaotic logistic maps with an external key of 80-bits. It also implements double chaotic skew tent maps with an external key of 128-bits. The initial conditions for both the logistic map and skew tent map are derived using the external secret key by providing weight age to its bits corresponding to their position in the key. A new image encryption algorithm is implemented which is based on the fusion/composition of the logistic and the skew tent maps. Experimental results show that the algorithm is secure against statistical and brute-force attacks. Also, it's efficient and quick enough for sensible use.

REFERENCES

[1] Kocarev Ljupco," Chaos based Cryptography: a brief overview", Circuit ans Systems Magazine, IEEE, Vol 1, Isuue 3,pp 6 -21,2001.
[2] Priya R.Sankpal and P.A.Vijaya," Image encryption using Chaotic Maps: A Survey", Fifth International Conference on Signal and Image Processing (ICSIP), pp 102-107, 2014.
[3] N.K. Pareek, Vinod Patidar, K.K. Sud, "Image encryption using chaotic logistic map", Image and Vision Computing, 24,pp 926–934,2006.
[4] Hazem Mohammad Al-Najjar, Asem Mohammad AL-Najjar," Image Encryption Algorithm Based on Logistic Map and Pixel Mapping Table".
[5] Mrinal Kanthi Mandal, Gourab Dutta Banik, Debasish Chattopadhyay and Debashis Nandi," An Image Encryption Process bassed on Chaoitc Logistic Map",IETE Technical Review, Vol 29,Issue 5, pp 395 – 404,Sept-Oct 2012.
[6] Yin Dai, Xin Wang, "Medical Image Encryption Based on a Composition of Logistic Maps and Chebyshev Maps", Proceeding of the IEEE International Conference on Information and Automation Shenyang, China, June 2012.
[7] Sarika Tyagi, Deepak chaudhary, "Adapted Encryption Algorithm with Multiple Skew Tent Map", IJCSMC, Vol. 2, Issue. 4, pp422 – 428, April 2013.
[8] Ruisong Ye and Wei Zhou," A Chaos-based Image Encryption Scheme Using 3D Skew Tent Map and Coupled Map Lattice", International Journal of Computer Network and Information Security, 1, 38-44, 2012.
[9] Ruisong Ye, Weichuang Guo," A Chaos-based Image Encryption Scheme Using Multimodal Skew Tent Maps", Journal of Emerging Trends in Computing and Information Sciences, ISSN 2079-8407, Vol. 4, No.10, October 2013.

BIOGRAPHY

Priya R. Sankpal received post graduate degree from VisVeswaraya Technological University, Belgaum in 2005. She is currently working as Assistant Professor in the Dept. of Electronics & Communication Engineering, BNM Institute of Technology, Bangalore and is pursuing research. Her areas of interest are Image Processing, Communication and Embedded Systems.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 6, June 2016

Dr. P A Vijaya obtained BE degree from MCE Hassan, ME &Ph.D from IISc Bengaluru. She is currently heading the Department of Electronics & Communication Engineering, BNM Institute of Technology, Bangalore. She has 29.5 years of teaching experience with 101 publications in reputed International Journals & Conferences. Three research scholars have obtained Ph.D degree from VTU under her guidance. She is currently guiding 4 research scholars in the area of Pattern Recognition, Image Processing & Real Time Embedded Systems.