ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

A Highly Secure Digital Image Transfer Using Chaotic Logistic Map

S.Ramya, Y.Sai Sravya, Y.Sai Likitha, M.Supraja, Brenie Sekar M.E

RMD Engineering College, Chennai, Tamilnadu, India

Department of Electronics and Communication, RMD Engineering College, Chennai, Tamilnadu, India

ABSTRACT: In today's world of information and speed it is necessary to protect the sensitive data from unauthorized access while maintaining the speed and accuracy. A new image encryption method that uses secret communication using Steganography using chaotic logistic map encryption method is proposed. The proposed method was tested for coloured images. To evaluate the performance, MATLAB Simulations are done .The experiment results shows the PSNR (Signal to Noise Ratio) of message image to extracted image is maximum and MSE (Mean Square Error) is minimum.

KEYWORDS: image encryption, chaotic, Steganography.

I. INTRODUCTION

In recent years a lot of image encryption algorithms have been proposed. The traditional encryption algorithm such as Rivest, Shamir, & Adleman (RSA), Advanced Encryption Standard(AES), and Data Encryption Standard(DES) are appropriate for text encryption but not appropriate for image encryption If encrypting image by the traditional ways, the relativity of the adjacent pixel points is very great and it is easily attacked by the statistical analysis. So the security of the system is less.

Due to the important properties of chaos signals, that includes pseudo-random, non-periodicity, robustness and high sensitive to system parameters and initial conditions, combining cryptography with chaotic theory is considered one of the important fields in information security. The chaos based encryption algorithm paves a new efficient way to develop images security systems that satisfy the demand of highly secure image transmission over the communication channel.

In [1], a novel image encryption scheme based on image is diffused with bitwise exclusive-OR operation is performed. Here chaos are introduced. In [2], a novel algorithm for image encryption based on logistic chaotic map with modifying parameter is proposed. The plain image is shuffled by using modified parameter of logistic map, and then the shuffled image is encrypted by using dynamical algorithm.[8],a novel algorithm that proposes to use Arnold map is used. [10], a colour image is extracted into RGB plain image and it is encrypted separately.

Now an improved method is proposed. The grey image is obtained from a colour image, which is then encrypted to separate R, G and B plane. Then they are combined to obtain a cipher image is covered with a support image and there LSB substitution method is used to obtain final Stego image.

II. THE PROPOSED ALGORITHM

The chaos-based image encryption is introduced for the purpose of attaining high diffusion and to transfer secured images. The secret key is used to process the encryption and decryption.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

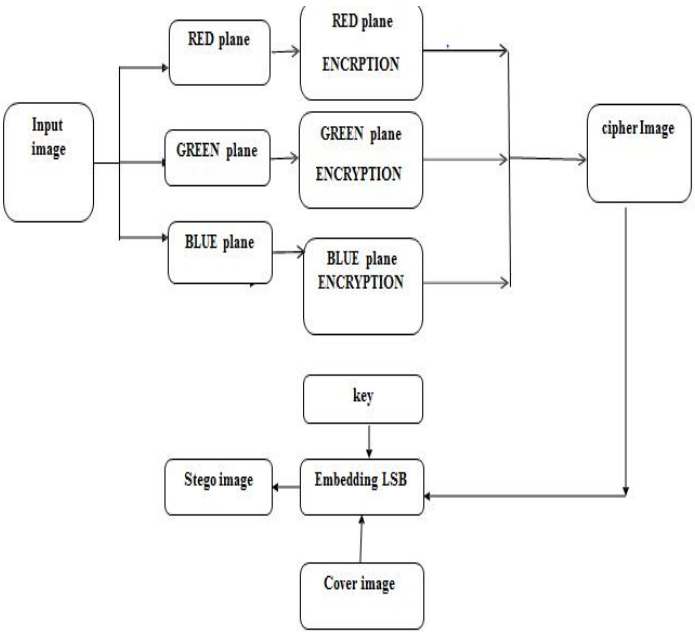
Vol. 8, Issue 3, March 2019

This paper is about use of chaotic maps and LSB substitution method. The level of security increases by using both the keys. The proposed algorithm produces cipher image after the encryption. This cipher image is secured with a key. The cover image is used to hide the cipher image using another key using LSB substitution method.

I. Encryption process:

In the encryption process, firstly divide the image into the Blocks, split that image into R, G and B planes based on secret key matrix. Later perform XOR image R with chaos key matrix. Repeat with the other two planes. By merging all the three planes, cipher image is obtained. This cipher image is hidden with another image called cover image. This is done by using LSB substitution key. Lastly, the stego image is obtained.

Encryption:



language. The outputs are based on proposed method. FIGURE 1 is the original message to be transmitted following the encryption process Figs. 2. The decryption process can be observed in Figs. 3.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

a)original image

FIG 2(a) R,G and B planes

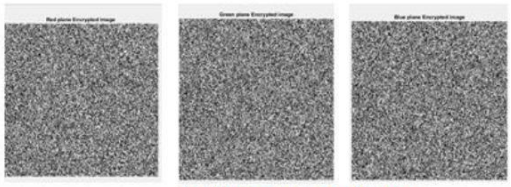


Fig 2(b)Encrypted R, G and B planes

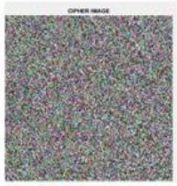


Fig 2(c) cipher image

Fig 2(d) support image

Fig 2(e) stego image

The reverse process of encryption is decryption process. In this method the stego image is decrypted using LSB key used in encryption method. The extracted image is divided into R, G and B planes with the help of chaotic key matrix. Finally, original image is obtained.

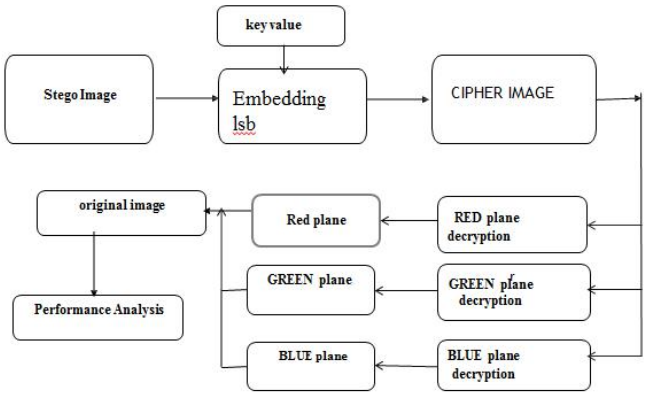
ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019



III. ALGORITHM

The algorithm proposed was implemented in MATLAB with the use of JAVA programming

Image encryption steps are as follows:

Step 1: Scan the first plain image I (i, j), and kind the first pixel knowledge matrix X.
Step 2: Set initial parameter values of $_0$ and μ in supply chaotic mapping and procedure the one-dimensional supply sequence. Convert the one-dimensional vector into a second sub-chaotic matrix.

Step 3: Set initial parameter values consequently for one more chaotic map (Tent, Singer, Piecewise, Chebysev or Sine) acquire another one-dimensional sequence of separate values. Convert the sequence into a second matrix, which forms another sub-chaotic matrix.

Step 4: Mix the sub-chaotic matrices to get the chaotic encoding matrix.

Step 5: Perform XOR operation on the first knowledge matrix X and also the final encoding matrix CM to get the ultimate encrypted image matrix.

Image decryption steps as follows

Step 6: Get the transmitted encrypted matrix EEC, and also the initial conditions and management parameters for the chaotic maps utilized in encoding.

Step 7: Generate the sub-chaotic matrix victimisation the initial conditions of supplying mapping.

Step 8: Generate the sub-chaotic matrix victimisation the initial conditions of another mapping.

Step 9: Mix the sub-chaotic matrices to get chaotic encrypted matrix.

Step 10: Perform XOR operation on the obtained encrypted matrix EEC and also the final encoding matrix CM to get the decrypted image.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

Steps involved in Cipher image hiding

Step1	Choose the quilt image 'C' that had regenerate by victimization MATLAB code.
Step 2	Convert the image 'C' into unsigned number format (uint8) and divide the quilt image into Red (R), inexperienced (G) and Blue (B) parts.
Step 3	Choose the quantity of input bits 'n' to be substituted in 'C'.
Step 4	Now, do the logic AND operation to the quantity of bits in R part of 'C' and substituted 'n' bits.
Step 5	Then do the bit OR operation to the output of on top of step and therefore the entire shifted message bits with 'n' bits.
Step 6	Repeat an equivalent for inexperienced and blue parts conjointly
Step 7	Do an equivalent method for all the chosen images and convert R, G and B parts into stego frame then when reconstruct all the frames into stego image, during which the message info has been embedded.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

Figure 3:

Fig 3(a) stego image

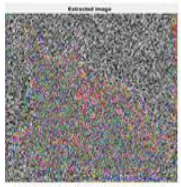


Fig 3(b) extracted image

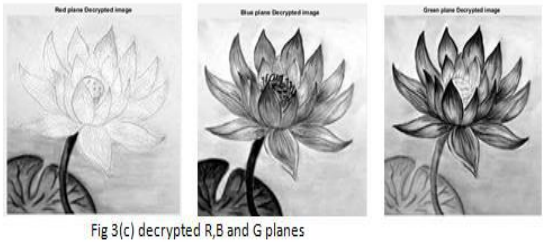


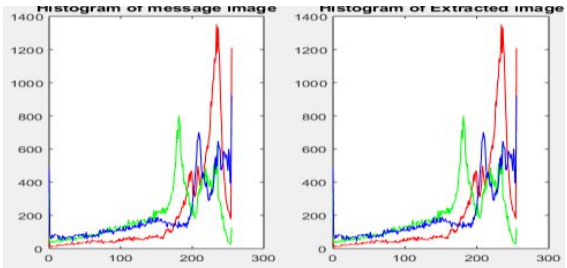
Fig 3(c) decrypted R,B and G planes

Fig3(d) decrypted original image

IV. PERFORMANCE ANALYSIS: A. HISTOGRAM

The original image histograms Fig.1 and the

matching encryption image is observed in Figure 3(d) and also histograms Figure 2(c) and Figure 2(e). As per the observation, the pixel values of the original image are high on certain values. Likewise, the histogram of encryption image appears to be highly uniform. This implies that features of the original image during the process of encryption will not be destructed.



The histogram of the cipher and stego image is based on LSB substitution method. The histogram of the stego-image is considered as high embedding capacity, robust to histogram attack and visual image quality. The histogram of the cipher-image appears to be uniform and shows a significant difference in comparison to the original image. The histogram of cipher-image R, G, and B components becomes uniform following the encryption. The histogram of cipher and stego image is

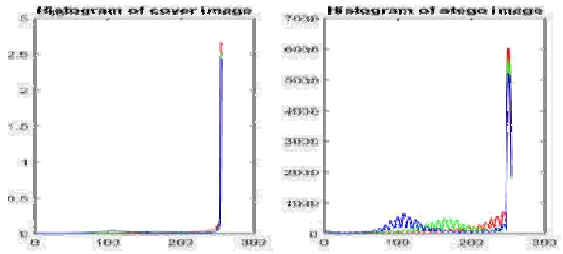
ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019



B.PSNR and MSE:

PSNR is the ratio between maximum power of signal to power of noise. It is described in logarithmic decibel scale.

It is mainly expressed in terms of MSE. A noise free mxn image I with noise approximation K,

MSE= $^{1}\sum_{=0}^{-1}\sum_{=0}^{-1}[(,)-(,)]$ PSNR=10.log10(^{2})

M= maximum pixel value of image. Generally, the obtained image after the decryption must have the high PSNR and low MSE. As per the results from above figure 2 and 3,

PSNR is about 67.925 and MSE is about 0.01. Average PSNR and MSE values for different images

FIGURE	PSNR	MSE
1	89.89	6. xe-5
2	88.13	9x e-5
3	91.14	4.8x e-5
4	91.13	4.8x $^{-5}$
5	88.13	9.6 xe-5
6	75.05	1.6x e-5
7	88.92	8x e-5

IV. CONCLUSION

A multi-chaos-based image encryption algorithm has been proposed in this paper. PFA algorithm is used to obtain a robust image for encryption and decryption process. Since, it increase the security and the efficiency of encryption and decryption process, the proposed method holds good. Several experiments were executed to demonstrate the security and dependability of the proposed algorithm for encryption image. This experiment includes the analysis of histogram, PSNR and MSE.

REFERENCES

[1] L. Xiangyu, L. Qiuyang, and S. Chandel, "Social Engineering and Insider Threats," 2017 International Conference on Cyber- Enabled Distributed Computing and Knowledge Discovery (CyberC), 2017.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijareeie.com

Vol. 8, Issue 3, March 2019

[2] L. Chunil and L. Donghui, "Computer network security issues and countermeasures", 2012 IEEE Symposium on Robotics and Applications(ISRA), 2012.
[3] C. Naveen, T. V. S. Gupta, V. R. Satpute, and A. S. Gandhi, "A simple and efficient approach for medical image security using chaos on EZW," 2015 Eighth International Conference on Advances in Pattern Recognition (ICAPR), 2015.
[4] Y. Lou and T. Hu, "A novel image security system based on cellular automata and improved chaotic system," 2012 5th International Congress on Image and Signal Processing, 2012.
[5] P. R. Sankpal and P. A. Vijaya, "Image Encryption Using Chaotic Maps: A Survey," 2014 Fifth International Conference on Signal and Image Processing, 2014.
[6] M.S. Baptista, Cryptography with chaos, Physics Letters A 240 (1998) 50–54.
[7] Z. Kotulski, J. Szczepanski, Discrete chaotic cryptography (DCC): New method for secure communication, in: Proceedings of NEEDS'97, 1997.
[8] R. Matthews, The derivation of a chaotic encryption algorithm, Cryptologia XII (1) (1989) 29–42.
[9] T. Xiang, K.W. Wong, X.F. Liao, An improved chaotic cryptosystem with external key, Communications in Nonlinear Science and Numerical Simulation 13 (9) (2008) 1879–1887.
[10] Z. Kotulski, J. Szczepanski, K. Gorski, Z. Paszkiewicz, A. Zugaj, Application of discrete chaotic dynamical systems in cryptography– DCC method, International Journal of Bifurcation and Chaos 9 (1999) 1121–1135.
[11] E. Alvarez, A. Fernandez, G.P. Jimenez, A. Marcano, New approach to chaotic encryption, Physics Letters A 263 (1999) 373–375.
[12] W.K. Wong, L.P. Lee, K.W. Wong, A modified chaotic cryptographic method, Computer Physics Communications 138 (2000) 234–236.
[13] K.W. Wong, A fast chaotic cryptography scheme with dynamic look-up table, Physics Letters A 298 (2002) 238–242.
[14] M.K. Khan, J. Zhang, Multimodal face and fingerprint biometrics authentication on space-limited tokens, Neurocomputing 71 (13–15) (2008) 3026–3031.
[15] N.K. Pareek, V. Patidar, K.K. Sud, Discrete chaotic cryptography using external key, Physics Letters A 309 (2003) 75–82
[16] Sankpal PR, Vijaya PA. Image encryption using chaotic maps: a survey. InSignal and Image Processing (ICSIP), 2014 Fifth International Conference on 2014 Jan 8 (pp. 102-107). IEEE.
[17] Ephin M, Joy JA, Vasanthi NA. Survey of Chaos based Image encryption and decryption techniques. InAmrita International Conference of omen in Computing (AICWIC'13) Proceedings published by International Journal of Computer Applications (IJCA) 2013.
[18] A. Akhshani, S. Behnia, A. Akhavan, H. Abu Hassan, Z. Hassan, Optics Communications 283 (17) (2010) 3259.
[19] Yoon Ji Won, Kim Hyoungshick,Communications in Nonlinear Science and Numerical Simulation 15 (12) (2010) 3998.
[20] Yang Tang, Zidong Wang, Jian-an Fang,Communications in Nonlinear Science andNumerical Simulation 15 (9) (2010) 245.
[21] Mao YB, Chen GR, Lian SG. A novel fast image encryption scheme based on 3D chaotic baker maps. Int J Bifurc Chaos 2004;14(10):3613– 24.
[22] A. Akhavan, A. Samsudin, A. Akhshani,"Cryptanalysis of an image encryption algorithm based on DNA encoding", Optics & Laser Technology, vol. 95, pp.94-99, 2017.