INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE

ISSN: 2057-5688

A HYBRID IMAGE ENCRYPTION IN DATA SECURITY SYSTEM BASED ON CHOATIC MAP

CH.ANUSHA[1], SK.MUNWAR ALI[2]

[1]PG Scholar, Dept of E.C.E, Eswar College Of Engineering, Narasaraopet, Palnadu Dt.

[2]Asst Professor, Dept Of E.C.E, Eswar College Of Engineering, Narasaraopet, Palnadu Dt.

ABSTRACT: Traditional permutation encryption algorithm is not robustness for noise disturbing and shears transformation attacks. In order to ameliorate the security of image encryption algorithm, we present an image encryption algorithm based on location transformation. The algorithm permute image based on chaotic system and storage everyone pixel of the image in multi-place, this encrypted image is robustness for noise disturbing and shear transformation attack. An extended magic square matrix-generating algorithm is also presented and it improves on the efficiency of the magic square matrix-generating algorithm. The simulation results show that the effect of decrypting image is good when the encrypting image is modified by noise disturbing and shear transformation attack

KEY WORDS: chaotic theory, image encryption, logistic map, combined chaotic system

1. INTRODUCTION: Now a day it is possible for anyone to transform digital information easily. Several security problems, which are associated with the development of digital signal transmission over an open network, are rising up. Many of application, such as medical image system, personal online photograph album, have strong demand for providing security in digital signal transmission.

During the last decade, researcher have proposed various types of efficient and robust encryption algorithms based on different principles [1-6]. Chaos based encryption is one of these efficient techniques due to its unique properties, such as the sensitive dependence on initial conditions and system parameters i.e. a tiny change of the initial input values leads to a great different of the output, unpredictable and its random-like properties, which are satisfied the requirements of cryptography [7, 8]. Especially, chaotic systems based image ciphers are very popular with the researchers as a good solution to image encryption in the past few years [9-11]. However, since the chaotic maps become more familiar to the public and the key space is small, there exists some weakness in security. As long as a little priori information, it has a possible way to predict some behaviors of traditional chaotic systems under some circumstances. In other words, it may provide privileged services to an attacker by estimating the parameters and initial values in a chaotic system based image cipher

Images have become popular with users for communication. Users often send sensitive pics each other over the internet. However,

ISSN: 2057-5688

the attackers can eavesdrop on their communication and see the images being transmitting. Encryption is the technique using which users can "hide" their original image. In Image encryption, users have to encrypt the image using a secret key and send the encrypted image or cipher image to the intended user. The receiver can then use the secret key to decrypt the image. This is possible due to image encryption and decryption. Chaos theory is a branch of mathematics that deals with non-linear dynamic systems. The systems are considered non-linear because of the multiple feedback between the components of the system. The systems are considered as dynamic because of the changes shown by it due to its current state. Such system often formed is known as chaotic maps. Chaotic map have high sensitivity to their initial values and control parameters, chaotic property, non-convergence, and state periodicity.

2. CURRENT SYSTEM

Cryptography includes changing over message content into an incoherent figure. Then again, steganography implants message into a spread media and conceals its reality. Both these methods give some security of information neither of only them is secure enough for sharing data over an unbound correspondence channel and are helpless against gatecrasher assaults. In this paper we propose a propelled arrangement of scrambling information that joins the highlights of cryptography, steganography alongside mixed media information stowing away. This framework will be more secure than some other these procedures alone and furthermore when contrasted with steganography and cryptography joined frameworks.

a). Encryption Algorithm: The message will initially be scrambled utilizing Asymmetric Key Cryptography system. The information will be encoded utilizing essential DES calculation. This figure will presently be covered up into a sight and sound record. The figure will be spared in the picture utilizing an altered piece encoding strategy by truncating the pixel esteems to the closest zero digit (or a predefined digit) and afterward a particular number which characterizes the 3-D portrayal of the character in the figure code arrangement can be added to this number. For each character in the message a particular change will be made in the RGB estimations of a pixel. (This change ought to be under 5 for each of R,G and B esteems) This deviation from the first worth will be novel for each character of the message. This deviation likewise relies upon the particular information square (lattice) chose from the reference database. For every byte in the information one pixel will be altered. In this way one byte of information will be put away per pixel in the picture. In this strategy the figure arrangement can be decoded without the first picture and just the altered picture will be transmitted to the collector. In the initial couple of lines of picture properties, the qualities of the picture will be encoded and spared in order to give

ISSN: 2057-5688

us the data if the picture is altered or adjusted or the picture augmentation has been changed like jpg to gif. These properties can be utilized in the translating (distinguishing the right square of information from the information lattice). So just the right encoded picture in the right arrangement will deliver the sent message. For unscrambling, the beneficiary must realize which picture to decipher and in which arrangement as changing the picture configuration changes the shading dispersion of the picture. Each picture gives an irregular information on decoding that has no significance. Yet, just the right organization unscrambling gives the first message. In the wake of concealing the information in the picture, the picture will be sent to the collector. The recipient ought to have the unscrambling key (private key) which will be utilized to interpret the information.

2. Unscrambling Algorithm: The message can be decoded utilizing a backwards work (as utilized in customary strategies) utilizing the recipient's private key. This key can be a piece of the picture or content or any trait of the picture. The beneficiary's private key is utilized to distinguish the reference framework from the reference database. Subsequent to choosing the right matrix, the x and y part of the picture can characterize the square that has been utilized to encode the message and the RGB esteems can point to the information in the square distinguished by the x, y segment. The figure is recovered by getting the distinction in the pixel esteem from the nearest predefined esteem (zero truncation). These numbers will currently characterize the spared bit and will shape the figure content. This figure would now be able to be unscrambled utilizing a backwards capacity of the DEA calculation to get the message content.

MERITS

- We can hide text data in any image.
- Easy to handle.

DEMERITS

- Easy to hack.
- Computational complexity was high.

3. PROPOSED SYSTEM

In the image encryption scheme which uses chaotic maps, usually chaotic map are used to generate the keys or actual values using which the pixels or bits of the image is encrypted. The user can specify the initial conditions of the chaotic map which then generates the string or number of characters required to encrypt the full image. The other part of the scheme would deal with the encryption and decryption of the image just like any other encryption scheme. However, it is important to note that users have to keep the initial condition as a secret to ensure that the attacker doesn't decrypt your encrypted images. In this project, we used 2 chaotic maps: Piecewise linear chaotic map (PWLCM) and Logistic-Tent map.

- Piecewise linear chaotic map (PWLCM)

ISSN: 2057-5688

- Piecewise linear chaotic map

Where the value of p is the interval (0,0.5) and initial value of x should be in the interval (0,1). The users can specify the values of p and x which serves as the secret key. Using these initial values, required length of key stream can be calculated. PWLCM has a uniform invariant distribution and very good ergodicity, confusion, and determinacy, so it can provide excellent random sequence, which is suitable for information encryption.

i) Logistic-Tent Map

Individually both the maps have mainly 2 problems: First, its chaotic range is limited only within, Even within this range, there are some parameters which make the Logistic map to have no chaotic behaviours. This is verified by the blank zone in its bifurcation diagram. A positive value of Lyapunov Exponent means that the chaotic map has a good chaotic property. However, for r < 3.57, the exponent is less than zero. Second, the data range is smaller than [0,1] thus the values generated are not uniform and hence not really suitable for generating pseudo-random sequences.

ii) Encryption Scheme:

1) Before we begin the encryption scheme, we need to create the bit stream to encrypt the image from the chaotic map: PWLCM. The user needs to specify to initial parameters (u0,x0) to generate the bit stream from the chaotic map. Once the bit stream is generated, then we need to make sure that values are between 0 and 255 so we use this equation:

Let's assume that the size of the image is M x N. Then we need to iterate (M x N + N0) number of values. We discard the initial N0 to avoid any bad values in the stream.

Once we have the values in integer, we decompose them into bit planes. We need 8 bit planes namely, b1, b2,b3,b4,b5,b6,b7 and b8. We need to combine these bit planes into 2 groups as b1 and b2, putting higher bit planes in one group and lower bit planes in another.

2) We read the image and decompose into bit planes and form 2 groups A1 and A2.

iii) Diffusion phase:

•Calculate the sum of elements in A2. Number of elements in A2 is L = 4MN.

•Cycle shift A2 by the sum to obtain A11.

•Encrypt the first element of A11 with last element of A11, first element of A2 and b1 using this equation:

•Change the value of i =2 till L to encrypt the matrix A11 using following equation:

•Use the same method to encrypt the A2.

- Calculate the sum of elements in B2 and cycle shift right the matrix A2 to get A22
- Use the following equation to encrypt the first element of A22.
- Change the value of i=2 till L to encrypt A22 using the following equation:

iv) Confusion Phase:

- Calculate the sum of elements of B1 and B2 to obtain the initial value to obtain bitstream from the chaotic map PWLCM:

ISSN: 2057-5688

•Using the obtain 2 sequences Y and Z, using Y(i), we swap the values of B1(i) with B2(Y(i)) and we swap the values of B2(i) with B1(Z(i)) for all values of i from 1 to L
•Finally, combine the bitplanes back to the image which gives the cipher/encrypted image.

v) Decryption scheme

The decryption process is just the reverse process of encryption process. Suppose the decrypted image is D image. Then its size is (m, n) . For gray value of every pixel in D image, consider the encrypted image may be attacked, so we may reconvert k × l different values for one pixel. In our decryption algorithm, we choose the median of the k × l different values as the gray value of every decrypted pixel. In order to farther improve the decryption process's capability of anti-jamming. We can process the
•Decryption process is the reverse of the encryption.
•Using the key to obtain the sequences Y and Z using which reverse-swap the values.
• In diffusion phase, one has to solve the equation using cross-multiplication method to obtain the original image.

4. SECURITY ANALYSIS

a) Key sensitivity

In key sensitivity, analysis is done to check if image can be decrypted when the attacker has all the key except one bit value changed. To do this analysis, key is taken and an image is encrypted. Then the value of the key or more specifically, one bit from the bit stream used to encrypt is changed and an image is encrypted again. Now, both the images are compared. Ideally, there should not be any match between these 2 images. If there is a high percentage of match between the images, then it has failed this analysis.
This same analysis is also done in the decryption process, where the one bit of the decryption key is changed and output images are compared to see if there is any match.

b) Histogram analysis

In the histogram analysis, we obtain the histogram of the image which gives the intensity of the image over a spectrum. We check the histogram of the encrypted image to ensure that it is uniform the spectrum to avoid the attacker decrypting the image

5. RESULTS

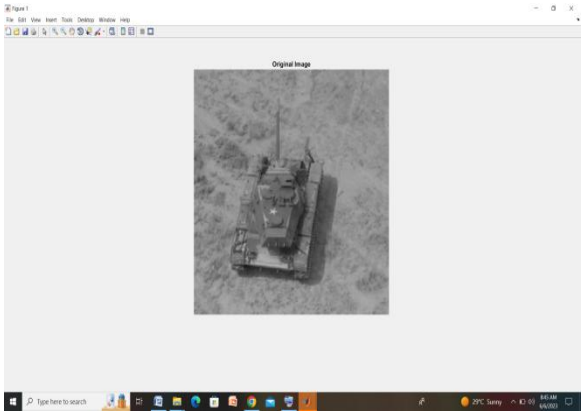

Fig 5.1 : input image

INTERNATIONAL JOURNAL OF TECHNO-ENGINEERING
IJTE
ISSN: 2057-5688

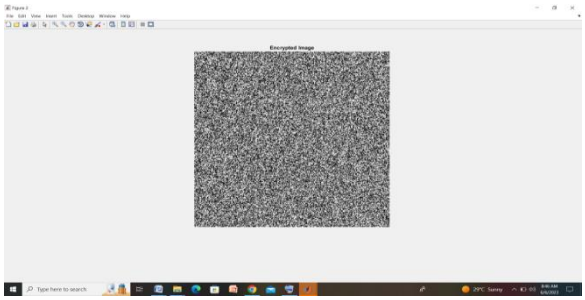

Fig 5.2 : encrypted image using Chaotic System

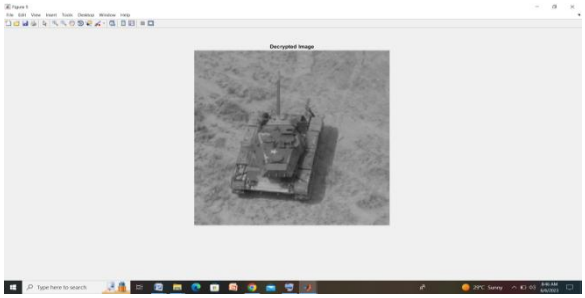

Fig 5.3: decrypted output

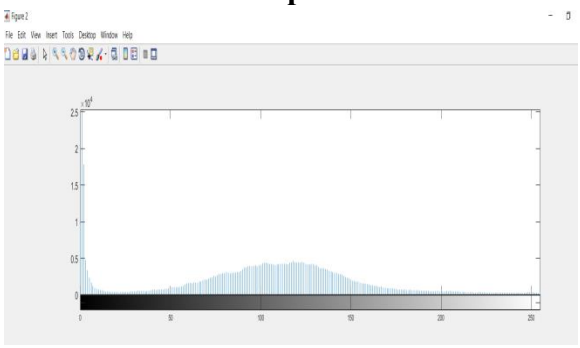

Fig (a) input image **histogram**

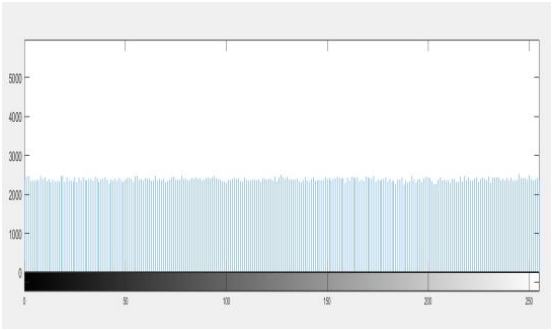

Fig (b) output image **histogram**

Fig 5.4: Performance Analysis by Using Histogram Analysis

6. CONCLUSION

An effective image encryption algorithm with two independent chaotic functions allowing parallel computing is presented to enhance the diffusion and confusion functions. For low entropy plain images, which maintain their properties throughout many encryption rounds, a second chaotic function is incorporated to generate random numbers exploited together with exclusive-or operations for perturbing the integrity of such images even in first round. To increase the resistance encrypted system

REFERENCE

[1]N. A. Saleh, H. N. Boghdad, S. I. Shaheen, A. M. Darwish, "High Capacity Lossless Data Embedding Technique for Palette Images Based on Histogram Analysis," Digital Signal Processing, 20, pp. 1629−1636, 2010.

[2] J. Tian, "Reversible Data Embedding Using a Difference Expansion," IEEE Trans. on Circuits and Systems for Video Technology, 13(8), pp. 890−896, 2003.

ISSN: 2057-5688

[3] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible Data Hiding," IEEE Trans. on Circuits and Systems for Video Technology, 16(3), pp. 354−362, 2006.

[4] M. U. Celik, G. Sharma, A. M. Tekalp, and E. Saber, "Lossless Generalized-LSB Data Embedding," IEEE Trans. on Image Processing,

[5] X. Hu, W. Zhang, X. Li, and N. Yu, "Minimum Rate Prediction and Optimized Histograms Modification for Reversible Data Hiding," IEEE Trans. on Information Forensics and Security, 10(3), pp. 653-664, 2015.

[6] X. Zhang, "Reversible Data Hiding with Optimal Value Transfer," IEEE Trans. on Multimedia, 15(2), 316−325, 2013.

[7] W. Zhang, X. Hu, X. Li, and N. Yu, "Optimal Transition Probability of Reversible Data Hiding for General Distortion Metrics and Its Applications," IEEE Trans. on Image Processing, 24(1), pp. 294-304, 2015.

[8] S. Lian, Z. Liu, Z. Ren, and H. Wang, "Commutative Encryption and Watermarking in Video Compression," IEEE Trans. on Circuits and Systems for Video Technology, 17(6), pp. 774−778, 2007.

[9] M. Cancellaro, F. Battisti, M. Carli, G. Boato, F. G. B. Natale, and A. Neri, "A Commutative Digital Image Watermarking and Encryption Method in the Tree Structured Haar Transform Domain," Signal Processing: Image Communication, 26(1), pp. 1−12, 2011.

[10] X. Zhang, "Commutative Reversible Data Hiding and Encryption," Security and Communication Networks, 6, pp. 1396−1403, 2013.

[11] X. Zhang, "Reversible Data Hiding in Encrypted Image," IEEE Signal Processing Letters, 18(4), pp. 255−258, 2011.

[12] W. Hong, T.-S.Chen, and H.-Y. Wu, "An Improved Reversible Data Hiding in Encrypted Images Using Side Match," IEEE Signal Processing Letters, 19(4), pp. 199−202, 2012.