International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
ISSN: 2457-0362
www.ijarst.in

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

Dr. Sudhakar K[1], Akshadaw[2], Bhargavi[2], Sathwika Sri[2], G. Mounika[2]

[1]Professor & Head, [2]UG Student, [1,2]Department of Electronics and Communication Engineering
[1,2]Malla Reddy Engineering College for Women, Maisammaguda, Hyderabad, Telangana, India

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, 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 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

Procedures for The results of the simulation demonstrate that the data included found in the matching decrypted picture is lost when either noise disrupting or shear transformation are employed to assault the encrypted image. Which indicates that the aforementioned permutation transform lacks resistance to noise disturbance nor shear transformation attacks. To address this issue and strengthen the previously mentioned picture encryption scheme, we offer the following solution. To begin, we are going to provide a quick summary of what integer wavelet transform is and how it works. Second, we'll explain the suggested encryption method.

3.1 Image Encryption:

We'll pretend the uncompressed picture has dimensions of N1XN2, and that every pixel's gray value is conveyed by 8 bits (ranging from 0 to 255). In this notation, the bits of a pixel are represented by bi,j,0,bi,j,1,...,bi,j,7, the gray value by, and the total number of pixels by N(N=N1XN2).So, that means Bits are encrypted by first calculating the exclusive-or of the original bits using a set of pseudo-random bits. Using encrypted picture is made using the stream cipher algorithm, which is:

$$[[f]] = \text{Enc}(f, K) = f \oplus K$$

Where f is the unencrypted picture and [[f]] is the encrypted version. Here, K represents a key stream encrypted through the key K.

3.2 DWT –SVD TECHNOLOGY

Utilizing DWT, DCT, and SVD on both the cover and hidden images, this study employs a watermark approach to accomplish watermarking.

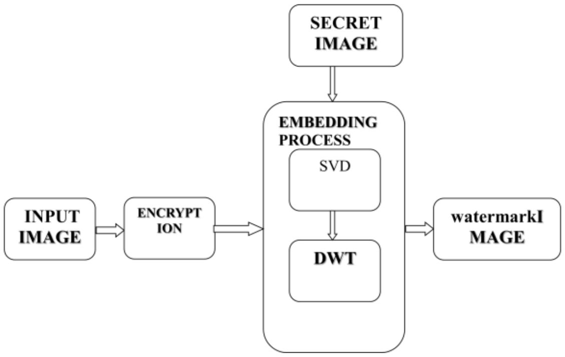

Fig 3.1 : Watermark Embedding Procedure.

Hide information throughout the wavelet domain's high-resolution detail bands (HL, LH, and HH), which the human visual system (HVS) are less sensitive to, and in doing so improve robustness without sacrificing visual quality. Taking one integer data set and transforming it into a different one, that's what integer wavelet transform does. After applying the DWT transformation on the cover photo, we receive the LL, LH, HL, and HH coefficients. The component with higher frequencies has been extracted and will be re-DWT transformed. This yields the LL1, LH1, HL1, and HH1 coefficients. The DCT function is subsequently applied to the cosine of the highest frequency component after this additional modification. The pre-processing involves taking a secret picture that is one-fourth the size that the cover image and then dividing it into a diagonal matrix & two orthogonal unitary non-negative matrices U and V. The dimensions of each of these matrices is identical to that of the hidden picture. The recovered secret picture undergoes a series of discrete cosine changes. The matrices U, V, and are each subjected to their own individual cosine transformations. Both the cover picture and the hidden image have the same size and class after being cosine converted. The sections of the picture both belong to identical class, making it simple to embed a hidden image inside the main image. Since the human visual system is not particularly sensitive to elevated frequency content in a cover picture, the altered secret image may be substituted there. The cover picture is broadcast over a long distance after undergoing all inverse changes necessary to render it visible. During the decoding process, a DWT tree is employed to isolate the high-frequency components of the watermark picture, and then the cosine transform was used to eliminate the encrypted data. The filtered value, expressed as a Singular value decomposition, undergoes an inverse cosine transformation, while the resulting values have been multiplied according with the formula.

$$A_{nxp}= U_{nxn}\, S_{nxp}\, V^{T}_{pxp}$$

3.3 DATA EXTRACTION AND IMAGE DECRYPTION

when the collector has the information concealing key and has obtained a scrambled image containing the additional data, he can decode the LSB layers using wet paper coding to determine the k-th LSB about encoded pixels. However, if the receiver has the cryptosystem's private key, they may execute unscrambling to get the initial plaintext image.

3.4) 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

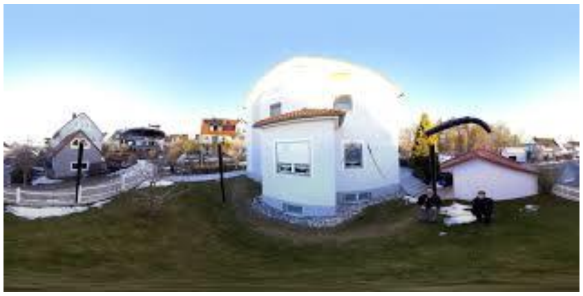

Fig 5.1 : Cover image

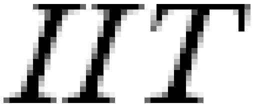

Fig 5.2: Secret Image

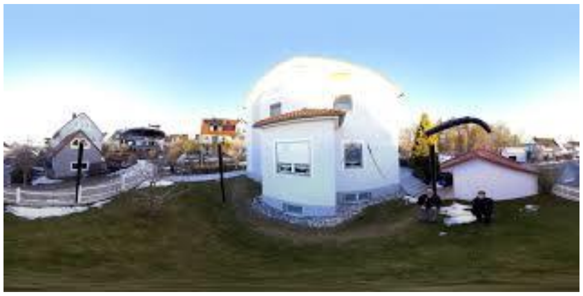

Fig 5.2 : encrypted image using Chaotic System

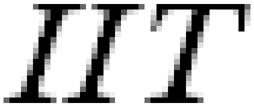

Fig 5.3: decrypted output

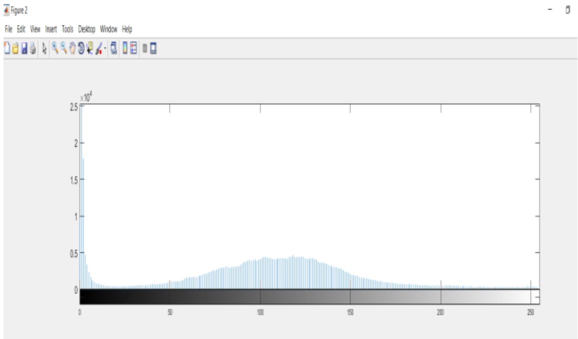

Fig (a) input image **histogram**

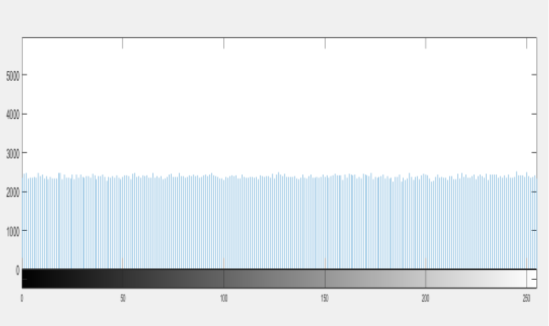

Fig (b) output image **histogram**

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.

[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.