AN ACUTE METHOD OF ENCRYPTION & DECRYPTION BY USING HISTOGRAMS AND CHEAT IMAGES

Ashish Kumar Singh ,Madan Kushwaha , Abhishek Kumar

[1]*Assistant Professor, Department of CS&A,, Krishna Institute of Technology ,Kanpur Uttar Pradesh, India*

[2,3]*Assistant Professor, Department of CSE, Bansal Institute of Engineering & Technology, Uttar Pradesh, India*

---***---

Abstract - *Images are different from textual data in many aspects such as highly redundancy and correlation, the local structure and the characteristics of the amplitude-frequency. The conventional encryption techniques can not applied to the images. As a result, image encryption came into play to perform cryptographic operations on images. In recent years, lots of work did in this area. In this paper, we propose an image encryption technique based on logistic map and cheat image. Cheat images used in this technique are the images selected from the public network together with the chaotic matrices generated by the logistic map. Encryption and Decryption, both processes require the cheat image to perform their task. The proposed encryption technique is secure and robust enough in practical communication from the view point of the computer experiments such as cheat characteristic analysis, differential attack analysis, sensitive analysis and statistical analysis.*

Key Words: Image Encryption, Logistic Map, Cryptography, Cheat Image.

1.INTRODUCTION

By the rapid development of the Networking systems allowed large files such as digital images to be easily transfers over the network. And for this reason, there is a need for Image Cryptography. Image cryptography consists of encryption and decryption of images. Color Image is basically consists of pixels which measure the intensity and chrominance of light. The brightness information in each spectral band is the actual information stored in digital image data. Pixel values are correlated with the neighboring pixels. One may easily guess the value of pixels from the neighboring pixel values.

Information hiding and Encryption are generally two approaches which are used to protect digital images. Information hiding usually uses watermarking, steganography, anonymity and cover channel whereas encryption includes conventional encryption and others such as chaotic encryption [1]. Ergodicity, mixing property and sensitivity to initial conditions/system parameters are some fundamental properties of chaotic system, are analogous to some ideal cryptographic properties i.e. confusion, diffusion, balance and avalanche properties. Chaos-based cryptosystem has two iterative stages, In the confusion stage, pixels are permuted but the values of pixels are unchanged whereas in diffusion stage, the pixel values are modified sequentially so that a tiny change in one pixel is spread out to many pixels, hopefully the whole image [2].

There are n permutation rounds in the confusion stage with n>=1 are required to decorrelate the relationship between adjacent pixels. To achieve a satisfactory level of security, the whole confusion-diffusion rounds are repeated for a number of times. Chaotic maps parameters governing the permutation and the diffusion should better be different in different rounds. Round key generator with a seed secret key as input are used to achieve it

In this proposed scheme, we used the cheat image for the encryption and decryption process. Cheat image are the images selected from the public network.

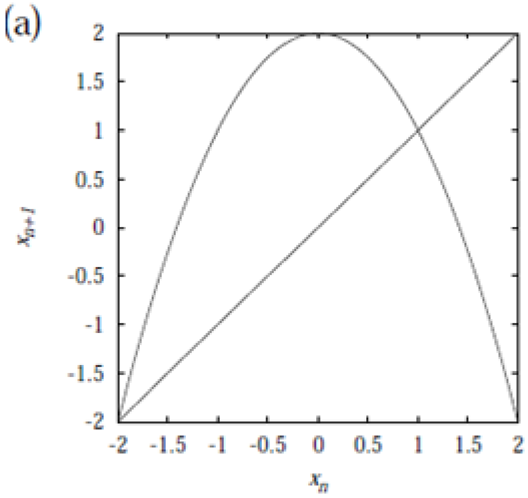
1.1 LOGISTIC MAP-

The Logistic Map

$$X_{n+1}=a-x_n^2$$

(2.1)

is the simplest one-dimensional map displaying a singularity which depends on a single parameter a[3]. Each value in the range of the map ‘f’ has exactly two preimages, which will prove to be a key ingredient to generate chaos. This most important consequences of the singularity located at x=0 is shown from its graph [fig 2.1(a)].



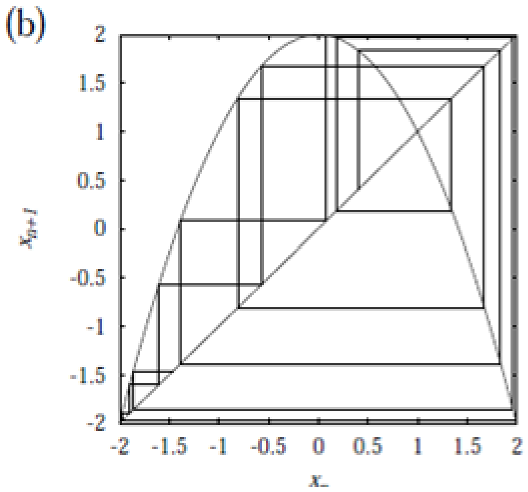


Figure 2.1: (a) Graph of the logistic map for a=2. (b) Graphical representation of the iteration of (2.1).

As in the iteration (2.1), the action of the logistic map is represented algebraically; it's also represented geometrically as in [fig 2.1(b)]. Logistic map displayed the various behavior which are easily explored as this map depends on a single parameter a. Two main types of dynamical regimes can be observed: "stationary or periodic" regimes and "chaotic" regimes. A finite set of different values that are forever repeated in fixed order are eventually visited by the iterations in the first case. In the latter case, the state of the system seemingly evolves in a disorder way and never repeats itself exactly.

The logistic map is not only that the organization in parameter space of these periodic and chaotic regimes can be completely understood with simple tools, but that despite of its simplicity it displays the most important features of low-dimensional chaotic behavior.

1.2 CONFUSION AND DIFFUSION

Claude Shannon in his paper "Communication Theory of Secrecy Systems", published in 1949, identified that confusion and diffusion are two properties of the operation of a secure cipher. Confusion and Diffusion are two main properties of an ideal cryptosystem. Confusion makes the relationship between the plaintext and the cipher texts as complex as involved as possible; diffusion has the property that the redundancy in the statistics of the plaintext is DISSIPATED in the statistics of the cipher text. In a cipher with good diffusion, cipher text changed completely in an unpredictable or pseudorandom manner if we change the one bit of the plain text. The strict avalanche criterion states that if we chose the i^{th} bit randomly from the input and flips it, then the probability that the j^{th} bit of output will be changed should be one half, for any i and j. Cipher text is depend on the entire key and in different ways on different bits of the key. In particular, if we change the single bit of the key, cipher text changed completely. Correlation is reduced between the plaintext and cipher text in the confusion whereas the data located at some coordinates of the input block are transposed to the other coordinates of the output block in diffusion.

2. PROPOSED WORK

Selection of the platform, the language used etc. is the important considerations in the implementation of any software. The major implementation decisions that have been made before the implementation of this project are as follows-

a) Selection of the platform (operating system).
b) Selection of the programming language for development of the application.
c) Coding guidelines to be followed.

Matlab (Matrix Laboratory), a fourth generation programming language developed by MathWorks is a numerical computing environment. It allows matrix manipulations, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs written in other lamguages, including Fortan, C and C++ [4].

2.1 Permutation

In this process, we perform the permutation process on input image and cheat image. We take the initial parameter to perform the permutation task. These initial parameters are used as a secret key to perform the permutation process on the input image and cheat image. Both input and cheat image are permutated using pixel permutation approach.

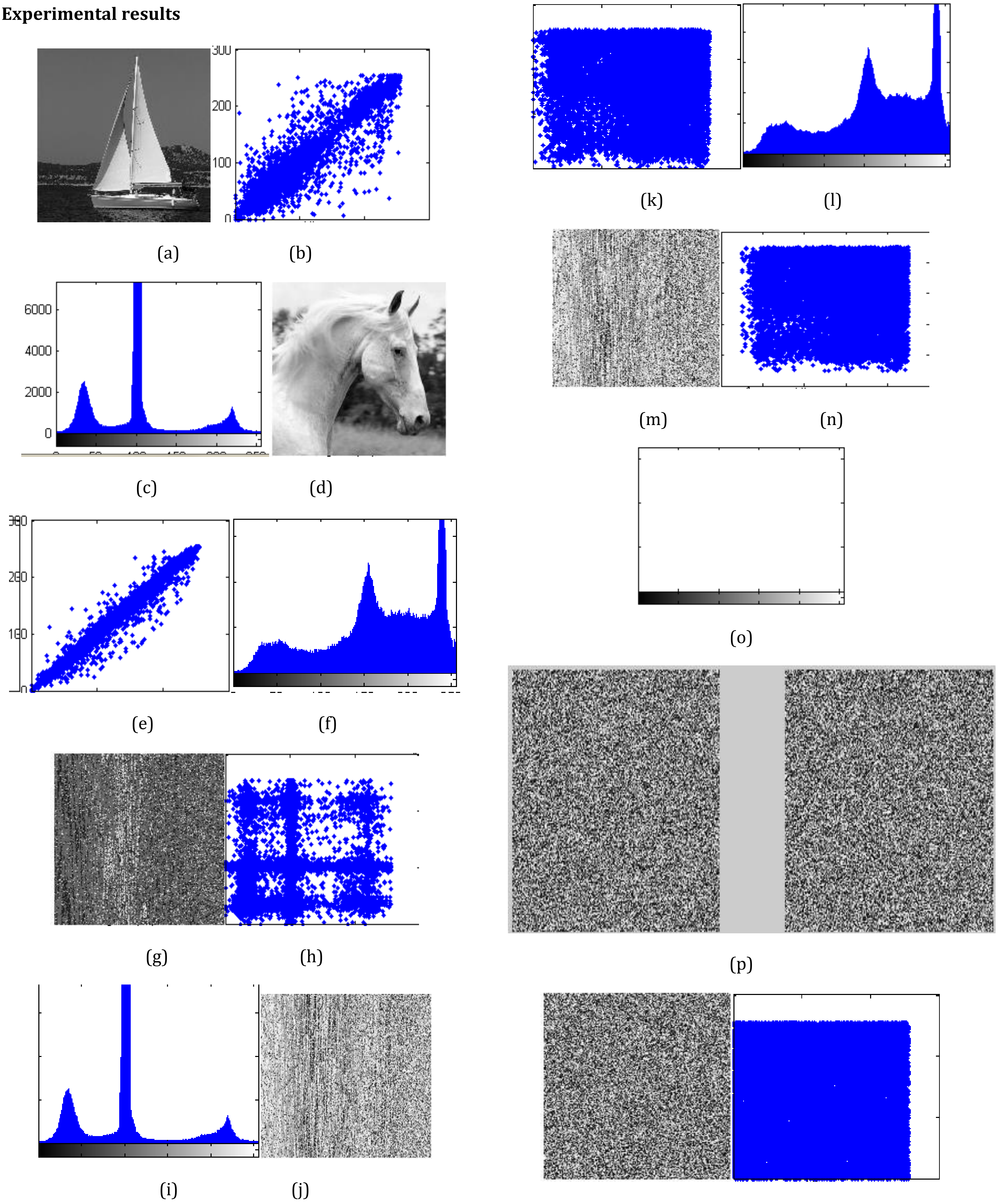
i. Encryption

Encryption is the process of transforming the information using an algorithm to an unreadable form except those who has special knowledge, usually referred as a key. In our proposed approach, we take the input image together with the cheat image. Cheat image is the image from the public network and One can perform cryptographic tasks i.e. encryption and decryption, if he has a knowledge of cheat image. Same image is used as a cheat image in both encryption and decryption process. In our approach, we just take the input image and cheat image, then we perform the permutation process on the input image and cheat image. Now, we generate the X0 from the cheat image using logistic map. Now then, we generate the Q1 and Q2 from the X0 using the secret key parameters. Now, we generate the encrypted image using Q1 and Q2.

ii. Decryption

Decryption is the process of converting data from unreadable form into an original data that is being encrypted using key. The same key is used in both encryption and decryption process. In decryption, we take the encrypted image and apply the decryption algorithm together with the same cheat image which we used at the time of encryption. For decryption process, we

Experimental results



(a) (b)

(c) (d)

(e) (f)

(g) (h)

(i) (j)

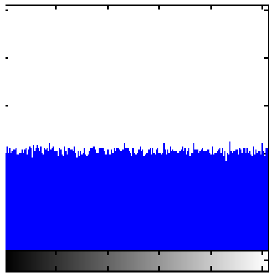
(k) (l)

(m) (n)

(o)

(p)

(q) (r)



(s)

Fig 5 (a) plain image **(b)** correlation of plain image **(c)** histogram of plain image **(d)** cheat image **(e)** correlation of cheat image **(f)** histogram of cheat image **(g)** permuted input image **(h)** correlation of permuted input image **(i)** histogram of permuted input image **(j)** permuted cheat image **(k)** correlation of permuted cheat image **(l)** histogram of permuted. cheat image **(m)** X0 **(n)** correlation of X0 **(o)** histogram of X0 **(p)** Q1 and Q2 **(q)** encrypted image **(r)** correlation of encrypted image **(s)** histogram of encrypted image.

2.2 SECURITY AND PERFORMANCE ANALYSIS

In this section, we will discuss the statistical analysis, sensitivity analysis, differential analysis and cheat characteristic analysis which is the main security characteristics of the proposed encryption scheme. These are the main concerns and needed to describe here because a good encryption scheme should be robust against all kinds of cryptographic, statistical and brute force attacks.

i. Statistical Analysis

We analyzed the Histograms and correlations of two adjacent pixels in the cipher images to prove the proposed cryptosystem against any statistical attacks.

ii. Differential attack

To see the influence of changing a single pixel in the plain image on the encrypted image by the proposed image encryption algorithm, pixels change rate are calculated.

iii. Sensitivity analysis

Small change in the secret key would produce a completely different encrypted image i.e. An ideal cryptosystem should be sensitive with respect to the secret key. We observe that the correlation coefficients are very small which proves that the proposed cryptosystem is highly key sensitive.

iv. Cheat characteristics analysis

Cheat image plays a very important role in this proposed system in which it uses for both encryption and decryption process. With the only knowledge of secret key, one cannot decrypt the image until he has knowledge of cheat image.

v. Information Entropy Analysis

The information entropy values of some images of USC-SIPI image database are calculated by using (9).

3. CONCLUSIONS

An assistant image called cheat image is needed in the encryption and decryption process. Cheat images are the common images from the public network which are neglected by the attackers. We choose the initial parameter of the logistic map as a secret key. One cheat image is used to encrypt the number of plain images if it's not attracting the attention of the attacker. The experimental results are shown and the performance analysis are described in detail to demonstrate that the proposed encryption scheme is robust and secure enough to be used in practical communication.

REFERENCES

[1] Nisha Kushwah, Madhu Sharma, "Chaotic Map Based Block Encryption", IJCA (0975-8887) Volume 71-No. 16, June 2013

[2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps", Int. J. Bifur. Chaos, vol. 8(6),1998, pp. 1259-1284. Intro first time Chapter 2

[3] CS 223B: "Introduction to Computer Vision", Carlo Tomasi- Stanford University.

[4] Linhua Zhang, Xiaofeng Liao, Xuebing Wang, "An image encryption approach based on chaotic maps", Chaos, Solitons and Fractals 24(2005) 759-765.

[5] N. Pareek, V. Patidar and K.K. Sud, "Image encryption using chaotic logistic map", Image. Vision. Comput, vol. 24(9), 2006, pp. 926-934.

[6] K. W. Wong, BS. H. Kwok and W.S. Law, "A Fast Image Encryption Scheme based on Chaotic Standard Map", Phys. Lett. A, vol 372(15), 2008, pp. 2645-2652.

[7] E. Solak and C. Cokal, "Comments on ' Encryption and decryption of images with chaotic map

lattices',” Chaos, vol. 18(3), 2008, pp. 038101-038103.

[8] D. Arroyo, S. Li, J.M. Amigo, G. Alvarez and R. Rhouma, “Comments on 'Image Encryption with Chaotically Coupled Chaotic Maps',” Physica D, Vol 239(12), 2010, pp. 1002-1006.