Novel Image Encryption of Color Image based on Henon Chaotic Systems and its Analysis

Vikas Chaturvedi
Govt.Engg.College, Ajmer,
Rajasthan, India

Prakriti Trivedi
Asst.Professor
Govt.Engg.College, Ajmer,
Rajasthan, India

R K Pandey[1],
Parvinder Singh[2]
[1]Govt.Engg.College, Ajmer,
Rajasthan, India
[2]IIT Rajasthan, Jodhpur, India

ABSTRACT
In this paper a novel image encryption scheme is presented based on Henon Chaotic System for color images in order to perform secure transmission of image. The proposed cipher provides good transposition and substitution properties by performing EX-OR operation and circular right bit shift operation. The security of image encryption is enhanced effectively. The proposed method has also found its applications in the field of military environment. In first step, Arnold Cat Map is used for initial permutation. It performs shuffling of pixel positions. In second step, shuffled image is encrypted pixel by pixel based on Henon Chaotic System. The encryption includes first and third chaotic key for EX-OR operation and second chaotic key for right bit circular shift. The security of proposed encryption scheme has been analyzed using statistical analysis, Local Entropy analysis and key sensitivity analysis. The result shows that this scheme is more secure and more efficient.

Keywords
Image Encryption, Arnold Cat Map, Henon Chaotic Mapping, Entropy.

1. INTRODUCTION
The public internet is a world-wide computer network. Its use is increasing rapidly. The multimedia technology is also developing rapidly. In multimedia every type of information such as audio, video, image can be represented, stored, transmitted and processed in a digital form, so this type of digital data can be communicated through digital network. Network security measures are needed to protect the data during their transmission. Today image has been widely used in daily life like in financial records, military applications, medical field, archaeological field etc. So in the present era we have to do lot of research in image security. So the main issue in cryptography is image encryption. The traditional encryption algorithm such as RSA, DES, AES [4] etc are not suitable for image encryption. The reason behind this is the properties of image such as bulk storage capacity, strong correlation among pixels, high redundancy. In recent years, many algorithms had been developed which was based on chaotic based system [2, 3, 5, 6].But each of them contain some type of limitations. Image Cipher based on mixed transformed logistic map is only used for encryption of fixed image size. The computational power of this method is very high. Some other image encryption algorithms are based on Henon Chaotic System and Arnold Cat Map [3].Such algorithms work only for gray scale image. A symmetric image encryption scheme based on 3D-Chaotic Cat Map is presented in [6, 7].However the encryption arithmetic based on 3D-Chaotic map is a computationally expensive process and the key space is not independence. Such algorithms perform a fixed right circular shift on each pixel of image. So the proposed novel method provides a good speed and efficiency for RGB image. Now the new method which is presented in this paper uses Arnold Cat Map for shuffling pixel position in RGB image. After this the EX-OR operation and circular right shift bit is performed on shuffled image for encryption. Furthermore, three keys are used which are based on Henon Chaotic System. The first and third key generate binary stream for EX-OR operation and second key generate a random number for right circular shift of each pixel. Our proposed scheme has following advantages over the traditional encryption techniques:-

1. Mean of entropy value is higher.
2. Method of encryption and circular shifting is dynamic in nature.
3. Existence of decryption technique is also available in our proposed scheme.

The rest of the paper is organized as follows: Section 1 gives a brief introduction of the Arnold Cat Map. Section 2 explains introduction about Henon Chaotic mapping. Section 3 describes proposed encryption scheme. Section 4 shows the simulation results. Finally Section 5 concludes the work.

2. ARNOLD CAT MAP SYSTEM
It is a two-dimensional invertible chaotic map which is proposed by Arnold known as an Arnold Cat Map. Assume that the dimension of original RGB image I is N*N. The Arnold Cat Map defines as follows:

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \cdot \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod(N)$$

Where p and q are the two dimensional Arnold Cat Map generalized parameter. In this map mainly two control parameters p and q are always positive integer. The (x_{n+1}, y_{n+1}) is the new position of pixel after shuffling and (x_n, y_n) is the original position of pixel in original image

where n=0,1,2….. After some iteration $(x_{n+1}, y_{n+1}) = (x, y)$ here the number of iterations is known as period. So the Arnold Cat parameters p, q and the number of iterations uses as a secret key. The Arnold Cat Map performs only shuffling of image pixels. After shuffling statistical properties [4] of cipher image and original image are same. After that we use Henon Chaotic System for diffusion and for improving the security.

3. HENON CHAOTIC SYSTEM

There are many chaotic systems one of the most known and widely used chaotic system is Henon Chaotic map. It is firstly discovered in 1978. It is described as following:

$xi+1 = 1 - a\,x_i^2 + yi$

$yi+1 = bxi$,i=0,1,2, -------

This Henon map presents as a simple two dimensional map. Because of its simplicity, lot of research is done in recent years. Still under the change of parameters a and b, the complete picture of all bifurcations is far from completion. If the parameter value of a=0.43 and b=1.79, then the system is chaotic. The chaotic system has excellent properties like sensitive dependence on system parameters and initial conditions, pseudorandom property and topological transitivity. These properties fulfill some requirements of cryptography. In our scheme the Henon Chaotic System is converted into one dimensional chaotic map. This map is defined as

$Xi+2 = 1 - a\,x_{i+1}^2 + bxi$

There are two parameters a & b such that a ε [0.2, 0.9] and b ε [1.079, 1.87].The initial value of x0=0.0100121 and x1=0.001214 represented as a secret key. The value of Henon Chaotic map is also used for generating the random binary number for circular right bit shift.

4. PROPOSED SCHEME

We use a RGB image which is stored as a two dimensional array of pixels. The height and width of the plain image is represented by H and W.

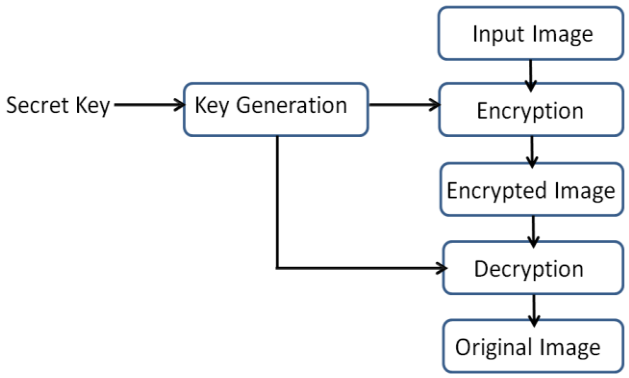

Figure 1: Flow chart of Colored image encryption by new approach.

4.1 Key Generation:

With the help of Henon Chaotic Map, the key has been generated. We use one dimensional Henon Chaotic map. This map is defined as

$Xi+1 = a\,x_i^2 + 1 + bxi$

There are two parameters a and b such that a=0.43 and b=1.79. The initial value of x0=0.02124 and x1=0.123456 represented as a secret key

Encryption by Arnold Cat Map: Every pixel of image is shuffled by Arnold Cat Map. At this stage the pixel value will not change. In next step we use Henon Chaotic map to change the pixel values.

4.2 Encryption:

Now we perform the diffusion on shuffled image by changing the value of each pixel through X-OR operation and right bit circular operation. The exclusive or operation will be completed bit by bit between the pixel value and first chaotic key. After that the value generated by second chaotic key for each pixel is used for right bit shift operation on each pixel of the image.

4.3 Decryption:

We can reconstruct the shuffled image exactly using the same secret keys. We follow the reverse process of encryption. We can get original image by using inverse of Arnold Cat Map which is described as follows:

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix}^{-1} \cdot \begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} \bmod(N)$$

5. SECURITY ANALYSIS

The good encryption scheme provides security services such as confidentiality and integrity. For a good encryption scheme, it is required that it resists all known attacks such as brute force attack, statistical attack, cipher text only attack etc. Some security analyses have been performed on the proposed image encryption technique. For experimental analysis purpose we use original RGB image with the size of 256* 256.

5.1 Statistical Analysis:

Statistical Analysis demonstrates the confusion and diffusion properties of encrypted image which strongly resist the statistical attack. These analyses mainly analyze correlation between adjacency pixels.

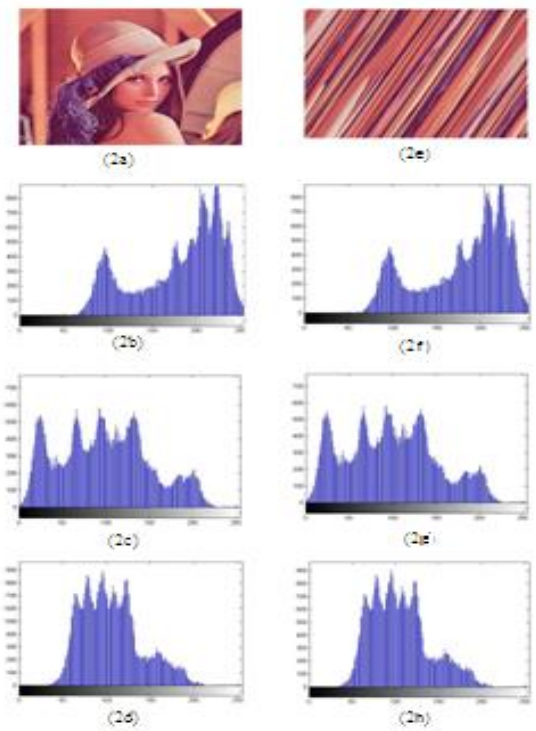

Figure 2.

Figure 2(a) shows the original image and figure 2(b),(c),(d) represent the histogram of RGB component of original image. Figure 2(e),(f),(g),(h) describes the image after shuffling and histogram of shuffled image. For purpose of analysis p=q=2 in Arnold Cat Map. The result shows histogram of original image and shuffled image are same.

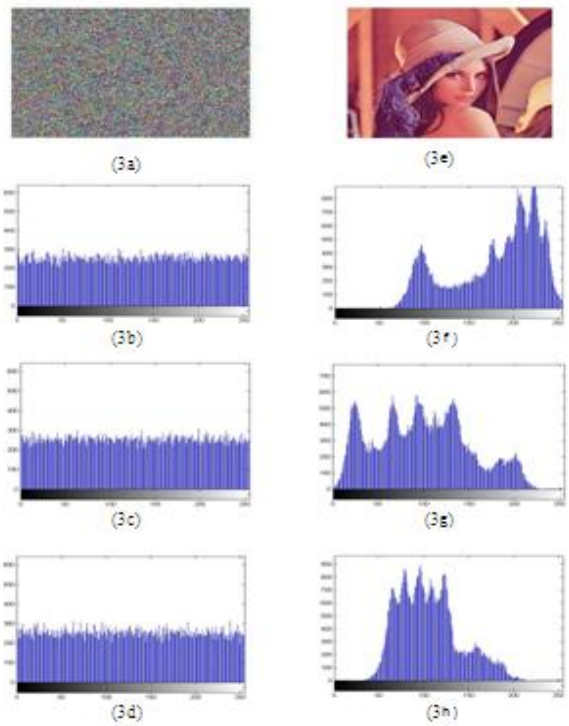

Figure 3

Figure 3(a),(b),(c),(d) describes the cipher image and histogram of RGB components. The receiver can reconstruct the image after the decryption process from cipher image. Figure 3(e),(f),(g),(h) illustrates the decrypted original image and its corresponding histogram.

5.2 Key Space Analysis:

It is required that every encryption scheme should be sensitive to secret key and for resist the brute force attack, key space should be large enough. In our encryption scheme the initial values and parameters of three Henon Chaotic Map are used as key space. The key space is approximately 256. Figure 4 describes the Key sensitivity of our scheme with secret keys.

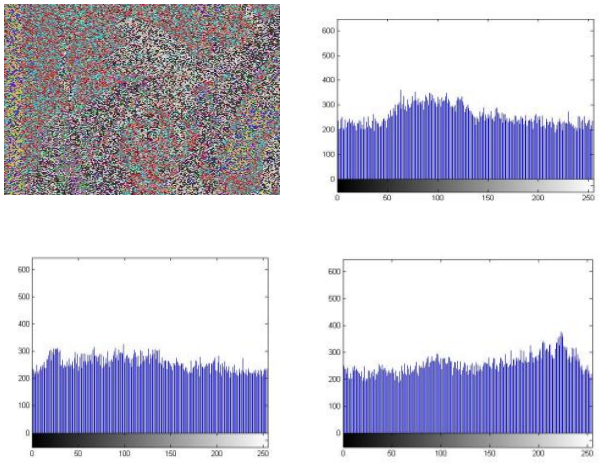

Figure 4

Which is decrypted wrong key and p=q=2. Now when this new changed key is decrypted, we can observe the change in histogram. So undoubtedly, the key space is large enough and the secret keys are very secure.

5.3 Entropy Analysis:

Entropy is a physical quantity that represents the statistical properties of the source itself. It can be interpreted as measuring the average uncertainty of the source. Let M be a discrete information source with each discrete signal mi, then the entropy of M is

$$H(m) = -\sum_{i=1}^{N} p(m_i)\log p(m_i)$$

Where p(mi) represents the probability of occurrence of symbol mi.

6. CONCLUSION

In this paper a novel secure cryptosystem for direct encryption of color images, based on transformed henon chaotic maps has been proposed. The new scheme combines the X-or operation and circular right bit shift. The both theoretical and experimental analysis shows that the encryption scheme is very effective. The scheme provides large key space for encryption, so it is very suitable to resist all types of brute force attacks. The new encryption schemes not only shuffle

the pixel position of original image, but also change the pixel values according to secret key. Key sensitivity is also very much in this new scheme. The simulation result shows that the new cryptosystem is very fast, so you can use this system in real time digital communication.

7. REFERENCES

[1] Bowman, M., Debray, S. K., and Peterson, L. L. 1993. Reasoning about naming systems.

[2] I Shatheesh Sam, P. Devaraj, Raghuvel S. Bhuvaneswaran, A novel image cipher based on mixed transformed logistic maps, Nov 2011,Springler

[3] Xu Shu-Jiang, Wang Ying-Long, Wang Ji-Zhi, Tian Min,A Novel Image Encryption Scheme Based on Chaotic Maps,2008,IEEE.

[4] Chen Wei-bin, Zhang Xin ,Image Encryption Algorithm Based Henon Chaotic System,2009,IEEE

[5] Jing Sun & Zhengquan Xu & Jin Liu & Ye Yao An objective visual security assessment for cipher-images based on local entropy,Mar 2010,Springer.

[6] Chen Wei-bin, Zhang Xin ,Image Encryption Algorithm Based Henon Chaotic System,2009,IEEE

[7] Jing Sun & Zhengquan Xu & Jin Liu & Ye Yao An objective visual security assessment for cipher-images based on local entropy,Mar 2010,Springer.

[8] WANG De,ZHANG Yuan-biao. Image encryption arithmetic based on S-boxes scrambling and chaos theory ,Computer Engineering and Applications,2008,44(19):50-52 (in Chinese)

[9] G. Chen.Y. Mao. K. Charles." A symmetric image encryption scheme based on 3D chaotic cat maps." Chaos Solution & Fractals. pp.749-761. Dec 2004.

[10] K. Wang. W. Pei. "On the security of 3D Cat map based symmetric image encryption scheme." Physics Letters A, pp.432-439. May. 2005