# Image Encryption Using Shuffled Card Algorithm And Novel Transformed Henon Chaotic Mapping And Their Comparative Analysis

[1*] Shashank Gupta, [2] Lalitsen Sharma

*[1*]Lecturer in Department of I.T., M.I.E.T, Jammu, [2] Associate Professor in Department of CS and IT, Jammuu University, Jammu*

## Abstract

*In recent times, a variety of encryption algorithms on image encryption have been reported and broadly used. In this paper, firstly the encryption is performed on a gray scale image by simply using shuffling algorithm in MATLAB and calculated the entropy value of the cipher images at different levels of encryption. Secondly, 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 exclusive OR operation and circular right bit shift operation. Lastly, a comparative analysis is performed on both the above encryption techniques based on the unintelligible degree of their cipher images. This way security of image encryption is enhanced effectively. Application of this method is found in the field of military and medical.*

## 1. Introduction

The public internet is a world-wide computer network and its use is increasing rapidly. The multimedia technology is also developing rapidly. Network security measures are needed to protect the data during their transmission. In the present era, image has been widely used in daily life like in financial records, military applications, medical and archaeological field. In image encryption, cryptography and image security there is enough scope of research. The traditional encryption algorithm such as RSA, DES, AES [1] etc are not suitable for image encryption due to the some 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, 4, 5]. But each of them contains 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 images. A symmetric image encryption scheme based on 3D-Chaotic Cat Map is presented in [5, 6]. 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. In the proposed method there are mainly two phases. In the first phase, we generate a new key for encryption based on a secret key given by user. In the second phase, according to Henon Chaotic map and Arnold Cat Map [3], encryption is performed on the original image. Now in this paper, firstly, encryption is carried out a gray scale image by using shuffle card algorithm. Secondly, 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. Lastly, a comparative analysis is performed on both the encryption techniques.

The rest of the paper is organized as follows: Section 2 describes the technique of encryption of gray scale image by shuffling algorithm. Section 3 gives a brief introduction to the Arnold Cat Map. Section 4 explains introduction about Henon Chaotic mapping. Section 5 describes proposed encryption scheme based on transformed Henon Chaotic Mapping. Section 6 analyzes the security of the proposed encryption technique. In Section 7, a comparative analysis of the shuffled card algorithm and proposed encryption technique is presented. And finally Section 8 concludes the proposed work and suggests the future work.

## 2. Encryption technique of a gray scale image using shuffled card algorithm

In this paper, firstly a gray scale image is taken as a source image for encryption with width and height of equal sizes. Now in the first level of encryption, image is divided into four equal parts. Now these four parts are shuffled clockwise, so that the resultant shuffled image is unintelligible to human vision. After this in the level 2, the shuffled image is taken as a source image and its four individual parts are now broken down separately into four equal parts and a total of sixteen parts is again shuffled clockwise. Likewise, this technique is applied up to level seven. Finally in the level 7, a high degree of randomness is created in the image, so that this uncertainty is meaningless to human.

In order to perform the encryption on a gray scale image using MATLAB, we have taken LEENA (256 * 256 pixels) and divide this image into four equal sub-blocks and try to shuffle these sub-blocks clockwise. Now as shown in the Figure 1, as the size of sub-blocks of the image gets reduced in consecutive levels of encryption, the degree of the security of the image is unintelligible to normal human vision.

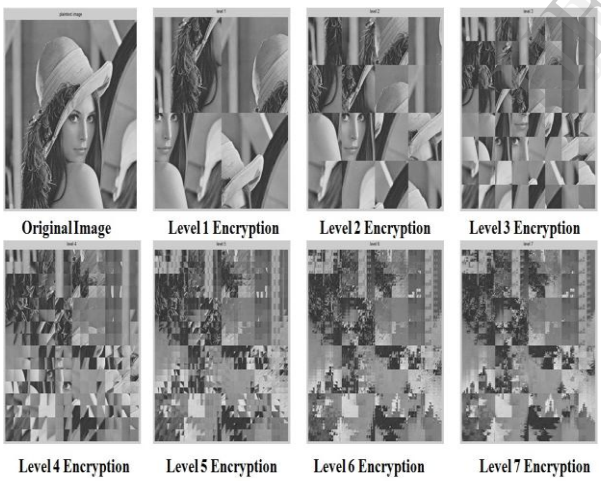


**Figure 1. Encryption of a Gray Scale Image (LEENA).**

Now in order to evaluate the security of the image, we calculate the entropy value of the cipher images at different levels of encryption. As the level of encryption increases, entropy value also gets increased. But as we reach up to the level 6, entropy value gets saturated.

## 3. Arnold cat map system

It is a two-dimensional invertible chaotic map which is proposed by Arnold known as a Arnold Cat Map. Assume that the dimension of original RGB image I is N*N. The Arnold Cat Map is defined 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 parameters of two dimensional Arnold Cat Map. In this map mainly two control parameters p and q are always positive integer. The (xn+1, yn+1) is the new position of pixel after shuffling and (xn, yn) is the original position of pixel in original image where n=0, 1, 2….. Based on the value of p and q, the size of N after T iteration (xn+1, yn+1) = (xn, yn). Here T is called period. The value of 'T' depends on the image. 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 the cipher image and original image are same. After this, we have used the Henon Chaotic System for diffusion and improving the security.

## 4. Henon Chaotic System

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

$x_{i+1} = 1 - a\,x_i^2 + y_i$

$y_{i+1} = bx_i$, i = 0,1,2 -------

This Henon map presents as a simple two dimensional map. Because of its simplicity, a lot of research has been 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

$X_{i+2} = 1 - a\, x_{i+1}^2 + bx_i$

There are two parameters a and b such that $a \in [0.2, 0.9]$ and $b \in [1.079, 1.89]$.The initial value of $x_0 = 0.0100121$ and $x_1 = 0.001214$ are 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.

## 5. Proposed technique

In the proposed method, dynamic right shift is performed which implies for each image, the number of right bit shift are based on the secret key, which implies an efficient and superior security. We have used 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.

### 5.1. Key Generation

For Key generation, one dimensional Henon Chaotic map has used and it is defined as

$X_{i+1} = a\, x_i^2 + 1 + b\, x_i$

There are two parameters a and b such that a = 0.43 and b = 1.79.The initial value of $x_0 = 0.02124$ and $x_1 = 0.123456$ are 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.

### 5.2. Encryption

The diffusion operation performed 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.

### 5.3. Decryption

The shuffled image can be reconstructed 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:

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

## 6. 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 analysis has been performed on the proposed image encryption technique. For the performance and experimental analysis, we use an original RGB image with the size of 256* 256 and analysis is done on it.

### 6.1. Statistical Analysis

Statistical analysis demonstrates the confusion and diffusion properties of encrypted image which strongly resist the statistical attack. This analysis mainly analyzes correlation between adjacency pixels. Fig. 2 shows the original image, shuffled image and their histograms of RGB components of original image and shuffled image. For the purpose of analysis p=q=2 in Arnold Cat Map, the result shows histogram of original image and shuffled image are same.

Fig. 3 describes the cipher image, original image and histogram of RGB components. The receiver can reconstruct the image after the decryption process from the cipher image.

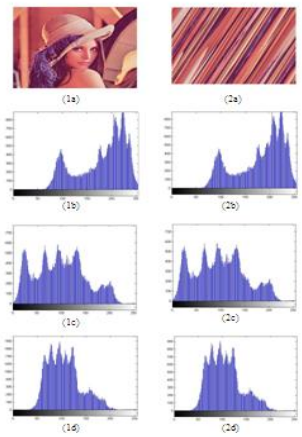

**Figure 2. Original RGB Image, Shuffled Image and their Corresponding Histograms**

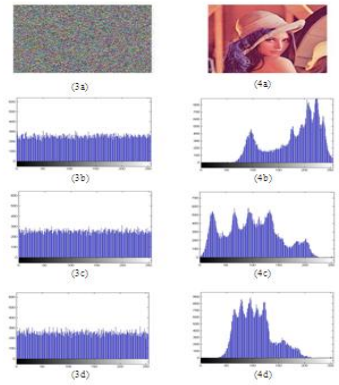

**Figure 3. Cipher image, Original (Deccrypted) Image and their Corresponding Histograms**

## 6.2. Key Space Analysis

It is required that every encryption scheme should be sensitive to secret key and must resist the brute force attack. key space should be large enough. In the proposed encryption scheme, the initial values and parameters of Henon Chaotic Map are used as a key space. There are two initial parameters and four different initial security keys for generating the three Henon chaotic keys. So the total key space is approximately 256. In addition to this, the initial parameter is also used as key space. If the figure 3 is decrypted using different chaotic keys at one place, then this technique will not work. If figure 3 is decrypted using different keys then Fig. 4 shows that using a different key the original image will not be recovered. This can be clearly seen in the Fig. 4, that some change has been observed in the histogram as compared to the histograms of Fig. 3. We can observe the change in histogram. So undoubtedly, the key space is large enough and the secret keys are very secure.

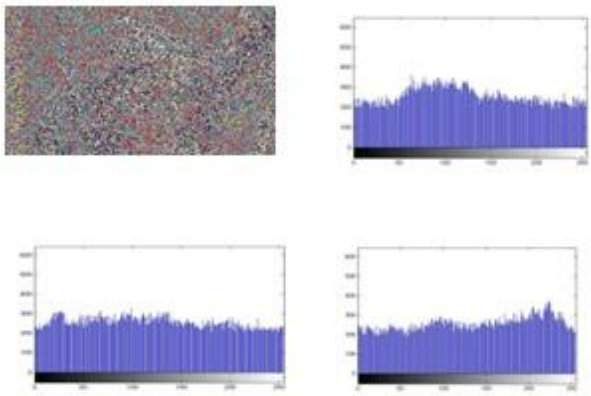

**Figure 4. Cipher Image and their Corresponding Histograms**

## 7. Comparative Analysis of Shuffled Card Algorithm and Proposed Henon Chaotic Mapping

We have discussed both the shuffled algorithm for the encryption of a gray scale image and a novel secure cryptosystem for direct encryption of color images, based on transformed Henon chaotic maps. Based on the above analysis of both these techniques of image encryption, the following are some of the inferences from both these techniques which is elaborated as shown below:-

- Image Encryption by shuffled card algorithm works only for gray scale images where as the Image Encryption using proposed transformed Henon Chaotic Mapping works both for gray scale and color images.
- The shuffled card technique does not utilize any secret key for encryption and decryption. On the other hand, the proposed encryption technique makes use of the transformed Henon Chaotic Mapping for secret key generation.
- In order to perform the encryption of image, the shuffled card algorithm recursively shuffles the part of image clockwise. But in the proposed technique, each and every pixel of the image is shuffled by Arnold Cat Map.

- The proposed encryption technique not only shuffles the pixel position of the image but also change the value of the pixels. Due to which security of cipher image is greater as compared to the shuffled card technique of image encryption.

- The key space analysis of the proposed technique is very large, so that it can defend against attacks like brute force attack etc.

- Entropy value of a cipher image in the shuffled card algorithm saturate at a certain level of encryption. The entropy value generally saturates from level 5 onwards with a value of 6.73.

## 8. Conclusion and Future Work

In this paper, we have discussed a novel technique for the encryption of RGB image using transformed Henon Chaotic Mapping scheme and tries to compare this technique with the encryption of a gray scale image using shuffled card algorithm. This new scheme combines the EX-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 scheme not only shuffles the pixel position of original image, but also changes 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. On the other hand, the proposed technique in this paper will probably be further optimized and enhanced and new objective assessment algorithms would be developed based on the characteristics of cipher images. We also believe that it will be very significant to further research on video encryption.

## 9. References

[1] Jing Sun, Zhengquan Xu, Jin Liu, Ye Yao, An objective visual security assessment for cipher-images based on local entropy, Multimedia Tools and Applications, Vol. 53, Issue 1, pp. 75-95, May 2011.

[2] Xu Shu-Jiang, Wang Ying-Long, Wang Ji-Zhi, Tian Min,A Novel Image Encryption Scheme Based on Chaotic Maps, 9th International Conference on Signal Processing (IEEE-ICSP), pp. 1014-1018, 2008.

[3] Chen Wei-bin, Zhang Xin ,Image Encryption Algorithm Based Henon Chaotic System, IEEE International Conference on Image Analysis and Signal Processing (IASP), pp. 94-97, 2009.

[4] De Wang, Yuan-Biao Zhang, Image encryption arithmetic based on S-boxes scrambling and chaos theory ,Computer Engineering andApplications,2008,44(19):50-52 (in Chinese)

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

[6] K. Wang, Liuhua Zou, . "On the security of 3D Cat map based symmetric image encryption scheme." Physics Letters A (Elsevier), pp.432-439, Aug, 2005.