IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 2, Ver. II (Mar - Apr.2015), PP 103-108
www.iosrjournals.org

An Image Encryption and Decryption using Chaos Algorithm

G.Chaitanaya[1,] B.Keerthi[2,] A.Saleem[3,] A.Trinadh Rao[4,] K.T.P.S.Kumar[5,]
1,2,3,4(Department of ECE, Lendi Institute of engineering and technology,gundapu.
5(Assistant professor ,Department of ECE, Lendi institute of engineering and technology)

Abstract: *In a well-developed digital world, security plays a key role in transmission of images. To overcome these challenges Encryption and Decryption techniques need to be applied. In this paper we have applied the chaotic encryption and chaotic decryption on an image by doing pixel shuffling and using chaotic maps. Chaotic nature i.e., randomness property is present in both Henon map and Arnold cat map. Pseudorandom values generation plays an important key role in Henon maps and iteratively pixel shuffling is done in Arnold cat map. A sorting Technique is followed on key values produced by Henon map. By using those sorted positions, shuffle the pixel values generated by Arnold cat map iteratively. In this way the images are provided with high security for confidential transmission.*

Keywords: *Encryption and Decryption, Chaotic map, Pseudo-Random values, Pixel shuffling, sorting.*

I. Introduction

Now-a-days technologies are developing faster. As the amount of data increases the method of handling it has become a hard task. As everything has its pros and cones, the risk of data corruption, forging, data extraction, etc., has been a boon to the hackers. Hence to protect from the above the technology called cryptography was introduced. Cryptography means the method of storing and transmitting required data in a particular form so that legal users can only read and process it. Modern cryptography involves computer science algorithms and mathematical concepts. Cryptography techniques can be applied on any data like text, images, videos, etc., But in real time scenarios, as the methods of encryption and decryption has been low in speeds, which may result to significant latency.

Text Encryption and Image Encryption are different from their kind. Most existing encryption standards aim at, image encryption compared with text encryption (or more generally, multimedia encryption) has its own characteristics and special features with many unique specifications. Hence we have chosen to implement the project “Chaos Encryption and Decryption using pixel Shuffling” It provides an efficient algorithm for encrypting images which takes shorter computational time and low computing power and gives high encryption strength. Chaos is referred to as unpredictability. Chaos can also be defined as a study of nonlinear dynamic systems. Chaos was discovered by Edward N. Lorenz in 1963, and is a phenomenon that occurs in non-linear system. Chaos has vigilant characters when compared with any other image encryption which stands against any static attacks. It is most extensively used practically against any static attacks.

Our project mainly concentrates on image encryption and it decryption which involves key generation and pixel Shuffling. In this approach we generate key using the random numbers.

Randoms are widely classified into two types they are True Random Numbers(TRNGS) and Pseudo Random number generation (PRNGS).The formula used in the pseudo random number generation is

$$\mathbf{Xi+_1=k\ (x_i)}$$

Where X is a random vector and K is an applied function.

II. Arnold’s Cat Map

Arnold Cat map was discovered by Valdimir Arnold in 1960. IT takes the logics from linear algebra and uses them to change the pixel positions with respect to the original image.

The Arnold Cap Map is a discrete system that stretches and folds its trajectories in phase space.

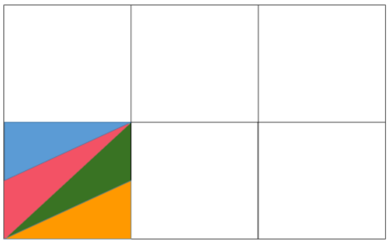


Fig 1(a). A Sample image showing the linear map

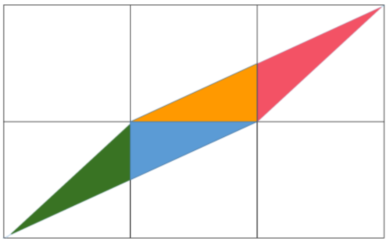


Fig 1(b). An Arnold Map View

Now comesto the ACM, a chaotic map known as the ACM is a discrete system that streches and folds the trajectories in phase space which will be a torus.

Mathematically the ACM is defined as the following:

Let X=$\begin{bmatrix} x \\ y \end{bmatrix}$ be the n×n matrix,

Then the ACM transformation is,

$$\Gamma:\rightarrow\begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod n$$

$$=\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} \bmod n$$

i.e $\quad \Gamma:(x,y)\rightarrow(x+y,x+2y) \bmod n$

here mod is the remainder of $\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$ and n

1.1 Experimental Analysis:

Through the experimental analysis, it shows how the ACM behaves chaotic in nature. The graphical representation of the pseudo-random numbers generated by the map, how the numbers are repeated after 12000 iteration while taking 20000 iteration and behaves chaotic in nature, is shown below

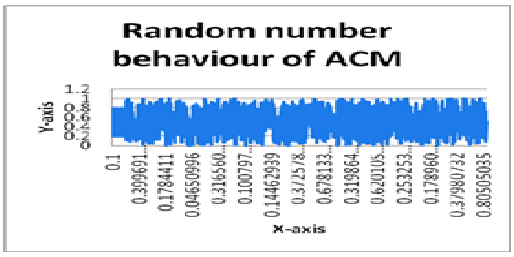


Fig 2. Random number behavior of ACM

III. Henon Map

The Henon Map is a discrete-time dynamic system introduced by Michel Henon. It is a simplified model of Poincare section of the Lorenz model. It is one of the most studied examples pf dynamical systems that exhibit chaotic behavior. It takes (x_0, y_0) in the plane and maps it to a new point.

$$Xn+_1=y_n+1-a \times x_n\times x_n$$
$$Yn+_1=b \times x_n$$

It depends on two parameters a and b. Classical Henon Map has values of a=1.4 and b=0.3. For the classical values the Henon map is chaotic. For other values of a and b the map may be chaotic, intermittent, or coverage to a periodic orbit. We can obtain an overview of different parameter values by

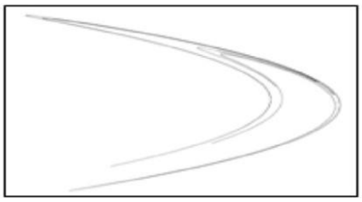


Fig 3(a) : Actual Henon Actor

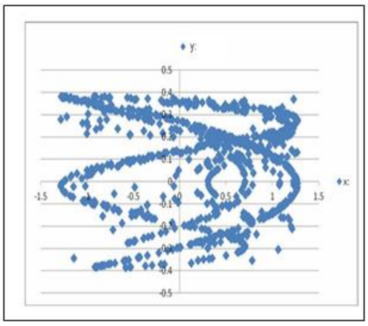


Fig 3(b). Actual Henon map generated through graph

1.2 Experimental Analysis:

Through the experimental analysis, it shows how the henon map behaves chaotic in nature. The pseudo-random number generated by the map, which is used as key in the process of encryption, from different iteration is shown below.

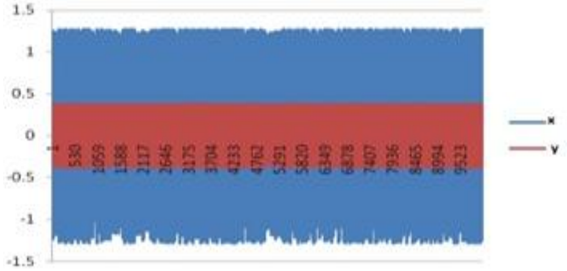


Fig 4. Experimental analysis of chaotic nature of Henon map through different iteration

IV. Present Work

First we have taken a standard image for the process of encryption. The image should be of .jpg or .jpeg, .png, .gif image format. The imagepixels areextracted which is depending upon the dimensionofthe image i.e. image height and image width and store in an array. After that the pixel shuffling is done by using the Arnold's Cat map which behaves chaotically, whose equations are given below:

$$Xn+_1 = (2 * x_n + y_{n)})\text{mod } 1$$
$$Yn+_1 = (xn + y_{n)})$$

Here the pixel shuffling is done to confuse the position of pixels of the image which are not exactly located by the attacker and creates a random vision in his mind. The new pixel values are now stored in a new array.

After that the Henon map is used to generate the key values. Here we are going to generate the key values by using the henon map because the key values that are generated are repeated after a large iteration as compare to the different chaotic maps like Traditional map, Logistic map, Barker's map, Tinkerbell map etc. The equations that are used are given below:

$$Xn+_1 = y_{n\,+}\ 1 - a \times x_n \times x_n$$
$$Yn+_1 = b \times x_n$$

Where the values of a & b is 1.4 & 0.3 respectively.

The main reason to choose Henon map is its entropy calculus is very high as compare to other chaotic maps as above mentioned [16]. If S is a given set of random numbers then the entropy of the given set H(S) can be calculated as

$$H(S) = - \sum P(s)*[\log 1/P(s)] \text{ bits}$$

Where s belongs to S and P(s) is the probability of occurrences of s in sample space S.

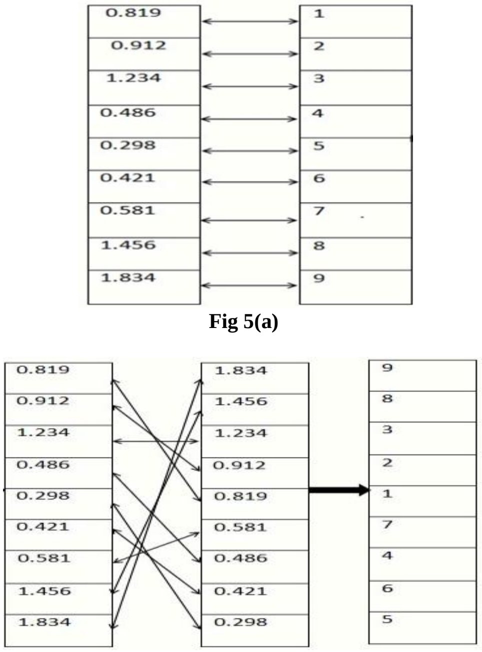
The table below shows elements generated from Henon map taking iteration for 'n' from 1 to 9.

(9 elements are taken as an example to explain the encryption process where as actual number of elements generated for Lena image).

0.819	0.912	1.234	0.486	0.298	0.421	0.581	1.456	1.834

Now sort the elements of each block in ascending or descending order and compare the disorder between the original and sorted elements of eachblock andtabulate the index change. Index the elements as shown in fig5(a). Arrange the elements in decreasing order and tabulation of the displacement in the index is noted by comparing the elements before and after sorting as in fig 5(b).

In the fig (6) column 1 represents intensity value of image, column 2 represents the tabulated index value obtained from the previous step and column 3 represents the arranged intensity value according to column 2.



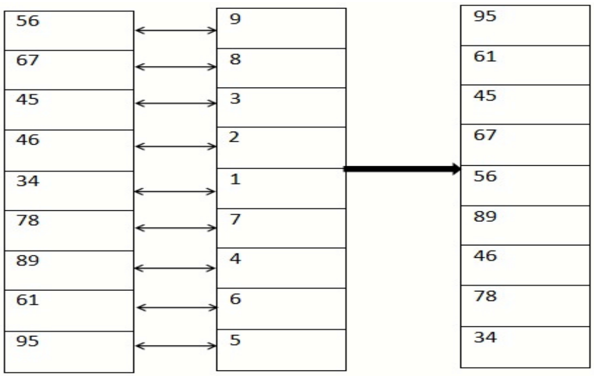
0.819	1
0.912	2
1.234	3
0.486	4
0.298	5
0.421	6
0.581	7
1.456	8
1.834	9

Fig 5(a)

0.819	1.834	9
0.912	1.456	8
1.234	1.234	3
0.486	0.912	2
0.298	0.819	1
0.421	0.581	7
0.581	0.486	4
1.456	0.421	6
1.834	0.298	5

Fig 5(b)

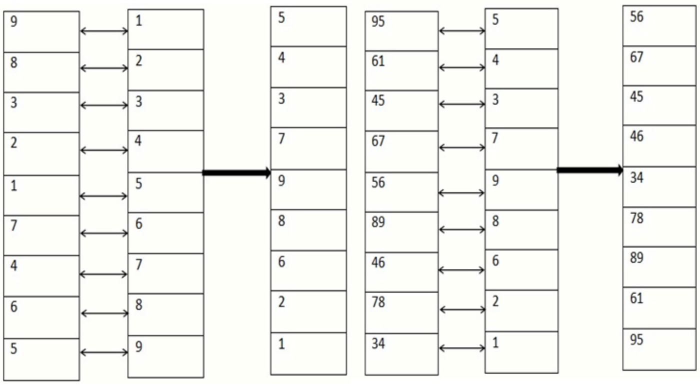
Fig 5. Arranging elements in decreasing order and tabulation of the displacement in the index



56	9	95
67	8	61
45	3	45
46	2	67
34	1	56
78	7	89
89	4	46
61	6	78
95	5	34

Fig (6) Ordering of pixel values

Decryption is done by the reverse process followed for encryption. In fig 7(b) column 1represents the sequence of received elements; column 2 represents sorted index elements obtained from the encryption process and column 3 represents resorted index elements. At the receiving point, the same random sequence is generated with Henon map to obtain back he sorted index elements as in fig 7(a) and original pixel values are obtained back as in Fig 7(b) Fig 7(a) Fig 7(b) Fig (7) decryption process



9	1	5
8	2	4
3	3	3
2	4	7
1	5	9
7	6	8
4	7	6
6	8	2
5	9	1

Fig 7(a)

95	5	56
61	4	67
45	3	45
67	7	46
56	9	34
89	8	78
46	6	89
78	2	61
34	1	95

fig 7(b)

Fig 7. Decryption Process

V. Algorithm

The following Algorithm used for the process of chaotic encryption and decryption using Henon map and Arnold Cat map:

1.1 Encryption Algorithm:

The actual image of .jpeg or .bmp or .jpg or .png format is chosen for encryption technique.

1. Pixel values should be generated from input image by using dimensions of image.
2. Pixel shuffling technique is done on input image by using Arnold Cat map.
3. Chaotic Pseudo-Random key values are generated by using Henon map.
4. Sorting operation is done on Henon Key values.
5. After sorting actual indexes of the sorted key values should be stored.
6. Pixel shuffling is done again on Arnold Cat image by using Henon Sorted key values.
7. Encrypted image is generated when all the above steps are over.

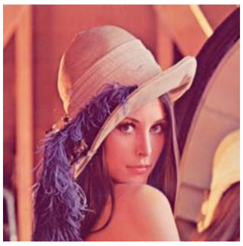
1.2 Decryption Algorithm:

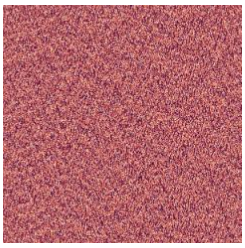
The encrypted image which obtained from Encryption process is chosen for this decryption technique.

1. Pixel values should be generated from input image by using dimensions of image.
2. Pixel reshuffling technique is done on input image by using Arnold Cat map.
3. Chaotic Pseudo-Random key values are generated by using Henon map.
4. Sorting operation is done on Henon Key values.
5. After sorting actual indexes of the sorted key values should be stored.
6. Pixel reshuffling is done again on ArnSold Cat image by using Henon Sorted key values.
7. Decrypted image i.e., original image is regenerated when all the above steps are over.

VI. Experimental Analysis

Below are the sample output of the images, which are used to find the cipher and the decrypted image.


Original image


Encrypted image

Decrypted image

Decrypted image using wrong key

VII. Conclusion

This paper describes about an image encryption technique using the concept of chaotic system. The chaotic system is highly sensitive to initial values and parameters of the system. The proposed method utilizes the randomness of the chaotic maps i.e. Arnold's cat map and Henon map, in order to encrypt the image. In this algorithm the pixel position is shuffled according to the randomness of the chaotic elements, which is derived by using the Arnold's cat map and the Pseudo-random number or key values are generated by using the Henon Map. Later in the decryption process, the decrypted image is brought by using the same key value used at the time of encryption. We suggest that this encryption scheme is suitable for applications like internet image encryption and secure transmission of confidential information in the internet.

Reference

[1]. Mintu "An Image Encryption & Decryption Approach Based on Pixel Shuffling Using Arnold Cat Map & Henon Map" by Agyan Kumar Prusty, AsutoshPattanaik, Swastik Mishra published in 2013 International Conference on Advanced Computing and Communication Systems(ICACCS-2013), Dec.19-21, 2013, Coimbatore, India,IEEE2013.

[2]. "Chaos Image Encryption using Pixel shuffling" by Manjunath Prasad and K.L.Sudha in CCSEA 2011,CS &IT 02 DOI: 10.5121/csit.2011.1217

[3]. "An Efficient Image Cryptographic Technique by Applying Chaotic Logistic Map and Arnold Cat Map" byS.VaniKumari and G.Neelima in IJARCSSE , september 2013 , ISSN: 2277 128X.

[4]. M. Sharma and M.K. Kowar, "Image Encryption Techniques Using Chaotic Schemes: a Review." International Journal of Engineering Science and Technology, vol. 2, pp. 2359–2363, 2010.

[5]. Chengqing Li, Shujun Li, Muhammad Asim, Juana Nunez, Gonzalo Alvarez, Guanrong Chen. On the "Security defects of an image encryption scheme."

[6]. Image and Vision Computing, vol. 27, pp. 13711381, 2009.

[7]. Yupu Dong; Jiasheng Liu; Canyan Zhu; Yiming Wang; "Image encryption algorithm based on chaotic mapping" Computer Science and Information Technology (ICCSIT), 2010.

[8]. International Conference on Volume: 1 'Publication Year:, Page(s): 289 – 291.Long Min; Huang Lu, "Design and Analysis of a novel Chaotic Image Encryption." International Conference on Computer Modelling and Simulation (ICCMS'10), vol 1, pp. 517-520, 2010.

[9]. Ranjan Bose and Amitabh Banerjee, "Implementing symmetric cryptography using chaos functions." 7th Int. Conf. On Advanced Computing and Communications Dec 20-22, Roorkee, India, 1999.

[10]. Li S, Mou X, Cai Y. "Pseudo-random bit generator based on couple chaotic systems and its applications in stream-cipher cryptography." LNCS, 2247. Berlin, pp. 316–29, 2001.

[11]. H.S. Kwok, W. K. S.Tang, "A fast image encryption system based on chaotic maps with finite precision representation." Chaos, Solitons and Fractals, vol. 32, pp. 1518–1529, 2007.

[12]. Chen Wei-bin; Zhang Xin; "Image encryption algorithm based on Henon chaotic system" Image Analysis and Signal Processing, IASP 2009.

[13]. International Conference, Publication Year: 2009

[14]. Cheng H "Partial Encryption for Image and Video Communication." M.S. Thesis, Univ. Alberta, Edmonton, Canada, 1998.

[15]. Li S, Li Q, Li W, Mou X, Cai Y in "Statistical properties of digital piecewise linear chaotic maps and their roles in cryptography and pseudo-random coding." IMA IntConf Crypt & Coding, 2260. Berline, pp. 205–21, 2001.

[16]. S. Behnia, A. Akhshani, H. Mahmodi and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps." Chaos, Solitons and Fractals, vol. 35, pp. 408–419, 2008.