International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 04 | Apr-2018 www.irjet.net p-ISSN: 2395-0072

An Image Cryptography using Henon Map and Arnold Cat Map.

Pranjali Sankhe[1], Shruti Pimple[2], Surabhi Singh[3], Anita Lahane[4]

[1,2,3] UG Student VIII SEM, B.E., Computer Engg., RGIT, Mumbai, India
[4]Assistant Professor, Department of Computer Engg., RGIT, Mumbai, India

---

Abstract - *In this digital world i.e. the transmission of non-physical data that has been encoded digitally for the purpose of storage Security is a continuous process via which data can be secured from several active and passive attacks. Encryption technique protects the confidentiality of a message or information which is in the form of multimedia (text, image, and video).In this paper, a new symmetric image encryption algorithm is proposed based on Henon's chaotic system with byte sequences applied with a novel approach of pixel shuffling of an image which results in an effective and efficient encryption of images. The Arnold Cat Map is a discrete system that stretches and folds its trajectories in phase space. Cryptography is the process of encryption and decryption of the data and used for making data, images secure and confidential . There is also a other side where the attackers, unauthorized user gets an opportunity to reuse, retrieve, disturb the images. In this paper we will apply the chaotic encryption and chaotic decryption on an image. Chaotic Algorithm is a well-used method in real time secure image transmission system.*

Key Words: **Encryption and Decryption, Chaotic maps, Arnold cat map, Henon map, Pseudo-Random values, Pixel shuffling, Cryptography, Chaotic System.**

1.INTRODUCTION

Multimedia is defined as the field that deals with different forms of information such as text, images, audio and videos in an integrated fashion. Now-a-days digital images are used frequently for communication. Any information shared over Internet needs high level of protection from intruders Cryptography is the art of protecting information by transforming readable information (plain data) into unreadable format (cipher) with the help of well-structured encryption algorithms and secret keys. Cryptography scheme is of two types. One is known as symmetric key cryptography in which a single secret key is used for both, encryption at sender's end and decryption at receiver's end. Chaotic systems are sensitive, non-liner, deterministic and easy to reconstruct after filling in the image. Henon map is one of the chaotic map used for generating Pseudo-random sequence required for encryption. 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.

2. METHODOLOGY

2.1 HENON MAP

1. The Henon map is a discrete time dynamic system introduces by michel henon.
2. The map depends on two parameters, a and b, which for the classical Henon map have 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 converge to a periodic orbit.
3. These slopes arise from the linearizations of the stable manifold and unstable manifold of the fixed point. The unstable manifold of the fixed point in the attractor is contained in the strange attractor of the Henon map.
4. It is a simplified model of coincare section of the lorenz model it is one of the most studied example of dynamically systems that exhibits chaotic behaviour it takes (x0,y0) in the plane and map it to a new point.
5. FORMULA: Xn+1=Yn+1-a*xn*xn Yn+1=b*xn

Here, the parameters, a and b are prime importance as the dynamic behaviour of system depends on these values.The system cannot be chaotic unless the value of a and b are 1.4 and 0.3 respectively. For other values of a and b, the map behaves as chaotic, intermittent, or obtain a periodic orbit. Initial points X1 and Y1 [11] work as a symmetric key for chaotic cryptographic system used for encryption at sender's end and decryption at receiver's end. Since Henon map is deterministic so decryption of the cipher image will reconstruct the original image at receiver's end with the same initial points X1 and Y1. Thus, sensitivity of key and encryption algorithm together contributes to avoid all kind of cryptanalysis attacks.

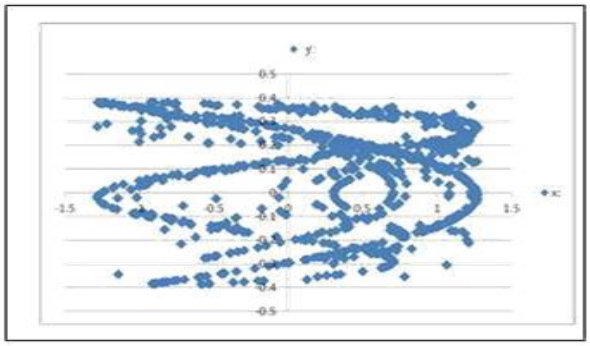

Fig 2.1: Henon key

2.2 ARNOLD'S CAT MAP

1. 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 Cat Map is a discrete system that stretches and folds its trajectories in phase space.
2. Arnold cat map has a unique hyperbolic fixed point (the vertices of the square). The linear transformation which defines the map is hyperbolic: its eigen values are irrational numbers, one greater and the other smaller than 1 (in absolute value), so they are associated respectively to an expanding and a contracting eigenspace which are also the stable and unstable manifolds. The eigenspace are orthogonal because the matrix is symmetric.
3. Defining the momentum variable pt = qt - qt-1, the above second order dynamics can be re-written as a mapping of the square 0 q, p ¡ N
4. Arnold cat Map is a transformation that can be applied to an image. The pixels of the image appear to be randomly rearranged, but when the transformation is repeated enough times, the original image will reappear.

If we let X a$=\begin{pmatrix} x \\ Y \end{pmatrix}$ be a $n \times n$ matrix of some image, Arnold's cat map is the transformation

$$R\begin{pmatrix} x \\ Y \end{pmatrix} \rightarrow \begin{pmatrix} x+y \\ x+2y \end{pmatrix} \text{mod n}$$

For example, 3.142 mod1 142 or 150 mod100=50 or

$$\begin{pmatrix} 123 \\ 154 \end{pmatrix} \text{mod } 100 = \begin{pmatrix} 23 \\ 54 \end{pmatrix}$$

Since the signs of both arguments are the same sign in the Exercise,the modulo will simply be the reminder of long division of $\begin{pmatrix} x+y \\ X+2y \end{pmatrix}$ and n

To better understand the mechanism of the transformation let us decompose it into its elemental pieces.

1. Shear in the x-diection by a factor of 1.

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ y \end{bmatrix}$$

2. Shear in the y-direction by a factor of 1.

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ x+y \end{bmatrix}$$

3. Evaluate the modulo.

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ y \end{bmatrix} \text{mod} n$$

Fig 2.2.1 : Arnold map

Included below is a visual aide illustrating these steps. The first step shows the shearing in the x and y-directions, followed by evaluation of the modulo and reassembly of the image.

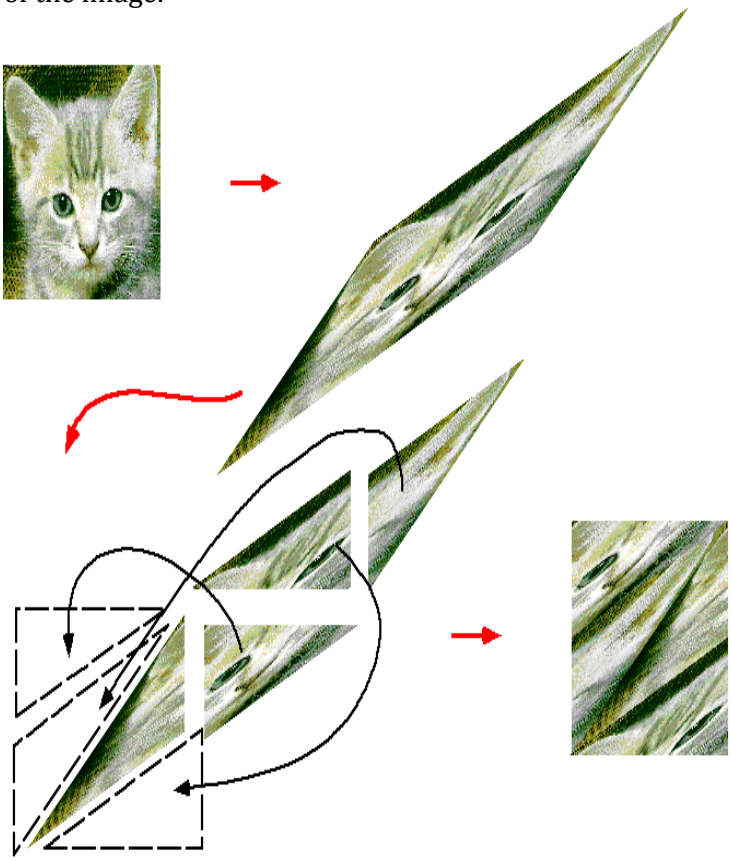

Fig 2.2.2: original image stretch by Arnold cat and pixel shuffel

3. ALGORITHMS.

3.1. ENCRYPTION ALGORITHM

3.1.1. The original image of .jpg or .jpeg format is chosen for the process of encryption.

3.1.2. Pixel extraction is done of the input image by taking the image dimension i.e. Height and Width of the image.

3.1.3. Pixel shuffling of pixels of the input image is done by using the Arnolds Cat map which is chaotic in nature.

3.1.4. Generation of Key values or the pseudo-random numbers using the Henon map which is chaotic in nature.

3.1.5. XOR operation is done between the pixel values generated from the input image and the key values generated by Henon map.

3.1.6. Cipher image or Encrypted image is done successfully and encryption process is over.

3.2 DECRYPTION ALGORITHM

3.2.1. The cipher image which got from the process of encryption is chosen for the process of decryption.

3.2.2. Pixel extraction is done of the cipher image by taking the image dimension i.e. Height and Width of the cipher image.

3.2.3. Pixel shuffling of pixels of the cipher image is done by using the Arnolds Cat map which is chaotic in nature.

3.2.4. Generation of Key values using the Henon map which behaves chaotically.

3.2.5. XOR operation is done between the pixel values and the key values generated by Henon map.

3.2.6. Original image is brought back from the cipher image successfully and decryption process is over.

4. SYSTEM DESIGN ARCHITECTURE.

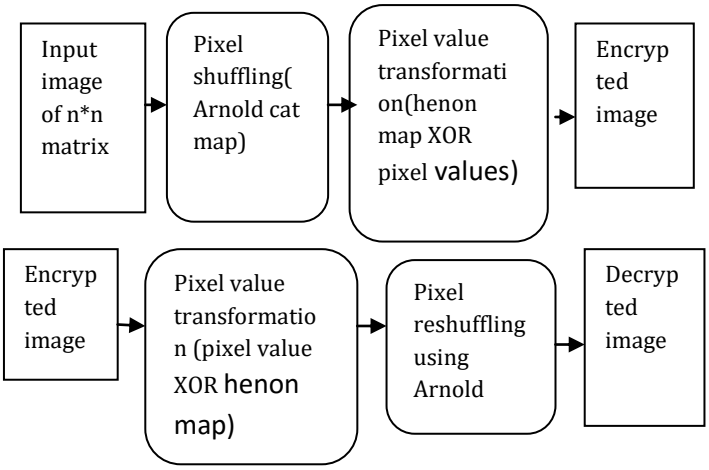

Fig 4: Architecture of image encryption and decryption

5. RESULTS.

In this section, results of the proposed image encryption algorithm are illustrated to appreciate the efficiency of proposed algorithm. Here, test image of size 256×256 is shown in Figure 5(a). The initial parameters for Henon map are chosen as a=1.4 and b=0.3 to make the system chaotic. Secret symmetric key for encryption is a combination of X1=0.01 and Y1=0.02. Figure 5(b) and Figure 5(c) illustrates shuffled image after two iterations and encrypted image respectively.

Figure 5.1: Encryption by Chaotic System

5.1.a)Original image | 5.1.b)Shuffle image | 5.1.c)Cipher image

Figure 5.2: Decryption by Chaotic System

5.2.a) cipher image | 5.2.b)shuffled image after decryption | 5.2.c) original image

Example of Arnold cat map.

For example, a 101 *x* 101 image has a period of twenty-five; whereas, a 124 *x* 124 image, as we just learned, has a period of fifteen. Other luminaries have found a relationship where this experimenter failed – but it certainly cannot be claimed to be elegant nor robust .

After fifteen iterations, the pixel – as would any other pixel in the image – has returned to its initial position, and it would continue eternally along this circle if iterated accordingly. This agrees with the earlier observation that the 124 *x* 124 image has a period of fifteen.

ordinary pixel $\begin{bmatrix} 52 \\ 13 \end{bmatrix}$ of the 124 *x* 124 image considered previously. It takes the following path:

$$\Gamma\begin{bmatrix} 32 \\ 13 \end{bmatrix} = \begin{bmatrix} 32 & 13 \\ 13 & 2\cdot 32 \end{bmatrix} \bmod 124 = \begin{bmatrix} 45 \\ 58 \end{bmatrix} \to \begin{bmatrix} 103 \\ 37 \end{bmatrix} \to \begin{bmatrix} 16 \\ 53 \end{bmatrix} \to \begin{bmatrix} 69 \\ 122 \end{bmatrix}$$

$$\to \begin{bmatrix} 67 \\ 65 \end{bmatrix} \to \begin{bmatrix} 8 \\ 73 \end{bmatrix} \to \begin{bmatrix} 81 \\ 30 \end{bmatrix} \to \begin{bmatrix} 111 \\ 17 \end{bmatrix} \to \begin{bmatrix} 4 \\ 21 \end{bmatrix} \to \begin{bmatrix} 25 \\ 46 \end{bmatrix} \to \begin{bmatrix} 71 \\ 117 \end{bmatrix}$$

$$\to \begin{bmatrix} 64 \\ 57 \end{bmatrix} \to \begin{bmatrix} 121 \\ 54 \end{bmatrix} \to \begin{bmatrix} 51 \\ 105 \end{bmatrix} \to \begin{bmatrix} 32 \\ 13 \end{bmatrix}$$

6. IMPLEMENTATION OUTPUT

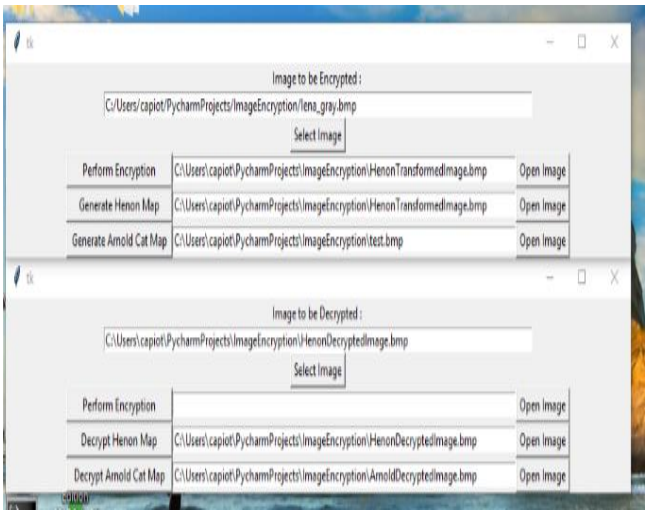

Fig 6.1 : GUI of henon and Arnold cat map.

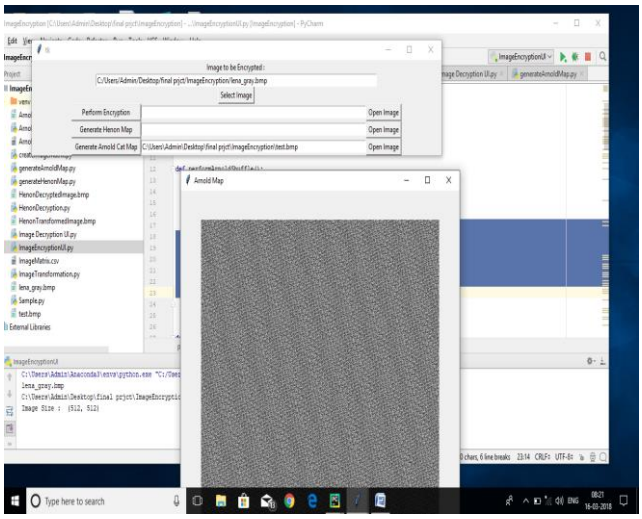

Fig 6.2: output of Arnold cat map

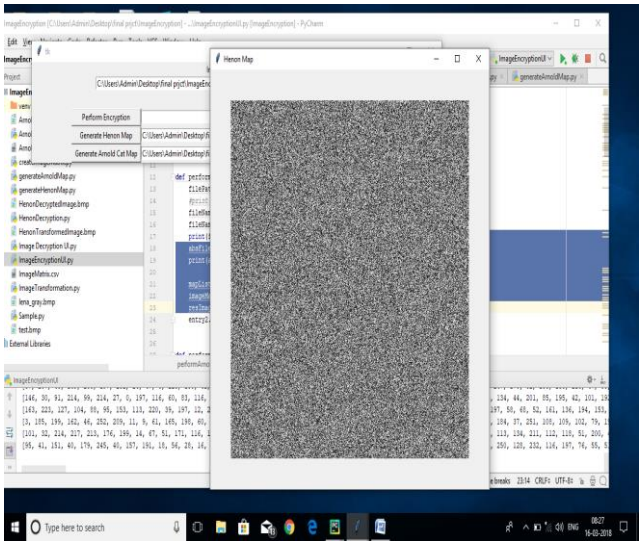

Fig 6.3: henon map output

7. CONCLUSION

In this paper, the chaotic system is highly sensitive to initial values and parameters of the system the security relies on a secret key along with the image encryption technique. Chaos is known for randomness, so it is highly secured. We used the randomness property of chaotic scheme i.e Arnold cat map and Henon map. The key value is generated using henon map and pixel shuffling is done using Arnold cat map. The process of decryption is same as encryption the same key is used for both the processes. This process will help to secure the data and unauthorized people cannot access the data.

REFERENCES

[1] Anita A. Lahane, Pranjali Sankhe, Surabhi Singh, Shruti Pimple," An Image Encryption and Decryption Using Chaotic Technique" Multicon-W:-CRTCE-2018 ISBN : 978-0-9994483-0-4 paper id-111

[2] 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

[3] G.Chaitanya,B.Keerthi,A.Saleem,"Animage Encryption and decryption using chaos algorithm" IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) eISSN:2278-2834,P-ISSN: 2278- 8735. Volume 10,IssUe ,Ver.11 (MarApr2015),pp103-108 http://www.osrjournal.org

[4] Yung Dong jiasheng Liu;canyan zhu; yiming wang;"Image encryption algorithm based on chaotic mapping" computer science and information technology(ICCSIT),2010

[5] Komal D Patel, SonalBelani "Image Encryption Using Different Techniques: A Review" International Journal of Emerging Technology and Advanced Engineering www.ijetae.com (ISSN 2250-2459, Volume 1, Issue 1, November 2011).

[6] Mayank mishra,prashant singh,chinmay garg "A new algorithm of encryption and decryption of image using chaotic mapping" international journal of information computation technology ISSN 0974-2239 Volume4 number7(2014)pp.741-746 international research publication house http://www.irphouse.com

[7] 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.

[8] M. Suneel, "Cryptographic Pseudo-random Sequences from the Chaotic Henon Map." Sadhana, vol. 34, no. 5, pp. 689–701, 2009.

[9] N.K.Pareek,V.Patidar,K.K.Sud "image encryption using chaotic logistic map" image and vision computingvol24,no.9,2006,pp.926934 http://www.irjet.org

[10] 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.

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