IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email:editoriijcs@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5992

# Arnold Cat Map Behavior Analysis To Image Pixels Scrambling

**Dr.O.Srinivasa Rao [1], B. Lakshmi Durga[2]**

[1] Associate Professor of CSE,
Department of CSE, UCEK, JNTUK, Kakinada

[2] M.Tech (IT) Student,
Department of CSE, UCEK, JNTUK, Kakinada

**ABSTRACT**

***Image scrambling techniques scramble the pixels of an image in such a manner that the image becomes chaotic and indistinguishable. This makes the scrambles images difficult to decode thus providing a high level of security to the images. Chaotic maps are usually used for pixel scrambling. One of the chaotic maps which is widely used in scrambling of image pixels is Arnold cat map. Arnold cat map algorithm utilizes the randomness of the chaotic map to shuffle the image pixels. This paper presents the analysis of Arnold cat map properties and periodicity.***
**Keywords:** Image scrambling, Chaotic map, Arnold's cat map, periodicity

## 1. INTRODUCTION

Digital information and data are transmitted more often over the Internet now-a-days. The availability and efficiency of global computer networks for the communication of digital Information and data have accelerated the popularity of digital media [1].To protect the digital information against unauthorized access has become extremely important. Data encryption is one of the most secure ways to protect data. Encryption of images is different from that of texts due to some intrinsic features of images such as bulk data capacity and high correlation between pixels [2][3],which are generally difficult to handle by traditional methods such as Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA) and Advanced Encryption Standard (AES).

Chaos is one of the emerging research direction in multimedia encryption and decryption. Chaos is discovered by Edward Lorenz in 1963[4]. Chaos system is dynamically non linear, a periodic, sensitive to initial conditions and deterministic in nature [5, 6, 7, 8]. The major core of encryption system consists of one or several chaotic maps serving the purpose of either just encrypting or scrambling the image. All image scrambling algorithms can be divided into two categories [9]. One is for confusion which changes position of pixels and the other is diffusion which changes the value of the pixels. Arnold cat map shuffles the position of pixel without changing the value of the pixel. In the scrambling process, the arrangement of the pixel values is changed from its original configuration to provide higher level of confusion[10].To achieve a higher level of unpredictability and randomness in the scrambling process the parameter of this differential have been choose critically.

## 2. Arnold Cat Map

Arnold transformation is commonly known as cat face transformation [11]. Arnold's cat map in recognition of Russian mathematician Vladimir I. Arnold, who discovered in 1960's using an image of cat [12, 13]. When applied to the digital image randomizes the original position of its pixels and the image becomes noisy. However, if iterated enough times the original image reappears. There are some words related to the ACM, one is torus and the other is phase space. A torus is the surface of a revolving circle in three dimensional spaces, around a disconnected axis that is coplanar to the circle. A phase space is a space in which all possible states of a system are represented, where the different states are all represented by one unique point in that phase space. Arnold transmission is given by the formula.

$$\Gamma: (x, y) \rightarrow (2x + y, x + y) \bmod n \qquad (1)$$

Equivalently in matrix notation that is

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email:editoriijcs@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5992

$$\Gamma\left(\begin{bmatrix}x\\y\end{bmatrix}\right) = \begin{bmatrix}2 & 1\\1 & 1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} \bmod n = \begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}\begin{bmatrix}1 & 0\\1 & 1\end{bmatrix}\begin{bmatrix}x\\y\end{bmatrix} \bmod n \quad (2)$$

We can also represent this as the system shown below,

$x_{n+1} = (2 * x_n + y_n) \bmod n$

$y_{n+1} = (x_n + y_n) \bmod n$

$x_n, y_n$ is the pixel location of the original image

N is the size of the input image

$x_{n+1}, y_{n+1}$ is the new pixel location in the shuffled image after applying Arnold transformation

Different number of iterations can produce different shuffling results. Arnold cat map introduces tension by performing matrix multiplication and folding by mod operation of matrix. Suppose a point (x, y) is an unit square rectangular the point (x, y) can be mapped to another point (x`, y`) as shown in the below graph (Fig .1). For example we assume n=11.

(x ,y) -> (2x+y, x+ y) mod 11

(1, 3) -> (2*1+3, 1+3) -> (5, 4) mod 11 -> (5, 4)

(4, 5) -> (2*4+5, 4+5) -> (13, 9) mod 11-> (2, 9)

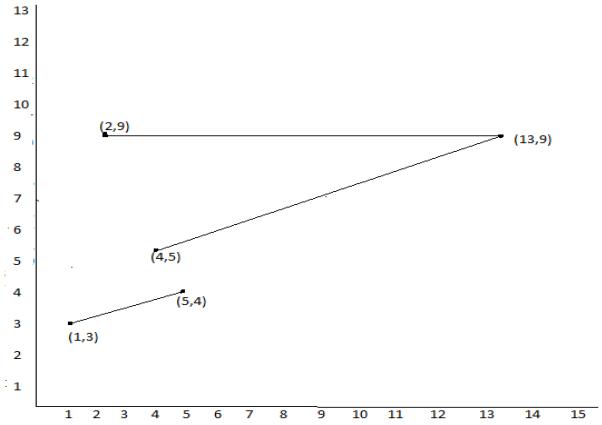


Fig .1 Mapping of pixel positions from original to new position

In the graph the pixel positions at (1, 3) are mapped to (5, 4) and the pixel positions at (4, 5) are mapped to (2, 9). After several iterations the correlation among the adjacent pixels can be completely disturbed. Arnold cat map algorithm can
randomize the image properly without reducing the value of the pixel in the image.

**3. Algorithm Performance Analysis**

An algorithm is satisfactory only when it is robust against all kinds of statistical and brute-force attacks. Here some
analysis has been performed on the Arnold cat map algorithm like Histogram analysis, Correlation coefficient analysis
etc.

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email:editoriijcs@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5992

### 3.1. Behavior and periodicity nature of ACM

An experiment is performed in MATLAB to determine the chaotic behavior and periodic nature of Arnold cat map. For this the following 124*124 image of Lena is iterated [14] with the transformation ţ and the original image re appears after 15 iterations.

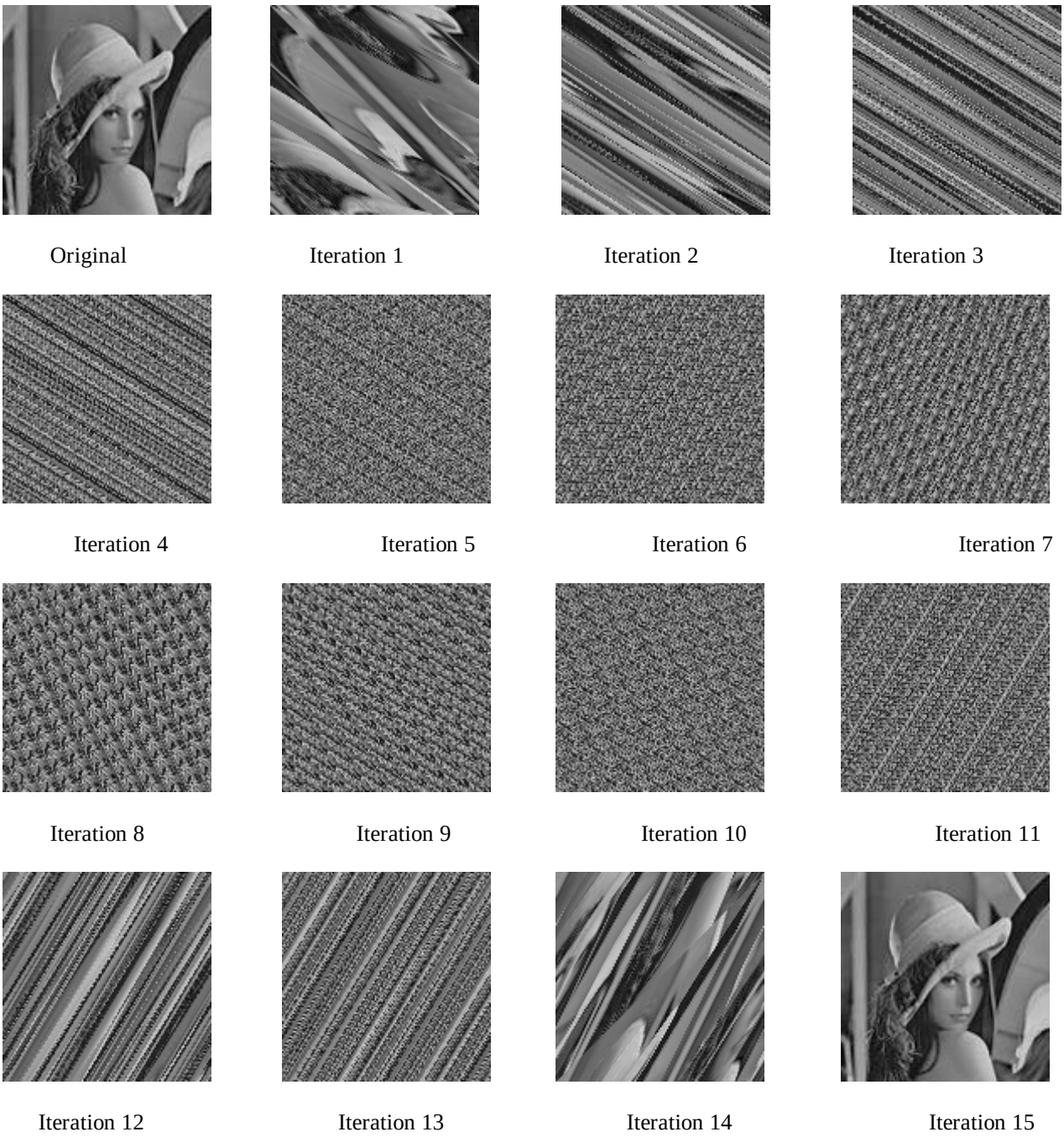


Fig.2. Results of simulation

As can be seen in the adjacent picture, the original image of the Lena is sheared and then wrapped around in the first iteration of the transformation. After some iterations, the resulting image appears rather random or disordered, yet after further iterations the image appears to have further order, multiple smaller copies arranged in a repeating structure and even upside-down copies of the original image and ultimately returns to the original image.

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email:editoriijcs@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5992

Arnold transformation is cyclical, that is when iterated to a certain step it will regain the original image. After Arnold transformation the image will become "chaotic state" but continue to use the Arnold transformation the image appears as original image and it has been proved that the periodicity of Arnold transformation has some relation with the size of the image. Table 1 gives the corresponding Arnold periodicity and shuffling time with different sizes of the square image which is performed on Sony laptop with Hardware specifications as, AMD E-350 processor (1.6GHz), Hard Disk Drive (320GB) and RAM (2GB). Clearly the periodicity of Arnold transformation is related to the image size but disproportionately, The No of iterations and shuffling time varies with the size of the image which is shown in a graph (Fig. 3).

**Table1**: Arnold periodicity and shuffling time

| Image | S.NO | Size | No of iterations | Shuffling time (in sec) |
|---|---|---|---|---|
| Lena .jpg | 1 | 32 * 32 | 24 | 3 |
| | 2 | 64 * 64 | 48 | 5 |
| | 3 | 124 * 124 | 15 | 2 |
| | 4 | 188 * 188 | 48 | 8 |
| | 5 | 254 * 254 | 384 | 85 |
| | 6 | 378 * 378 | 72 | 29 |
| | 7 | 512 * 512 | 384 | 256 |
| | 8 | 764 * 764 | 285 | 393 |
| | 9 | 1024 *1024 | 768 | 1868 |

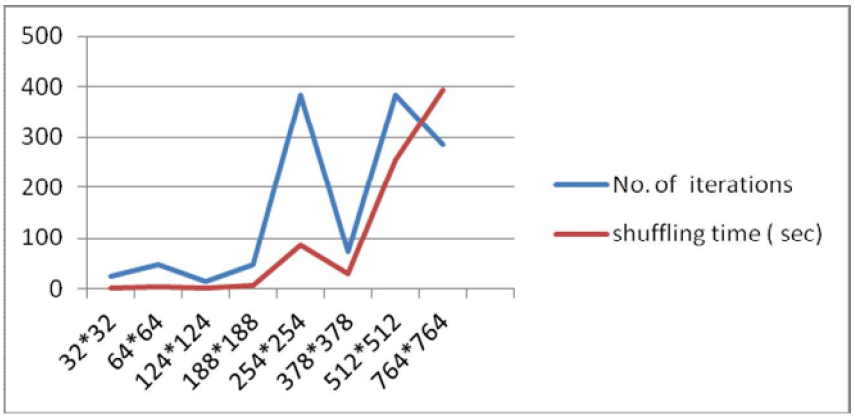


Fig. 3 The No of iterations and shuffling time changes with the image size

The various observations and properties that are drawn from the experimental study of the Arnold transformation.

- Arnold's cat map works only for square images ,it doesn't work for rectangular images
- The encryption times are different because the image shuffling and reshuffling varies on the no of iterations for example 64*64 takes 48 iterations, where as 124*124 image took only 15 iterations to retain the original image
- No of iterations depend upon only the dimension of the image not the type of image
- Even if no of iterations are same for different dimensions of the image, the shuffling time is different

(64*64) -> 48 iterations -> 5sec
(188*188) -> 48 iterations -> 8sec

- The number of iterations needed to restore the image can be never exceed 3N ( N is the size of the image)

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email:editoriijcs@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5992

- The results after applying the Arnold cat map will be shuffled image that contains all of the same pixels values of the original image
- Arnold transformation is periodic in nature which means that the pixels return to their original position after specific number of iterations

### 3.2 Histogram analysis

An image histogram illustrates how pixels in an image are distributed by graphing the number of pixels at each intensity level. In general histogram of original image is not uniformly disturbed. We compare the histograms of leena.png before and after shuffling to analyze the performance of the algorithm. Arnold cat map shuffles only the position of the pixels in the image, since the histogram of the plain image is same as the shuffled image. The histograms of the original image and various iterations is shown in Fig .4

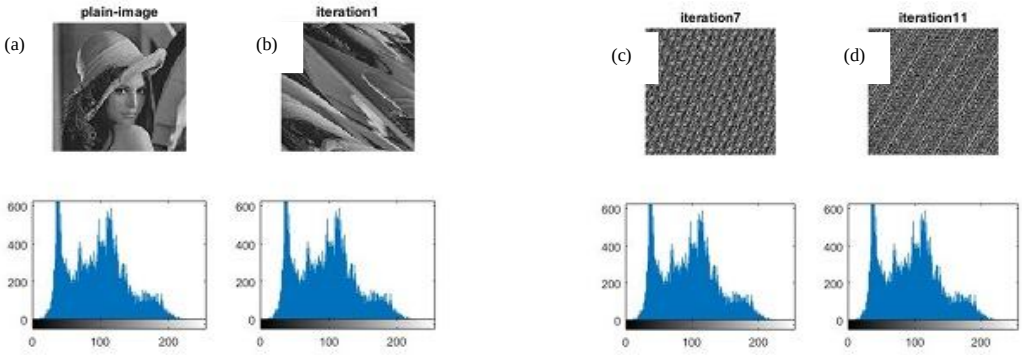


Fig. 4 Histograms of plain - image and the shuffled images

### 3.3 Coefficient Correlation Analysis

Correlation analysis gives a statistical measure of the similarity between the adjacent pixels of the encrypted image. In the original image the adjacent pixels are highly correlated to each other as they are closely located. After the image is shuffled using Arnold cat map the correlation is completely destroyed as almost all the pixels are scattered. The value of the Correlation coefficient lies between -1 and 1. If value of the correlation coefficient is '0' then it indicates adjacent pixels of the image are completely different and if value of correlation coefficient is '1' then adjacent pixels of the image are identical. The correlation coefficient is given by

$$\rho = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (4)$$

$$cov(x,y) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))(y_i - E(y)) \quad (5)$$

$$D(x) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))^2 \quad (6)$$

$$E(x) = \frac{1}{L}\sum_{i=1}^{L}(x_i) \quad (7)$$

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email:editoriijcs@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5992

Where x and y are grey levels of two adjacent pixels in the image, N is the number of pairs of adjacent pixels. Consider a image with size 124*124, when applied Arnold transformation generates 15 iterations. The correlation between the original image and iterations obtained by the Arnold transformation are listed in table 2.The relation between the horizontal, vertical and diagonal correlations in shown in Fig.6

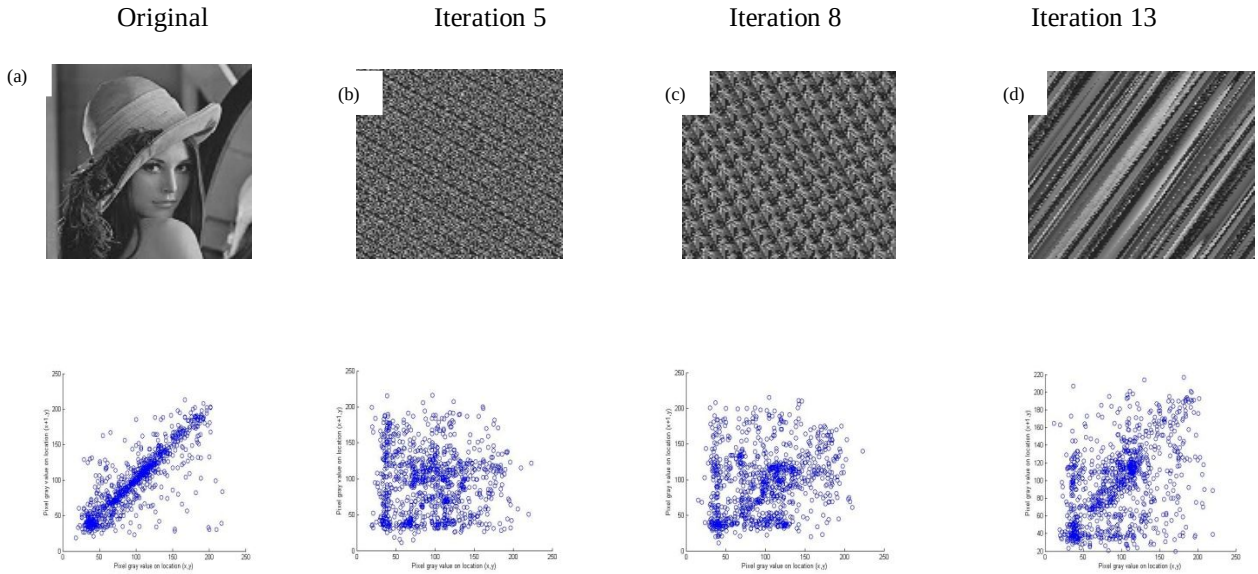


Fig. 5 Correlation of two horizontally adjacent pixels in the Plain-image and Shuffled images

**Table2**. Correlation coefficient of original image and shuffled image

| Pixel relation | Horizontal Correlation | Vertical Correlation | Diagonal Correlation |
|---|---|---|---|
| Original | 0.8718 | 0.9163 | 0.9123 |
| Iteration2 | 0.7051 | 0.5861 | 0.5848 |
| Iteration4 | 0.1383 | 0.0943 | 0.0959 |
| Iteration6 | -0.1128 | -0.0038 | -0.0039 |
| Iteration8 | 0.2148 | 0.3072 | 0.3075 |
| Iteration10 | -0.0327 | -0.0563 | -0.0571 |
| Iteration12 | 0.0995 | 0.2327 | 0.2348 |
| Iteration14 | 0.7153 | 0.8273 | 0.9123 |

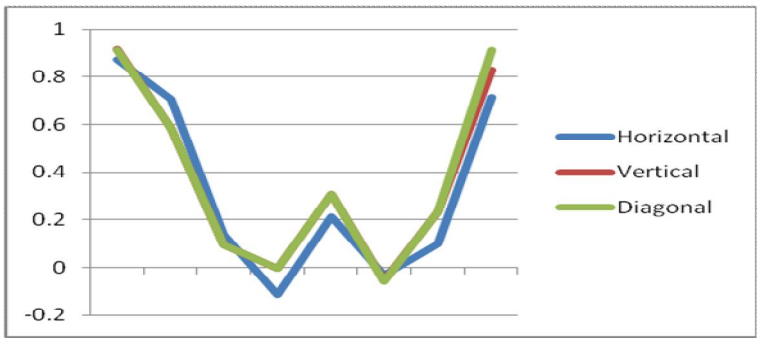


Fig .6 Relation between Horizontal, Vertical and Diagonal Correlation

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email:editoriijcs@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5992

### 3.4 MSE and PSNR

Image distortion can be measured using MSE as given in below equation. Peak Signal to Noise Ratio is the ratio between the maximum possible value of a signal and the power of distorting noise that affects the quality of its representation. MSE and PSNR are calculated using

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}[(I(x,y) - \hat{I}(x,y))^2] \quad (8)$$

$$PSNR = 10 \log_{10} 255^2/MSE \quad (9)$$

After the image is shuffled using Arnold cat map, PSNR is calculated for the shuffled image with respective to the original to know whether any noise is generated during the shuffling process. The results are listed in table 3

**Table3**. MSE and PSNR Results

| Pixel relation | MSE | PSNR |
|---|---|---|
| Iteration1 | 4.019e+03 | 12.0973 |
| Iteration3 | 3.7505e+03 | 12.3900 |
| Iteration5 | 3.7824e+03 | 12.3532 |
| Iteration7 | 3.7671e+03 | 12.3708 |
| Iteration9 | 3.7787e+03 | 12.3574 |
| Iteration11 | 3.8019e+03 | 12.3307 |
| Iteration13 | 3.7758e+03 | 12.3607 |
| Iteration15 | 0 | Infinity |

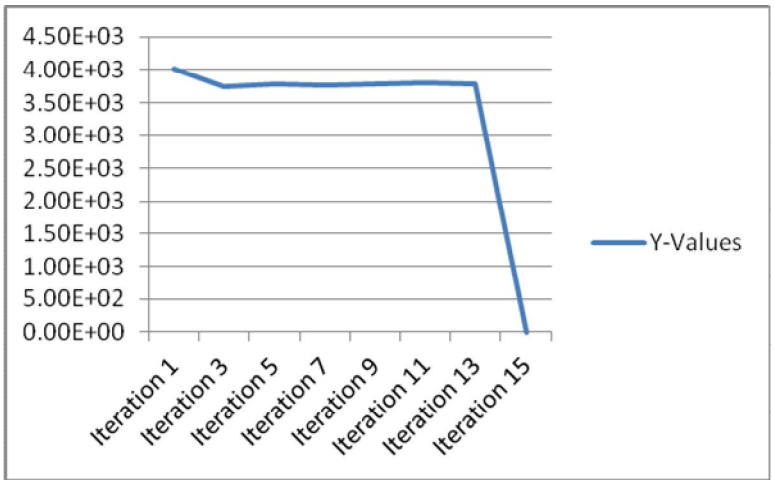


Fig .7 The variations of MSE value at each shuffled image

IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email:editoriijcs@ipasj.org
Volume 6, Issue 4, April 2018 ISSN 2321-5992

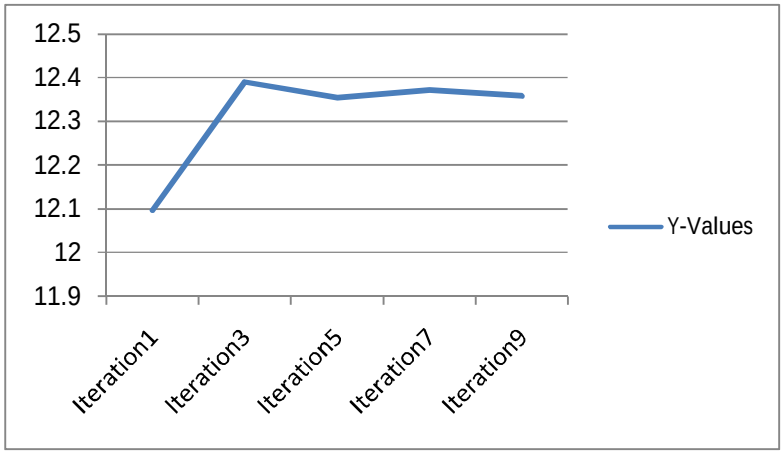


Fig.8 The change in PSNR value at each Iteration

**4. Conclusion**

Arnold's cat map is simple and efficient in implementation to shuffle the image pixels and to completely disturb the correlation between the pixels but it is unsatisfactorily insensitive to changes in its controlling parameters. For image shuffling using the Cat map, the image may be recovered by iterating the chaotic map for some rounds under some control parameters. Arnold cat map has a lower key space so it can be combined with other chaotic maps to produce the encryption that is more resistant to brute force attacks.

**References**

[1] Pragati Thapliyal, Madhu Sharma "Image Encryption Scheme Using Chaotic Map". International Journal of Multidisciplinary in Cryptology and Information Security, volume 4, No.1, January- February 2015

[2] Chen GR, Mao YB. "A Symmetric Image Encryption Scheme Based on 3D Chaotic Cat Maps". Chaos, Solitons & Fractals 2004, vol 21, pp 749–61, 2004.

[3] Chiaraluce F, Ciccarelli L. "A New Chaotic Algorithm for Video Encryption". IEEE Trans Consum Electron2002, vol 48, pp 838–43, 2007.

[4] Hossain, Md Belayat, Md Toufikur Rahman, and Shariful Islam. "A new approach of image encryption using 3D chaotic map to enhance security of multimedia component." Proceedings of IEEE International Conference on Informatics, Electronics and Vision, 2014, pp. 1-6.

[5] Kocarev L. Chaos-based cryptography: a brief overview. IEEE Circ Syst Mag 2001;1(3):6–21.

[6] Kocarev L, Jakimovski G. Chaos and cryptography: from chaotic maps to encryption algorithms. IEEE Trans Circ Syst—I 2001;48(2):163–9.

[7] Mao YB, Chen G. Chaos-based image encryption. Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neurocomputing and Robotics. New York: Springer-Verlag; in press, 2004.

[8] Banerjee, Santo, ed. Chaos Synchronization and Cryptography for Secure Communications: Applications for Encryption: Applications for Encryption. IGI Global, 2010

[9] Mohamed H. Beheril, Mohamed Amin\ Xianhua Song2, Ahmed A. Abd EI-Latifl "Quantum Image Encryption Based on Scrambling-Diffusion (SD) Approach" 2016 2nd International Conference on Frontiers of Signal Processing

[10] Fahad bin Muhaya, Muhammad Usama and Fahim Akhter "chaos based secure storage and transmission of digital medical images". Appl .Math.Inf.Sci.8,No.1L,27-33(2014)

[11] Zhenwei Shang Honge Ren Jian Zhang "A Block Location Scrambling Algorithm of Digital Image Based on Arnold Transformation" The 9th International Conference for Young Computer Scientists

[12] A. Jolfaei and A. Mirghadri, "A Novel Image Encryption Scheme Using Pixel Shuffler and A5/1." Proceedings of the 2010 International Conference on Artificial Intelligence and Computational Intelligence(AICI10), Sanya, China, 2010.

[13] Agyan Kumar Prusty, Asutosh Pattanaik, Swastik Mishra "An Image Encryption & Decryption Approach Based on Pixel Shuffling Using Arnold Cat Map & Henon Map"

2013 International Conference on Advanced Computing and Communication Systems (ICACCS -2013), Dec. 19 – 21, 2013, Coimbatore, INDIA

[14] Gabriel Peterson "Arnold's Cat Map" Math 45 – Linear Algebra , Fall 1997

[15] Fredrik Svanstrom " properties of generalized Arnold's discrete cat map".