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

Image Encryption Using Arnold Transformation & Random Permutation

Ashis Kashyep[1], Sharma Prashant Kumar[2], Girish D. Bonde[3]

[1,2]B.E.(Student) Electronics & Telecommunication Department J.T.M.C.O.E. Fizpur
[3]Assistant Professor, Dept. of Electronics & Telecommunication Engineering, J.T. Mahajan college Of Engineering Faizpur , Maharashtra , India

---

Abstract - *Encyption is an effective way to protect the content of digital media. Arnold transform is a significant technique of image Encryption. Security of information is main aspect in network communication. The information may be in the form of text, voice and multimedia. There are various encryption method to secure image from unauthorized parties. In the proposed work, image is encypted using different combination random permutation techniques. In today's growing world of digital technology, access to the multimedia content is very easy. Encryption process prevents the image data from unauthorized user. The primary goal is security management. This will provide integrity, accuracy and safety of image which is travelling over internet.*

***Key Words*: Encryption, Arnold Transformation, Random Permutation.**

1. INTRODUCTION

Information security becomes an important and urgent issue not only for individuals but also for business and governments. Security of multimedia data is receiving more and more attention due to the widespread transmission over various communication networks. It has been noticed that the traditional text encryption schemes fail to safely protect multimedia data due to some special properties of these data and some specific requirements of multimedia processing systems, such as bulky size and strong redundancy of uncompressed data. Security of image data is very important in many areas, such as privacy and copyright protection, security communication, and also in military applications. Image Encryption is a good method for providing security to image data, by making image visually unreadable and also difficult to decrypt it for unauthorized users [1].Digital image encryption technology is a way of securing digital image information. With the use of transformation techniques, it can change the original image into a disordered one beyond recognition, making it hard for those who get the image in unauthorized manner to extract information of the original image from the encrypted images.

Already there exist several image encryption methods in spatial domain, among which chaotic-based methods are most popular. Image position permutation includes matrix based transformation, for example: Arnold transformation, magic transformation, gray code and generalized gray code for permutation method, Permutation of IFS model based on fractal geometry and permutation based on Hilbert curve, FASS curve and Tangram algorithm. Image position permutation belongs to image coordinate permutation. Image pixel value transformation includes changing the number of 0,1 bits of the original image pixel, such as the well-known xor transformation, substitution transformation and the permutation that didn't change the number of 0,1 bits of the original image, such as circular bit shift of pixel value[2].

In the recent years, with the development of network and multimedia technology, multimedia data, especially image, audio and video data, is used more and more widely in human society. Some multimedia data, including entertainment, politics, economics, militaries, industries, education etc, are necessary to be protected by providing confidentiality, integrity, and ownership or identity. In this regard, to protect multimedia contents, cryptology, which appears to be an effective way for information security, has been employed in many practical applications [3].

2. RELATED WORKS

Image Encryption Using Arnold Transformation

The Arnold transform is an image scrambling technique that can be used to encrypt and decrypt image data. The transform is area preserving and invertible without loss of information. It is also known as cat map. The mapping can be done successively several times to completely obscure the image beyond recognition. Alice has the information about the number of times the transform is applied and can successfully recover the original image [2]. Images are composed of discrete units called pixels. A pixel is the basic unit representing some colour value, which when taken together form the image. The image is a m×n matrix, where m represents the number of rows of pixels and n the number of columns of pixels, and each entry in the matrix being a numeric value that represents a given colour.

Let X be the image matrix shown below, it is possible to examine selected entries in X. The numeric entries represent some colour value. It is a simple and elegant

demonstration and illustration of some of the principles of chaos namely, underlying order to an apparently random evolution of a system.

$$X = \begin{bmatrix} 217\ 217\ 217\ 217 \dots 217\ 217\ 217\ 217 \\ 251\ 251\ 251\ 251 \dots 251\ 251\ 251\ 251 \\ 251\ 251\ 251\ 251 \dots 251\ 251\ 251\ 251 \\ 251\ 251\ 251\ 251 \dots 251\ 251\ 251\ 251 \\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots\ \vdots \\ 251\ 251\ 251\ 251 \dots 251\ 251\ 251\ 251 \\ 251\ 251\ 251\ 251 \dots 251\ 251\ 251\ 251 \\ 251\ 251\ 251\ 251 \dots 251\ 251\ 251\ 251 \\ 217\ 217\ 217\ 217 \dots 217\ 217\ 217\ 217 \end{bmatrix} \quad (1)$$

Arnold's cat map is the transformation

$$T\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} mod\ n$$

Where, mod is, the modulo of the $\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$ (2)

For understanding the mechanism of the transformation better, it can be decomposed into elemental pieces.

1. Shear in the *x*-direction by a factor of 1.

$$\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ y \end{bmatrix} \quad (3)$$

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

$$T\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x \\ x+y \end{bmatrix} \quad (4)$$

The Arnolds transformation have the drawback that it requires only squared images. It cannot implement on different width and height images. Hence it requires the reshaping of the image in nxn image matrix.

The Arnolds transformation have the drawback that it requires only squared images. It cannot implement on different width and height images. Hence it requires the reshaping of the image in n x n image matrix.

Following steps include in encryption algorithm by Arnold transformation

1. Input original image.
2. Resize the original image into n x n matrix.
3. apply the Arnolds transformation to n x n matrix by using the equation

$$T\begin{bmatrix} x \\ y \end{bmatrix} \rightarrow \begin{bmatrix} x+y \\ x+2y \end{bmatrix} mod\ n$$

Where, mod is modulo of $\begin{bmatrix} x+y \\ x+2y \end{bmatrix}$

a) Shear in x- direction by factor of 1.
b) Shear in y- direction by factor of 1.
c) Evaluate modulo

4. Reassemble the image.

Image Encryption Using Random Permutation:

The development of image encryption using chaotic random permutation is attracted in recent year. The basic permutation can be performed in three ways such as bit, pixel and block permutation. The permutation of bits is effective in significantly reducing the correlation thereby decreasing the perceptual information, whereas the permutation of pixels and blocks are good at producing higher level security compared to bit permutation [4]. A pixel in a digital image is collection of 8 bits therefore maximum available key of bit permutation is equal to 8! (40320) .The pixel permutation can be performed by shuffling the pixel position according to the encryption key. The encryption key size can be one dimensional (1-D) or two dimensional (2-D) for pixel permutation. 2-D key has more number of encryption key as compare to 1-D key. The encrypted image can be decrypted only if attacker has knowledge of key and large numbers of possible key spaces make it infeasible to extract the original information.

The encryption algorithm includes following steps:

1. Input original image.
2. Find the size of original image (total number rows and columns)
3. Reshape the matrix (total number of rows and columns) whose elements are taken column wise sequence.
4. Convert the sequence of decimal values into binary bits (unit 8).
5. Apply random permutation (p) to sequence.
6. Convert the sequence of binary bit values to decimal.
7. Reconstruct the sequence into image size (total number of rows and columns).
8. End.

The decryption algorithm includes following steps:

1. Input scrambled image
2. Reshape the matrix (total number of rows and columns) whose elements are taken column wise sequence.
3. Convert the sequence of decimal values into binary bits (unit 8).
4. Reconstruct the random permutation by using value (p).
5. Convert the sequence of binary bit values to decimal.
6. Reconstruct the sequence into image size (total number of rows and columns).
7. End.

3. Performance Parameters :

In Comparison of Both Two Methods Parameters are like as Entropy, Co-relation, Peak Signal Noise Ratio (PSNR), Mean Square Error (MSE), Number Of Pixels Change Rate (NPCR) And Unified Average Changing Intensity (UACI).

3.1 Information entropy:

It identifies the degree of uncertainty and uniform distribution in the system. Thus, an encryption technique should show randomness and uniform distribution in the encryption process. Information entropy is calculated by the following formula.

$$H(m) = -\sum_{i=0}^{2^N-1} P(m_i) log_2[P(m_i)]$$

Where p (mi) defines the probability of a pixel and N is the number of bits in each pixel. For a gray level image, each pixel has 8 bits, so the probability of a pixel is 1⁄28. Hence, information entropy of the gray level image is H (m) = 8. However, practically it is intricate to obtain ideal entropy; so slight difference is also tolerable.

3.2 Correlation analyses:

It assesses the correlation between two adjoining pixels of the plain-image and the cipher image [5]. An encrypted image should have low correlation between two abutting pixels. For example, xi and yi are two pixel pair then the correlation coefficient can be calculated by equation (5)

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2$$

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

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

where $\sqrt{D(x)} \neq 0$ *and* $\sqrt{D(y) \neq 0}$
Here xi and yi are gray level value of two adjacent pixels, N is the number of pairs (xi, yi) and E(x) is the mean of xi and E(y) is the mean of yi.

3.3 Number of Pixels Change Rate(NPCR):

NPCR evaluates the pixels change rate in the coded image after modification in one pixel of a prime image, consequently, high NPCR value is effective.

$$NPCR = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j) \times 100\ \%$$

Where $D(i,j) = 0$ else $D(i,j) = 1$

3.4 Unified Average Changing Intensity(UACI):

UACI computes the variation in intensity of the corresponding pixel of the plain image and the encrypted image. If C1 and C2 are the two cipher image after and prior to 1 bit change in the original image, then UACI can be calculated by following formula.

$$UACI = \left[\sum_{i=0}^{M}\sum_{j=0}^{N} \frac{C1(i,j) - C2(i,j)}{255}\right] \times \frac{100\%}{M \times N}$$

Where, M and N are the dimension and (i, j) is the coordinates of the image, With if $C1(i,j) = C2(i,j)$

3.5 Mean Square Error (M (1)

The mean square error (MSE) is the squared norm of the difference between the data and the approximation divided by the number of elements. The mean square error between a signal or image, X, and an approximation, Y, is the squared norm of the difference divided by the number of elements in the signal or image.

3.6 Peak Signal to Noise Ratio (PSNR):

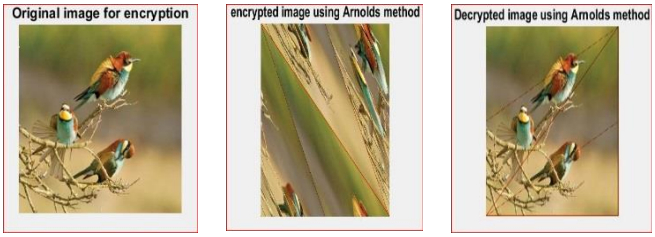
PSNR is the peak signal-to-noise ratio in decibels (dB). The PSNR is only meaningful for data encoded in terms of bits per sample, or bits per pixel. For example, an image with 8 bits per pixel contains integers from 0 to 255. The following equation defines the PSNR:

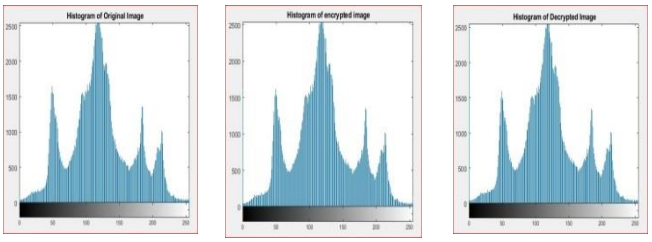
$$20 \log_{10}\left(\frac{2^B - 1}{\sqrt{MSE}}\right)$$

Where MSE represents the mean square error and B represents the bits per sample.

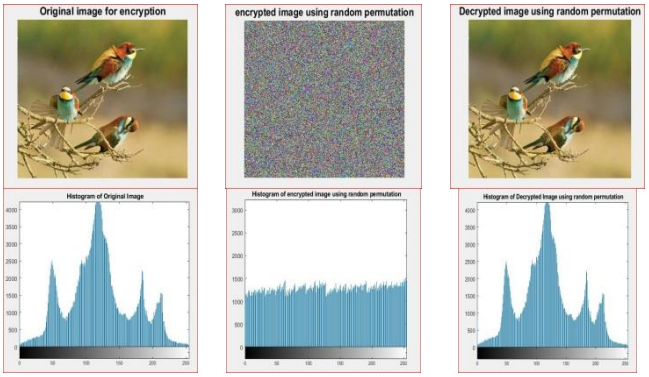
4. RESULTS :

Arnold Transformation : Image I

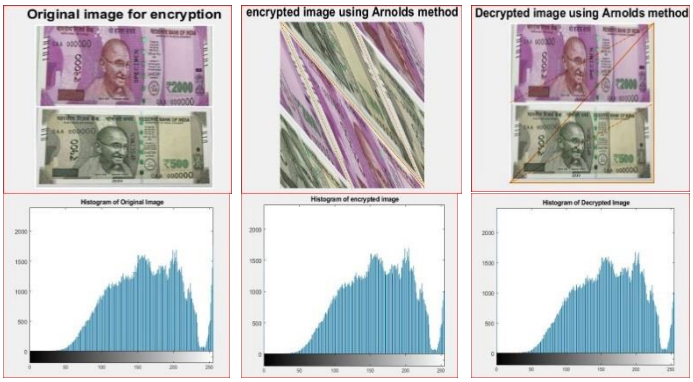




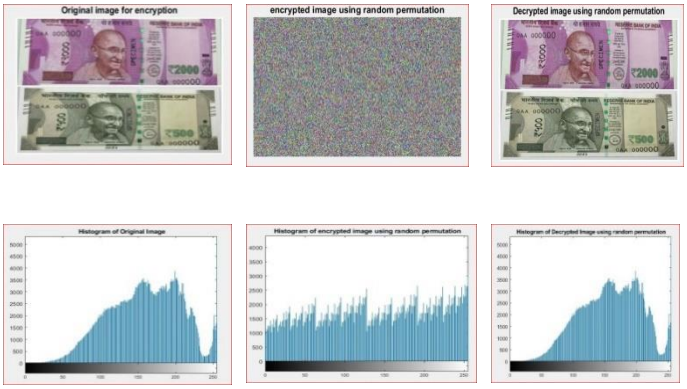
Random Permutation: Image I



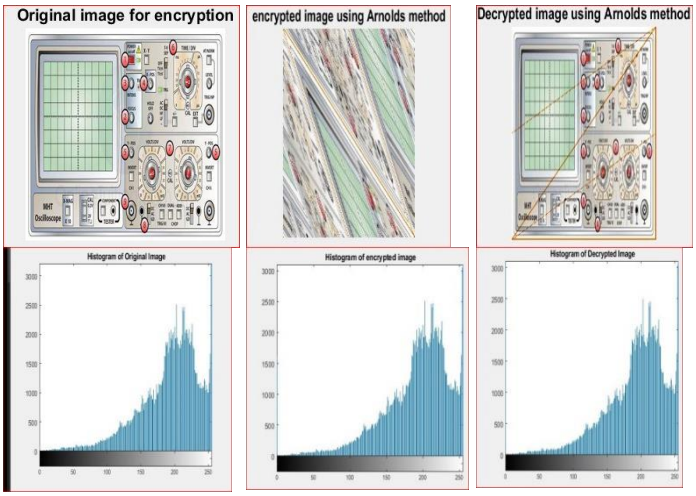
Arnold Transformation : Image II



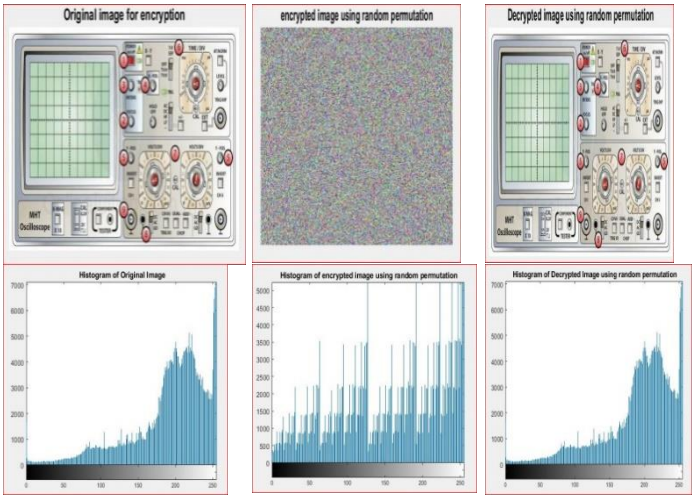
Random Permutation : Image II



Arnold Transformation : FIGURE III



Random Permutation : Image III



Comparison With Readings :

Arnold Transformation :

Parameters	Fig I	Fig II	Fig III
Entropy(original)	7.470171	7.468395	7.146435
Entropy(Encrypted)	7.477052	7.476485	7.174589
Corelation (Original)	0.822909	0.776512	0.478045
Corelation(Encrypted)	0.719970	0.455113	0.087267
PSNR IN dB	25.070465	19.741554	19.081243
MSE	202.317698	690.12049	803.444794
NPCR	0.991755	0.994049	0.990977
UACI	0.175235	0.209696	0.199089

Random Permutation :

Parameters	Fig I	Fig II	Fig III
Entropy(Original)	7.502477	7.515674	7.207396
Entropy(Encrypted)	7.996904	7.967016	7.708355

Corelation(Original)	0.831721	0.806821	0.490561
Corelation(Encrypted)	0.002874	0.000986	0.001099
PSNR In dB	Infinity	Infinity	Infinity
MSE	0.000000	0.000000	0.000000
NPCR	0.996026	0.995920	0.993947
UACI	0.289958	0.291542	0.302359s

5. CONCLUSION :

In this paper, we have presented image encryption techniques. Image Encryption using Arnold's transformation and Random permutation. Experimental studies were conducted by applying both encryption techniques. The effectiveness of proposed method is validated by statistical analysis, visual testing, entropy analysis, and differential analysis which have been presented in previous section. It is found that the Random Permutation Encryption Method is better than the Arnold Transformation Method

REFERENCES :

[1] Makera M Aziz, Dena Rafa Ahemad 'Simple Image Scrambling Algorithm Based on Random Number Generation" IJARCSSE, volume 5, issue 9,September 2015.

[2] S.Liping,Qin, Z. Liu Bo, Q. Jun, L.Huan," Image Scrambling Algorithm Based on Random Shuffling Strategy"3rd IEEE Conference on Industrial Electronics and Applications, 2008,pp. 2278 – 2283

[3] Zhaopin Su, Guofu Zhang and Jianguo Jiang (2012). Multimedia Security: A Survey of Chaos-Based Encryption Technology, Multimedia - A Multidisciplinary Approach to Complex Issues, Dr. Ioannis Karydis (Ed.).

[4] T. Shivakumaar and R. Venkateshan,"A New Image Encryption Method Based on Knights Travel Path and True Random Number" Journal of Information Science and Engineering 32, 133-152 (2016) .

[5]Khalid Hamdnaalla, Abubaker Wahaballa, Osman Wahballa, " Digital Image Confidentiality Depends upon Arnolds Transformation and RC4 Algorithms" International journal of Video & Image Processing and Network Security IJVIPNS-IJENS volume 13, No. 04. August 2013.

[6]. 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, 2008

[7]Ravi Praksh Devangan et.al, " Image Encryption using Random Permutation by Different Keys" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 10, October 2015.

[8]Shao Z. Qin, B. Liu J. Qin and H Li., "Image Scrambling Algorithm Based on Random Shuffling Strategy", in ICIEA 2008, pp. 2278-2283 S

Authors:

Ashis Kashyep,
BE (E&Tc)Students,
J T M C O E Faizpur
Maharashtra.

Sharma Prashant Kumar
BE (E&Tc)Students,
J T M C O E Faizpur
Maharashtra.

Girish D Bonde,
Assistant Professor
J T M C O E Faizpur
Maharashtra.