

IMAGE TRANSCRIPTION USING ARNOLD TRANSFORMATION & XOR

A Project Work Submitted
of the requirements for the Degree of
BACHELOR OF TECHNOLOGY
in
COMPUTER SCIENCE & ENGINEERING
by

RITTICK MONDAL (Roll No. 10700117034)
&
ABHIRUP CHAKRABORTY (Roll No. 10700117065)

Under the supervision of
Prof. Chinmay Maiti



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
COLLEGE OF ENGINEERING & MANAGEMENT, KOLAGHAT
(*Affiliated to MAKAUT, WB*)

Purba Medinipur – 721171, West Bengal, India
July 2021



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

COLLEGE OF ENGINEERING & MANAGEMENT, KOLAGHAT

(Affiliated to MAKAUT, WB)

Purba Medinipur – 721171, West Bengal, India

CERTIFICATE OF APPROVAL

This is to certify that the work embodied in this project entitled “**Image Encryption Algorithms using Arnold Transformation & XOR**” submitted by Rittick Mondal, Abhirup Chakraborty, to the Department of Computer Science & Engineering, is carried out under my direct supervision and guidance.

The project work has been prepared as per the regulations of MAKAUT and I strongly recommend that this project work be accepted in partial fulfilment of the requirement for the degree of B.Tech.

Supervisor

Prof. Chinmay Maiti

Asst. Prof. Dept. of CSE

Countersigned by ,

Prof. (Dr.) Tapas Kr. Maity

Head, Department of CSE



DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

COLLEGE OF ENGINEERING & MANAGEMENT, KOLAGHAT

(Affiliated to MAKAUT, WB)

Purba Medinipur – 721171, West Bengal, India

Certificate by the Board of Examiners

This is to certify that the project work entitled “**Image Encryption Algorithms using Arnold Transformation & XOR**” submitted by Rittick Mondal, Abhirup Chakraborty, to the Department of Computer Science and Engineering of College of Engineering of Management, Kolaghat has been examined and evaluated.

The project work has been prepared as per the regulations of MAKAUT and qualifies to be accepted in partial fulfilment of the requirement for the degree of B. Tech.

Project Coordinator

Board of Examiners

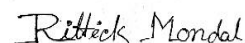
ACKNOWLEDGEMENT

It gives us great pleasure to find an opportunity to express our deep and sincere gratitude to our project guide Mr. Chinmay Maiti. We do very respectfully recollect his constant encouragement, kind attention and keen interest throughout the course of our work. We are highly indebted to him for the way he model and structured our work with his valuable tips and suggestions that he accorded to us in every respect of our work.

We are extremely grateful to the Department of Computer Science & Engineering, CEMK, for extending all the facilities of our department.

We humbly extend our sense of gratitude to other faculty members, laboratory staff, library staff and administration of this Institute for providing us their valuable help and time with a congenial working environment.

Last but not the least, we would like to convey our heartiest thanks to all our classmates who from time to time have helped us with their valuable suggestions during our project work.



RITTICK MONDAL

University Roll No. 10700117034

University Registration No.171070110032

Date:- 9th July, 2021



ABHIRUP CHAKRABORTY

University Roll No. 10700117065

University Registration No. 171070110001

ABSTRACT

Encryption is a process of encoding information .This process converts the original representation of the information none as plane text into an alternative form none as cipher text. We use encryption for security purpose. It is used in medical field, to study the environment and weather, to study the properties of different materials in industries, for human perception etc. Here we used Arnold Transformation for encryption process and different combination and process are used to achieve better result. Experimental results show that the new algorithm improve the image security effectively to avoid deciphering and it is also can restore the image as almost the same as the original image, which reaches to the purpose of image safe and reliable transmission.

CONTENT

1. Introduction	7
1.1 What is Encryption	8
1.2 Why Encryption ?	8
1.3 Different Types of Image Encryption	8
1.3.1 DES Encryption	9
1.3.2 AES Encryption	9
1.3.3 RSA Encryption	9
1.4 Application of Image Encryption	10
2. Different Image Encryption Technique	11
2.1 Arnold Transformation	11
2.1.1 Modified Arnold Transformation	11
2.2 Fibonacci-Q Transformation	12
2.3.1 Generalized Fibonacci Transformation	12
2.3 XOR Operation Based Encryption	13
2.4 Fibonacci-Lucus Transformation	14
3. Proposed Encryption Algorithm	15
3.1 Block Diagram of Encryption Process	15
3.2 Decryption Algorithm	16
3.3 Block Diagram of Decryption Process	17
4. Experimental Result	18
5. Conclusion	26
6. Reference	27

1. INTRODUCTION

With rapid advancement in Internet and networking technologies during the recent years, communication and information exchange have become much easier and faster but at the same time the issues related to data security and confidentiality have become a major concern of the time. To cater to this need of information security, a number of hidden and secret communication techniques such as cryptography, anonymity, covert channels, Steganography, Watermarking etc have been developed. Out of all these methods, the digital image Steganographic methods have been heavily used by the researchers during the last few decades for the purpose of secret communication and information authentication due to the size and popularity of digital images.

The digital image Steganographic methods generally depends upon various image scrambling techniques in order to further improve the level of security of the hidden information. Image scrambling techniques scramble the pixels of an image in such a manner that the image becomes chaotic and indistinguishable. These scrambling techniques generally use several keys for encryption and decryption and without the correct keys and an appropriate method; the third party users cannot access the secret information even if they are able to sniff the medium. Hence, the message remains highly secured against unauthorized access. Even though, a number of image scrambling techniques have been developed by different researchers during the last two decades, a lot of research is still going on in this area. Here in this paper we have developed a simple but powerful 2x2 chaotic map combining the most famous Fibonacci and Lucas series.

1.1 What is Encryption?

Encryption is a way of scrambling data so that only authorized parties can understand the information. In technical terms, it is the process of converting human-readable plaintext to incomprehensible text, also known as cipher text. In simpler terms, encryption takes readable data and alters it so that it appears random. Encryption requires the use of a cryptographic key which is a set of mathematical values that both the sender and the recipient of an encrypted message agree on.

Data can be encrypted "at rest," when it is stored, or "in transit," while it is being transmitted somewhere else.

1.2 Why Encryption?

Nowadays, information security is becoming more important in data storage and transmission. Images are widely used in different-different processes. Therefore, the security of image data from unauthorized uses is important. Image encryption plays an important role in the field of information hiding. Encryption is a way of keeping your data safe and confidential as it is sent over the internet. Whenever you send personal information across the internet, be it passwords, credit card information or personal contact details, encryption stops others from seeing what you are doing.

1.3. Different Types of Image Encryption.

The three major encryption types are DES, AES, and RSA. While there are many kinds of encryption - more than can easily be explained here - we will take a look at these three

significant types of encryption that consumers use every day. Most of the others are variations on older types, and some are no longer supported or recommended. Tech is evolving every day and even those considered to be modern will be replaced by newer versions at some point.

1.3.1. DES encryption:

The **DES** (Data **Encryption** Standard) **algorithm** is a symmetric-key block **cipher** created in the early 1970s by an IBM team and adopted by the National Institute of Standards and Technology (NIST). The **algorithm** takes the plain text in 64-bit blocks and converts them into cipher text using 48-bit keys.

1.3.2. AES encryption:

AES encryption refers to the process of concealing electronic data using an approved 128-bit, 192-bit, or 256-bit symmetric encryption algorithm from the Advanced Encryption Standard (AES), also known as FIPS 197. The AES is a computer security standard for cryptographically securing electronic information, usually secret and top-secret government information.

1.3.3. RSA encryption:

The **RSA algorithm** is an asymmetric **cryptography algorithm**; this means that it uses a public key and a private key (i.e two different, mathematically linked keys). As their names suggest, a public key is shared publicly, while a private key is secret and must not be shared with anyone.

1.4 Application of Image Encryption:

Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Many image content encryption algorithms have been proposed.

Internet communication: Streaming digital images also require high network bandwidth for transmission. For effective image transmission over the Internet, therefore, both security and bandwidth issues must be considered.

Multimedia system: Internet multimedia applications have become very popular. Valuable multimedia content such as digital images, however, is vulnerable to unauthorized access while in storage and during transmission over a network.

Medical imaging: Medical images are regarded as important and sensitive data in the medical informatics systems. For transferring medical images over an insecure network, developing a secure encryption algorithm is necessary.

Military encrypted communication: unit is ideal for protecting communications in military contexts. This universal encryption platform has been successfully installed in helicopters, for example the Super Puma type. Further projects involving the NH90 and Dauphin helicopters are under way. The HC-2650 was designed for military application and is therefore accordingly robust and suitable for problem-free use in motor vehicles, tanks, aircraft and helicopters. Installation in civilian aircraft (e.g. for VIPs, such as Presidential transport), is also possible, and has in fact been implemented.

2. Different Image Encryption Techniques

2.1 Arnold's transformation:

Definition: It is a transformation $\Gamma : T^2 \rightarrow T^2$ such that:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N} \quad (1)$$

Where, $x, y \in \{0, 1, 2 \dots N-1\}$ and N is the size of a digital image. A new image is produced when all the points in an image are manipulated once by equation.

2.1.1 Modified Arnold Transformation:

The security level of the encrypted text becomes low when it is encrypted using the basic Arnold transform as it constitutes a single 2x2 map and therefore, can easily be decrypted by any 3rd party user, using the same map.

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} k+1 & k \\ 1 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N} \quad (2)$$

OR

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} k & k+1 \\ 1 & 1 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N} \quad (3)$$

Where, $x, y \in \{0, 1, 2 \dots N-1\}$ and N is the size of a digital image and $k \in \{0, 1, 2, 3, \dots\}$.

As in both the cases the transform matrices are 2x2 uni-modular matrices therefore, are periodic in nature and scramble a square image into an indistinguishable format. Unlike equation (1) where there is a single map, equation (2) and (3) provides a number of maps for different values of k

and hence increases the security level of the scrambled message against hit and trial decryption by an unauthorized user. In fact it can be easily be seen that the transposes of the 2x2 maps given in equations (2) and (3) the matrices obtained by swapping the rows as well as their transposes; all the 8 variants of $\begin{bmatrix} k+1 & k \\ 1 & 1 \end{bmatrix}$ generalisations of the AT and can be used for the purpose of image encryption.

2.2 Fibonacci-Q Transform:

This is a special case of the basic AT with periodicity. The equation of the transformation is as given below:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N}$$

Li-Ping Shao et al further worked on the set of triangular periodic transforms and used those for image scrambling in their paper. The generalized triangular map is given by $\begin{bmatrix} 0 & 1 \\ 1 & k \end{bmatrix}$, $k \in \{0, 1, 2, \dots\}$ and the other three possible variants of this which can be obtained by rearranging the values of the matrix. Though these are the simplest forms of 2D transforms, one important limitation of all these triangular matrices is, one out of the two coordinates of the image points always remains constant and only one coordinate changes during the iterations making the scrambling pattern less random.

2.2.1 Generalised Fibonacci Transform:

Named after Leonardo of Pisa, popularly known as Fibonacci, the Fibonacci sequence F_n , is a sequence of integers given by the recurrence relation

$$F_n = \begin{cases} 0 & \text{If } N = 0 \\ 1 & \text{If } N = 1 \\ F_{n-1} + F_{n-2} & \text{Otherwise} \end{cases}$$

The series constitutes the numbers: 0,1,1,2,3,5,8,13,21, 34..

It can be easily seen that a 2x2 matrix formed by any four consecutive terms of the Fibonacci series is a uni-modular matrix and can be considered as an image scrambler. A generalized Fibonacci Transform is defined as:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} F_i & F_i + 1 \\ F_i + 2 & F_i + 3 \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N}$$

Where, $x, y \in \{0, 1, 2 \dots N - 1\}$, F_i is the i^{th} term of the Fibonacci series and N is the size of a digital image.

Denoting $\begin{bmatrix} F_i & F_i + 1 \\ F_i + 2 & F_i + 3 \end{bmatrix}$ as FT_i , the first matrix of this series will be given

$$\text{By : } FT_i = \begin{bmatrix} F_1 & F_2 \\ F_3 & F_4 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$$

Like the modified AT, in this case too there are a number of different maps with different periodicities and different scrambling patterns and hence these transforms also, just like the Modified ATs, can be considered as more secured encryption methods over the basic AT and Fibonacci-Q transform.

2.3 X-OR Operation Based Encryption:

XOR is a logical operation, pronounced *exclusive or*. XOR acts like a toggle switch where you can flip specific bits on and off. If you want to "scramble" a number (a pattern of bits), you XOR it with a key. If you take that scrambled number and XOR it again with the same key, you get your original number back. you take a key, such as 0101, then you use that to XOR your string (in binary format) to achieve an encrypted string.

0101 XOR <-- key

1011 <---- original message

1110 <-- send message

You send 1110 to your receiver. That receiver then takes the received string and XORs it with the key to obtain the original message:

1110 XOR <--- received message

0101 <-- key

1011 <--- original message

2.4 Fibonacci-Lucas Transformation:

The Fibonacci-Lucas Transform can be defined as the mapping $FL: T^2 \rightarrow T^2$ such that:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{bmatrix} F_i & F_{i+1} \\ L_i & L_{i+1} \end{bmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \pmod{N}$$

Where $x, y \in \{0, 1, 2, 3, 4, 5, 6 \dots N-1\}$, F_i is the i^{th} term of the Fibonacci series and L_i is the i^{th} term of the Lucas series, ($i=1, 2, \dots$), N is the size of the image.

Denoting $\begin{bmatrix} F_i & F_{i+1} \\ L_i & L_{i+1} \end{bmatrix}$ as FLT_i , the first matrix of the series will

be given by -

$$FT_i = \begin{bmatrix} F1 & F2 \\ F3 & F4 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 2 \end{bmatrix}$$

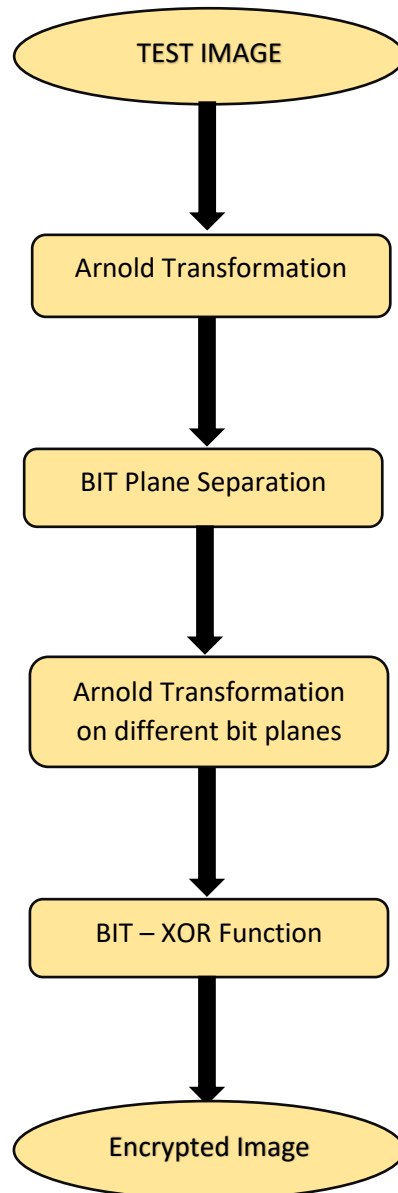
Continuing in this way we can form many Fibonacci transforms for different values of i . It will be periodic in nature with a maximum possible periodicity N^2-1 and produce scrambling patterns different from each other.

3. Proposed Encryption Algorithm

We used the following steps of the algorithm for our encryption purpose.

1. First take a test image (either rgb or grayscale) of any format (like jpg, jpeg, tif, tiff etc.)
2. Calculate the size of the test image. If needed resize the test image according to any size. Also transform it to grayscale image.
3. Write a function for the Arnold transform and call the function. This function will have two parameters one for test image another for no of iterations.
4. After the mentioned n of iterations save the scrambled image in a variable.
5. Now we write another function for bit xor.
 - a. In the bit xor function the previous scrambled image will be passed as a parameter.
 - b. Convert the image into a binary image and make the matrix of unsigned integer type.
 - c. Then split the planes of the image in 8 bit planes. After splitting again do Arnold transformation with different iterations for different bit planes.
 - d. Separate the high order bits and lower order bits and perform bit xor on high order bits with lower order bits (key).
 - e. High order bits get changed but lower order bits remain the same.
 - f. Place high order bits and lower order bits side by side and construct the matrix again.
 - g. Bit planes get merged and will make the picture again but in a more scrambled way.
6. Call the bit xor function and show the new entropy of the image.

3.1 Block Diagram Of Encryption Process:

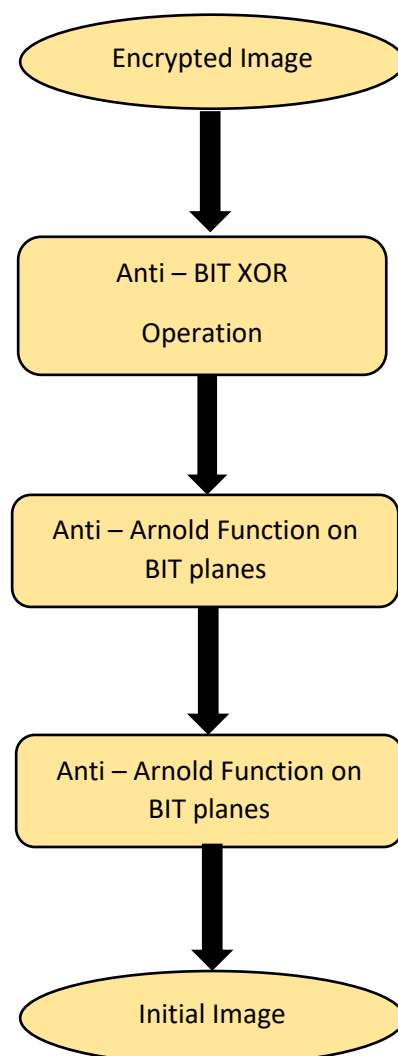


3.2 Decryption Algorithm:

We use the following steps for decryption purposes.

1. We take the encrypted image.
2. Then again call the bit xor function and encrypted image as the parameter of the function.
3. After calling the function we will get the scrambled image which we got after the Arnold transformation on bit planes.
4. We then call the Arnold transformation on the bit planes with remaining iterations to get the original image.
5. Then we call the Arnold transformation and iterate the image until we get our desired test image.

3.3 Block Diagram Of Decryption Process:



4. Experimental Results:

We implemented the proposed method of encryption with five different test images of grey-scale, each of size (512x512). The images are of lena, man, boat, peppers and baboon. The simulation results are studied on the basis of histogram analysis and information entropy test.

HISTOGRAM:-

Histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. For an 8-bit grey scale image there are 256 different possible intensities, and so the histogram will graphically display 256 numbers showing the distribution of pixels amongst those grey scale values.

ENTROPY:-

Entropy is a measure of image information content, which is interpreted as the average uncertainty of information source. Entropy is defined as corresponding states of intensity level which individual pixels can adapt. The entropy of an image is defined as follows:

$$\sum_{i=0}^{n-1} P_i \log_b P_i$$

where n is the number of grey levels (256 for 8-bit images), P_i is the probability of a pixel having grey level i , and b is the base of the logarithm function.

Histogram Deviation Calculation:-

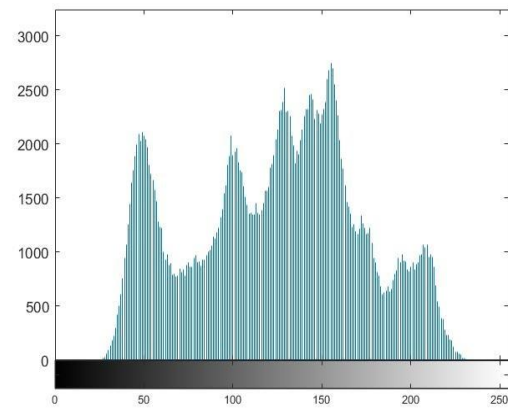
The Histogram Deviation calculation of the Six Grayscale encrypted images Lena, Airplane, Baboon, Cameraman, House, Lake are tabulated in Table, from which it can be said that the Histogram Deviation is less than that obtained using Random Scrambling and X-OR operation.

Test Image	Entropy of Test Image	Entropy of Encrypted Image	Histogram Deviation
Lena	7.445061	7.971984	0.631744
Airplane	6.702463	7.564171	0.937447
Baboon	7.358337	7.976405	0.749077
Cameraman	7.009716	7.835636	0.932861
House	6.486187	7.370343	0.904305
Lake	7.484219	7.971896	0.641937

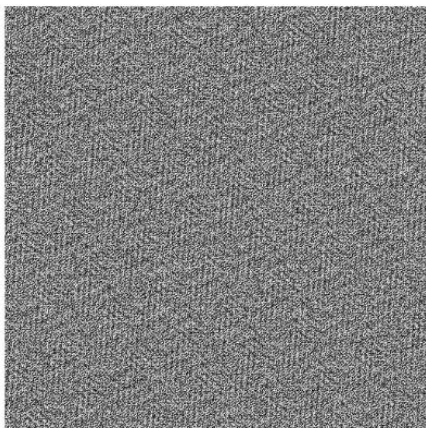
1. Experiment on Lena:-



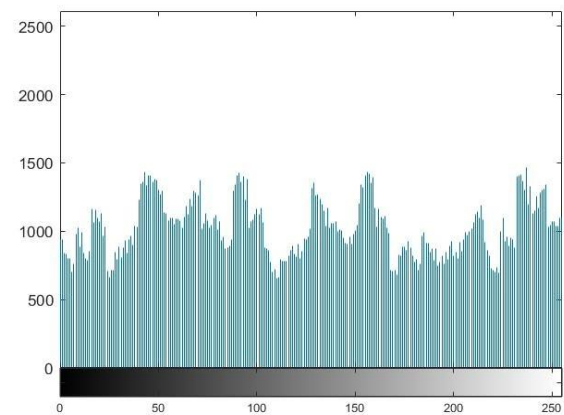
Test Lena Image



Histogram of Test Image



Encrypted Image

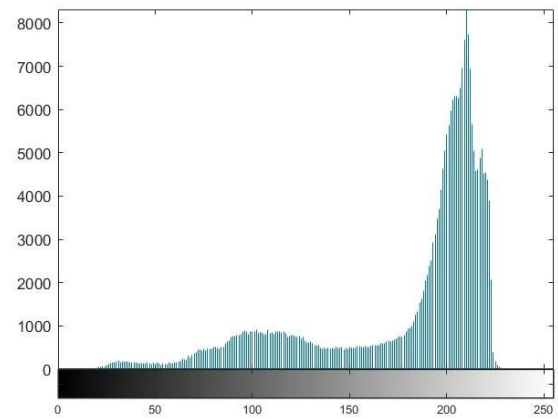


Histogram of Encrypted Image

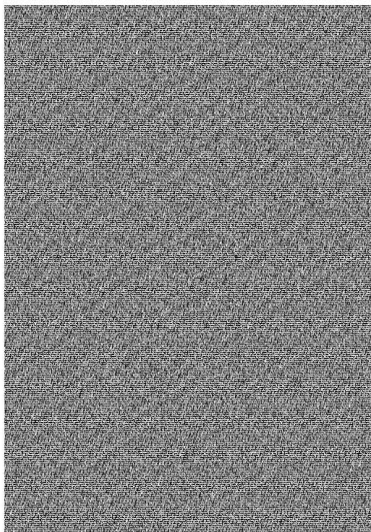
2. Experiment on Air-Plane Picture :-



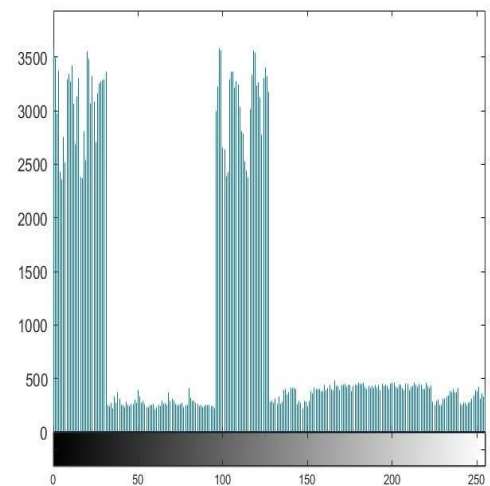
Test Air-Plane Image



Histogram of Air-Plane Image

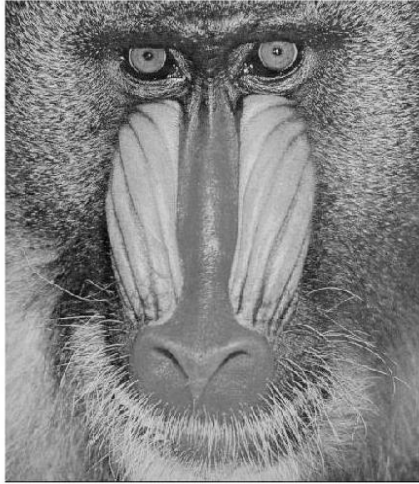


Encrypted Image

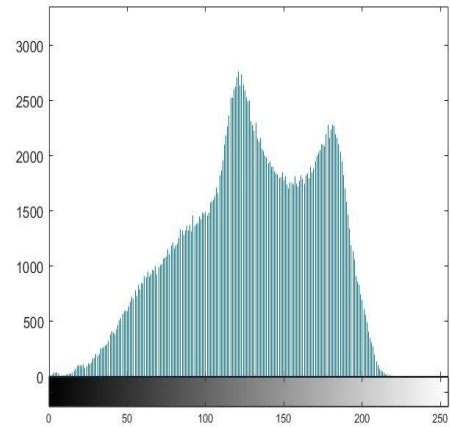


Histogram of Encrypted Image

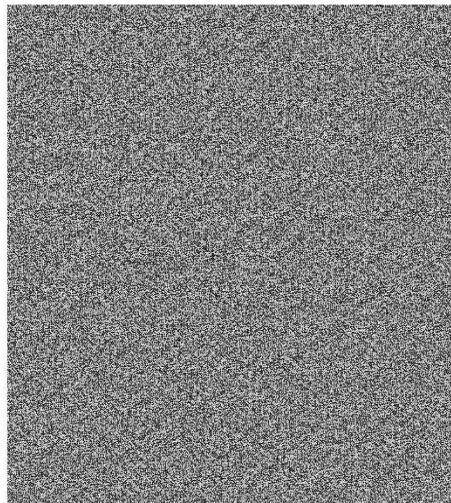
3. Experiment on Baboon Picture:-



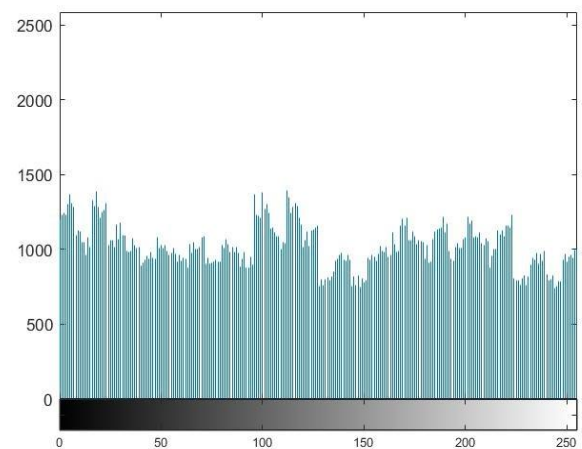
Test Baboon Image



Histogram of Baboon Image



Encrypted Image

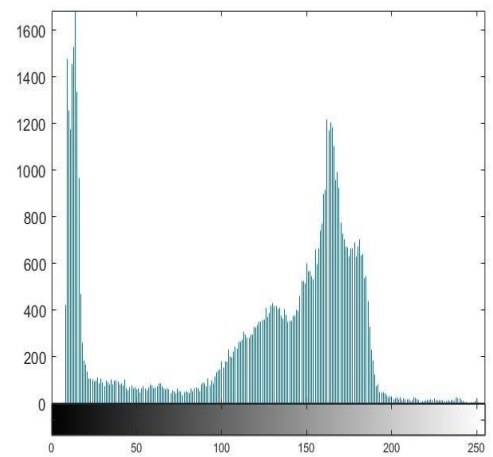


Histogram of Encrypted Image

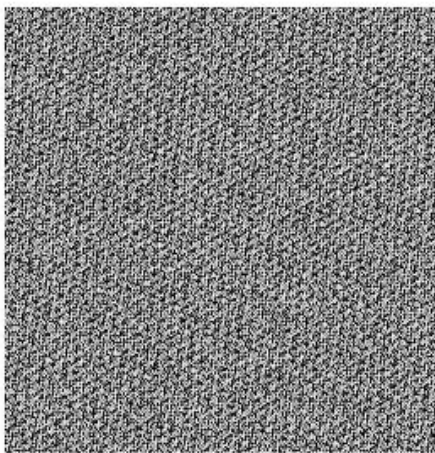
4. Experiment on Camera-man Picture:-



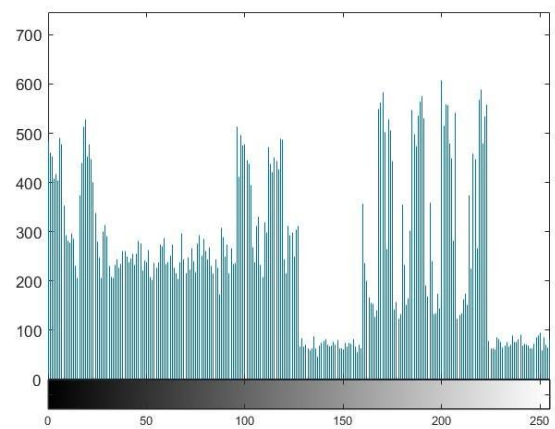
Test Camera-man Image



Histogram of Camera-man Image



Encrypted Image

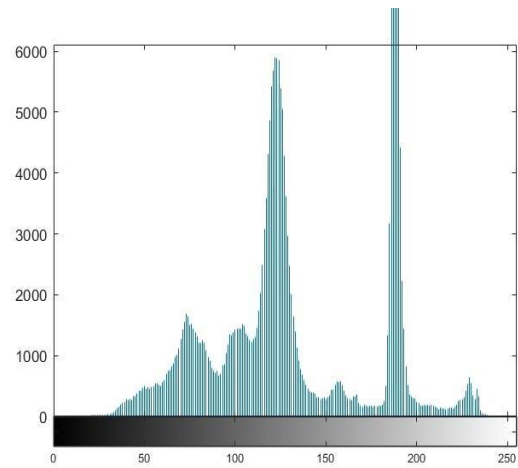


Histogram of Encrypted Image

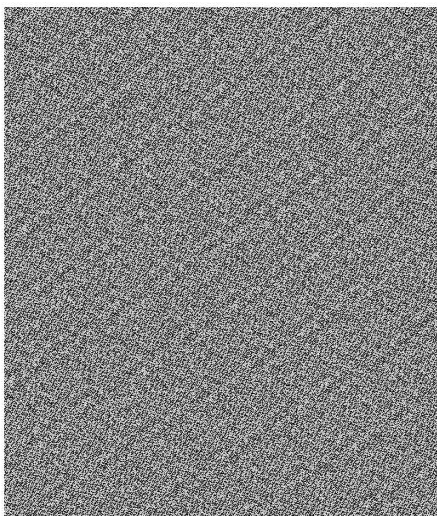
5. Experiment on House Picture:-



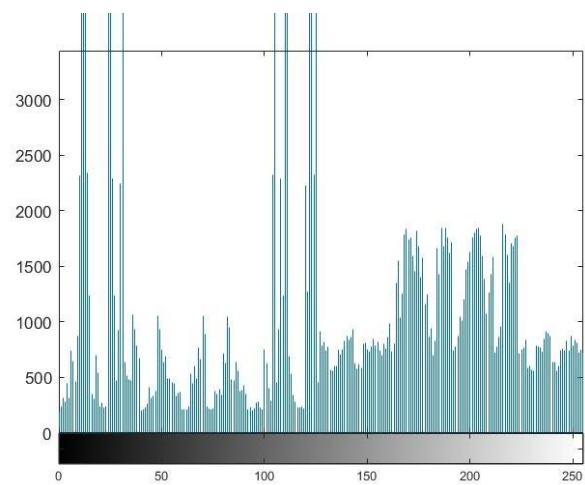
Test House Image



Histogram of House Image

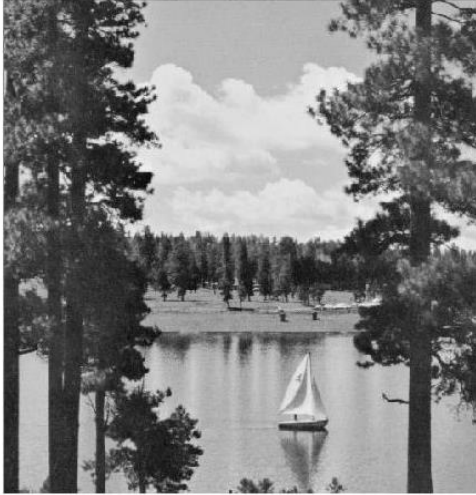


Encrypted Image

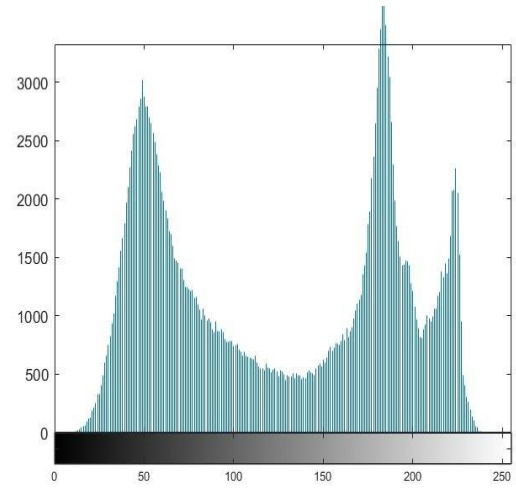


Histogram of Encrypted Image

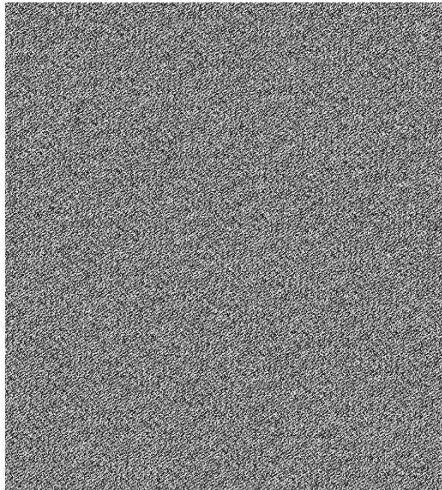
6. Experiment on Lake Picture:-



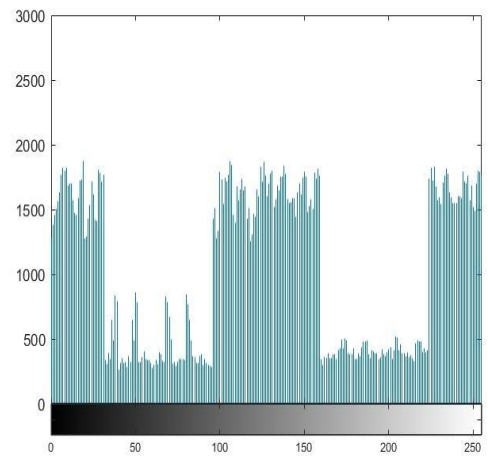
Test Lake Image



Histogram of Lake Image



Encrypted Image



Histogram of Encrypted Image

5. Conclusion:

There are many more complex modifications one can make to the images. For example, one can apply a variety of filters to the image. The filters use mathematical algorithms to modify the image. Some filters are easy to use, while others require a great level of technical knowledge. Here we use some mathematical algorithms like arnold transform, xor operation etc. At first we did Arnold transform to generate Arnold matrix and then we applied an XOR operation to get the encrypted image. Simulation results of using the conventional histogram analysis and the information entropy tests, show the effectiveness and robustness of the proposed algorithm. Histograms become nearly uniform and the entropy tends to 7.99 i.e. nearly 8(for both grey scale and RGB images). The study can be further continued using key sensitivity analysis, key space analysis, adjacent pixel correlation test, UACI and NPCR tests and robustness could be tried to maximize.

Using image processing techniques, we can sharpen the images, contrast to make a graphic display more useful for display, reduce amount of memory requirement for storing image information, etc., due to such techniques, image processing is applied in recognition of images as in factory floor quality assurance systems; image enhancement, as in satellite reconnaissance systems; synthesis as in law enforcement suspect identification systems.

6. References:

1. http://en.wikipedia.org/wiki/Arnold%27s_cat_map
2. Yang, D.L., N. Cai and G.Q. Ni, 2006. "Digital image scrambling technology based on the symmetry of Arnold transform", J. Beijing Inst. Technol., 15: 216-220.
3. W. Ding, W. Q. Yan, D. X. Qi, "Digital Image Scrambling Technology Based on ArnoldTransformation," Journal of Computer-aided Design &Computer Graphics, vol. 13, no. 4, pp. 338-341, 2001.
4. S. Lian, J. Sun, and Z. Wang, —A block cipher based on a suitable use of the chaotic standard map,II in Chaos, Solitons & Fractals 26(1), 117– 129 (2005).
5. G. Ye, —Image scrambling encryption algorithm of pixel bit based on chaos map,II in Pattern Recognition Letter 31, 347–354 (2010).
6. J. Fridrich, —Image encryption based on chaotic maps,II in IEEE Int. Conf. Systems, Man, and Cybernetics 2, 1105– 1110 (1997).
7. Z. Zhu, W. Zhang, K. Wong, and H. Yu, —A chaos-based symmetric image encryption scheme using a bit-level permutation,II in Information Sciences 181(6), 1171–1186 (2011).
8. C. Huang, and H. Nien, —Multi chaotic systems based pixel shuffle for image encryption,II in Opt. Commun. 282(11), 2123–2127 (2009). [6] D. R. Stinson, Cryptography: theory and practice, Chapman and Hall CRC (2006).