



Tribhuvan University

Institute of Science & Technology

**Analysis of Image Encryption using Chaotic, Hybrid Chaotic
and Block Cipher Approach**

Thesis

Submitted To:

Central Department of computer Science & information Technology

Tribhuvan University

Kirtipur, Kathmandu

Nepal

**In partial Fulfillment of the requirements for the Degree of Master of science in
Computer Science and Information Technology**

Submitted By:

Nirmal Kumar Chaudhary

September, 2018

Supervisor

Mr. Jagdish Bhatta

CDCSIT, Kirtipur, Nepal



Tribhuvan University
Institute of Science and Technology
Central Department of Computer Science and Information Technology

Student's Declaration

I hereby declare that I am the only author of this work and that no sources other than the listed here have been used in this work.

.....

Nirmal Kumar Chaudhary

Date: September, 2018



Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Supervisor's Recommendation

I hereby recommend that the dissertation prepared under my supervision by **Mr. Nirmal Kumar Chaudhary** entitled “**Analysis of Image Encryption using Chaotic, Hybrid Chaotic and Block Cipher Approach**” be accepted as in fulfilling partial requirement for completion of master Degree of science in computer science and information Technology.

.....

Mr. Jagdish Bhatta

(Supervisor)

Central Department of Computer Science & Information Technology

Tribhuwan University

Kritipur, Nepal

Date: September, 2018



Tribhuvan University
Institute of Science and Technology
Central Department of Computer Science and Information Technology

LETTER OF APPROVAL

We certify that we have read this dissertation and in our opinion it is appreciable for the scope and quality as a dissertation in the partial fulfillment for the requirement of Master's Degree in Computer Science and Information Technology.

Evaluation Committee

.....
Asst. Prof. Nawaraj Paudel
Head of Department
Central Department of Computer
Science & Information Technology
Tribhuvan University
Kritipur, Nepal

.....
Mr. Jagdish Bhatta
(Supervisor)
Central Department of Computer
Science & Information Technology
Tribhuvan University
Kritipur, Nepal

.....
(External Examiner)
Date: September, 2018

.....
(Internal Examiner)

Acknowledgement

I would like to express my sincere thanks to my supervisor **Mr. Jagdish Bhatta**, Central Department of Computer Science and Information Technology, Kirtipur, Nepal for his support, motivation, suggestions and guidance. His advice was inevitable and with his help I was able to work on my own interested field and complete my thesis on time.

I am also thankful to **Mr. Nawaraj Poudel**, Head of Department, CDCSIT who has provided all the help and facilities, which I required, for the completion of my thesis.

Moreover, I would like to express my heartfelt gratitude to all my teachers at Central Department of Computer Science and Information Technology, Tribhuwan University who have imparted knowledge in various subjects.

Last but not the least; I would like to express my thanks to all my friends and my lovely parents for direct and indirect supports for the completion of this thesis.

Abstract

Secured image transmission in the network is the biggest threat to the real world because of increasing network security problem, illegal and unauthorized access, malicious code and intruders. The security to the image is given by image encryption techniques. Image encryption is the process of changing the original image into a scramble, unrecognized form. There are various techniques and method for image encryption. In this study chaos based image encryption and block cipher technique are implemented and analyzed for the encryption. Arnold catmap and Arnold catmap with logistic map are used as native chaotic and hybrid chaotic approach respectively whereas AES is used as block cipher approach. The chaotic algorithms encrypt the image by shuffling and scrambling the pixel value of the image which is also called as confusion and diffusion process. The block cipher algorithm encrypt the image by extract the block of 128 bits pixel data from the image with the key of 128 bits. The chaotic and block cipher methods are applied to encrypt image and subjected to measures the different performance parameters like PSNR, NPCR, UACI, Histogram, encryption/ decryption time to measure the strength of the algorithms. The results show the Arnold catmap with logistic map has better NPCR and UACI value which makes it more robust method to defend differential attack or chosen plain text attack it is also computationally efficient since less time is taken for encryption/decryption process. AES has less PSNR value which helps to preserve image properties after decryption and the histogram of original and cipher image more variation in AES than other two approach so it is able to defend statistical attack or cipher text only attacks.

Keywords: *Image encryption, Chaos theory, Block cipher, Arnold catmap, Logistic map, AES.*

Table of Contents

Acknowledgement	i
Abstract	ii
List of Figures	v
List of Tables	vi
LIST OF ABBREVIATIONS	vii
Chapter 1	1
Introduction	1
1.1 Introduction	1
1.2 Statement of Problem	2
1.3 Objective	3
1.4 Thesis Organization	3
Chapter 2	4
Background Study and Literature Review	4
2.1 Background Study	4
2.1.1. Chaos Theory	4
2.1.2. Chaotic Maps	5
2.1.3 Chaotic Encryption	6
2.1.4 Block Cipher	6
2.1.5 Image Encryption	7
2.2 Literature Review	7
Chapter 3	11
Methodology	11
3. Methodology	11

3.1 Block cipher image encryption using AES	12
3.2 Chaotic map encryption using Arnold Cat Map	15
3.3 Hybrid Chaotic map encryption using Arnold cat map with Logistic map	16
Chapter 4.....	19
Implementation and Analysis	19
4.1 Implementation	19
4.1.1 Java Programming Language: J2SE overview	19
4.1.2 IntelliJ IDEA.....	19
4.2 Test Environment	20
4.3 Test Data Description.....	20
4.3.1 Sample Test Data	20
4.4 Analysis.....	21
4.4.1 Visual Assessment Analysis:	21
4.4.2 Differential Analysis:	23
4.4.3 Computational Speed Analysis:	25
4.4.4 Statistical Analysis:	27
4.6 Result.....	31
Chapter 5.....	32
Conclusion and Future Recommendation	32
5.1 Conclusion.....	32
5.2 Future recommendation	32
References	33
Appendix	36

List of Figures

3 Methodology for image encryption.....	12
4.5.3 Encryption time measurement.....	26
4.5.3 Decryption time measurement.....	26

List of Tables

4.5.1 PSNR Measures	21
4.5.2 NPCR & UACI Measures	23
4.5.3 Histogram Analysis	27

LIST OF ABBREVIATIONS

AES	(Advanced Encryption Standard)
CBC	(cipher block chaining)
CFB	(cipher feedback)
CTR	(counter)
CMBC	(Chaotic Map with Block Chaining)
DES	(Digital Encryption Standard)
DHS	(Dynamic Harmony Search)
GCM	(Galois/Counter Mode)
IDE	(Integrated Development Environment)
IDEA	(International Data Encryption Algorithm)
JDK	(Java Development Kit)
MSE	(Mean Square Error)
NPCR	(Number of Pixel Change Rate)
PSNR	(Peak Signal to Noise Ratio)
UACI	(Unified Average Change Intensity)

Chapter 1

Introduction

1.1 Introduction

Security is very important aspect of computer systems. The need for the development of the secured system has grown tremendously with the advent of e-commerce and e-transaction. Implementing security mechanism within a system includes enforcing confidentiality, integrity and availability. In today's world of technological advancements in web, multimedia and wireless networks, the multimedia data such as digital images, audio, video becomes a crucial means of communication. The public internet access leads to easiness in unauthorized access, illegal usage, malicious alteration and disruption of sensitive multimedia data for intruders and attackers. So, there is an increasing demand for building robust and efficient security methods for privacy protection of digital multimedia data while transmitting them over the Internet [6].

The security level of digital images over network has attracted much attention recently, and many different image encryption methods have been proposed to enhance the security of these images[13]. According to the image encryption scheme, the idea is to convert an image into the scrambled one that is hard to understand. On the other side, image decryption retrieves the original image from the encrypted one.

There are a number of traditional encryption techniques like DES, IDEA, RSA etc. These traditional encryption algorithms have shortcomings and they are not considered as ideal for image applications, mainly because of low level of efficiency when dealing with large and redundant blocks of image data. Moreover, these algorithms require more than the usual expected computation time and power while performing image encryption [7, 17]. In recent years a number of different image encryption schemes have been proposed in order to overcome image encryption problems. Due to desirable properties of non-linear dynamical systems such as pseudo-random behavior, sensitivity to initial conditions and ergodicity, the chaos-based encryption has suggested a new and efficient way to deal with the intractable problem of fast and highly secure image encryption. Most of the chaos-based image encryption algorithms are based on confusion and diffusion techniques. Confusion technique shuffles the positions of the pixels in plain- image to get visually disordered and unrecognized image. A diffusion technique alters the statistical characteristics of image by modifying the gray-values of pixels.

In the color image encryption there are three planes RGB (Red, Green, and Blue). Each of these three planes is quantized separately. The pixels of the original image are scrambled and mingled through random sequence which is chaotic in nature. The original image can be recovered after several iterations depending on initial conditions. The scrambling takes place by arranging pixels and taking each bit of image and XORed with random sequence that is generated [4]. The features like non-deterministic, randomness, periodicity of chaotic maps make the digital image data more secure.

Recently, a number of chaos-based encryption schemes have been proposed. Some of them are based on one-dimensional chaotic maps and are applied to data sequence or document encryption [14]. For image encryption, two-dimensional or higher-dimensional chaotic maps are naturally employed as the image can be considered as a 2D array of pixels [20]. The colored image consists of three 2D arrays of pixels for the color channels R, G, and B.

In this study the chaotic- based image encryption using Arnold cat map, hybrid chaotic encryption using Arnold cat map with logistic map and block cipher encryption using AES is implemented and analyzed so as to analyze strength of chaotic and block cipher strategies by preserving the quality of image and ensuring the security of the image data.

1.2 Statement of Problem

Many digital services like multimedia systems, medical and military imaging systems, and public internet communication require reliable security in storage and transmission of digital images. Due to growth of internet, cell phones, multimedia technology in our society, the digital image security is the most critical problem. In these technology digital images plays more significant role than the traditional texts. It demands serious protection of users' privacy for all applications. Together with higher security level, maintaining quality of image data without losing the parametric properties of original image is equally important. In this context, building a secure image encryption framework with better efficiency, confidentiality and quality preference is of utmost research concentration. The traditional cryptosystems has been found not effective for multimedia data because of low scale performances and security threats [1,13]. The complex properties of ergodicity, unpredictability and sensitivity to initial states in chaotic systems has opened door for their used in cryptography.

Thus, the secured framework using native chaotic with Arnold cat map and hybrid chaotic encryption based on Arnold cat map with logistic and block cipher AES is built and the model is analyzed with different performance parameters to attain the best model in different parametric area along with securing the image quality.

1.3 Objective

The objectives of this study are

- To implement the chaotic based image encryption techniques namely Arnold cat map based, hybrid chaotic using Arnold cat map with logistic map and block cipher based image encryption using AES.
- To perform differential, statistical, visual assessment and computational analyses using the parameters NPCR (Number of Pixel Change Rate), UACI (Unified Average Change Intensity), Histogram, PSNR (Peak Signal to Noise Ratio) and encryption/decryption time respectively.

1.4 Thesis Organization

The flow of thesis goes on this manner.

Chapter 1 consists of introduction, problem statement and objectives.

Chapter 2 describes about the background study for the research and literature review of the related work by different authors.

Chapter 3 includes the overview of the methodology of Arnold cat map, Arnold catmap with logistic map and AES

Chapter 4 contains the implementation overview of the Arnold cat map, Arnold cat map with logistic map and AES in java platform along with the empirical analysis of different performance parameters of methodology.

Finally chapter 5 conclude with the main theme of the work.

Chapter 2

Background Study and Literature Review

2.1 Background Study

Chaos theory, chaotic map, block cipher and image encryption are the topic to be discussed in background study which is given below:

2.1.1. Chaos Theory

Chaos word has been derived from the Greek, which refers to unpredictability and it is defined as a study of nonlinear dynamic system. Chaos theory is a mathematical physics which was developed by Edward Lopez. Chaos is closely related to some dynamics of its own characteristics. The behavior of the chaos system, under certain conditions, presents phenomena which are characterized by sensitivities to initial conditions and system parameters. Through the sensitivities, the system responses act to be random. Furthermore, many cryptographic algorithms have adopted popular chaotic models that represent chaos by using mathematical models such as logistic map, Lorenz map, Henon map, and Rössler attractor. Lorenz map is characterized by its attractor having two nonlinear terms while in Rössler attractor there is only one nonlinear term and this makes the complexity of Lorenz attractor and its chaos higher than those in Rössler attractor. Other algorithms have divided the images into several blocks and tried to define a permutation for each block using a logistic map to encrypt the original image [21]. The mathematics behind the chaos theory is related with the given definition

Definition Let V be a set. $F:V \rightarrow V$ is said to be chaotic on V if

1. F has sensitive dependence on initial conditions.
2. F is topologically transitive.
3. Periodic points are dense in V .

Definition $F:J \rightarrow J, F:J \rightarrow J$ has sensitive dependence on initial conditions if there exists $\delta > 0$ such that, for any $x \in J$ and any neighborhood N of x , there exists $y \in N$ and $n > 0$ such that $|F^n(x) - F^n(y)| > \delta$.

Definition $F:J \rightarrow J, F:J \rightarrow J$ is said to be topologically transitive if for any pair of open sets $U, V \subset J$ there exists $k > 0$ such that $F^k(U) \cap V \neq \emptyset$.

The first is the general idea of dynamical chaos. The second and third seem to imply some sort of ergodicity. Some of the chaos theory that are used by the chaotic map are given below

Henon map

Henon map [20] is defined as

$$X_{n+1} = 1 - aX_n^2 + Y_n$$

$$Y_{n+1} = bX_n$$

Tent map

A piecewise linear, one-dimensional map [16] on the interval $[0, 1]$ exhibiting chaotic dynamics and given by

$$x_{n+1} = \mu \left(1 - 2 \left| x_n - \frac{1}{2} \right| \right).$$

Lorentz map

Lorentz map [4] is defined as

$$X(1) = s * (y(i-1,2) - y(i-1,1))$$

$$X(2) = r * y(i-1,1) - y(i-1,2) - y(i-1,1) * y(i-1,3)$$

$$X(3) = y(i-1,1) * y(i-1,2) - b * y(i-1,3)$$

$$y(i,:) = y(i-1,:) + h * X$$

Sine map

Sine map [12] is defined as $X_{n+1} = a x_n^2 \sin(\pi x_n)$ where $x_0 = 0.7$ and $a = 2.3$. For the interval $(0, 1)$ it generates chaotic sequence.

2.1.2. Chaotic Maps

In arithmetic, a chaotic map [8] is evolution function that exhibits some form of chaotic behavior. Maps is parameterized by a discrete-time or a continuous-time parameter. Separate maps typically take the shape of iterated functions. Chaotic maps typically occur within the study of self-propelled systems. Chaotic maps typically generate fractals.

Chaotic map has number of features like deterministic, sensitive to initial condition, randomness, this features makes the chaotic system completely different and unique in the encryption field. There are different dimension of chaotic map like 1D, 2D, 3D. Basically the higher dimension are used to get the high ended security services. Tent map, logistic map, Arnold catmap, baker map,

henon map etc. are the some of the abundantly used map, besides it hybrid chaotic approach are also used for the better security purpose. The properties of the chaotic map can be enhanced with the intermixing of one chaotic map with the others in case of hybrid map. The chaos based cryptosystem also carried a special meaning in the image encryption process as it uses the security strength of two different techniques.

2.1.3 Chaotic Encryption

Chaotic map uses chaotic function of different chaotic methods. The behavior of the chaotic function can be reflected with the help chaotic encryption. Chaotic encryption uses a mathematical function of the chaotic map to shuffle and scramble the image. Chaotic methodology generally concentrates on changing the pixel value and pixel position so that others cannot read the original pixel information in the digital image. Chaotic encryption uses a number of parameters as a secret key which ensures high randomization of the image data during encryption. The chaotic based cryptosystem adds a new paradigm for image encryption. This paradigm uses the concept of chaotic technique and cryptographic algorithm for the security of image data.

2.1.4 Block Cipher

Cryptography is the knowledge of protecting the privacy of information during communication under antagonistic situations. Nowadays, cryptography plays an important role in the developing information technologies and proliferating computer network communication. There are number of method in cryptography to handle the encryption/decryption process where some handle the data in bit level and some works with block of data. Those which works with bit level is stream ciphers whereas those which works with block of data is block cipher.

Block cipher is a cryptographic method that applies a deterministic algorithm along with a symmetric key to encrypt a block of text, rather than encrypting one bit at a time as in stream ciphers. For example, a common block cipher, AES, encrypts 128 bit blocks with a key of predetermined length: 128, 192, or 256 bits.

The block cipher approach uses a block of image pixel value with a secret key to encrypt the pixel and change it to unrecognized form. The method operates on the block so it is fast and efficient approach than stream cipher which works with bits only.

Different modes of operation are used with block cipher in order to enhance the services and security level of block cipher. Some of the commonly used mode are CBC, CFB, GCM,CTR[19].

2.1.5 Image Encryption

Image encryption is the process of changing the image data into an unrecognized form. It provides security from the malicious sources by hiding the significance information of the image data. Image encryption is different from text encryption due to some inherent features of image such as bulk data capacity and high correlation among pixels. Due to this features of image it is difficult to handle the image data by conventional methods. Number of different approaches have been proposed for encrypting the image but the chaotic approach are established as a efficient approach because of it's chaotic behavior. The desirable cryptographic properties of chaotic maps such as initial conditions and random-like behavior can be used to develop new encryption paradigm. The chaos – based cryptographic algorithms have suggested new ways to develop efficient image encryption schemes. The random-like nature of chaos is effectively spread into encrypted images

2.2 Literature Review

The authors in [1] have proposed a new Chaotic Map with Block Chaining (CMBC) cryptosystem for image encryption. The new technique gains both the advantageous features of chaos and CBC chaining block cipher. The high level of efficiency and simplicity provided by the chaotic map together with the confusion and diffusion properties added to the system by involving CBC make the proposed scheme efficient and secure against most of the familiar attacks.

Adrian-Viorel Dianconu [2] suggested an efficient permutation at circular intra-inter bit-level based confusion strategy. The cryptosystem's design uses a promiscuous random number generating strategy in the starting stages of the encryption manner for reckoning of the matrices (cipher). Using the random patterns of real numbers produced in association with multilevel discretization method, di-bit pairs are generated which are directly proportional to image dimensions. This chaos system reduces the iterations of Fridrich's structure encryption scheme.

Ahmed Bashir Abugharsa et al. [3] has also used AES algorithm to encrypt image, they have first rotated the plain image to generate another image with the help of magic cube. The original image is divided into six sub-images and these sub-images are divided amongst a number of blocks and attached to the faces of a Magic Cube and to confuse the relationship between the plain image and

the encrypted image, the rotated image is fed into an AES algorithm which is applied to each pixel of the image to encrypt the image even further.

The authors in [4] suggested a scheme established on chaos and permutation-substitution network to encrypt image. It is a combo of 4 phases of cryptography and uses two chaotic systems to control the architecture of encryption process for a desirable lofty encryption performance. A dispersion phase works on bitwise XOR logical operation and a different chaotic map is designed. An exchange phase with basis on S-boxes and by a permutation function we accomplish block alteration phase, MAP function, to bolster the analytical efficiency of the encryption scheme.

Benyamin Norouzi, and Sattar Mirzakuchaki introduced an encrypting technique established on the novel substitution stage using chaotic functions. This algorithm chiefly comprises of two main phases' confusion and diffusion [5]. The permutation of pixels of images is done by some chaotic maps and treated as confusion process while in diffusion process, the conversion of pixels in a unique way such that even a small variance in a pixel of the authentic input image stimulate the corresponding encrypted image to be assessed differently.

Chen et al [9] deals with a new domain using frequency domain. This paper made use of two transform affine transform and the gyrator transform. The affine transform was used twice in the encryption process. The parameter of these transform served as the secret key. Initially the RGB image was broken down into its 3 independent components. A function of the affine transform was then used to mix these R, G and B components.

In [10], the authors discussed some algorithms for the encryption of image established on chaotic structure, but the inhibitions of weak security due to small-scale key space in chaotic one-dimensional cryptosystems are prevalent. This research proposes a distinct nonlinear chaotic technique where a tangent function and power function is used despite of linear function. Its structure variables are retrieved by analyzing experimentally. And then in a password system a technique for encrypting a image is designed. The experimentally obtained results exhibit that the method for encrypting a image established on NCA gives benefits of desirable high-level security caused due to huge key space, which maintains the required efficiency. On comparison to the other security algorithms in this field like DES, AES, the suggested technique for encrypting an image is more secure.

Khadijeh Mirzaei et.al [12] advanced a grayscale image encrypting manner using Dynamic Harmony Search (DHS) for achieving maximum or peak entropy and minimum correlation. In this method, a cipher image is created practicing chaotic map then the maximum or peak entropy and minimum correlation coefficient is achieved employing harmony search algorithm. The plane image is diffused to maximize the entropy and minimize the correlation coefficient using DHS algorithm, in the proximate step we use a fitness function. Permutations are applied horizontally and vertically on the best image (cipher) obtained from previous step to achieve more image security

Ansari et.al [18] proposed a distinct approach for encrypting an image which uses chaotic maps in the Frequency Domain. The Discrete Cosine Transform (DCT) of image is evaluated and shuffling of image is performed by 2D baker's map. Two baker's map are used where first uses the primary set keys and the other is used with Gaussian image generated with mean variance. The gain of both baker's maps and DCT are XORed repetitively. The scattering pattern is formed by a number generator which engender a random pattern based on Gaussian distribution. The suggested encryption method uses two Baker's map thus capable of accommodate the key space up to 128 bits. The technique is derived on MATLAB.

Wenhao Liu et.al [23] suggested a novel two-dimensional SIMM hyper chaotic map based on close-loop intonation coupling model. A junction-decomposition mechanism is given for encrypting the color image. Chaotic shift transform is combined to obtain good scrambling Effect. On combination of CST with 2D-SIMM map, a fast encryption scheme is formed that is highly secure, has low time ramification and can resist common attacks.

The work done in [24] suggests an encryption manner established on hybrid (CA) cellular automata and depth conversion integral imaging. In a standard RGB representation of image, the R, B and G channels are analogous to each other so the same encryption process is practiced on each channel in alongside. The authentic input colored image is combo of three channel and CGII is for recording them as EIA. The recorded EIA is converted into depth-converted EIA using mapping algorithm. Each of these converted channel is hidden by a pseudo-random progression. The concealed depth-converted EIA is shuffled by a sequence, introduced by chaotic logistic map. Finally, all these three channels are merged to form an encrypted image.

Zhenjunq Tang et.al [25] proposed an encryption method for numerous colored greyscale images for creating a more secured image transmission. The input grayscale image is prorate into bit-planes and swapping of bit-blocks among various bit-planes takes place randomly. XOR logical operation is enforced between these scrambled data and a matrix controlled using a chaotic map which operates as a secret key. The components of grayscale image i.e. green, red, alpha and blue are viewed to generate an encrypted image.

Zhi-liang ZHU et. al [26] have suggested a unique method established on chaos technique. This method uses the principle of puzzle cube for shuffling all pixel values in a 3-dimension plane, and modifying them using the pseudo-random pattern obtained by compound chaotic map i.e., a combo of sine map, chaotic map and cosine map. The method generally achieves the goal of high speed and various experimental analysis prove that it achieves a very high security level.

Chapter 3

Methodology

3. Methodology

The methodology includes implementing Arnold cat map and Arnold cat map with logistic map as a part of study for the native chaotic and hybrid chaotic approach respectively. The study includes traditional AES as a block cipher based image encryption. Each of the modules is analyzed using the primary and secondary image data. The secondary image data is the benchmark of image datasets and in the format of gif, jpeg, tiff, bmp etc. like sipi images, dicom images, chest ray image and the different captured images is taken as primary data. The input image from primary and secondary data set is extracted with its corresponding pixel values and the pixel values is subjected to the different encryption modules. All of the enciphered image results are evaluated in terms of statistical attack, differential attack, visual assessment and computational speed.

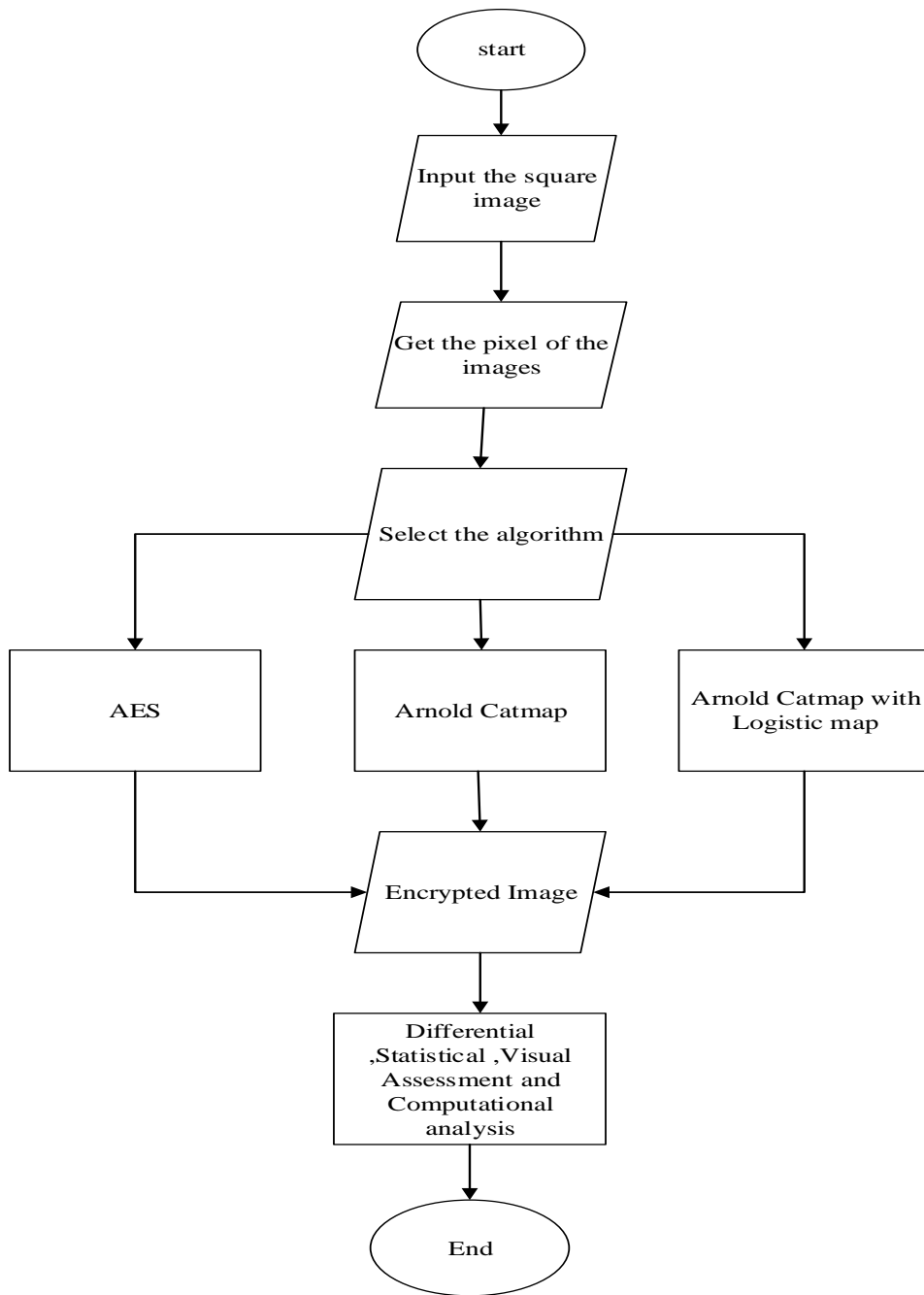


Fig 1: Methodology for Image Encryption

3.1 Block cipher image encryption using AES

The Advanced Encryption Standard (AES) algorithm [11] is a symmetric block cipher that processes image which is of blocks size 128 bits using three different cipher key size of lengths 128,192 or 256 bits. Based on the key size length used, the number of execution rounds of the algorithm is 10, 12 or 14 respectively. The proposed system consists of block size of 128 bits and key size of 128 bits. The algorithm is applied for both image encryption and decryption. As the key size is of 128 bits it will take 10 rounds.

AES Image Encryption is the conversion of original image i.e plain image into encrypted image i.e. cipher image. The round consists of the following stages for image encryption:

- Substitute Bytes
- Shift Row
- Mix Columns
- AddRoundKey

Substitute Bytes: The Sub Bytes transformation includes non-linear byte substitution, operating on each of the state bytes independently. This is done by using a once-recalculated substitution table called S-box. S-box table contains 256 numbers (from 0 to 255) and their corresponding resulting values.

Shift Row: Shift Rows transformation includes, the rows of the state are cyclically left shifted. Row 0 remain unchanged; row 1 does shift of one byte to the left; row 2 does shift of two bytes to the left and row 3 does shift of three bytes to the left.

Mix Columns: In Mix Columns transformation, the columns of the state are considered as polynomials over $GF(2^8)$ and multiplied by modulo + 1 with a fixed polynomial $c(x)$, given by:

$$c(x) = \{03\} + \{01\} + \{01\}x + \{02\} \quad (1)$$

AddRoundKey: In the AddRoundKey transformation, a Round Key is added to the State resulted from the operation of the Mix Columns transformation by a simple bitwise XOR operation. The Round Key of each round is derived from the main key using the Key Expansion algorithm. The encryption and decryption algorithm needs ten 128-bit Round Key

Reverse of encryption is called decryption. It means conversion of cipher image into plain image. The round consists of the following stage for image decryption:

- AddRoundKey
- InverseShiftRow
- InverseSubstituteByte
- InverseMixColumns

AddRoundKey: AddRoundKey is its own inverse function because the XOR function is its own inverse. The round keys have to be selected in reverse order.

InverseShiftRow: InvShiftRows exactly functions the same as Shift Rows, only in the opposite direction. The first row is not shifted, while the second, third and fourth rows are shifted right by one, two and three bytes respectively.

InverseSubstituteByte: The InvSubBytes transformation is done using a once recalculated substitution table called InvS-box. That InvSbox table contains 256 numbers (from 0 to 255) and their corresponding values.

InverseMixColumns: In the InvMixColumns transformation, the polynomials of degree less than 4 over $GF(2^8)$, which coefficients are the elements in the columns of the state, are multiplied modulo $(x^4 + 1)$ by a fixed polynomial $d(x) = \{0B\}x^3 + \{0D\}x^2 + \{09\}x + \{0E\}$, where $\{0B\}$, $\{0D\}$; $\{09\}$, $\{0E\}$ denote hexadecimal values.

The input images is of different dimension, it extract the pixel value of the image which is divided into the block of 4x4 matrix. The input matrix iterate to the different round of the AES like add round key, substitute byte, shift row and mix column respectively to give the ciphered image. In add round key, the subkey is combined with the input state matrix and the subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

In substitute Byte, transformation of state matrix from add round key is done using s-box table and the corresponding value are replaced in the state matrix.

In shift row operation the four rows are shifted cyclically to the left by offsets of 0, 1,2 and 3. It creates diffusion to the matrix bytes.

In Mix column, the current state matrix is multiplied by the fixed matrix. In this way the operation continues for the 10 rounds finally it produces the cipher image.

The process is reverse for the decryption process all the operation are carried in reverse order except add round key it remains the same as encryption.

3.2 Chaotic map encryption using Arnold Cat Map

Arnold's Cat Map [22] 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. The Arnold's cat map is a simple discrete system that stretches and folds the trajectories in phase space, which is another typical feature of chaotic processes. The phase space for this simple system can be represented by a square, and the stretching and folding process scrambling effect is relatively best in Arnold's Cat Map. The Arnold Cat Map takes concepts from linear algebra and uses them to change the positions of the pixel values of the original image. The result after applying the Arnold Cat Map will be a shuffled image that contains all of the same pixel values of the original image.

The transformation that is used by the Arnold cat map is based on a matrix with a determinant of Eq(2) that makes this transformation reversible and can be described as:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & P \\ Q & PQ + 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{mod } n \quad (2)$$

Here P and Q are integers and (x, y) is the original position that is mapped to the new position (x', y'). P and Q represent the parameter used in the method which is generally taken as a prime number value. Reverse mapping using Eq (3) is a phase in decryption process to transform the shuffled image into the input image. The number of iterations in the permutation step must be equal to that of the reverse transformation.

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} PQ + 1 & -P \\ -Q & 1 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix} \text{mod } n \quad (3)$$

Arnold's Cat Map (ACM) algorithm

It uses chaotic sequence generated by Arnold cat map to encrypt image data and it is possible through the following steps:

Step 1: Input any arbitrary square image

Step 2: Use num as variable which is represented the No. of Iterations

Step 3: Determine the No. of rows and columns. Which are represented by the variables row and col respectively.

Step 4: for inc = 1 to num

Step 5: for row1 = 1 to row

Step 6: for col1 = 1 to col

Step 7: nrowp = row1

Step 8: ncolp = col1

Step 9: for ite = 1 to inc

Step 10: Shuffle the positions of the pixels of the image using Eq. (2)

Step 11: end

Step 12: Result the new encryption image

Step 13: end

Step 14: end

Step 15: end

Reverse the steps from 1 to 15 and using the Eq. (3) for decryption process.

The image pixel position is the input to the catmap equation, the catmap take the linear sequences of the image pixel position and shuffle the position, resulting the encrypted image, the process is iterated till the last pixel position. The decryption process is reversed of encryption process.

3.3 Hybrid Chaotic map encryption using Arnold cat map with Logistic map

The Arnold's cat map is a simple discrete system that stretches and folds the trajectories in phase space, which is another typical feature of chaotic processes. The phase space for this simple system can be represented by a square, and the stretching and folding process scrambling effect is relatively best in Arnold's Cat Map. The Arnold Cat Map takes concepts from linear algebra and uses them to change the positions of the pixel values of the original image. The result after applying the Arnold Cat Map will be a shuffled image that contains all of the same pixel values of the original image. Consider $N \times N$ image and x and y be the row and column number of the pixels in

the image. Thus x and y both ranges from 1 to N. Arnold's Cat Map transformation of the image is obtained by implementing the below equation:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & P \\ Q & PQ + 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{mod } n \quad (4)$$

Where P and Q are positive integers, and determinant of matrix A is 1. The value of P and Q depends on the key size. When Arnold cat map algorithm is executed once, the original pixel positions coordinate will be transferred from the (x, y) to a new pixel position (x', y'); then the process is repeated with the A matrix multiplied. The pixels will continue to move until they return back to their original position; the number of moves is T and the size of the pixel space is n = 0, 1, 2... N-1. Pixels move with periodicity, and T, p, q and the original image's size N are correlated; thus, whenever the values change, it generates a completely different Arnold cat map. After being multiplied few times, the correlation between the pixels will be completely chaotic.

However, Arnold cat map encryption algorithm has periodicity, which reduce its encryption security, thus Logistic map is used to enhance the security of the chaos system.

The logistic map [16] is a polynomial mapping of degree 2, often cited as an archetypal example of how complex, chaotic behavior can arise from very simple non-linear dynamical equations. Mathematically, the logistic map is written as:

$$x(n+1) = \lambda \times x(n) \times (1 - x(n)) \quad (5)$$

Where x is map's variable and x (0) acts as its initial condition, λ is system parameter and n is number of iterations needs to be applied. Here λ ∈ [0, 4]. When λ ∈ [0, 3], the value of x reaches a fixed value after several iterations without any showing any chaotic dynamics. When λ ∈ [3, 3.57] the map oscillates between 2 fixed values without any chaotic dynamics. The map exhibits chaotic dynamics for 3.57 < λ < 4 and x (n) ∈ (0, 1) for all n. The initial value λ and x (0) acts as secret key when employed in an encryption system. To successfully decrypt the message, exact values of both λ and x (0) are needed at the receiver end. Thus, the algorithm becomes entirely key dependent which makes the extraction of information from the encrypted image difficult for the attacker.

The Arnold cat map adds the permutation steps to the original image which changes the shuffle pixel position of the original image thus forming cipher image. The cipher image is then used with

the logistic map which adds diffusion to the pixel position and changes the sequences of the pixel randomly thereby increasing the randomness property of an encrypted image.’

In the diffusion stage, pixel values are modified sequentially by mixing with the key stream elements that are generated by a one-dimensional chaotic map. Logistic Map is used for performing diffusion of the permuted image. Generally, the modification to one particular pixel depends not only on the corresponding key stream element but also on the accumulated effect of all the previous pixel values, as described by:

$$C(n) = X(n) \oplus P(n) \oplus C(n-1) \quad (6)$$

where $P(n)$, $X(n)$, $C(n)$, and $C(n-1)$ represent the current plain pixel, key stream element, output cipher-pixel and the previous cipher-pixel, respectively. Such diffusion algorithm can spread a significant difference in the plain image to large scale pixels in the ciphered image and thus differential attack can be resist. Additionally, to cipher the first pixel, $C(-1)$ has to be set as a seed.

Encryption process:

Step 1: Load the plain image.

Step 2: Perform permutation using Arnold Cap Map for desire rounds with keys P and Q.

Step 3: Perform diffusion using Logistic Map for desire round on permuted image with keys λ , X_0 and C.

Decryption process

Step 1: Perform inverse diffusion using Logistic map for same round on encrypted image with key λ , X_0 and C.

Step 2: Perform inverse permutation by using Arnold cat map for same rounds on the previously diffused image with keys P and Q

Chapter 4

Implementation and Analysis

4.1 Implementation

The Arnold catmap, Arnold catmap with logistic map and AES algorithm are implemented in the Java programming language of community free edition IntelliJ Idea 2017 and JDK version of 9.0.4 in windows platform of 64 bit OS with core i5 processor. The java IDE platforms for professional developers by jetbrain enables the dynamic environment for the analyzing the code, looking connection between symbols across all project files and languages.

4.1.1 Java Programming Language: J2SE overview

The programming language used in the implementation is java programming language. It's a general-purpose, fast, secure, reliable, platform-independent, object-oriented programming language. Java platform Standard Edition (SE) is a computing platform for development and deployment of portable code for desktop and server environments. The platform uses java programming language and is a part of the java software platform family. Java SE defines a range of general purpose APIs such as Java APIs for the java class library and includes the java language specification and the Java virtual machine specification. Oracle has two products that implement Java Platform Standard Edition (Java SE) 8: Java SE Development Kit (JDK) 8 and Java SE Runtime Environment (JRE) 8. JDK 8 is a superset of JRE 8, and contains everything that is in JRE 8, plus tools such as the compilers and debuggers necessary for developing applets and applications. JRE 8 provides the libraries, the Java Virtual Machine (JVM), and other components to run applets and applications written in the Java programming language.

4.1.2IntelliJ IDEA

IntelliJ IDEA 2017.1.4 is a Java integrated development environment for developing computer software. It is developed by Jet Brains, and is available as an Apache 2 Licensed community edition, and in a proprietary commercial edition. Both can be used for commercial development. IntelliJ IDEA Community Edition is the open source version of IntelliJ IDEA, a premier IDE (Integrated Development Environment) for Java, Groovy and other programming languages such as Scala or Closure.

The Community Edition includes an intelligent code editor that has all the smarts for understanding Java, XML and Groovy code, refactoring's, code inspections and intentions, super-fast navigation and search, testing frameworks integration: JUnit and TestNG and swing UI designer.

4.2 Test Environment

All of the algorithm are tested on the JDK and JRE of version 9.0.4 with an IntelliJIDEA as an IDE. The implementation of the algorithm is done in Acer aspire M5 with Intel (R) core™ i5-3337U CPU @ 1.80GHz core processor with Installed RAM of 6GB and Usage of 4.58GB and system type of 64 bit operating system and x64 based processor. The disk requirement for development tools is 181 MB.

4.3 Test Data Description

Test data is taken for the experiment analysis are the different image formats. The input images types is of .bmp, .jpeg, gif, tiff, bmp types. The image data are both primary and secondary. The secondary type of image datasets are the standard images like Lena, Peppers, Baboon, Cameraman, d2, s1,x1,baby etc. of different dimension from SIPI Image dataset from [27], DICOM image from [29] and chest ray medical image from [28]respectively. The primary image are the captured images from camera.

4.3.1 Sample Test Data

Test data is taken from different repository like sipi image dataset, dicom images, chest ray image, image etc. acts as a secondary image and the captured images is taken as the primary image for the experimentation purpose.

Suppose a standard lena image of dimension 256x256 has a pixel value as

$$\begin{bmatrix} 104 & 134 & 144 & 139 & 150 & \dots & \dots & \dots & \dots \\ 88 & 124 & 140 & 139 & 152 & \dots & \dots & \dots & \dots \\ 84 & 123 & 141 & 140 & 154 & \dots & \dots & \dots & \dots \\ 81 & 120 & 135 & 124 & 139 & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{bmatrix}$$

The pixel value is subjected to different implemented model in the following ways. The AES algorithm divide the image pixel into the block of 128 bits and manipulate the pixel value for encryption process accordingly. In the same way the Arnold catmap uses the pixel location to scramble the pixel position with the help of its encrypting equation and in case of Arnold catmap

with logistic map, initially the pixel position is shuffle by the Arnold catmap and later the logistic map is applied to scramble the pixel value, thus resulting the encrypted image.

4.4 Analysis

The algorithms implemented during this study are analyzed from various dimensions. Computational analysis based on encryption and decryption time, differential analysis based on Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI), statistical analysis based on histogram analysis and visual assessment analysis based on Peak Signal to Noise Ratio (PSNR) of input images and enciphered images has been done.

4.4.1 Visual Assessment Analysis:

Visual assessment analysis is done to measure the performance of the decryption procedure. For that the PSNR value will be calculated. It is the ratio of mean square difference of the component for the two images to the maximum mean square difference that can exist between any two images. Greater the value of PSNR higher the image quality and when we compare between original image and decrypted image but it is just opposite if we compare the original image with encrypted image i.e. lowest PSNR value results the best outcomes. The PSNR and MSE values for different set of images are measured and compared for visual assessment analysis.

$$MSE = \frac{1}{M \times N} \sum_{i=1}^N \sum_{j=1}^M [I(i, j) - I'(i, j)]^2 \quad (7)$$

$$PSNR = 10 \times \lg \left(\frac{255^2}{MSE} \right) \quad (8)$$

PSNR for the sample test data image are

Table 1:PSNR Measures

S.N.	Image	Method	PSNR(decibel)
1	Baboon.jpg 512x512 Size=235KB SIPI image dataset	AES	11.93
		Arnold catmap	12.50
		Arnold catmap+logistic map	13.08

2	Peppers.bmp 512x512 Size=2611.2KB SIPI Image dataset	AES	10.82
		Arnold catmap	11.09
		Arnold catmap+logistic map	11.89
3	Cameraman.gif 256x256 Size=17.8 KB SIPI image dataset	AES	9.52
		Arnold catmap	10.00
		Arnold catmap+logistic	10.56
4	Nkc.jpg 300x300 Size=96 KB Camera Captured Primary Image	AES	11.32
		Arnold catmap	12.53
		Arnold catmap+logistic	12.75
5	Baby.bmp 2000x2000 Size=13510 KB Capture image dataset	AES	7.89
		Arnold catmap	9.71
		Arnold catmap+logistic	9.99
6	X2.bmp 1000x1000 Size=1447 KB Chest ray image	AES	7.53
		Arnold catmap	10.80
		Arnold catmap+logistic	11.08
7	S1.tiff 1024x1024 Size=1025 KB Sipi image dataset	AES	10.65
		Arnold catmap	11.7
		Arnold catmap+logistic	12.08
8	D2.jpg	AES	7.21

	800x800 Size=647 KB Dicom image dataset	Arnold catmap	12.28
		Arnold catmap+logistic	12.49

The PSNR value of the original image with cipher image is calculated and it is observed that the PSNR of AES technique has PSNR value of 7-9 which is less compared to other two approaches which ensures that the algorithm has good visual assessment. The lesser the PSNR value, the lesser destruction of image properties hence more improvement the decrypted image is obtained. The PSNR value in the range of 7-9 is considered for the better results. The chaotic method has more PSNR value so it results into the loss of image properties.

4.4.2 Differential Analysis:

Differential analysis is done for security measures. It is a technique which observe how difference in input affects differences on the output. NPCR (Number of pixel change) and UACI (Unified Average Change Intensity) are the two widely used security analyses in image encryption community for differential analysis. NPCR concentrates on the absolute number of pixels which changes value in differential attacks while the UACI focuses on the averaged difference between two paired cipher images. The image from sipi dataset, dicom images chest-ray medical images are taken for experimentation to predict which methods results the best outcomes. NPCR and UACI can be calculated using the following equation.

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \quad (9)$$

$$UACI = \frac{1}{W \times H} \left(\sum_{i,j} \frac{|C(i,j) - C'(i,j)|}{255} \right) \times 100\% \quad (10)$$

NPCR and UACI of the sample datasets are

Table 2: NPCR and UACI Measures

S.N.	Image	Method	NPCR	UACI
1	Baboon.jpg 512x512 Size=235KB	AES	86.68	64.14
		Arnold catmap	96.99	22.98
		Arnold catmap+logistic map	99.98	26.67

2	Peppers.bmp 512x512 Size=2611.2KB	AES	0.0030	0.0020
		Arnold catmap	84.80	25.96
		Arnold catmap+logistic map	99.98	34.35
3	Cameraman.gif 256x256 Size=17.8 KB	AES	0.0063	0.0021
		Arnold catmap	0.0089	0.0030
		Arnold catmap+logistic	0.67	0.334
4	Nkc.jpg 300x300 Size=96 KB	AES	83.23	20.76
		Arnold catmap	90.99	30.32
		Arnold catmap+logistic	99.95	32.85
5	Baby.bmp 2000x2000 Size=13510 KB	AES	80.21	21.34
		Arnold catmap	92.14	29.83
		Arnold catmap+logistic	99.34	32.44
6	X2.bmp 1000x1000 Size=1447 KB	AES	6.89e-7	2.43e-7
		Arnold catmap	9.99e-5	1.4e-7
		Arnold catmap+logistic	5.04e-4	2.10e-4
7	S1.tiff 1024x1024 Size=1025 KB	AES	3.814E-4	3.23e-7
		Arnold catmap	8.45e-4	4.34e-7
		Arnold catmap+logistic	0.0024	5.37e-5
8	D2.jpg	AES	93.32	0.067

800x800 Size=647 KB	Arnold catmap	98.95	0.234
	Arnold catmap+logistic	99.99	0.343

The above results generalises the different technique in differential analysis for the image. It is seen that Arnold catmap with logistic map have good results than that of arnold cat map and AES because the value it generate is high for NPCR and UACI are high in the range of 98-99 and 30-33. But the case for AES on this category is lower so arnold cat with logistic map is strong on this category to resist the differential attacks.

4.4.3 Computational Speed Analysis:

Computation analysis is the measures of time consumed by the algorithms. We measure the value of encryption and decryption time for computational performance for different set of images in milliseconds to find which techniques has good results and it is observed from the given below bar graph that the AES has relatively high encryption/decryption time. It is also seen that as the image sizes increases the time consume by the algorithm get increased compare to other two chaotic approach so from this observation it can be conform that AES is computationally inefficient than that of other two approaches. Arnold catmap has less computational time therefore in this category Arnold catmap works well.

The Encryption and Decryption time of different methods are shown below:

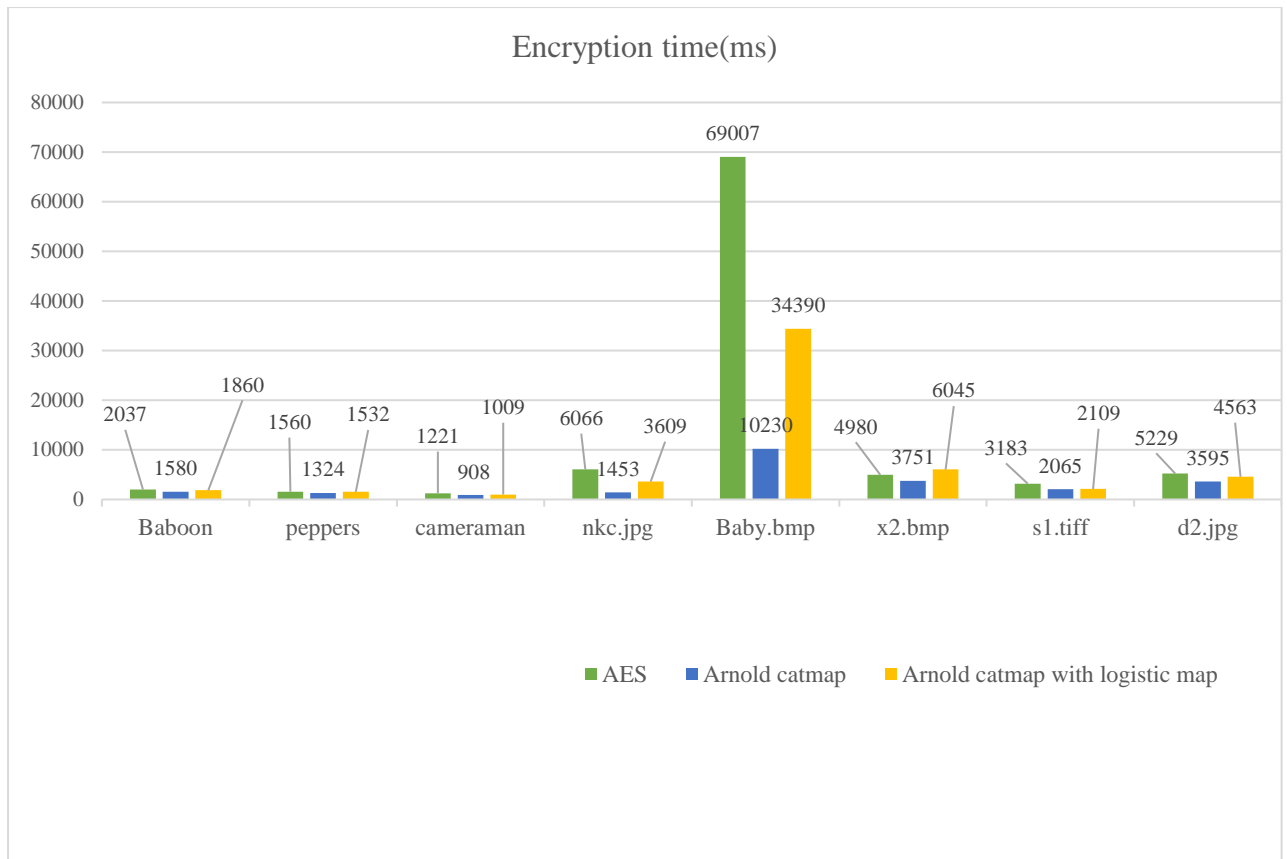


Fig 2: Encryption time measurement

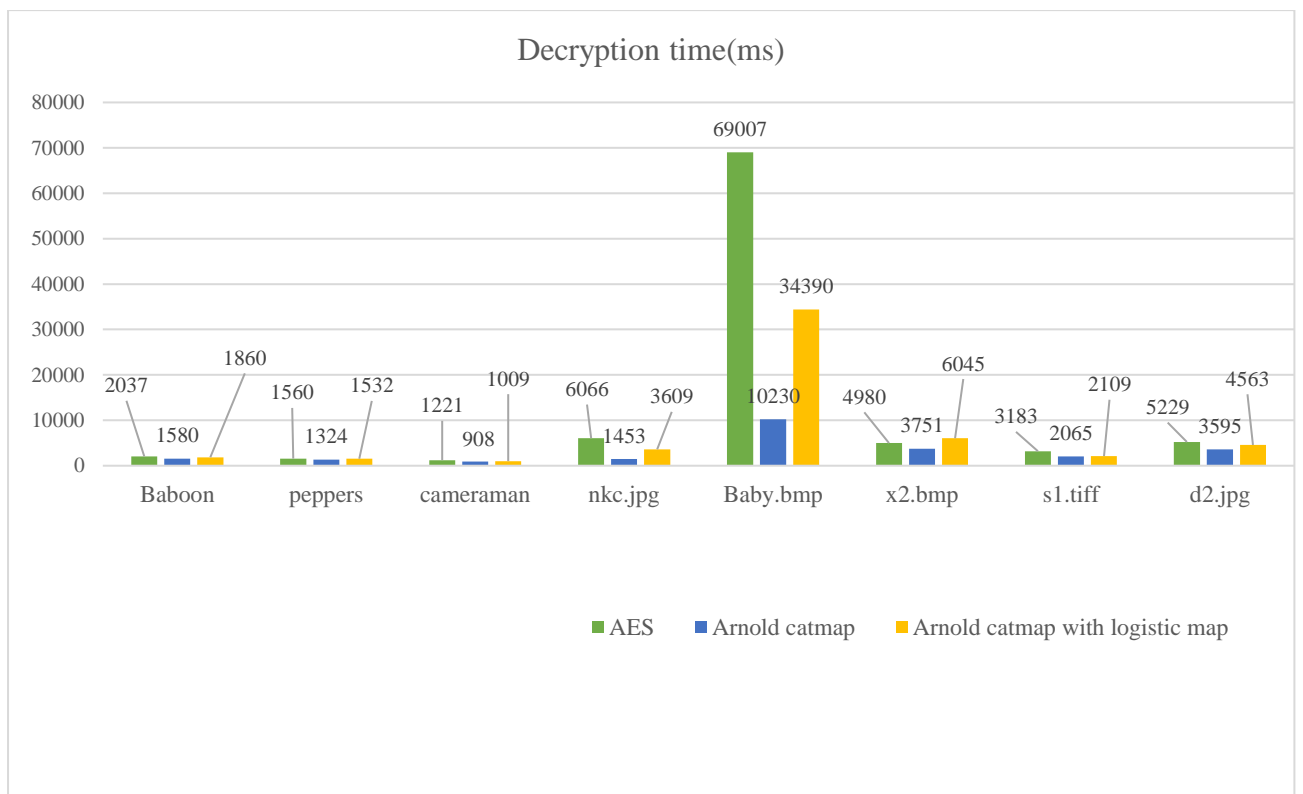



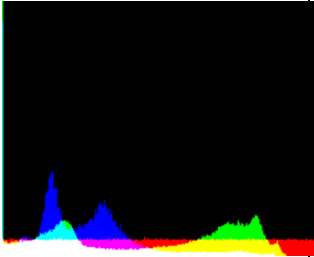
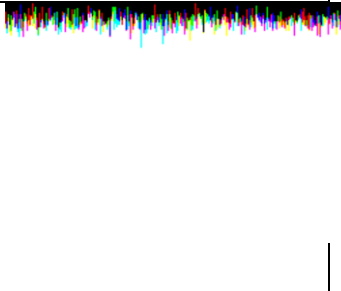
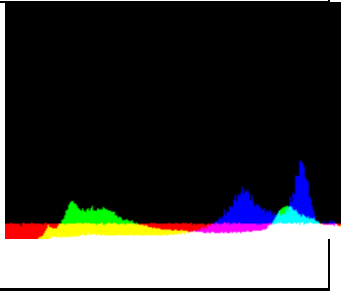
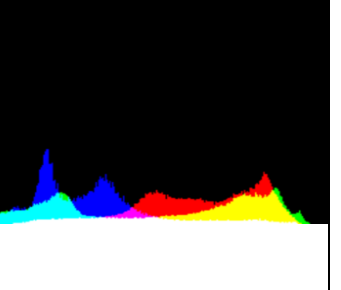
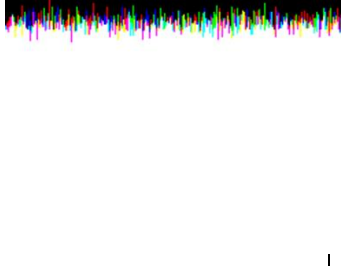
Fig 3: Decryption time measurement

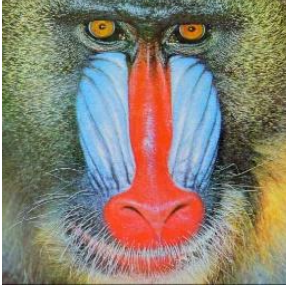
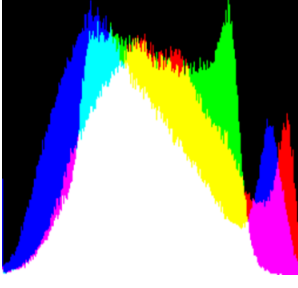
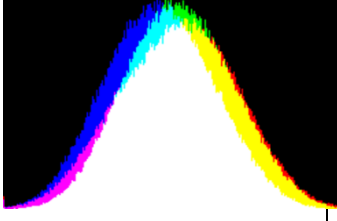
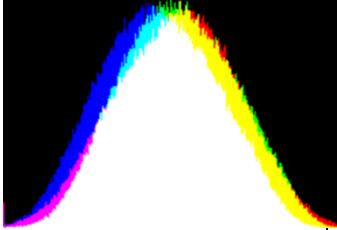

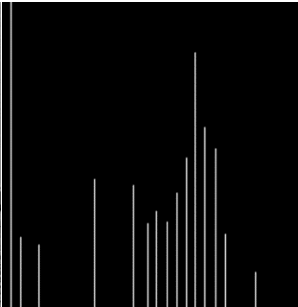
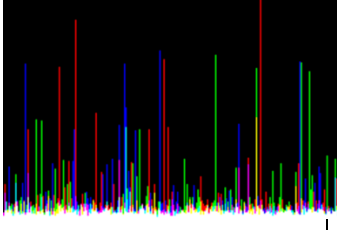
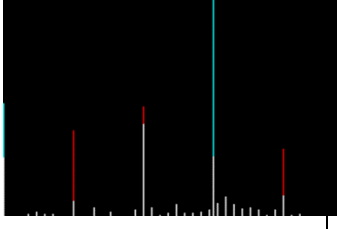
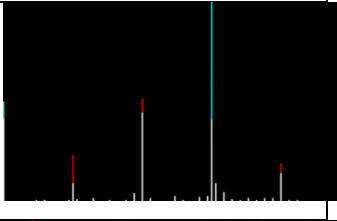

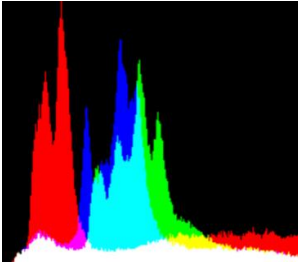
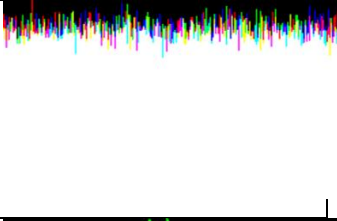
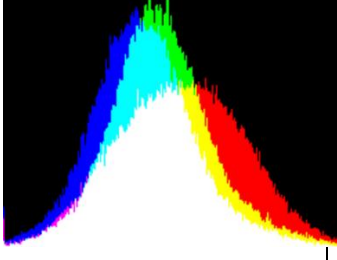
4.4.4 Statistical Analysis:

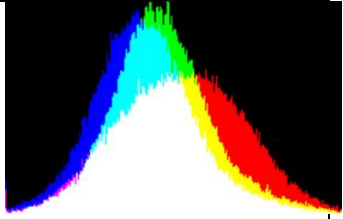

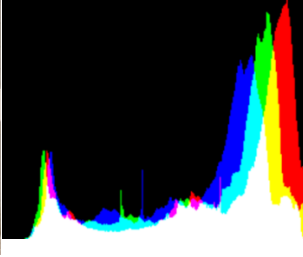
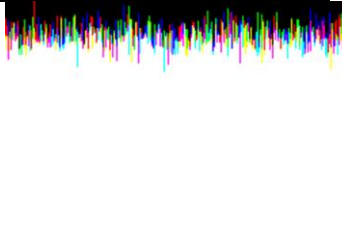
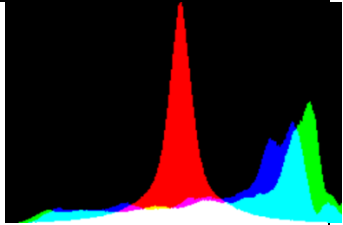
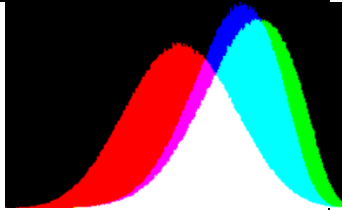
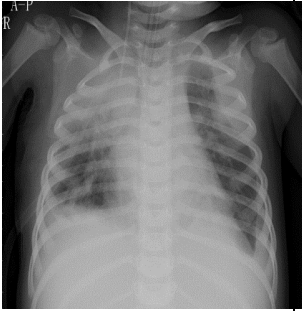
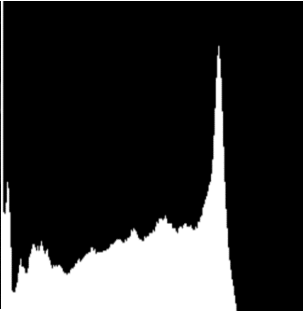
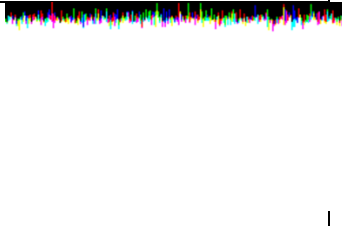
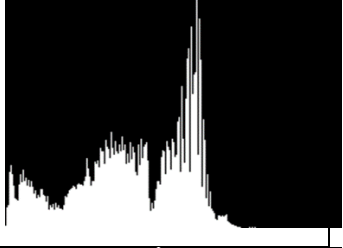

Statistical analysis has been carried out with the help of histogram analysis. The histogram of an image normally refers to a histogram of the pixel intensity values. This histogram is a graph showing the number of pixels in an image at each different intensity value found in that image. Histogram of input image and cipher image is analyzed graphically.

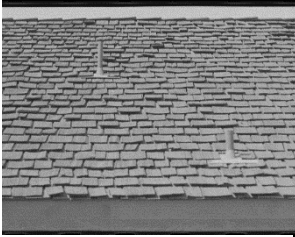
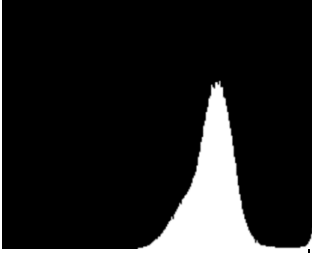
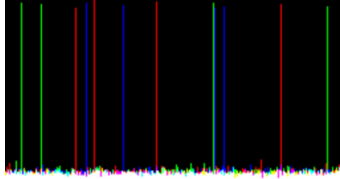
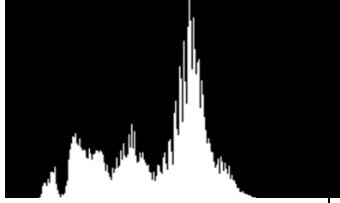
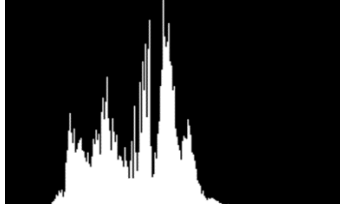

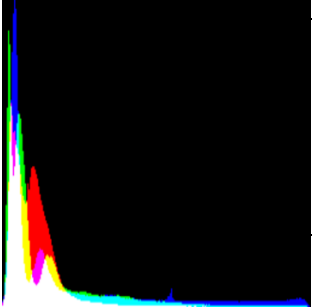


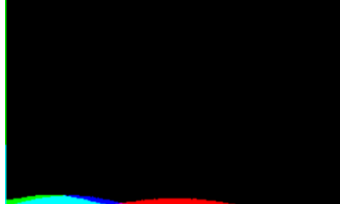
Histogram of the sample dataset are

Table 4: Histogram Analysis

S.N	Image	Plain image histogram	Method	Cipher image histogram
1	 Peppers.bmp		AES	
Arnold catmap				
Arnold catmap+logistic map				
2.			AES	

	 Baboon.jpg		Arnold catmap	
			Arnold catmap+logis tic map	
3.	 Cameraman.gif		AES	
			Arnold catmap	
			Arnold catmap+logis tic	
4.	 Nkc.jpg		AES	
			Arnold catmap	

			Arnold catmap+logis tic	
5.			AES	
	Baby.bmp		Arnold catmap	
			Arnold catmap+logis tic	
6.			AES	
	X2.bmp		Arnold catmap	
			Arnold catmap+logis tic	

7.	 S1.tiff		AES		
				Arnold catmap	
				Arnold catmap+logistic	
8.	 D2.jpg		AES		
				Arnold catmap	
				Arnold catmap+logistic	

It is seen that the histogram of AES cipher and original image has a significant difference, since greater the difference in histogram more robust the security mechanism is imposed. The AES method has greater difference in histogram of cipher and plain image from the above results than that of other two approaches so AES has strong impact on histogram analysis to secure the image from intruders than that of other two approaches.

4.6 Result

The overall analysis of image in different field of categories shows that AES method is computationally inefficient method with other two approach. With the increase in the image size AES performance get degraded by approximately 50% than that of Arnold catmap and Arnold catmap with logistic map.

The results also shows that AES has maintain the image quality after decrypting the image although other two approaches are unable to maintain as this can be illustrated by the above results of PSNR value. The PSNR value of AES method in the range from 7.5 statistically represent good value which conforms that the original image and decrypted image is similar without losing much of its image properties. But Arnold catmap and Arnold catmap with logistic map has significantly has higher PSNR value which ranges from 9 onwards, this value of PSNR results in a change of visual properties of the image. The values also shows that image is more distorted by the hybrid chaotic methods.

Besides it AES resembles quality performance in the histogram analysis of the image, since the histogram of cipher and original image has more variation. The greater the difference reduces the chances of attacks by the intruders since it doesn't give any hint of original image data. The Arnold catmap and Arnold catmap with logistic map although shows the differences but it is very less.

The Arnold catmap with logistic map a hybrid approach has good differential analysis value which in the range of 95-99.99 and 28-34 for the NPCR and UACI respectively for different set of image. This value is able to protect the image from attackers as it able to hide the significant information of image data. Arnold catmap has significantly less impact on this categories but it is comparatively good than that of AES as it can be shown in the above mentioned figures.

Thus based on the above observation and result analysis Arnold catmap with logistic map is better in resisting differential attack and computationally efficient one, Arnold catmap is the efficient of all compared algorithm and AES has good characteristic of preserving image properties after decryption as it has less PSNR value and significant difference between the histogram of cipher and original image.

Chapter 5

Conclusion and Future Recommendation

5.1 Conclusion

Image encryption is the need of today world for the secure communication of image. Although number of approach has been invented for the secure image encryption. In this study chaotic, hybrid chaotic and block cipher has been implemented. The image data sets of different types were taken into account. All of the data sets were tested with the algorithm to measure the strength of algorithm.

Overall analysis and result from the above discussion conclude that chaotic, hybrid chaotic and block cipher approach creates a positive impact on image encryption. The features from each category of algorithm has been added to the image to provide a secure environment for the communication. The algorithm are implemented and analyzed with different parameters to test the strength of the algorithm and found that AES is computationally inefficient and has able to preserve the image properties after encryption i.e. AES has good result in PSNR and Histogram differences. The Arnold catmap with logistic map has high NPCR and UACI value which proves the strength of algorithm in the resisting differential attack although the hybrid chaotic method seem to preserve the less image properties. The Arnold catmap method is found to be computationally efficient one compared to other two method.

5.2 Future recommendation

Image data though maintain the certain secured properties with chaotic and hybrid chaotic and block cipher approach, although lots of work can be carried out in near future like to know the periodicity of the Arnold cat map. The approaches of higher dimension 2D, 3D chaotic map has been also established as a next level of work to build a secured and efficient image encryption framework. The chaos based cryptosystem is also equally creates a significance impact on the image encryption process so if it should be also carried the remarkable impact can be made in this research. The mechanism to preserve the loss of image properties that are likely to appear after decrypting the image is the major matter to be concerned by the chaotic and hybrid chaotic method. Additionally, the cryptanalysis of the analyzed algorithms can also be performed in future to determine security threat and attack strengths.

References

- [1] Abuhaibal I.S.I., Abuthraya H.M., Hubboub H.B., Salamah R.A.: Image Encryption Using Chaotic Map and Block Chaining, International Journal on Computer Network and Information Security, Vol. 7 ,2012
- [2] Adrian-V. “Circular inter-intra bit-level permutation and chaos-based image encryption”, Information Sciences, Volumes 355–356, August 2016
- [3] Ahmed B.A., AbdSamad B.H.B, Hamida A. “A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm” September 2012.
- [4]Akram B., Ahmed A., Safya B., “A novel image encryption scheme based on substitution-permutation network and chaos”, European Association for Signal Processing, 2016
- [5] Benyamin N., Sattar M., “Breaking an Image Encryption Algorithm based on the New Substitution Stage with Chaotic Functions”, Optics - International Journal for Light and Electron Optics 127(14), Volume 127, Issue 14, July 2016
- [6] CaudleE.S., "Communication theory of secrecy system", Bell system Tech, 1949
- [7] Chandel, Gajendra S., Pragna P. "Image Encryption with RSA and RGB randomized Histograms." *Image* 3, no. 5 (2014).
- [8] Chengqing L., “On the security of a class of Image Encryption Scheme”, IEEE International Symposium on Circuit & System ,ISCAS, Department of Electronics Engineering, University of Hong Kong , pg 3290-3293,2008
- [9] Hang C., Xiaoping D., Zhengjun L., ChengweiY.,”Color image encryption based on the affine transform and gyrotor transform”, Optics and Lasers in Engineering, vol. 51, no. 6, pp. 768–775 ,Jun. 2013.
- [10] Haojiang G., Yisheng Z., Shuyun L., Dequan L., “A new chaotic algorithm for image encryption”, Audio, Language and Image Processing,. International Conference, 2005, 2008.
- [11] Joan D. and Vincent R., *AES Proposal: Rijndael*, AES Algorithm Submission, September 3, 1999.
- [12] Khadijeh M.T., Mehrzad K.J., “A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map”, Optics and Lasers in Engineering, Volume
- [13]Lei Z., Jiansheng G., Alireza J., Abdolrasoul M., “Image encryption using chaos and block cipher” 2010.

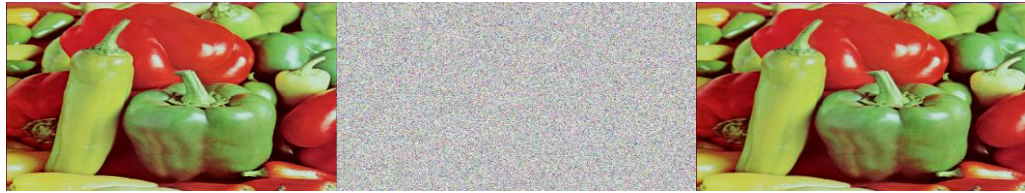
- [14] Menezes A.J., Oorschot P.C.V., Vanstone S.A., "Handbook of Applied Cryptography" CRC Press, Boca Raton, 1997.
- [15] Radhadevi P., Kalpana P. "Secure Image Encryption Using AES" International Journal of Research in Engineering and Technology.
- [16] Robert M. "Simple mathematical models with very complicated dynamics", May 1976.
- [17] Schneier B., "Applied Cryptography: Protocols, Algorithms and Source Code in C", New York 1996,
- [18] Shoaib A., Neelesh G. Sudhir A., "An Image Encryption Approach Using Chaotic Map in Frequency Domain", International Journal of Emerging Technology and Advanced Engineering- Volume 2, Issue 8, August 2012
- [19] Stinson, D.R., "Cryptography: Theory and Practice", CRC Press, Boca Raton, 1995.
- [20] Suneel M., "Cryptographic pseudo-random sequences from the chaotic Henon map," ' vol. 34, no. 5, pp. 689–701, 2009
- [21] Victor G. , Carmen G. "Chaos Encryption Method Based on Large Signal Modulation in Additive Nonlinear Discrete-Time Systems" Proc. of the 5th WSEAS Int. Conf. on Non-Linear Analysis, Non-Linear Systems and Chaos, Bucharest, Romania, October 16-18, 2006.
- [22] Vladimir I. A. "*Ergodic Problems in Classical Mechanics*", 1968.
- [23] Wenhao L., Kehui S., Congxu Z., "A fast image encryption algorithm based on chaotic map", 2016
- [24] Xiaowei L., Chengqing L., In-Kwon L., "Chaotic image encryption using pseudo-random masks and pixel mapping", European Association for Signal Processing, Volume 125, August 2016
- [25] Zhenjun T., Juan S., Xianquan Z., Ronghai S., "Multiple-image encryption with bit-plane decomposition and chaotic maps", Optics and Lasers in Engineering, Volume 80, May 2016
- [26] Zhi-liang Z., Chong W., Hua C., Hai Y., "A Chaotic Image Encryption Scheme Based on Magic Cube Transformation", IEEE Conference Publications, 2011
- [27] <http://sipi.usc.edu/database>
- [28] <https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia>

[29] <https://www.osirix-viewer.com/resources/dicom-image-library/>

Appendix

1. Input image= pepper.bmp; Size =2.55 MB; Image dimension= 512x512

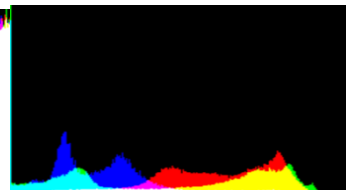
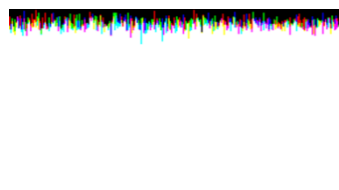
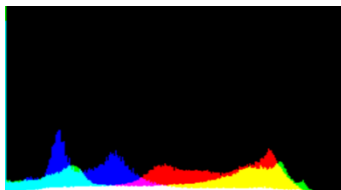
AES analysis



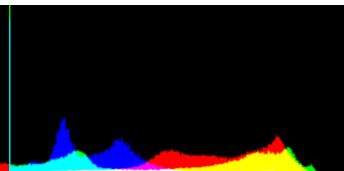
Original image

Encrypted image

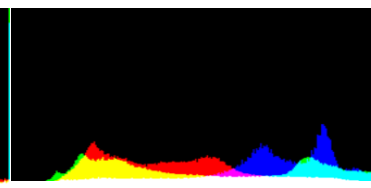
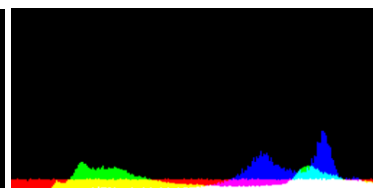
Decrypted image



Arnold catmap Analysis



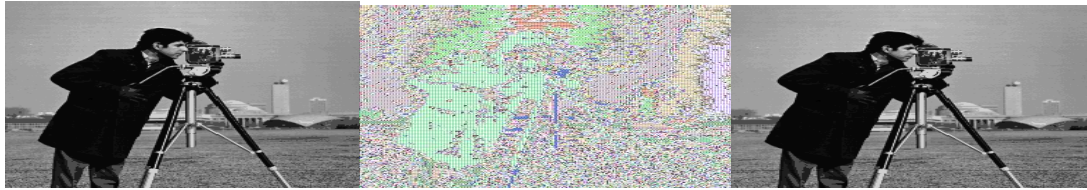
Arnold catmap with logistic map analysis



2. Input image = cameraman.gif size = 17.8 KB

Dimension=256x256

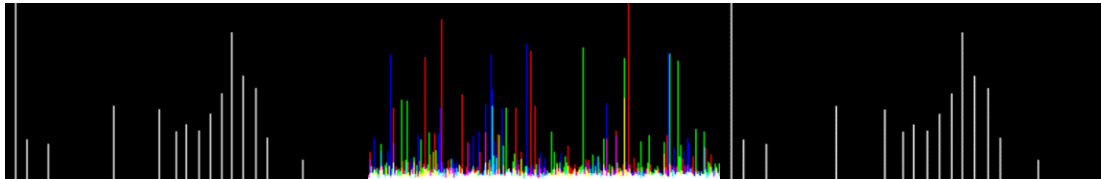
AES analysis



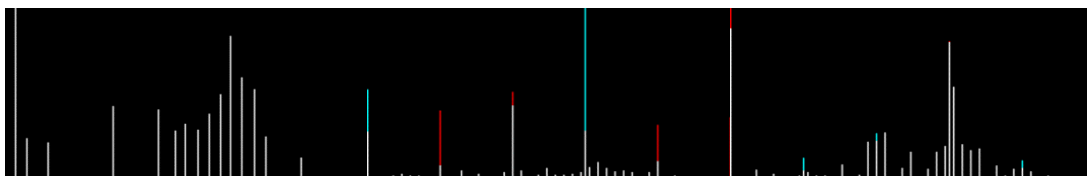
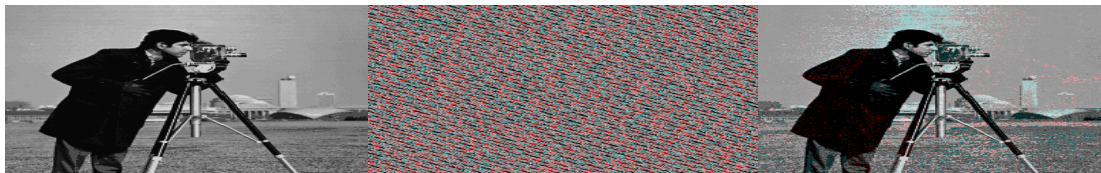
Original Image

Encrypted image

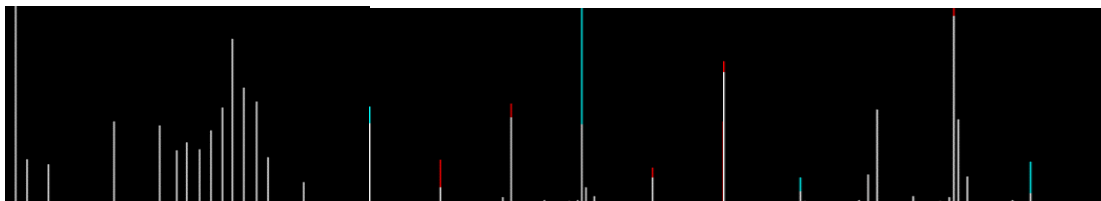
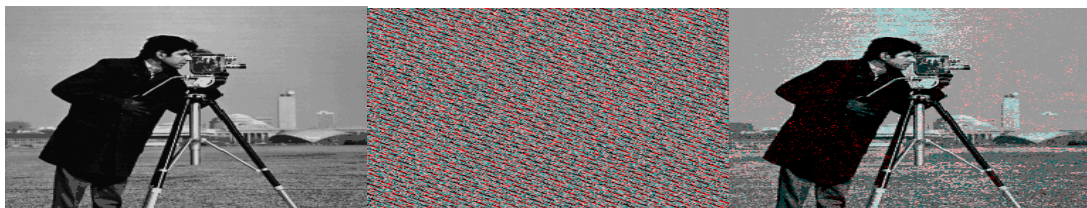
.Decrypted image



Arnold catmap Analysis

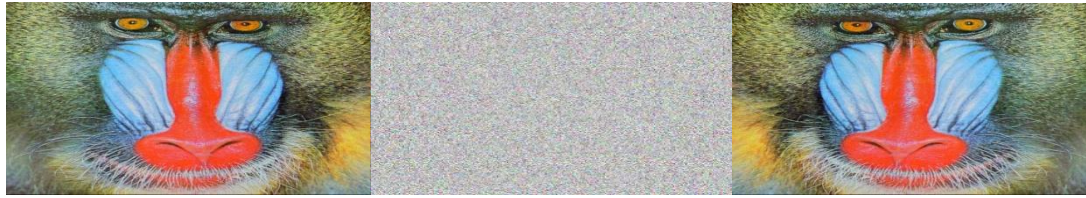


Arnold catmap with logistic analysis



3. Input image = Baboon.jpg size = 235 KB Dimension=512x512

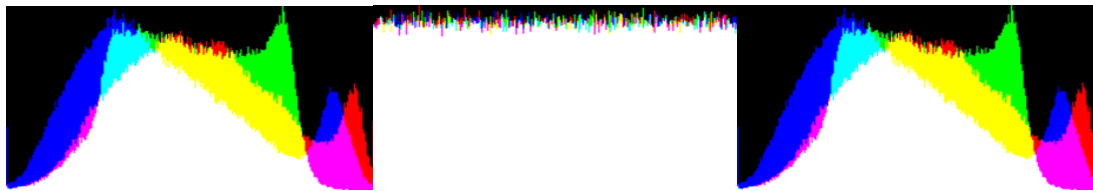
AES analysis



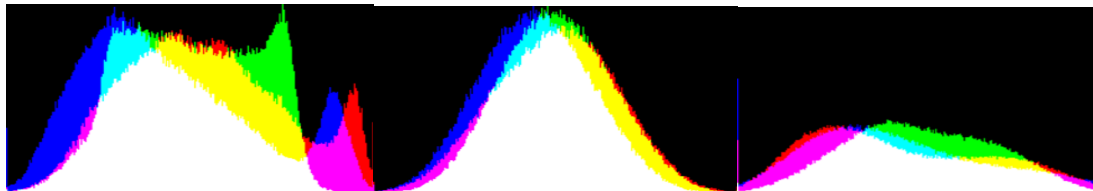
Original Image

Encrypted Image

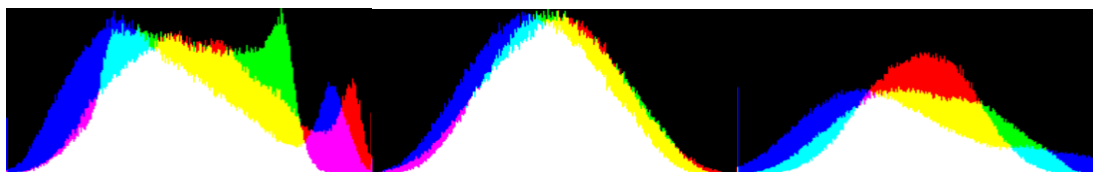
Decrypted Image



Arnoldcat map analysis



Arnold catmap with logistic map analysis



4. Input image= nkc.jpg Size=96KB Dimension=300x300

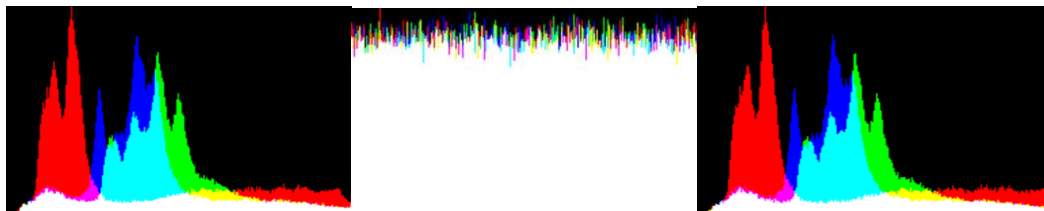
Analysis of AES method



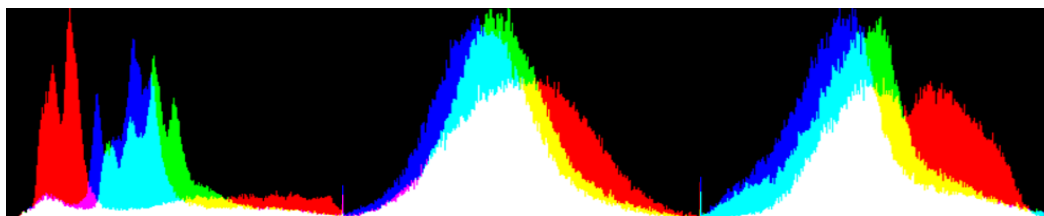
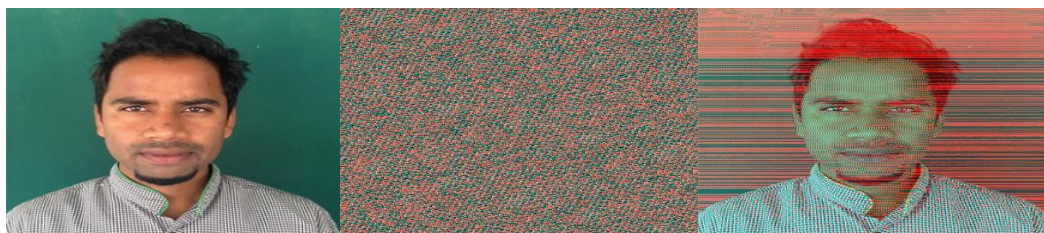
Original Image

Encrypted Image

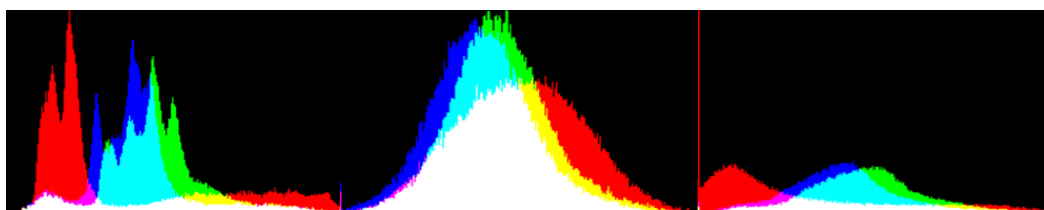
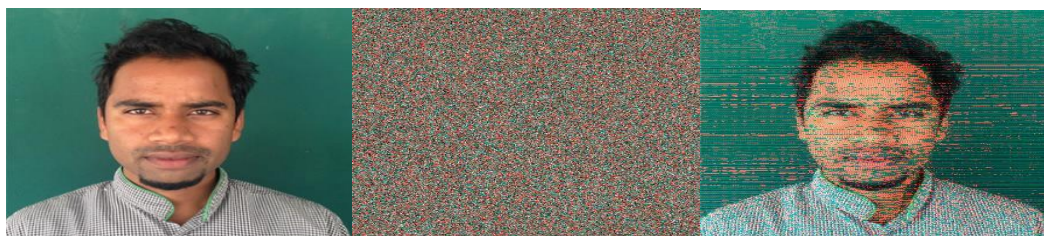
Decrypted Image



Analysis of Arnold catmap method



Analysis of Arnold with logistic map



5. Input image= d2.jpg Size=647KB Dimension=800x800

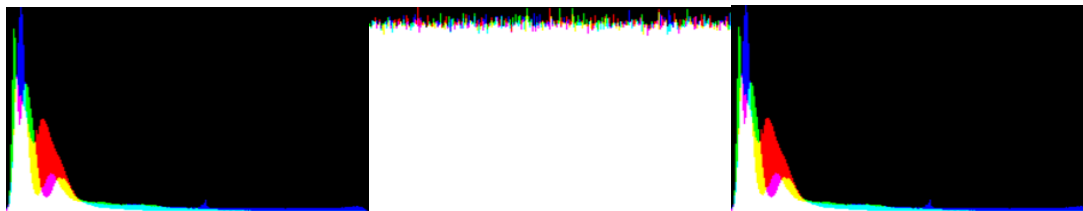
AES analysis



Original Image

Encrypted Image

Decrypted Image



Arnold catmap Analysis



Analysis of Arnold with logistic map



6. Input image= x2.bmp Size=1447KB Dimension=1000x1000

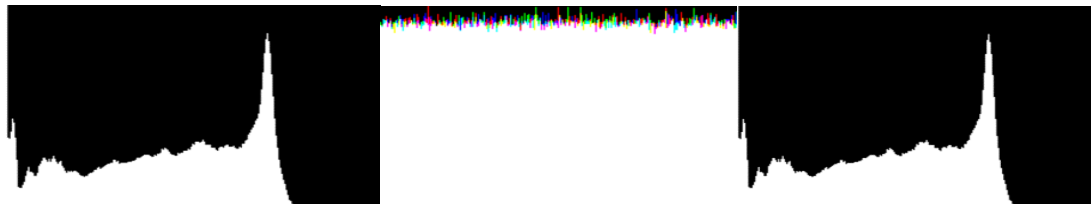
Analysis using AES



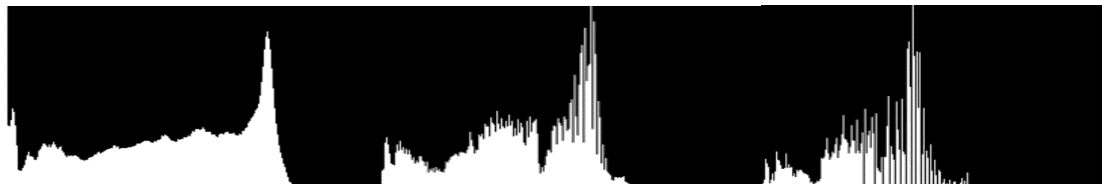
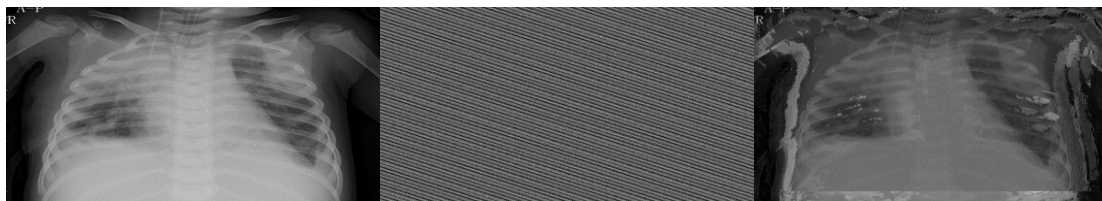
Original Image

Encrypted Image

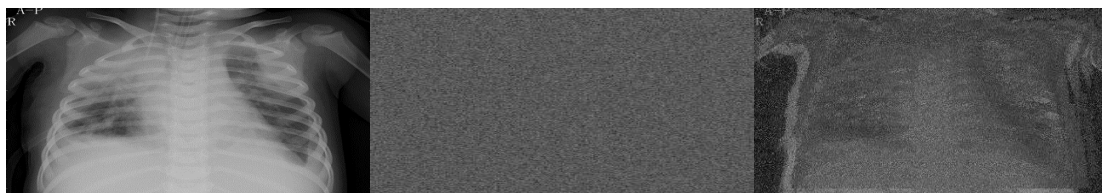
Decrypted Image



Arnold catmap

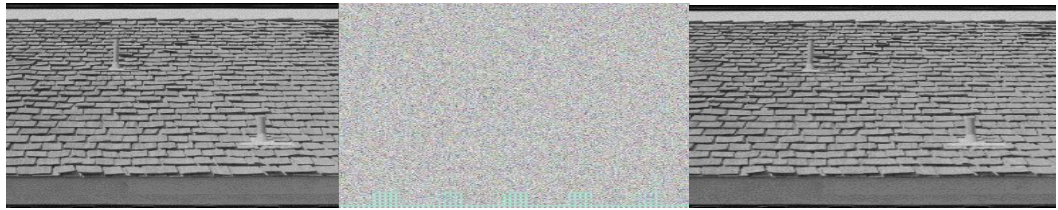


Arnold catmap with logistic map



7. Input image= s1.tiff Size=1025KB Dimension=1024x1024

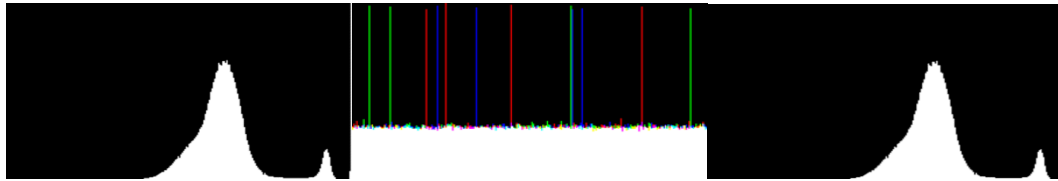
AES Analysis



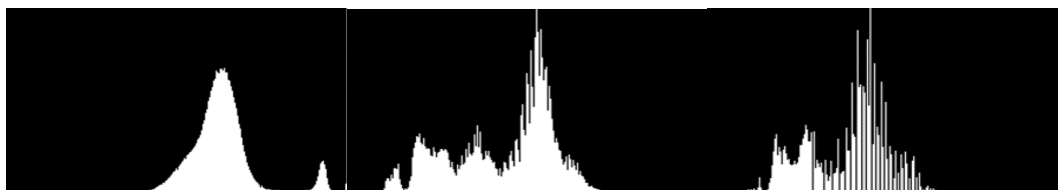
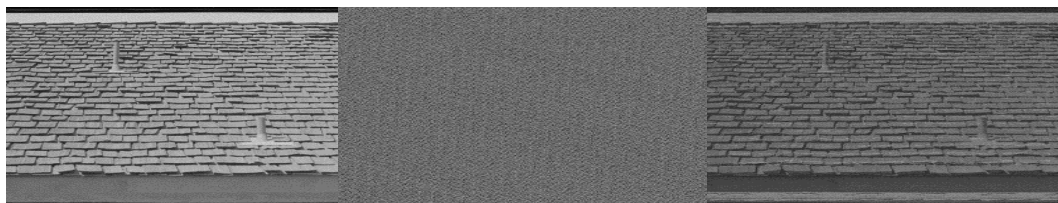
Original Image

Encrypted Image

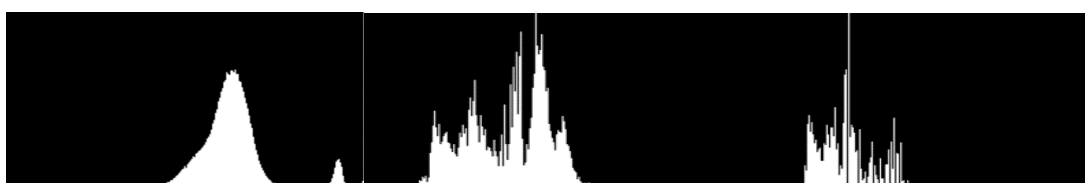
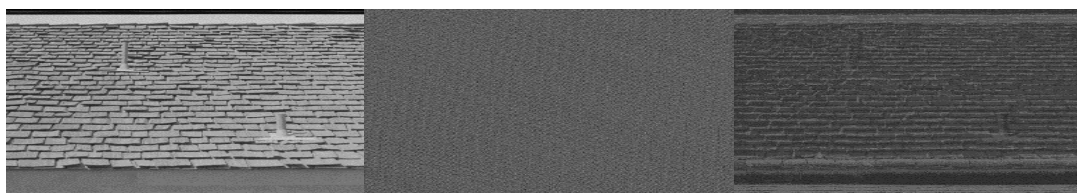
Decrypted Image



Arnold catmap Analysis



Arnold with logistic



8. Input image= baby.jpg Size=13510KB Dimension=2000x2000

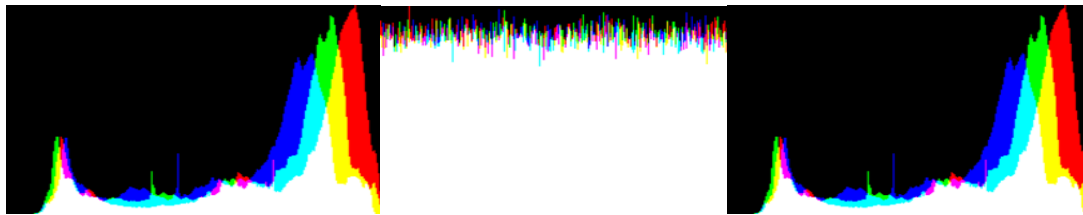
AES analysis



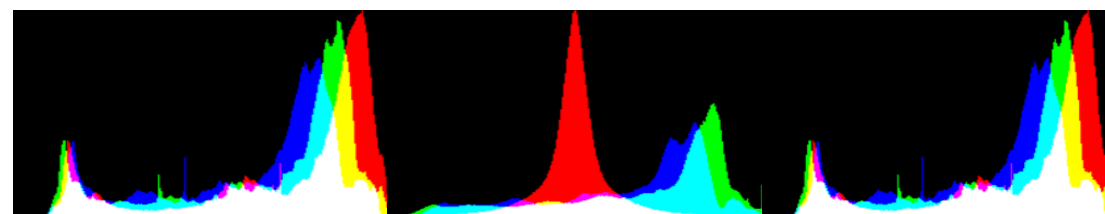
Original Image

Encrypted Image

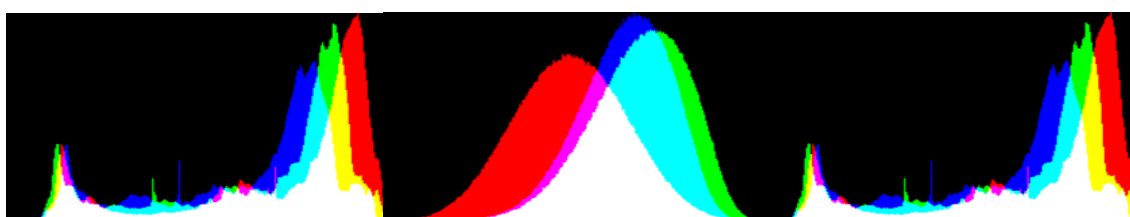
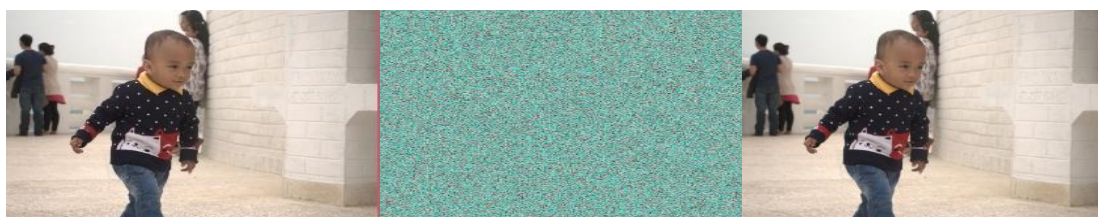
Decrypted Image



Arnold cat map analysis



Arnold with logistic map



Code appendix

AES

```
public class AES{

    // public constructor for AES
    public AES(String text,String key){
        this.key=new Keys(key);
        //this.key.print();
        this.text=new Polynomial[4][4];
        this.setText(text);
    }
    // creates structured text
    private void setText(String text){
        int firstHalfByte;
        int secondHalfByte;
        for(int i=0;i<32;i+=8){
            for(int j=0;j<8;j+=2){
                firstHalfByte=Polynomial.hexVal(text.charAt(i+j));
                secondHalfByte=Polynomial.hexVal(text.charAt(i+j+1));
                this.text[(i>>3)][(j>>1)]=new Polynomial((firstHalfByte<<4|secondHalfByte));
            }
        }
    }
    // add round key
    private void addRoundKey(int round){
        for(int i=0;i<4;i++){
            for(int j=0;j<4;j++){
                this.text[i][j]=Polynomial.add(this.text[i][j],key.getKey(round*4+i,j));
            }
        }
    }
    // substitute Sbox
    private void subBytes(){
```

```

for(int i=0;i<4;i++)
    for(int j=0;j<4;j++){
        int row=(this.text[i][j].get()&(15<<4))>>4;
        int col=this.text[i][j].get()&15;
        this.text[i][j].set(Sbox.getSbox(row,col));
    }
}
// substitute inverse Sbox
private void invSubBytes(){
    for(int i=0;i<4;i++)
        for(int j=0;j<4;j++){
            int row=(this.text[i][j].get()&(15<<4))>>4;
            int col=this.text[i][j].get()&15;
            this.text[i][j].set(Sbox.getInvSbox(row,col));
        }
}
// shift rows
private void shiftRows(){
    Polynomial temp[]=new Polynomial[4];
    for(int i=0;i<4;i++){
        for(int j=0;j<4;j++)
            temp[j]=this.text[j][i];
        for(int j=0;j<4;j++){
            this.text[j][i]=temp[(j+i)%4];
        }
    }
}
// shift rows
private void invShiftRows(){
    Polynomial temp[]=new Polynomial[4];
    for(int i=0;i<4;i++){
        for(int j=0;j<4;j++)
            temp[j]=this.text[j][i];
    }
}

```



```

    for(int j=0;j<4;j++){
        this.text[j][i]=temp[(j-i+4)%4];
    }
}
}
// mix columns
private void mixColumns(){
    Polynomial temp[]=new Polynomial[4];
    for(int i=0;i<4;i++){
        for(int j=0;j<4;j++){
            temp[j]=this.text[i][j];
        }
        for(int j=0;j<4;j++){
            this.text[i][j]=Polynomial.mul(temp[j], new Polynomial(2));
            this.text[i][j]=Polynomial.add(this.text[i][j],Polynomial.mul(new
Polynomial(3),temp[(j+1)%4]));
            this.text[i][j]=Polynomial.add(this.text[i][j],temp[(j+2)%4]);
            this.text[i][j]=Polynomial.add(this.text[i][j],temp[(j+3)%4]);
        }
    }
}
// mix columns
private void invMixColumns(){
    Polynomial temp[]=new Polynomial[4];
    for(int i=0;i<4;i++){
        for(int j=0;j<4;j++){
            temp[j]=this.text[i][j];
        }
        for(int j=0;j<4;j++){
            this.text[i][j]=Polynomial.mul(temp[j], new Polynomial(0x0E));
            this.text[i][j]=Polynomial.add(this.text[i][j],Polynomial.mul(new
Polynomial(0x0B),temp[(j+1)%4]));
            this.text[i][j]=Polynomial.add(this.text[i][j],Polynomial.mul(new
Polynomial(0x0D),temp[(j+2)%4]));

```

```

        this.text[i][j]=Polynomial.add(this.text[i][j],Polynomial.mul(new
Polynomial(0x09),temp[(j+3)%4]));
    }
}
}
// encrypt
public String encrypt(){
    // N-1 rounds
    for(int i=0;i<9;i++){
        this.subBytes();
    }
    return this.toString()
}
public String decrypt(){
    for(int i=9;i>0;i--){
        this.invSubBytes();
    }
    //this.addRoundKey(0);
    return this.toString();
}
// convert cipher to string
public String toString(){
    String s="";
    for(int i=0;i<4;i++){
        for(int j=0;j<4;j++){
            s+=String.format("%02X", this.text[i][j].get());
        }
    }
    return s;
}
// print cipher
public void print(){
    System.out.println(this.toString());
}

```

```

// text in structured form
private Polynomial text[][];
// Key
private Keys key;
}
Arnold camap
public static Point catMap(Point p, int mode)
{
    if(mode != Cipher.ENCRYPT_MODE && mode != Cipher.DECRYPT_MODE)
        return p;
    int x = p.x, y = p.y, x_new = x, y_new = y;
    if(mode == Cipher.ENCRYPT_MODE)
    {
        x_new = (2*x + y) % width;
        y_new = (x + y) % height;
    }
    else // mode == Cipher.DECRYPT_MODE
    {
        x_new = (width + (x - y)) % width; // the modulo operator may return a negative
        y_new = (height + (-x + 2*y)) % height; // value, so we add the modulus for positivity
    }
    return new Point(x_new, y_new);
}

```

```

Logistic map
public static Point logisticMap(Point p, int mode)
{
    if(mode != Cipher.ENCRYPT_MODE && mode != Cipher.DECRYPT_MODE)
        return p;
    int x = p.x, y = p.y, x_new = x, y_new = y;
    if(mode == Cipher.ENCRYPT_MODE)
    {
        double t_n = (Math.floor(Chaosdemo.x[y * width + x] * 1e14)) % (height * width);
    }
}

```

```

    x_new = (int) (t_n % width);
    y_new = (int) (t_n / width);
}
    else // mode == Cipher.DECRYPT_MODE
{
    double t_n = (Math.floor(Chaosdemo.x[height*width - (y * width + x)-1] * 1e14)) %
(height * width);
        x_new = (int) (t_n % width);
        y_new = (int) (t_n / width);
}
    return new Point(x_new, y_new);
}
}

```