A Presentation on

Comparison of different Chaotic Maps and their application to Image Encryption

Submitted to the Department of Information Technology

For the partial fulfilment of the degree of B.Tech in Information Technology

by

TRISHAN KUMAR HAZRA
Roll number: 510817018

AMIT KUMAR DEY
Roll number: 510817006

JAIMINIBEN
Roll number: 510817013

Batch of 2017-21
B.Tech. 3rd year

Under the supervision of
Professor SHYAMALENDU KANDAR

1856 १८५६
उत्तिष्ठत जाग्रत प्राप्य वरान् निबोधत
INDIAN INSTITUTE OF ENGINEERING SCIENCE AND TECHNOLOGY, SHIBPUR
भारतीय अभियांत्रिकी विज्ञान एवं प्रौद्योगिकी संस्थान, शिवपुर

Department of Information Technology
INDIAN INSTITUTE OF ENGINEERING SCIENCE AND TECHNOLOGY, SHIBPUR

Dec, 2019

Department of Information Technology
Indian Institute of Engineering Science and Technology, Shibpur

CERTIFICATE

This is to certify that the work presented in this report entitled "COMPARISON OF DIFFERENT CHAOTIC MAPS AND THEIR APPLICATION TO IMAGE ENCRYPTION", submitted by ______________________________, having the examination roll number _____________, has been carried out under my supervision for the partial fulfilment of the degree of Bachelor of Technology in Information Technology during the session 2017-21 in the Department of Information Technology, Indian Institute of Engineering Science and Technology, Shibpur.

SHYAMALENDU KANDAR
RAHAMAN
Assistant Professor
Department of Information Technology
Indian Institute of Engineering Science
and Technology, Shibpur

DR. HAFIZUR

Head of the Department
Department of Information Technology
Indian Institute of Engineering Science
and Technology, Shibpur

Date: 03-12-2019

Dean (Academic)
Indian Institute of Engineering Science
and Technology, Shibpur

Acknowledgements

We express our gratitude to our supervisor Professor SHYAMALENDU KANDAR (Department of Information Technology) and thank the department of Information Technology for the successful completion of our project.

Date: 03-12-2019

Trishan Hazra
Amit Kumar Dey
Jaiminiben
Department of Information Technology
Indian Institute of Engineering Science
and Technology, Shibpur

ABSTRACT

The objective of our project is to compare different chaotic maps and their application to image encryption. Multimedia data contains text, audio, video, graphics, images and with the increasing use of multimedia data over the internet, here comes a demand of secure multimedia data. Image encryption differs from other multimedia components encryption due to some intrinsic features, such as bulk data capacity and high correlation among pixels the earlier encryption techniques such as AES, DES etc. are not suitable for practical applications. The combination of chaotic theory and cryptography forms an important field of information security. We have tried to compare 3D and 2D logistic Maps by analyzing their
security parameters.

Contents

1 INTRODUCTION

The tremendous spreading out of the communication networks has evoked increased dependency on digitized information in our society. As a result, information is more vulnerable to abuse. Today the web is going towards multimedia data due to the development of network and multimedia technology. Multimedia data consist of image, audio, video, text, etc. The digital images become one of the most important information carriers which are helpful for biometric authentication, medical science, military, online personal photograph album, etc.

Chaos theory was first used in the computer system by Edward Lorenz 1963. During the last decade chaos based cryptography has received considerable attention due to noiselike signal for unauthorized person, ergodicity, mixing and sensitivity to initial conditions, can be connected with those of good ciphers, such as confusion and diffusion . There have been many image encryption algorithms based on chaotic maps like the Logistic map. Higher dimension chaos functions are far more secure from cryptanalytic attacks.

2 PRELIMINARIES AND DEFINITIONS

2.1 DYNAMICAL SYSTEMS

A dynamical system is in which a function describes the time dependence of a point in geometrical space.

The study of continuous-time dynamical systems is the study of differential equations; the study of discrete-time dynamical systems is the study of iterations of functions. The theory of dynamical systems is a very broad field closely intertwined with many other areas of mathematics. In particular, it has close relations with ergodic theory, probability theory, number theory, geometry, topology and mathematical physics.

Types of dynamical systems :

a.) Deterministic systems

b.) Non-Deterministic systems

A **deterministic system** is a system whose present state is in principle fully determined by the initial conditions.
It consists of a set of states, together with a rule that determines the present state in terms of past states.
No randomness is allowed in our definition of deterministic systems.

The systems studied in chaos theory are deterministic. If the initial state were known exactly, then the future state of such a system could theoretically be predicted. However, in practice, knowledge about the future state is limited by the precision with which the initial state can be measured, and chaotic systems are characterized by a strong dependence on the initial conditions. This sensitivity to initial conditions can be measured with Lyapunov exponents.

The dynamic system where the output cannot be predicted becauseThere are multiple possible outcomes for each input, or we can say It gives us different outputs every time we conclude it as a **Non-deterministic system**. Randomness is involved.

2.2 What is Chaos ?

By 'Chaos' we mean that the system obeys deterministic laws of evolution, but that the outcome is highly sensitive to small uncertainties in the specification of the initial state.

Among the study of different deterministic systems, Chaos theory is a branch of mathematics aimed at studying systems whose random states of disorder are governed by deterministic laws.Chaos theory is an interdisciplinary theory stating that, within the apparent randomness of chaotic complex systems, there are underlying patterns, constant feedback loops, repetition, self-similarity, fractals, and self-organization. The butterfly effect, an underlying principle of chaos, describes how a small change in one state of a deterministic nonlinear system can result in large differences to a later state (meaning that there is sensitive dependence on initial conditions)

It is not possible in practice to balance a ball on the peak of a mountain, even though the configuration of the ball perfectly balanced on the peak is a steady state. The problem is that the trajectory of any initial position of the ball near, but not exactly at, the steady state, will evolve away from the steady state. It is common to see behavior like this, in which unstable behavior is transient and gives way eventually to stable behavior in the long run. But there is no reason that an initial condition starting near a source is forced to end up attracted to a sink or periodic sink.

A chaotic orbit is one that forever continues to experience the unstable behavior that an orbit exhibits near a source, but that is not itself fixed or periodic. It never manages to find a sink to be attracted to. At any point of such an orbit, there are points arbitrarily near that will move away from the point during further iteration. This sustained irregularity is quantified by Lyapunov numbers and Lyapunov exponents.

Chaos is defined by a Lyapunov exponent greater than zero.

$$\lambda(x_0) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=0}^{n-1} \ln |f'(x_i)|$$

There are a number of characteristics one observes in a deterministically chaotic system:

- **Long term behavior is difficult or impossible to predict**: Even very accurate measurements of the current state of a chaotic system become useless indicators of where the system will be. One has to measure the system again to find out where it is.

- **Sensitive dependence on initial conditions** (a property noted by Poincare, Birkhoff, and even Turing): Starting from very close initial conditions a chaotic system very rapidly moves to different states.

- **Broadband frequency spectrum**: That is, the output from a chaotic system sounds "noisy" to the ear. Many frequencies are excited.

- **Exponential amplification of errors**: In any real world setting small amounts of external noise rapidly grow to control the system. If this noise is below measurement accuracy, so that an experimenter can't see or control the noise, then the system appears unpredictable. The microscopic "heat bath" is amplified to human scales.

- **Local instability versus global stability**: In order to have amplification of small errors and noise, the behavior must be locally unstable: over short times nearby states move away from each other. But for the system to consistently produce stable behavior, over long times the set of behaviors must fall back into itself. The tension of these two properties leads to very elegantly structured chaotic attractors.

2.3 Chaotic Maps

A chaotic map is a map (evolution function) that exhibits some sort of chaotic behavior. Maps may be parameterized by a discrete-time or continuous-time parameter. Discrete maps usually take the form of iterated functions. Chaotic maps often occur in the study of dynamical systems.

Chaotic maps often generate fractals. Although a fractal may be constructed by an iterative procedure, some fractals are studied in and of themselves, as sets rather than in terms of the map that generates them. This is often because there are several different iterative procedures to generate the same fractal.

An attractor is the value, or set of values, that the system settles toward over time.

A chaotic system has a strange attractor, around which the system oscillates forever, never repeating itself or settling into a steady state of behavior. It never hits the same point twice and its structure has a fractal form, meaning the same patterns exist at every scale no matter how much you zoom into it.

Types of Chaotic Maps :

1. One-dimensional maps

    - Logistic Map
    - Tent map
    - Skew-Tent map

2. Two-dimensional maps

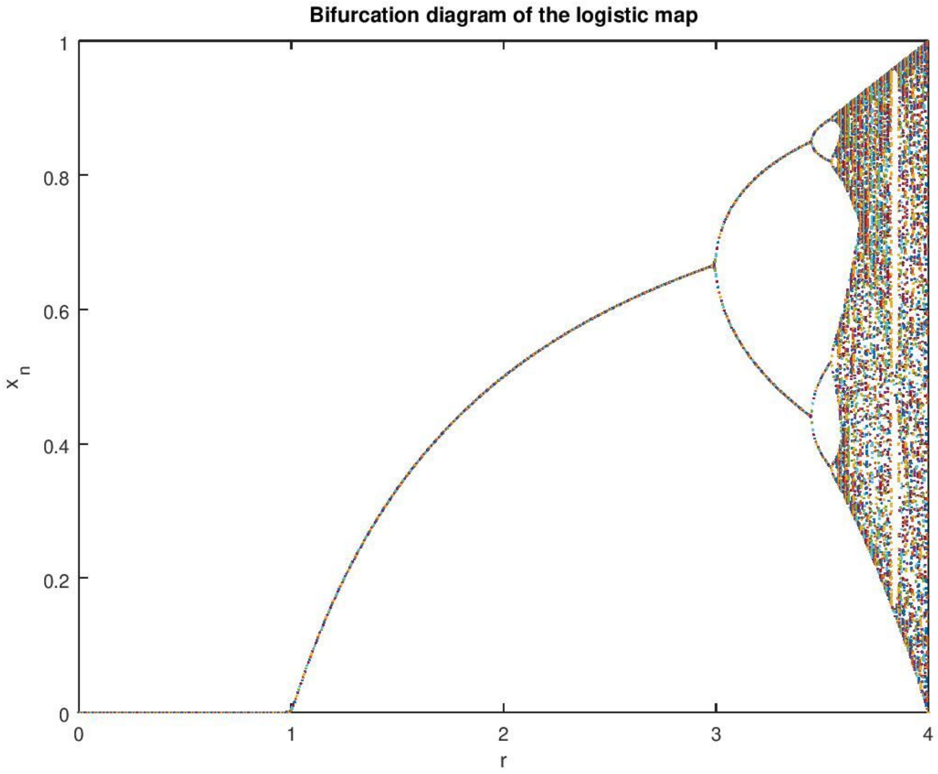
- Baker’s map
- Henon map
- Arnold's cat map

3. Three- dimensional maps

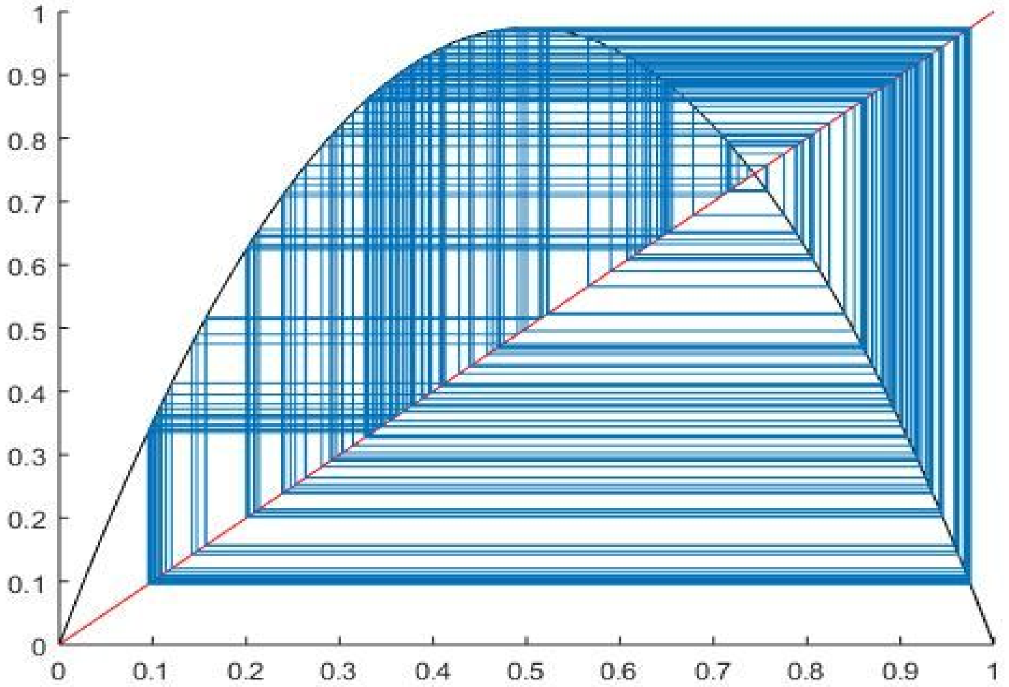
- Chebyshev map
- 3D logistic map

2.4 Visualization of Chaotic Maps

1. **Bifurcation Diagram:** It shows the values visited or approached asymptotically of a system as a function of bifurcation parameter in a system.



2. **Cobweb Plot:** It used to visualize iterated functions. A stable fixed point corresponds to an inward spiral, and unstable fixed points corresponds to an outward spiral. These spirals will center at a point where the diagonal y=x line crosses the function graph, this point is known as the fixed point.



3 REQUIREMENTS FOR IMAGE ENCRYPTION

The desired properties of an image encryption algorithm are:

- The image cannot be recovered easily if the key is not known.
- The image should be recovered fully, in its original form if the key is known.
- Decryption should be resistant to brute force attacks.
- If the key is known, the computational power required for image recovery should not be very high.

In order to use chaos theory efficiently in cryptography, the chaotic maps should be implemented such that the entropy generated by the map can produce required **confusion** and **diffusion**. Properties in chaotic systems and cryptographic primitives share unique characteristics that allow for the chaotic systems to be applied to cryptography. If chaotic parameters, as well as cryptographic can be mapped symmetrically or mapped to produce acceptable and functional outputs, it will make it next to impossible for an adversary to find the outputs without any knowledge of the initial values.

Since chaotic maps in a real life scenario require a set of numbers that are limited, they may, in fact, have no real purpose in a cryptosystem if the chaotic behaviour can be predicted. In numerous cases, chaos-based cryptography algorithms are proved unsecure. The main issue in many of the cryptanalysis algorithms is the inadequacy of chaotic maps implemented in the system.

With the emergence of chaos-based cryptography hundreds of new image encryption algorithms, all with the aim of improving the security of digital images were proposed. However, there were three main aspects of the design of an image encryption that was usually modified in different algorithms (chaotic map, application of the map and structure of algorithm). The initial and perhaps most crucial point was the chaotic map applied in the design of the algorithms.

The speed of the cryptosystem is always an important parameter in the evaluation of the efficiency of a cryptography algorithm, therefore the designers were initially interested in using simple chaotic maps such as tent map, and the logistic map. However, the new image encryption algorithms based on more sophisticated chaotic maps proved that application of chaotic map with higher dimension could improve the quality and security of cryptosystems.

Conventional cipher algorithms such as DES, IDEA, AES, 3DES etc. are not suitable for multimedia files due to public data capacity, strong pixel correlation and high redundancy which reduces the encryption performance.

Confusion: Confusion means that each binary digit of the cipher-text should depend on several parts of the key, obscuring the connections between the two.

Diffusion: Diffusion means that if we change a single bit of the plaintext, then (statistically) half of the bits in cipher-text should change and vice-versa.

4. WHY CHAOTIC MAPS FOR IMAGE ENCRYPTION?

Designing an encryption method uses both of the principles of confusion and diffusion.

Confusion means that the process drastically changes data from the input to the output, for example, by translating the data through a non-linear table created from the key. We have lots of ways to reverse linear calculations, so the more non-linear it is the more analysis tools it breaks.

Diffusion means that changing a single character of the input will change many characters of the output. Done well, every part of the input affects every part of the output, making analysis much harder. No diffusion process is perfect: it always lets through some patterns. Good diffusion scatters those patterns widely through the output, and if there are several patterns making it through they scramble each other. This makes patterns vastly harder to spot, and vastly increases the amount of data to analyse to break the cipher.

The long term behaviour of a **chaotic map** changes drastically with minor changes in the initial value, which gives us our ‘first key’. We start making modifications in the alignment of pixels, or pixel intensities by performing arithmetic operations on them, which in turn are functions of X_n, where n is the key for our algorithm.

We can use multidimensional chaotic maps and perform a variety of operations, which allows us to encrypt our image with many keys at each step.

Thus, it makes decryption of image almost impossible if the initial key values are unknown.

5. OUR IMPLEMENTATION OF IMAGE ENCRYPTION USING CHAOTIC MAPS

5.1 3D Logistic Map

There are 4 steps involved in the encryption process:

1. Conversion of RGB image to an 8-bit grayscale image.

2. Converting grayscale image into a 3D matrix of 0's and 1's where each binary stream in the position (i,j) is the binary representation of intensity of pixel at that position.

3. Generating a new 3D position matrix using chaotic equations with unique values which correspond to new positions of blocks after shuffling.

4. New image is encrypted image.

Repeating the steps in reverse order will give the decrypted image.

The 3D Logistic Map is given by the formulae:

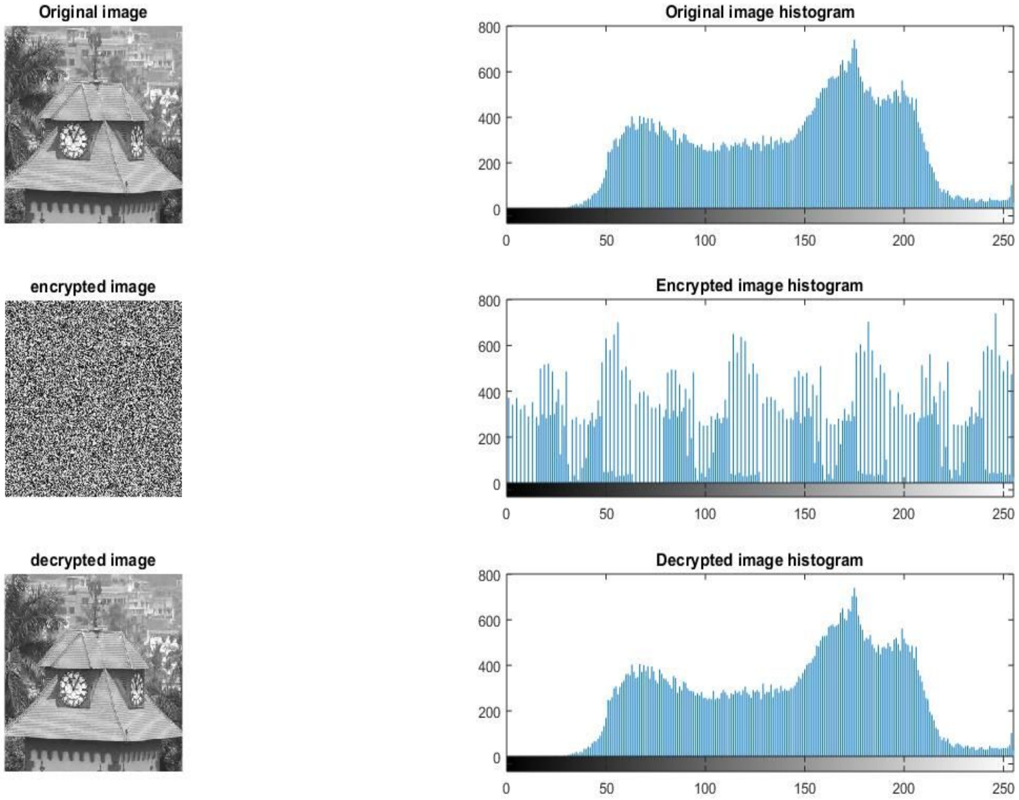
$$X_{n+1} = \gamma X_n(1-X_n) + \beta Y_n^2 X_n + \alpha Z_n^3$$

$$Y_{n+1} = \gamma Y_n(1-Y_n) + \beta Z_n^2 Y_n + \alpha X_n^3$$

$$Z_{n+1} = \gamma Z_n(1-Z_n) + \beta X_n^2 Z_n + \alpha Y_n^2$$

The 3D logistic map exhibits chaotic behaviour for $3.53 < \gamma < 3.81$, $0 < \beta < 0.022$, $0 < \alpha < 0.015$ and the initial value of x, y, z can be any value between 0 and 1. We take the initial value of $x_0 = 0.235$, $y_0 = 0.37$, $z_0 = 0.3735$, which serve as our keys in the encryption.

Results



5.2 Combination of 2D and 1D Logistic Map

There are 5 steps to complete the overall encryption process:

1. 3D Chaos Generation
2. Row Rotation
3. Column Rotation
4. XOR Rotation

The 2D Logistic Map is given by the formulae:

$x_{i+1} = r(3y_i + 1)x_i(1 - x_i)$

$y_{i+1} = r(3x_{i+1} + 1)y_i(1 - y_i)$

The 2D Logistic Map exhibits chaotic behaviour for $r > 3.9$ and the initial value of x, y can be any value between 0 and 1.

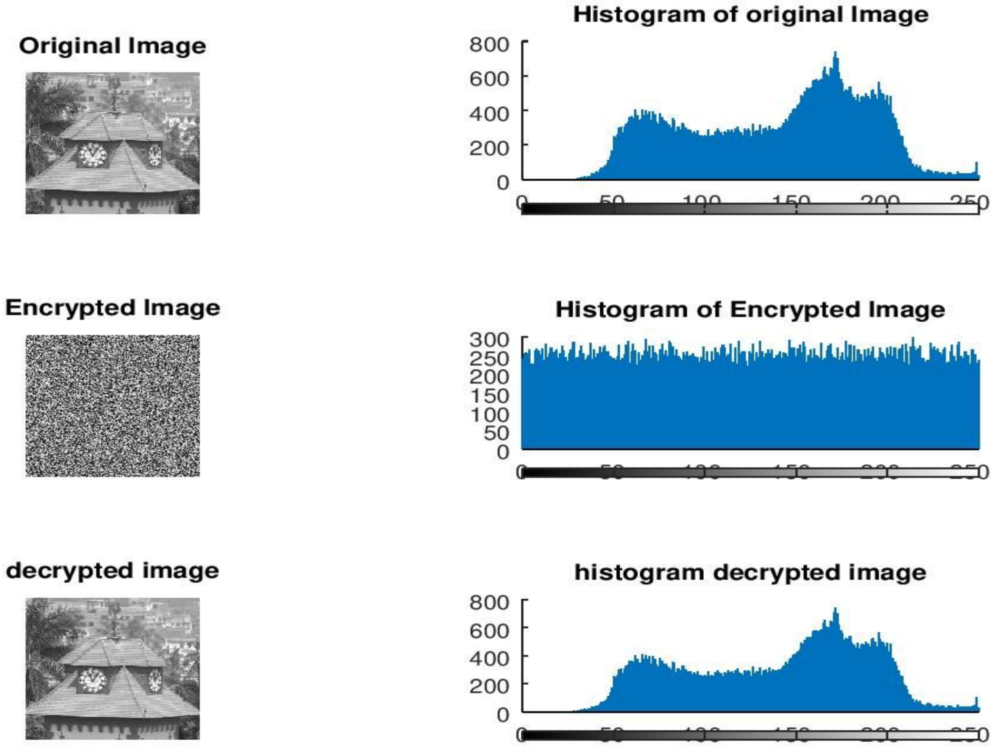
The initial values which serve as keys are $x_0 = 0.235$, $y_0 = 0.35$.

The 1D Logistic Map is given by the formulae:

$X_{n+1} = \mu X_n(1-X_n)$

From the bifurcation diagram of this map, for $0 < X_n < 1$ and $\mu = 4$ is the condition to make this equation chaotic.

Results

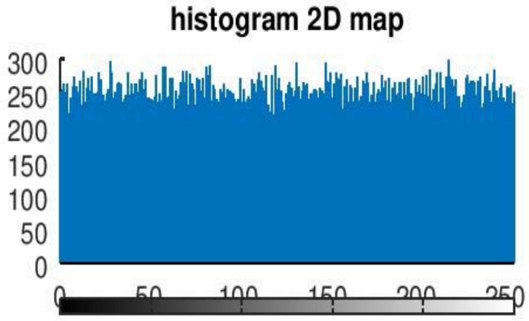

Original Image
Histogram of original Image
800
600
400
200
0
0
50
100
150
200
250
Encrypted Image
Histogram of Encrypted Image
300
250
200
150
100
50
0
0
50
100
150
200
250
decrypted image
histogram decrypted image
800
600
400
200
0
0
50
100
150
200
250

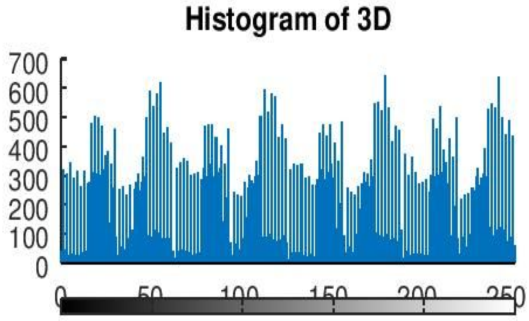
6. COMPARISON OF THE SECURITY PARAMETERS OF THE TWO METHODS

6.1. **Statistical Analysis**:

Due to high correlation value between adjacent pixels statistical attacks are so serious for image encryption.Statistical analysis performed to demonstrate it's superior confuse and diffuse properties which strongly resist statistical attacks.

Encrypted image histogram we can see that the entire pixel values are uniformly distributed which doesn't contain any information to the intruder.





We see that pixel values are more uniformly distributed in the case where a combination of 2D and 1D chaotic logistic map was used.

Thus, from the statistical analysis point of view, it provides more security.

6.2. Correlation Coefficient Analysis

In order to evaluate the encryption quality of the proposed encryption algorithm, the correlation coefficient is used to calculate the correlation coefficients between two vertically, horizontally adjacent pixels of an encrypted image, the following equation is used:

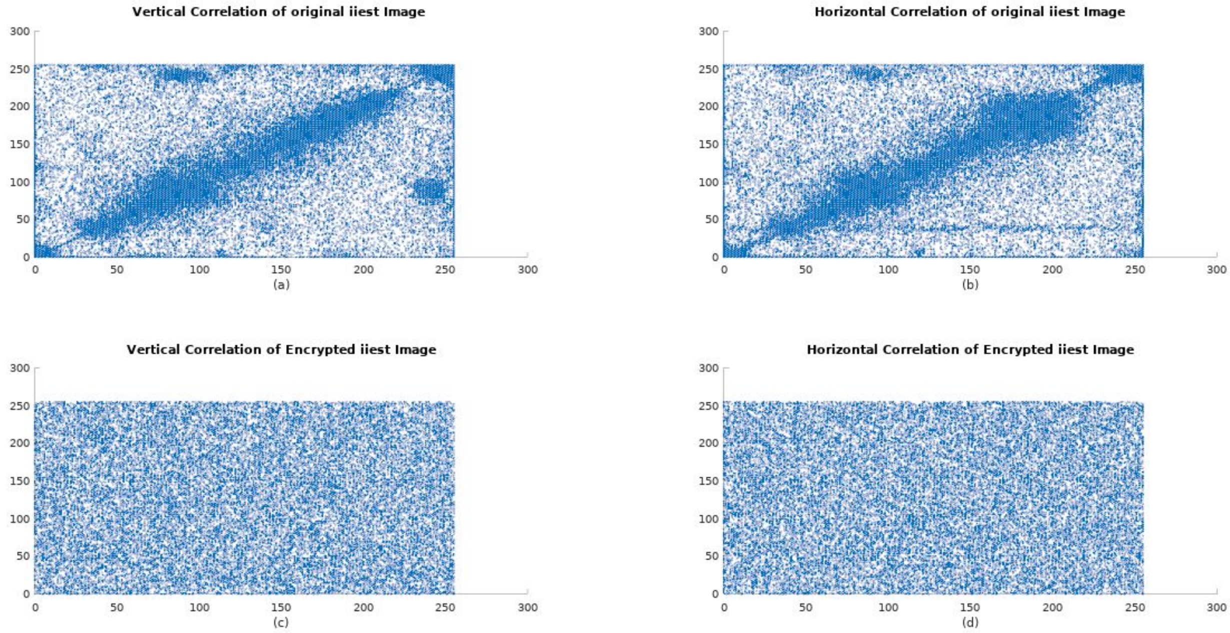
$$\gamma = \frac{Cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$D(x) = \frac{1}{M}\sum_{i=1}^{M}(x-\overline{x})^2$$

$$Con(x,y) = \frac{1}{M}\sum_{i=1}^{M}(x-\overline{x})(y-\overline{y})$$

The original image is highly correlated to the adjacent pixel and values are distributed near the center but after encryption pixel values are uniformly distributed as a result lower the correlation value.

Result for combination of 2D and 1D map:



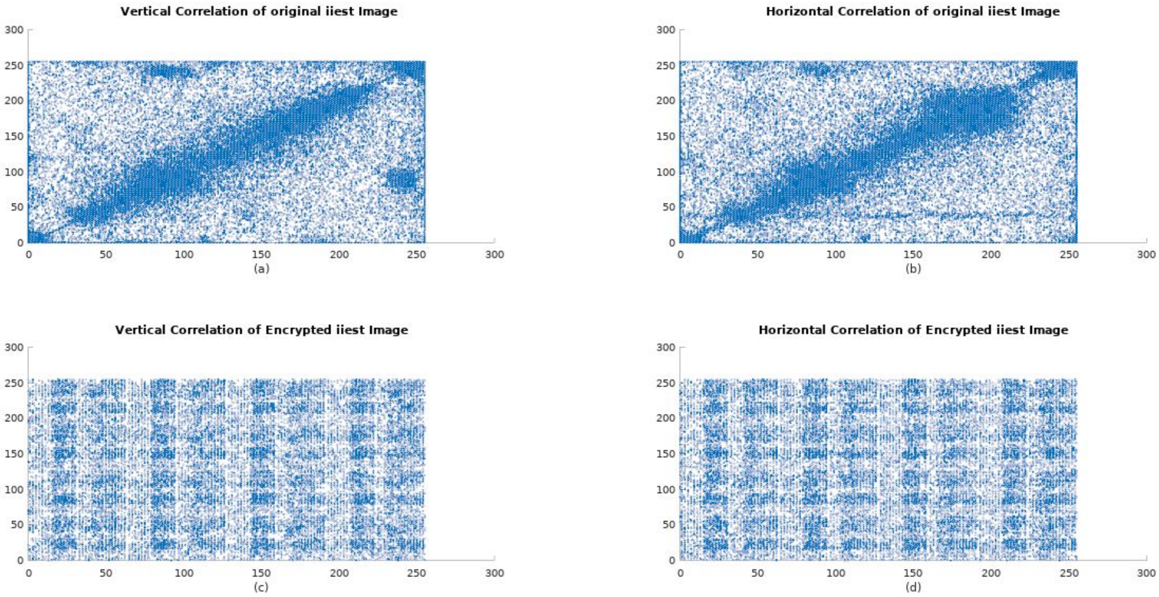
Vertical Correlation of original iiest Image

Horizontal Correlation of original iiest Image

Vertical Correlation of Encrypted iiest Image

Horizontal Correlation of Encrypted iiest Image

Results for 3D logistic map :



(a)

(b)

(c)

(d)

7. CONCLUSION

We implemented a simple 3D Chaotic Map, and a combination of 2D and 1D Chaotic Map along with a combination of position permutation and value transformation techniques.

A detailed Statistical analysis on both the methods has been done.We have discovered that the algorithms are highly sensitive to initial conditions and can be very strong against brute force attacks.

From our analysis we can also conclude that a combination of maps can be used for better security reasons.

Finally after tests like correlation coefficient analysis, we show that our algorithms provide good diffusion which scatters any patterns widely through the output, which makes patterns harder to spot and resistible against different attacks.

Having a high throughput, the algorithms are ready to be applied in fast real time encryption applications and suitable for practical use in the secure transmission of multimedia information over the Web.

8. REFERENCES

1. https://medium.com/@fabiograetz/the-stunning-beauty-of-chaos-theory-fd0e1597d68a
2. https://www.ibiblio.org/e-notes/Chaos/contents.html
3. https://www.wikipedia.org/
4. https://www.researchgate.net/publication/278680089_Comparative_Analysis_of_Color_Image_Encryption_Using_2D_Chaotic_Maps
5. https://www.sciencedirect.com/science/article/pii/S0143816614003273
6. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.88.5203&rep=rep1&type=pdf