**IMAGE ENCRYPTION BY DUAL CONFUSION AND DIFFUSION USING MULTIPLE CHAOTIC MAPS**

*Report submitted to the SASTRA Deemed to be University*

*as the requirement for the course*

**ECE 300: MINI PROJECT**

*Submitted by*

**ANAND RAJ**

**(Reg. No.: 123004020, B. Tech ECE)**

**KOTHURU BHANU TEJA**

**(Reg. No.: 123004121, B. Tech ECE)**

**VARDDHAMAANAN JAIN**

**(Reg. No.: 123004267, B. Tech ECE)**

**JUNE2022**

****

**SCHOOL OF ELECTRICAL AND ELECTRONICS ENGINEERING THANJAVUR, TAMIL NADU, INDIA – 613 401**



**SCHOOL OF ELECTRICAL & ELECTRONICS ENGINEERING**

**THANJAVUR – 613 401**

**Bonafide Certificate**

This is to certify that the report titled “**Image Encryption by Dual Confusion and Diffusion Using Multiple Chaotic Maps**” submitted as a requirement for the course, **ECE 300:** **MINIPROJECT** for B.Tech ECE, semester VI is a bonafide record of the work done by **Mr. Anand Raj (Reg. No.123004020, B. Tech ECE), Mr. Kothuru Bhanu Teja (Reg. No.123004121, B. Tech ECE) and Mr. U. Varddhamaanan Jain (Reg. No.123004267, B. Tech ECE)** during the academic year 2021-22, in the **School of Electrical & Electronics Engineering**, under my supervision. This thesis has not formed the basis for the award of any degree, diploma, associate-ship, fellowship or other similar title to any candidate of any University.

### Signature of Project Supervisor :

### Name with Affiliation : Ms. R. Sumathi, Asst. Professor, SEEE/ECE

### Date : 25/06/2022

### Mini Project *Viva voce* held on \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Examiner 1 Examiner 2**



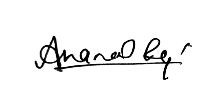
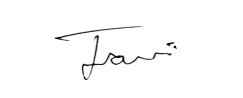
**SCHOOL OF ELECTRICAL & ELECTRONICS ENGINEERING**

**THANJAVUR – 613 401**

**Declaration**

We declare that the report titled “**Image Encryption by Dual Confusion and Diffusion Using Multiple Chaotic Maps**” submitted by us is an original work done by us under the guidance of **Ms. R. Sumathi, Assistant Professor, School of Electrical and Electronics Engineering, SASTRA Deemed to be University** during the sixth semester of the academic year 2021-22, in the **School of Electrical and Electronics Engineering**. The work is original and wherever we have used materials from other sources, we have given due credit and cited them in the text of the thesis. This thesis has not formed the basis for the award of any degree, diploma, associate-ship, fellowship or other similar title to any candidate of any University.

**Name of the candidate(s) Signature of the candidate(s)**

1. Anand Raj (123004020) 
2. Kothuru Bhanu Teja (123004121) C:\Users\Vardhu\Desktop\Mini Project\IMG-20220623-WA0024.jpg
3. U. Varddhamaanan Jain (123004267) 

**Date:** 25/06/2022

**Acknowledgements**

First and foremost, we thank the almighty for helping me to gain support in all forms to finish our mini project successfully. We express our sincere thanks to **Dr. S. Vaidhyasubramaniam, Vice Chancellor** and **Dr. R. Chandra Mouli, Registrar,** SASTRA UNIVERSITY, for permitting me to do this Mini Project as a part of our curriculum.

We would also like to thank **Dr. K. Thenmozhi, Dean (SEEE), Dr. Sridhar K, Associate Dean (ECE)** for their support provided during my course span in SASTRA Deemed University.

We are fortunate to have **Mrs. R. Sumathi**, **Associate Professor** as our project guide. Her valuable assistance and supervision guided us towards the successful completion of our Mini project. And also, we thank all the technical and non-technical staff of School of Electrical and Electronics Engineering Department.

Finally, we thank our parents and our friends for their constant encouragement without which this project would not have been possible.

**Abstract**

**Project Title:** Image Encryption by Dual Confusion and Diffusion Using Multiple Chaotic Maps

In the age of internet and social media, images have become the major part of the information traffic other than video streaming. Many confidential information in the form images go through the internet every day, so the need to secure them properly has become the need of the hour.

This projects proposes a new dual confusion and diffusion method for encrypting grey images with the use of multiple chaotic maps like logistic map and tent map and Lorenz attractor, to be implemented on python programming. Also, standard encryption analysis would be done to evaluate the effectiveness of the project.

**Key Words:** Image Encryption, Confusion, Diffusion, Chaotic maps, Logistic map, Tent map, Lorenz attractor

**Table of Contents**

**Title Page No.**

[Bona-fide Certificate](#_TOC_250005)  ii

[Declaration](#_TOC_250004)  iii

[Acknowledgements](#_TOC_250003)  iv

[Abstract](#_TOC_250002)  v

[List of Figures vii](#_TOC_250001)

[List of Tables](#_TOC_250000)  viii

Abbreviations ix

Notations ix

1. Introduction 1
2. Literature Survey 2
3. Proposed Methodology 4

3.1 Objective 4

3.2 Preliminaries 4

3.3 Experimental work 6

3.3.1 Encryption 6

3.3.2 Key Generation (Chaotic Maps) 8

3.3.3 Decryption 9

3.3.4 Analysis 10

1. Results and Discussion 12

4.1 Encryption Results 13

4.2 Decryption Results 14

4.3 Analysis and Comparisons 15

5. Conclusions and Future Scope 18

6. References 19

**List of Figures**

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Title** | **Page No.** |
| 3.1 | Fundamental flow schematic of the encryption process | 6 |
| 3.2 | Block diagram of the encryption process | 6 |
| 3.3 | Heirarchy of the key generation module | 8 |
| 3.4 | Block diagram showing the decryption process | 9 |
| 3.5 | Block diagram of the analysis process | 10 |
| 4.1 | Original Image- “Cameraman” 512x512 Greyscale image | 12 |
| 4.2 | Output Image of 1st Confusion | 13 |
| 4.3 | Output Image of 1st Diffusion | 13 |
| 4.4 | Output Image of 2nd Confusion | 13 |
| 4.5 | Final encrypted image | 13 |
| 4.6 | Final encrypted image | 14 |
| 4.7 | Output Image of reversal of 2nd Confusion | 14 |
| 4.8 | Output Image of reversal of 1st Diffusion | 14 |
| 4.9 | Output Image of reversal of 1st Confusion | 14 |
| 4.10 | Final Decrypted Image | 15 |
| 4.11 | Histogram Plot of the original image | 15 |
| 4.12 | Histogram Plot after 1st confusion and diffusion process | 16 |
| 4.13 | Histogram Plot after 2nd confusion and diffusion process | 16 |

**List of Tables**

|  |  |  |
| --- | --- | --- |
| **Table No.** | **Table name** | **Page No.** |
| 4.1 | Implementation specifications | 12 |
| 4.2 | UACI and NPCR values obtained for different test images | 17 |
| 4.3 | UACI and NPCR value Comparison with other methods | 17 |

**Abbreviations**

1. AES - Advanced Encryption Standards
2. DES - Data Encryption Standards
3. XOR - Exclusive OR
4. UACI - Unified Average Changing Intensity
5. NPCR - Number of Pixel Change Rate

**Notations**

**English Symbols:**

1. X - Lorenz system quantity 1
2. Y - Lorenz system quantity 2
3. Z - Lorenz system quantity 3
4. r - Lorenz system constant 2
5. t - Lorenz system constant 3
6. xn  - Nth iteration output of chaotic map

**Greek Symbols:**

1. α – Logistic map Control parameter
2. μ - Tent map Control parameter
3. σ - Lorenz system constant 1

**CHAPTER 1**

**INTRODUCTION**

In this technological world, data transfer over the internet has been increasing in rapid pace in the recent years. This has been the inspiration for a number of researchers to develop encryption techniques to secure digital media, particularly photographs as they comprise the majority part of the traffic of transmitting data.

The need for encryption has never been higher as vast availability of computer and internet access has made data more vulnerable than ever. Similarly, encryption processes keep getting cracked down regularly, so the demand for a new or improved methodology has never decreased.

In image encryption the image is scrambled to a form where it is not possible to be read and interpreted. Standard techniques like AES and DES don’t hold good in this case. Multiple stream cipher techniques get applied for this purpose.

Chaotic maps are known to show true randomness, which makes them suitable for key generation process. The randomness of the keyset directly shows the level of security of the system, so with the use of chaotic maps a very strong encryption algorithm can be build.

**CHAPTER 2**

**LITERATURE SURVEY**

1. **Chaos based duo confusion duo diffusion for colour images**

**Done by:** A. Sridevi & R. Sivaraman & Varun Balasubramaniam & Sreenithi & J. Siva & V. Thanikaiselvan & Amirtharajan Rengarajan.

Earlier image encryption techniques are likely to get attacked easily by hackers. So, Chaos-based encryption methods, which stand for randomness, are seen as more appropriate.

In RGB planes, colour image split and to achieve encryption duo confusion and duo diffusion through chaotic have been implemented.

In this proposed method, the RGB planes of the colour image were split and duo confusion and duo diffusion process are performed with the use of chaotic maps for key generation and the planes were put back together to get the encrypted image.

Then analysis metrics showed that the process was highly secure and random.

1. **Image Encryption Using Chaotic Maps: A Survey**

**Done by:** Priya Sankalp, Dr P. A. Vijaya

Data sharing despite inadequate security, has been overcome by chaotic systems. Initial conditions and control parameters affects the chaotic systems greatly which make them appropriate for image encryption.

1. **Image Encryption Based On Diffusion And Multiple Chaotic Maps**

**Done by:** [G.A.Sathishkumar](https://arxiv.org/search/cs?searchtype=author&query=G.A.Sathishkumar), [Dr.K.Bhoopathy bagan](https://arxiv.org/search/cs?searchtype=author&query=bagan%2C+D), [Dr.N.Sriraam](https://arxiv.org/search/cs?searchtype=author&query=Dr.N.Sriraam)

This paper showsnew encryption technique using multiple chaotic based circular mapping.

Using chaotic logistic maps, the first step is to get a pair of sub keys. Second, a logistic map sub keys are used to encrypt the image, and this transformation causes the diffusion process. Third, four separate chaotic maps are being used to create sub keys.A binary sequence is created based on the key to control the encryption algorithm.The receiver then uses the same sub keys to decrypt the images that were encrypted.

1. **UACI and NPCR randomness test for image encryption**

**Done by:** [Yue Wu](https://www.researchgate.net/profile/Yue-Wu-86?_sg%5B0%5D=3euVJnMi3QwgyXFrmj2JjA09zksTPLfl5tjS-QQIRGBssyeEn2Dz8_FWHbgtrO0MfBzACIc.17wjS82i5OllMjkaJ-RMXxkeOVl5KljBcscYq5O7PiLiLLmAJ8fn3ozUVQAjh4Yt5X-pJs8P249zThXfIdvDSQ&_sg%5B1%5D=TBllwzcPdJLGf1cxO9b98LrBOnXvmrkaUJI8Npn0faCXMprlMdQIos-Rk7W3HKinl2ke5Zs.YNqovOfsgJ0ZV4u0AlZjIktHOaj1H7Hm0Jx23U58nqbQU8HEJlyvOnRwJvr7hitMJFNtneQpYnThlvjTr5v01A)

 To evaluate the strength of image encryption algorithms, the unified averaged changed intensity (UACI) and the number of changing pixel rate (NPCR) are two most common analysis used. High NPCR/UACI score conveys very less risk to attacks.

Generating a mathematical model for ideally encrypted images, from which one can extract the predictions of the NPCR and UACI. These theoretical values are used to form statistical hypothesis of UACI and NPCR tests.

Numerous existing image encryption techniques are actually not as effective as they are suggested to be, as we compare experimental results with the obtained NPCR and UACI randomness tests.

1. **Performance analysis of encryption algorithms**

**Done by:** [Madhumita Panda](https://ieeexplore.ieee.org/author/37085496805)

This paper suggests the performance of different cryptographic algorithms; among them it will find out best method for our future use.

Evaluation done on both symmetric (DES, AES) as well as asymmetric (RSA) cryptographic algorithms and comparison has been conducted using evaluation parameter like encryption time & decryption time, and throughput.

The survey leads to the finding that traditional encryption algorithm do not give the desirable results in the case of images. Confusion and Diffusion with really random key set make a really strong image encryption system.

**Chapter 3**

**PROPOSED METHODOLOGY**

**3.1 OBJECTIVE**

The main objective of this project is to develop an image encryption algorithm by double confusion and diffusion with use of chaotic maps like Tent map, Logistic map and Lorenz attractor for key generation. The algorithm is intended to be a viable commercial option providing confidentiality in required fields.

**3.2 PRELIMINARIES**

**Confusion:**

It is a transpositioning process where the pixels are shuffled to distort the image from its original form. Each and every pixel of the original image is moved to a different position to create a intermediate encrypted image.

**Diffusion:**

It is the process of changing the pixel intensity value usually by performing XOR operation with another set of values. It increases redundancy in the output resulting in reducing the relation between the original and the encrypted image.

**Chaotic Maps:**

Chaotic maps are dynamical systems that show really random behaviour. These chaotic systems are very sensitive to initial conditions and control parameters which make them suitable for key generation, as for key generation the more randomness increases the level of security.

**Lorenz attractor:**

The Lorenz system, ﬁrst studied by Edward Lorenz around 1960 is a system of 3 ordinary differential equations that are non-linear.

The butterfly effect is real world application of the Lorenz attractor. The bifurcation of Lorenz system is very strong making it a preferable for key generation.

**Logistic map:**

It is very simple chaotic map that has been studied for its cryptographic applications. Logistic map is a non-linear quadratic equation that shows chaotic behavior. It expressed as:

Logistic map has been historically important for its simplicity and serving as the face of chaotic behavior. Its popularly used to calculate population dynamics.

**Tent map:**

Tent map which is mostly used for true random number generation behaves randomly as the value of μ approaches the upper limit of 2. For every value in the range, 0 ≤ μ ≤ 2, random values are generated within the range 0 ≤ x ≤ 1. It is expressed as:

**3.3 Experimental Work**

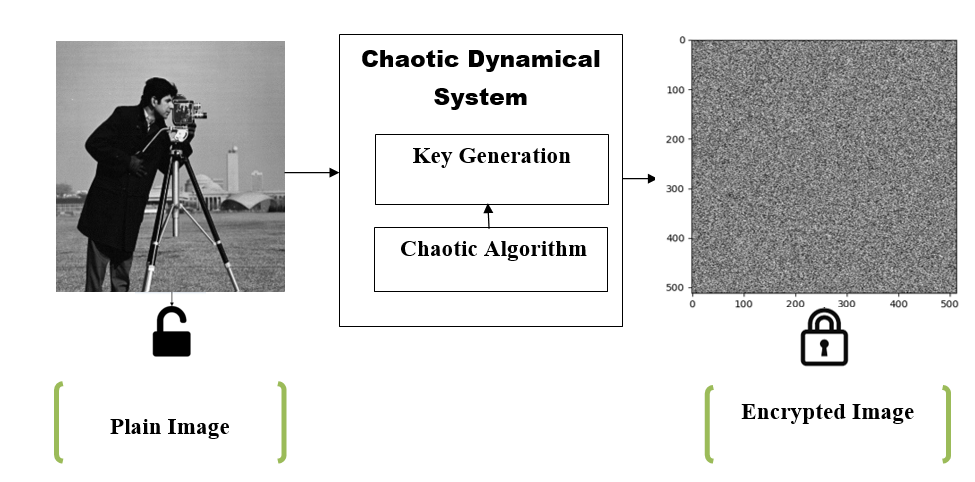
****

Fig.3.1: Fundamental flow schematic of the encryption process

**3.3.1 Encryption:**

Fig 3.2 Block diagram of the encryption process

The encryption process of this proposed method takes happens in 4 steps:

1. 1st Confusion- In this stage the original 512x512 grayscale image is passed through a confusion process where the pixels of the images get shuffled. For this process we generate key using Lorenz attractor, the x and y parameters returned from the Lorenz key module are used as the new coordinate for the pixels of the original image.
2. 1st Diffusion- In this stage the output image of the previous stage is passed through a diffusion process where the pixel intensity values get changes by XOR operation. For this process we generate key using Logistic map, the value returned from the Logistic key module is used as the value with which the pixel intensity values get XORed.
3. 2nd Confusion- In this stage output image of the previous stage passed through a confusion process where the pixels of the images get shuffled. For this process we generate key using Lorenz attractor, the x and y parameters returned from the Lorenz key module are used as the new coordinate for the pixels of the intermediate encrypted image.
4. 2nd Diffusion- In this stage the output image of the previous stage is passed through a diffusion process where the pixel intensity values get changes by XOR operation. For this process we generate key using Tent map, the value returned from the Tent key module is used as the value with which the pixel intensity values get XORed.

By the end of this process the fully encrypted image is obtained.

**3.3.2Key Generation (Chaotic Maps):**

Fig 3.3 Heirarchy of the key generation module

The key generation module returns the key set required fo reach and every step of of the process using the said chaotic maps.

The 3 dimensional lorenz attractor is used to make 2 dimensional key for the confusion processes while Tent and Logistic offer the keys for the diffusion process which is XORed with the pixel intensity values

**3.3.3 Decryption:**

Fig 3.4 Block diagram showing the decryption process

In the decryption process the encryption process is repeated in the reverse manner using the same keys to get the original image back.

The encrypted image is first passed through the 2nd diffusion process with the key generated from the tent map, which is then passed into the 2nd confusion iteration using Lorenz attractor as the key generator.

Again the intermediate image is sent through the diffusion and confusion stages that used the logistic map and the Lorenz attractor for generating the key.

As a result of this process we get back the original image as it was sent through for encryption process.

**3.3.4 Analysis:**

Fig 3.5 Block diagram explaining the analysis process

**UACI (Unified Average Changing Intensity):** It measures the average intensity of differences between the plain image and ciphered image. It’s ideal value is considered to be 33.4. But anything above 30 is considered to be very respectable

**NPCR (Number of Pixel Change Rate):** It measures the change rate of the number of pixels of the cipher image when only one pixel of the plain image is modified. It’s ideal value is considered to be 99.6

From our best knowledge, NPCR and UACI were first shown in 2004, by Yaobin Mao and Guanrong chen since then both NPCR and UACI became widely used security analysis process in image encryption for differential attacks

These methods are used to find the strength of encryption algorithms of an image to find whether they can withstand various types of differential attacks. Based on the NPCR and UACI, higher the value higher is the resistance to differential attacks.

**Histogram Analysis:** Histogram is nothing but graphical representation of tonal distribution in a digital image. Histogram is one of the simplest but an effective way of comparing 2 images. When encryption is done for an image the histograms in normal image and the encrypted image are completely different and after decryption number of histograms in decrypted image must be equal to the normal image used. By this histogram analysis we can find the difference between an encrypted image and a normal image.

This analysis is one of the straight-forward analysis method for illustrating the encryption quality. Histogram analysis is used to find the whether the image can resist the statistical attacks so it analysis the encrypted image and it shows how the quality of encryption is done in the process.

**Algorithm complexity:** Its nothing but measure of how many iterations are carried out in the process in specific amount of time.

**CHAPTER 4**

**RESULTS AND DISCUSSION**

|  |  |
| --- | --- |
| Operating System | Windows 10 |
| Programming Language | Python v3.9 (64 bits) |
| IDE | Visual Studio Code v1.68 |
| CPU | Intel Core i5 at 3.1 GHz |

Table 4.1 Implementation specifications



Fig 4.1: Original Image- “Cameraman” 512x512 Greyscale image

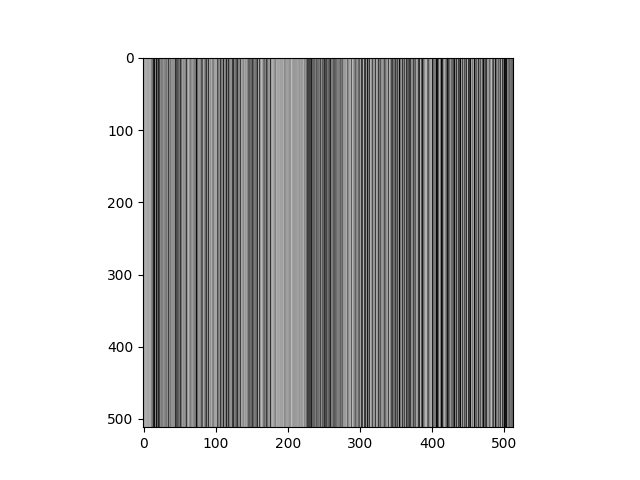
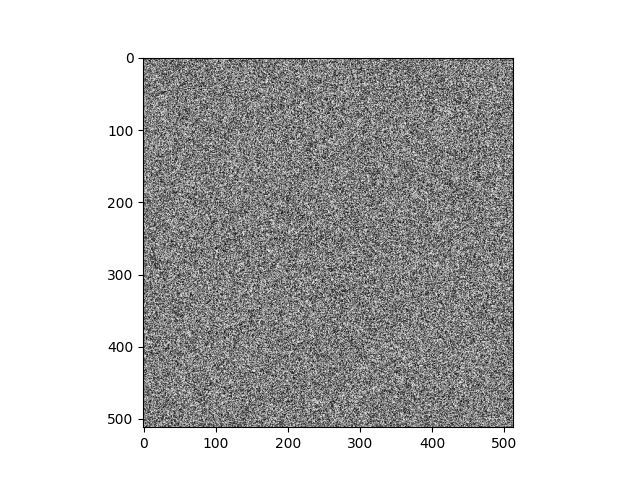
**4.1.1 Encryption Output:**

Fig 4.2: Output Image of 1st Confusion Fig 4.3: Output Image of 1st Diffusion

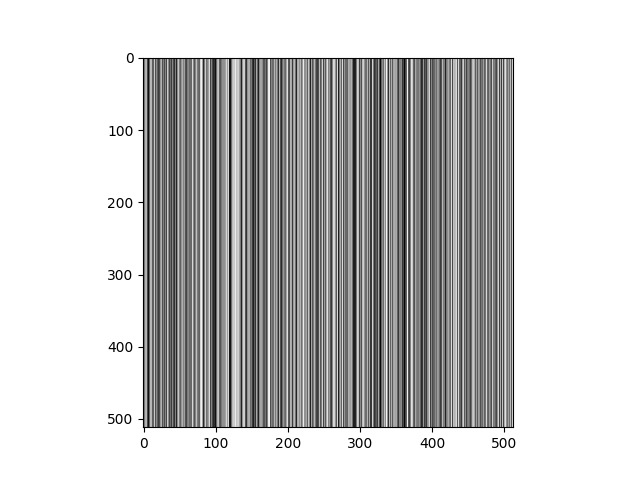
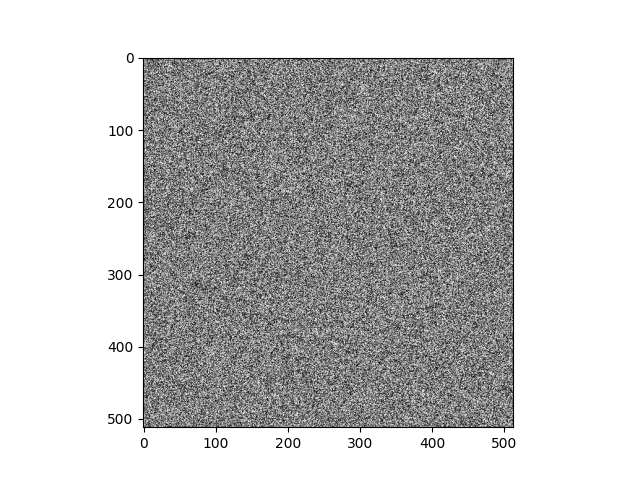
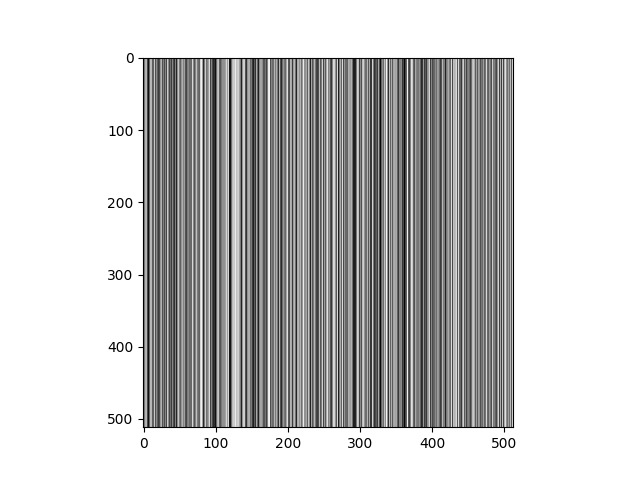
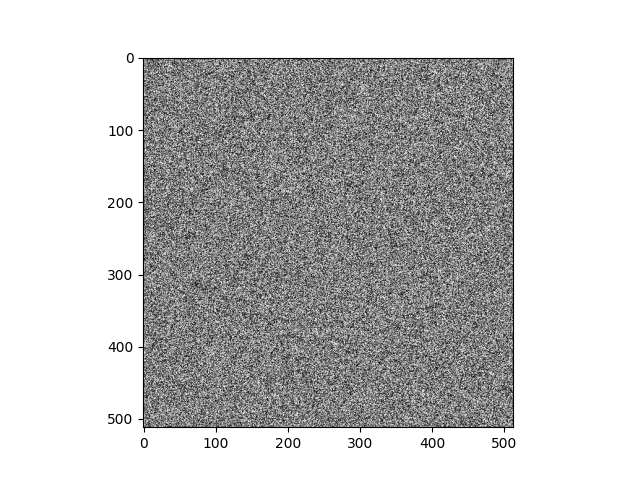
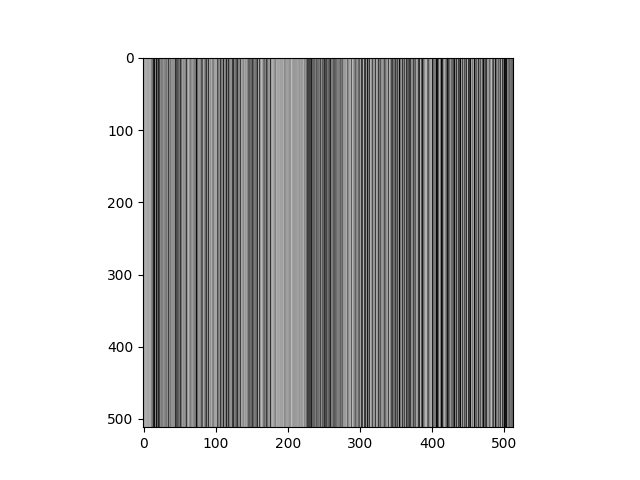


Fig 4.4: Output Image of 2nd Confusion Fig 4.5: Final encrypted image

**4.1.2 Decryption Output:**

We retrieve back the original form of the image from the encrypted form to make it readable again, for that we have to go through the entire encryption process in the reverse manner.

****Fig 4.6 Final encrypted image Fig 4.7 Output of the reversal 2nd confusion

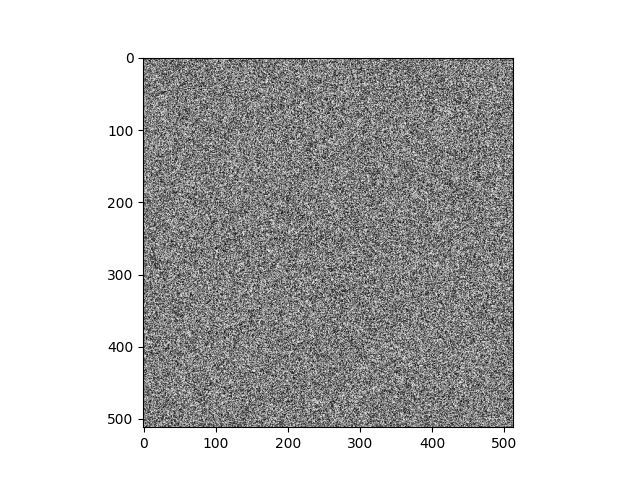
****

Fig 4.8 Output of reversal of 1st diffusion Fig4.9 Output of reversal of 1st confusion

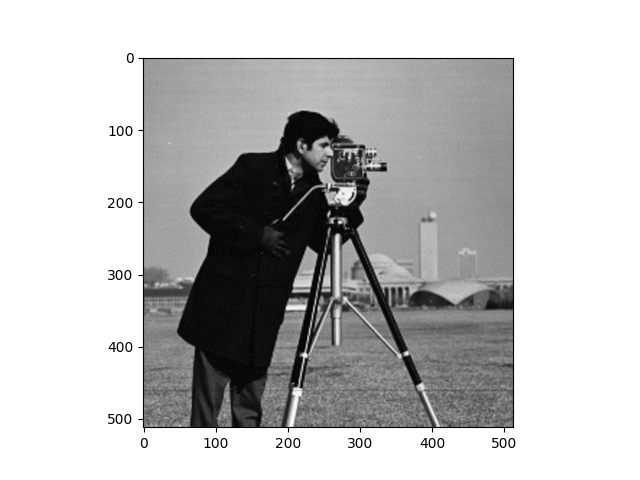


Fig 4.10: Final Decrypted Image

**5.2 Analysis and Comparison**

* **Histogram Analysis:**

Histogram shows the number pixels for each pixel intensity values.

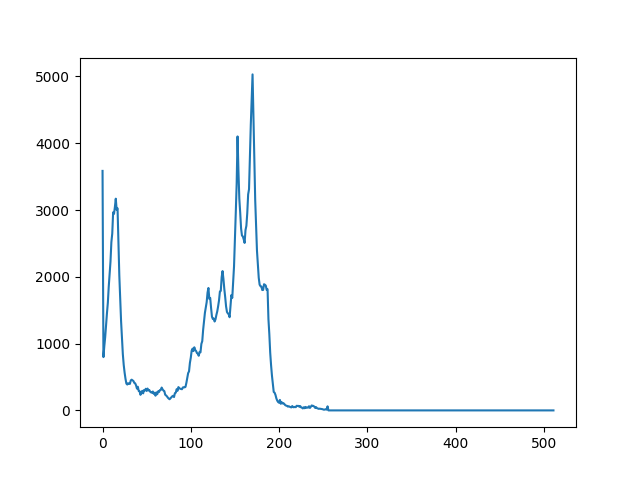


Fig. 4.11: Histogram Plot of original image

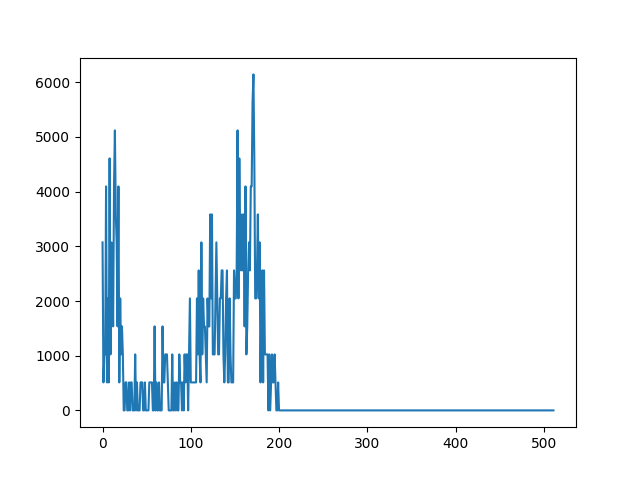


Fig. 4.12: Histogram Plot after 1st confusion and diffusion process

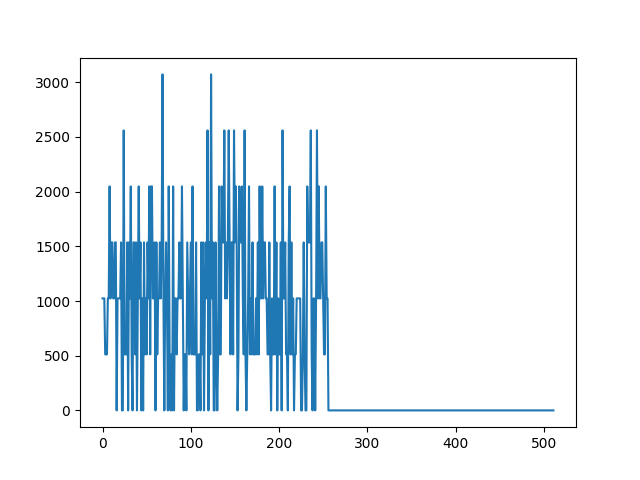
****

Fig. 4.13: Histogram Plot after 2nd confusion and diffusion process

As we can see the intensity of lot of pixels changes after multiple stages of encryption, this shows that the encryption process is scrambling the original image to an unreadable form.

* **Algorithm Complexity:** The code runs 4 encryption and 4 decryption loops each of order 512x512, this increases the complexity of the process making in unbreakable.

|  |  |  |
| --- | --- | --- |
| **Image** | **UACI value** | **NPCR value** |
| **Cameraman** | 31.2271 | 99.7167 |
| **Girl** | 27.8899 | 90.0596 |
| **Big house** | 31.8569 | 90.0148 |

Table 4.2 UACI and NPCR values obtained for different test images

|  |  |  |  |
| --- | --- | --- | --- |
| **S.no** | **Algorithm** | **UACI** | **NPCR** |
| 1 | Proposed method | 31.2271 | 99.7167 |
| 2 | DNA encoding | 33.33 | 99.61 |
| 3 | DNA coding and hyper chaotic system | 33.46 | 99.60 |
| 4 | Bit Shuffled ITM | 33.49 | 99.61 |

Table 4.3 UACI and NPCR value Comparison with other methods

**CHAPTER 5**

**CONCLUSION AND FUTURE SCOPE**

**5.1 CONCLUSION**

The proposed image encryption algorithm was simulated in python and the results were observed. This method is effective and can be accounted to provide better security than the existing methods. From the analysis done we can learn that this method can be used for commercial purposes too. This project also shows the use chaotic maps concept in an effective way. It was also observed that multiple stage confusion and diffusion tend to be a viable option for encrypting an image than a single stage process.

**5.2 FUTURE SCOPE**

Further analysis can be done to check the algorithm in depth. Other key generation techniques can be done using other existing chaotic maps too. Number of confusion and diffusion steps can also be increased to increase the robustness of the algorithm. It can be used in sensitive fields like military and medical imaging for improved security and confidentiality.

**CHAPTER 6**

**REFERENCES**

1. Huang CK, Nien HH (2009) Multi chaotic systems-based pixel shuffle for image encryption. Opt Commun 282:2123–2127 <https://doi.org/10.1016/j.optcom.2009.02.044>
2. A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption <https://link.springer.com/article/10.1007/s40745-021-00364-7>
3. An image encryption approach based on chaotic maps – LinhuaZhang, XiaofengLiao, XuebingWang<https://www.sciencedirect.com/science/article/abs/pii/S0960077904005600>
4. Elogri O, Karmouni H, Sayyouri M, Qjidaa H (2021) A novel image encryption method based on fractional discrete Meixner moments. Opt Lasers Eng 137:106346 <https://doi.org/10.1016/j.optlaseng.2020.106346>
5. Wang H, Xiao D, Chen X, Huang H (2018) Cryptanalysis and enhancements of image encryption using combination of the 1D chaotic map. Signal Process 144:444–452. https://doi.org/10.1016/j.sigpro.2017.11.005
6. Xian Y, Wang X, Yan X, Li Q, Wang X (2020) Image encryption based on chaotic sub-block scrambling and chaotic digit selection diffusion. Opt Lasers Eng J 134:2020. https://doi.org/10.1016/j.optlaseng.2020.106202
7. New insights into the existing image encryption algorithms based on DNA coding, Xianglian Xue , Dongsheng Zhou, Changjun Zhou https://doi.org/10.1371/journal.pone.0241184
8. A Novel Image Encryption Based on Bit-Shuffled Improved Tent Map, Aaditya Gupta, K Abhimanyu Kumar Patro, Richa Thawait https://www.researchgate.net/publication/313572161\_A\_Novel\_Image\_Encryption\_Based\_on\_Bit-Shuffled\_Improved\_Tent\_Map