Enhanced IoT Image Encryption: A Hybrid Approach Using Duffing and Henon Chaotic Systems

MSc Research Project
MSc In Cybersecurity

Mayur Gaikwad
Student ID: x22183655

School of Computing
National College of Ireland

Supervisor: Prof. Joel Aleburu

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Mayur Dattajirao Gaikwad

Student ID: X22183655

Programme: MSc in Cybersecurity **Year:** 2023-2024

Module: MSc Research Project/Internship

Supervisor: Prof. Joel Aleburu

Submission Due Date: 12/08/2024

Project Title: Enhanced IoT Image Encryption: A Hybrid Approach Using Duffing and Henon Chaotic Systems

Word Count:6655 Page Count : 22

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Mayur D. Gaikwad

Date: 12/08/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Enhanced IoT Image Encryption: A Hybrid Approach Using Duffing and Henon Chaotic Systems

Mayur Gaikwad
X22183655

Abstract

The fast growth of Internet of Things (IoT) devices has been developed in so many industries. Image encryption is a very important in data security which has been played for protecting sensitive visual information transmitted by IoT devices. This research is going to explore advanced image encryption techniques using chaotic maps which is mainly focusing on Tinkerbell, Duffing and Henon maps. There are 4 test images which includes Pepper, Lenna, Mandrill and Download which were used to find the performance of these encryption methods. For each technique the process includes loading and resizing the test images by performing color channel separation and applying chaotic mappings for encryption. The Tinkerbell map when combined with the Duffing map has been showed best results in terms of encryption strength. The implementation do includes generating chaotic sequences, scrambling image pixels and performing decryption to get the original images. Encryption and decryption processes were been tested with metrics such as the Number of Changing Pixels Ratio (NCPR) and Unified Average Changing Intensity (UACI) used to evaluate the performance of each method. Among the combinations tested the Duffing and Henon maps proved to be the most powerful by delivering best encryption capabilities and strongness. This technique includes using the Duffing map for its dynamic range and the Henon map for its ability to introduce complex type of chaotic behaviour. The results has been showed that Duffing and Henon as a combined encryption approach which gives increased security and better performance as compared to other chaotic map

Keywords: Image Encryption, Chaotic Maps, Tinkerbell Map, Duffing Map, Henon Map combinations.

1 Introduction

1.1 Background

Image encryption is a very important process that actually applies cryptographic techniques to transform the content of images into a good type of format which is secure and unreadable and also ensures confidentiality and integrity during transmission or storage. This method is very very important for safeguarding sensitive visual type of information from unauthorized trype of access. There are two main or primary types of image encryption techniques: asymmetric and symmetric encryption (Younes, 2019). Symmetric encryption is having the Advanced Encryption Standard (AES) which of course uses a single key for both encryption and decryption (Muttaqin and Rahmadoni, 2020) making it good or efficient for huge type of data encryption. Whereas asymmetric encryption is actually having the Rivest–Shamir–Adleman (RSA) algorithm which uses a pair of keys—a public key for the use in encryption and also a private key for the use in decryption—to enhance security by giving secure key exchange without sharing the decryption key. Image encryption serves so many types of purposes across various sectors, including healthcare, finance, and military. It of course protects confidential type of medical images, financial transactions, and classified imagery from unauthorized access or interception. The main and primary goals of image encryption include safeguarding data confidentiality for obviously ensuring data integrity and also preventing unauthorized access and giving secure data exchange. There are some common type of techniques which is used in image encryption include substitution and permutation, where pixels are rearranged and substituted based on a cryptographic key. There are some kind of transform domain techniques which includes applying transformations like Discrete Wavelet Transform (DWT) or Discrete Cosine Transform (DCT) to encrypt image coefficients. Chaotic systems use chaotic maps to generate encryption keys and of course add further complexity and security. Besides its advantages, image encryption faces some kind of challenges which is having or maintaining encryption speed for efficiently handling large image files, and ensuring compatibility with different image formats and resolutions. It's very very important and good to balance strong encryption with minimal impact on image quality.

1.2 Aim of the study

The main aim in this study is to firstly develop an enhanced image encryption method with the help of a hybrid approach of chaotic encryption technique which mainly includes the logistic map and possibly other chaotic systems like the Lorenz system or Henon map. Chaotic systems of course gives some kind of unique properties which is having sensitivity for initial conditions and pseudo-random behavior which can mainly enhance the security of encryption algorithms. By combining these chaotic systems, the study aims to create a robust encryption scheme that obviously ensures the integrity and other thing is confidentiality of image data transmitted over insecure channels or stored in some different kind of environments.

1.3 Research Objectives

There are some research objectives in this report are:

1. To create an efficient encryption technique by combining chaotic systems such as the Tinkerbell map, Duffing system and possibly Henon map to generate robust encryption keys.
2. To design and implement hybrid encryption techniques combining chaotic maps, such as Tinkerbell + Duffing, Tinkerbell + Henon, and Duffing + Henon.
3. To investigate how the use of chaotic encryption methods can actually do strengthen the security of image data by of course ensuring confidentiality against unauthorized access and data breaches.

1.4 Research Questions

There are some research questions in this report are:

1. How powerful are individual chaotic maps (Tinkerbell, Duffing and Henon) in having high-level security and randomness in image encryption?
2. What is the effect of combining chaotic maps like Tinkerbell +Duffing, Tinkerbell+Henon and Duffing+ Henon on encryption performance compared to using individual chaotic maps?
3. To what extent does the combined chaotic encryption approach improve resistance against known cryptographic attacks?

2 Related Work

2.1 Image Encryption Techniques

Image encryption techniques blend traditional and modern algorithms to secure visual data. Traditional methods like Substitution Techniques and Transposition Techniques provide robust encryption using symmetric keys, ideal for fast processing. Modern approaches such as RSA (Rivest-Shamir-Adleman) and AES-GCM (Galois/Counter Mode) offer asymmetric key encryption with enhanced security and authentication capabilities, crucial for secure data transmission over networks. Modern algorithms have evolved to address computational advancements and security vulnerabilities, ensuring resilience against sophisticated attacks while maintaining efficiency in handling large image data volumes. These combined methods will give good type of protection for sensitive visual information in digital environments.

2.2 Traditional Image Encryption Techniques

In traditional image encryption there are some kind of techniques which uses like substitution and transposition methods to secure visual data. Substitution techniques like the Caesar Cipher, Vigenère Cipher apply a keyword to of course shift pixels based on a predefined pattern. Transposition techniques such as Rail Fence Cipher, Columnar Transposition rearrange pixel positions according to a specific key. These methods actually focus on altering pixel values or positions in image content. But they may lack robustness against modern computational attacks. (Rachmawati et al., 2019) proposes a research approach combining the Caesar Cipher and Columnar Transposition Cipher modified with a Linear type of Congruential Generator for of course encrypting images to enhance security on the internet. They show the weakness of internet-transmitted information to unauthorized access with cryptographic techniques. The study uses a layered type of encryption method where images are first encrypted using the Columnar Transposition Cipher which is been followed by a secondary encryption with the Caesar Cipher incorporating a modified Linear Congruential Generator. The encrypted images are compressed with the Lempel Ziv Welch algorithm to optimize storage efficiency. Implemented in C#, the study also shows that their combined approach ensures data confidentiality, integrity, and security. Results also shows an average compression ratio (RC) of 67.05%, Compression Ratio (CR) which is of 1.49, and also 32.93% of Space Saving (SS) percentage for showing effective type of data protection and storage optimization challenges in internet-based information exchange

(Veera et al., 2024) proposes a method by of course combining the Card Deck Shuffle and Modified Caesar Cipher Algorithm for encrypting images, addressing kind of risk of information of security things in today's social networking era. Focusing on the importance of integrity in data sharing over unsecured connections, the method mainly focuses on preprocessing steps for secure information transmission. The Modified Caesar Cipher encrypts pixel type of values of images using a variable bit key, typically $n + 8$ bits where n exceeds 18, mainly increasing resistance to brute force attacks. Also, the Card Deck Algorithm firstly do pxels rearrangement which has been derived from the Modified Caesar Cipher output by obviously enhancing encryption robustness. The approach aims to secure sensitive information which is having in images across so many different multimedia applications. There are some challenges which includes optimizing key size for practical application while ensuring computational efficiency. (Sabry et al., 2018) introduces a hybrid encryption system combining the Caesar Cipher and Two Square Cipher with multiple keys, focusing the importance of maintaining the Integrity, Confidentiality and Availability of data in information security. This approach uses the strengths of both encryption techniques. The system is designed to enhance security against brute-force and statistical type of attacks for ensuring toughness and hardness in protecting sensitive information. There are some challenges which include optimizing the combination of both ciphers to maintain computational efficiency and scalability across different data types and sizes. (Bhandari, 2018) presents a novel type of encryption methodology which address the weakness of traditional Caesar cipher by obviously introducing a scheme that actually do integrates dynamically generated keysets from grayscale images with a modified cipher. The algorithm also iterates with the help of different key values from the keyset for each encryption cycle, generating unique cipher-texts in each iteration. (Haryono, 2020) proposes a study which mainly do focus on enhancing data security with the use of symmetric encryption algorithms: Hill Cipher, Caesar Cipher, Twofish and Blowfish,. These algorithms are chosen for their ability to of course encrypt and decrypt data using the same key which also ensures confidentiality in stored databases. Caesar Cipher operates by firstly shifting characters by a fixed number of positions, Hill Cipher divides text into blocks for encryption, Blowfish uses multiple type of iterations on 64-bit data for encryption, and Twofish accepts up to 256-bit data and performs 16 iterations, which gives stronger security thing and that also requires more memory and longer encryption times. There are some kind of challenges include optimizing performance and memory usage for each algorithm, as well as ensuring compatibility and scalability across different database sizes and configurations. Results also shows which is having different different levels of encryption strength and efficiency across the algorithms, with Twofish showing good and superior type of security but at the cost of increased computational resources, while Caesar Cipher and Hill Cipher give simpler implementations suitable for smaller datasets.

Table 2.1: Comparison Table

Study	Encryption Techniques	Key Features	Challenges	Results
(Rachmawai et al., 2019	Columnar Transposition Cipher, Caesar Cipher (modified with Linear Congruential Generator), Lempel Ziv Welch algorithm	Layered encryption, Compression	Implementation, Security robustness	Confidentiality, Integrity, Security enhancement, Compression efficiency
(Veera et al., 2024)	Modified Caesar Cipher, Card Deck Shuffle Algorithm	Image encryption, Security enhancement	Key size optimization, Computational efficiency	Enhanced image security, Multimedia application suitability
(Sabry et al., 2018)	Two Square Cipher, Caesar Cipher (with multiple keys)	Hybrid encryption, CIA Triad focus	Computational efficiency, Scalability	Resistance to brute-force and statistical attacks
(Bhandari, 2018)	Dynamically generated keysets from grayscale images, Modified cipher	Iterative encryption, Enhanced security	Computational efficiency, Cryptanalytic robustness	Sequential encryption, Resistance to modern cryptanalysis
(Haryono, 2020)	Caesar Cipher, Hill Cipher, Blowfish, Twofish	Symmetric encryption, Varying block sizes	Performance optimization, Memory usage	Encryption strength, Efficiency, Computational resource requirements

In their paper (Reddy and Bhukya, 2018) proposes a novel type of method to encrypt images using a modified Vigenère Cipher. The approach firstly begins by converting the digital image into Base64 format which of course serves as the input for encryption. Characters in the Base64 file are substituted using a predefined character table and a symmetric cipher key. This uses Vigenère poly-alphabetic substitution, where each character in the Base64 text is substituted multiple type of imes based on different parts of the key. The resulting ciphertext is transmitted to the receiver. Decryption actually includes with the help of same key and table to convert the ciphertext back into Base64, which is then decoded into the original image format (JPEG, PNG). This adaptation of the Vigenère Cipher for image encryption of course extended its traditional use from text to graphical data for presenting both challenges in having the algorithm and good results in securely transmitting and recovering images. In their study (Ahamed et al., 2020) proposes an enhanced method for encrypting SMS messages to address the weakness of traditional SMS encryption methods like the Vigenère cipher. They show that standard Vigenère cipher implementations can be easily cracked due to some kind of factors such as small key lengths and predictable permutations. To enhance security, the authors introduce a modified Vigenère cipher technique that combines the Rivest-Shamir-Adleman (RSA) asymmetric encryption algorithm. At last there is another study given by (Violeti et al., 2021) who has done and also discussed steganography as the practice of hidinh information within other types of data, with digital images being the most popular carrier format. They also show the importance of strong techniques for hiding and encrypting data, including file compression, locking, and encryption/decryption processes. The main objective is to of course ensure absolute confidentiality and secrecy for messages also for enhancing privacy and security in ICT developments.

2.3 Modern Image Encryption Techniques

Modern image encryption techniques utilize advanced cryptographic methods to enhance security. Key methods include Advanced Encryption Standard (AES) which is very famous and good symmetric encryption algorithm and another technique is Rivest-Shamir-Adleman (RSA) which is an asymmetric encryption technique for of course secure type of key exchange and also Elliptic Curve Cryptography is a technique (ECC) which actually gives good and high security with smaller type of key sizes. Chaos-based encryption uses chaotic maps for pseudo-random keys, while homomorphic type of encryption which actually allows kind of computation on those data which is encrypted without the use of decryption. Wavelet transform-based encryption combines wavelet transform and cryptography for secure image processing, and quantum cryptography uses principles of quantum mechanics to achieve unprecedented security. These techniques bolster image protection against complex threats.

In (Arab et al., 2019) an image encryption algorithm is proposed that will firstly combines the chaos sequence with a modified AES algorithm. The encryption key is generated with the help of Arnold chaos sequence, and the original image is encrypted with the modified AES algorithm with round keys produced by the chaos system. This approach enhances the diffusion kind of ability of the algorithm for obviously having the encrypted type of images which is actually resistant for reducing the algorithm's time complexity. The key space is very very large to brute-force attacks, and the method's sensitivity to starting values and input image ensures that minor changes will give to important type of alterations in the encrypted type of image. There is a statistical analyses which actually shows the algorithm's robustness against statistical attacks, with entropy tests showing values close to ideal, showing security.

In (Hafsa et al., 2021) an improved cryptographic approach for embedded systems is proposed, focusing on high security and speed, mainly for medical image encryption. This approach combines the AES and ECC using the speed of symmetric type of AES for data encryption and the security of asymmetric ECC for of course securing the symmetric session key exchange. The paper also introduces an optimized type of ECC hardware architecture which mainly balances area, power dissipation, and speed by using only 2 type of multipliers and proposes a 32-bit kind of multiplier and inverter architecture to reduce area occupancy and any power consumption. For encryption of images, the AES algorithm is modified by obviously reducing the mix-columns kind of transformation and replacing it with a permutation thing which is on column shifts, reducing time complexity for of course maintaining confusion things.

In (Chowdhary et al., 2020) an analysis is proposed for image encryption and decryption by hybridizing Elliptic Curve Cryptography (ECC) with Hill Cipher (HC), ECC with Advanced Encryption Standard (AES), and ElGamal with Double Playfair Cipher (DPC). ECC combined with AES is found to be mainly suitable for remote or of course private type of communications with smaller image sizes due to the efficient encryption and decryption times. The study's metric measurements and test cases shows that ECC and HC give a robust overall solution for image encryption, balancing security and performance effectively. In (Alsaffar et al., 2020) a comparative study between the AES and RSA encryption algorithms for image encryption with the help of MATLAB is been proposed. The study mainly focuses on evaluating the image encryption quality of each algorithm with the analysis of histogram and correlation results. There is another study which gave novel approach by (Sahwal et al., 2018) for image encryption with the help of a modified ECC algorithm is proposed by focusing on reducing complexity and improving performance. This study is going to introduce a modified version of ECC implemented in MATLAB by obviously using the Region of Interest (ROI) feature to decrease complexity and reduce error calculation. The proposed method does includes creating an index over the image using the ROI feature which is similar to a convex hull which helps in isolating the important portions of the image for encryption. The study shows that the modified ECC method when combined with the ROI technique mainly gives the conventional ECC approach. The comparative analysis between the proposed method and the traditional ECC approach has of course showed good improvements. The study also shows that the ROI approach maintains the encryption strength and security of ECC while increasing its performance. The results shows that the change ECC with ROI not only reduces computational complexity but also secures string type of image encryption by making it a very very good type of solution for practical things where processing time are very important. The introduction of ROI in ECC encryption gives a good type of advancement in the image cryptography which gives a powerful and good approach to secure image data. At last (Dawahdeh et al., 2018) combines ECC with Hill Cipher is proposed to increase the security and performance of image encryption. The motivation behind this hybrid approach is to transform the traditionally symmetric Hill Cipher which is not good on a shared private key over unsecured channels into an asymmetric technique using ECC. This change aims to reduce the security weaknesses of the Hill Cipher while using its simplicity and computational speed.

3 Research Methodology

3.1 Methodologies Used

3.1.1 Tinker Bell Map

The Tinkerbell map is a type of chaotic map which is been used in so many fields which includes cryptography and image encryption for its complex and unpredictable kind of behaviour. This map is known for its ability to produce highly sensitive and complex type of sequences by making it good for applications that require a high level of security. The Tinkerbell map has been generated sequences that show a huge range of behaviours which do includes chaos by depending on initial conditions. The Tinkerbell map is been used to create encryption algorithms that use its chaotic properties to increase data security. This do secures that small changes in input lead to importantly different outputs which is a very important feature for good encryption. This characteristic helps to hide the original data and makes it strong to different types of cryptographic attacks. The map is going to operate with iterative processes that transform input values into complex patterns which are then used to encrypt or modify data. Due to its chaotic nature the Tinkerbell map is powerful in generating pseudo-random sequences that can be applied to encrypt images or other types of data by giving a strong method for protecting sensitive type of information from unauthorized access.

$$x_{n+1} = x_n^2 - y_n^2 + ax_n + by_n$$

$$y_{n+1} = 2x_n y_n + cx_n + dy_n$$

3.1.2 Duffing Map

The Duffing oscillator is a well-known system in chaos theory and nonlinear dynamics which is used to study complex and chaotic behaviours in physical systems It is of course divide by its ability to show a range of dynamic behaviours from simple periodic oscillations to chaotic motion which do depends on so many parameters. The Duffing oscillator is been used to explore how small changes in system parameters can become to important changes in behaviour by making it a good tool for studying chaos and stability. This feature makes the Duffing oscillator which is mainly useful in fields like cryptography and signal processing where understanding and using chaotic dynamics can increase data security and system robustness. The Duffing oscillator's ability to produce chaotic sequences is been used in encryption algorithms to generate pseudo-random sequences that obscure data. This is achieved by utilizing the system's sensitive dependence on initial conditions where even tiny type of changes can lead to different results. There are some properties are important in designing encryption methods that do protect sensitive information by securing that encrypted data appears random and is good to decryption attempts without proper authorization.

$$\begin{aligned} x_{n+1} &= y_n \\ y_{n+1} &= -bx_n + ay_n - y_n^3. \end{aligned}$$

3.1.3 Henon Map

The Henon map is a discrete-time dynamical system which is been introduced by the French mathematician Michel Henon. It is famous for its role in studying chaotic systems due to its ability to produce complex and unpredictable type of behaviour from simple rules. This has been originally designed as a model to understand the changes of the solar system the Henon map has become an important tool in chaos theory. The map is been defined by a set of iterative processes that describe how points in a plane grow over time. It generates sequences that can show chaotic characteristics such as sensitive dependence on initial conditions where small changes in the starting point can manage to greatly different outcomes. This sensitivity is a hallmark of chaotic systems and makes the Henon map which is mainly useful for studying the nature of chaos and randomness. In practical applications the Henon map's properties are been used in so many fields which do includes cryptography and image processing. By using its chaotic behaviour the Henon map can produce pseudo-random sequences that increase the security of encryption algorithms and data scrambling techniques. Its capacity to generate complex and unpredictable type of sequences secures that encrypted information remains secure and difficult to decipher without the proper decryption key.

$$\begin{cases} x_{n+1} = 1 - ax_n^2 + y_n \\ y_{n+1} = bx_n. \end{cases}$$

4 Design Specification

The design of the proposed system is going to use lightweight and good hardware devices suitable for the IoT and edge computing environments. The main hardware platform has been chosen is based on the ARM Cortex-A8 processor which is a mostly done architecture known for its balance between performance and power performance. This processor is a part of many inserted systems and gives a strong performance profile while maintaining a low power footprint by making it good for IoT applications that require constant operation with low energy consumption.

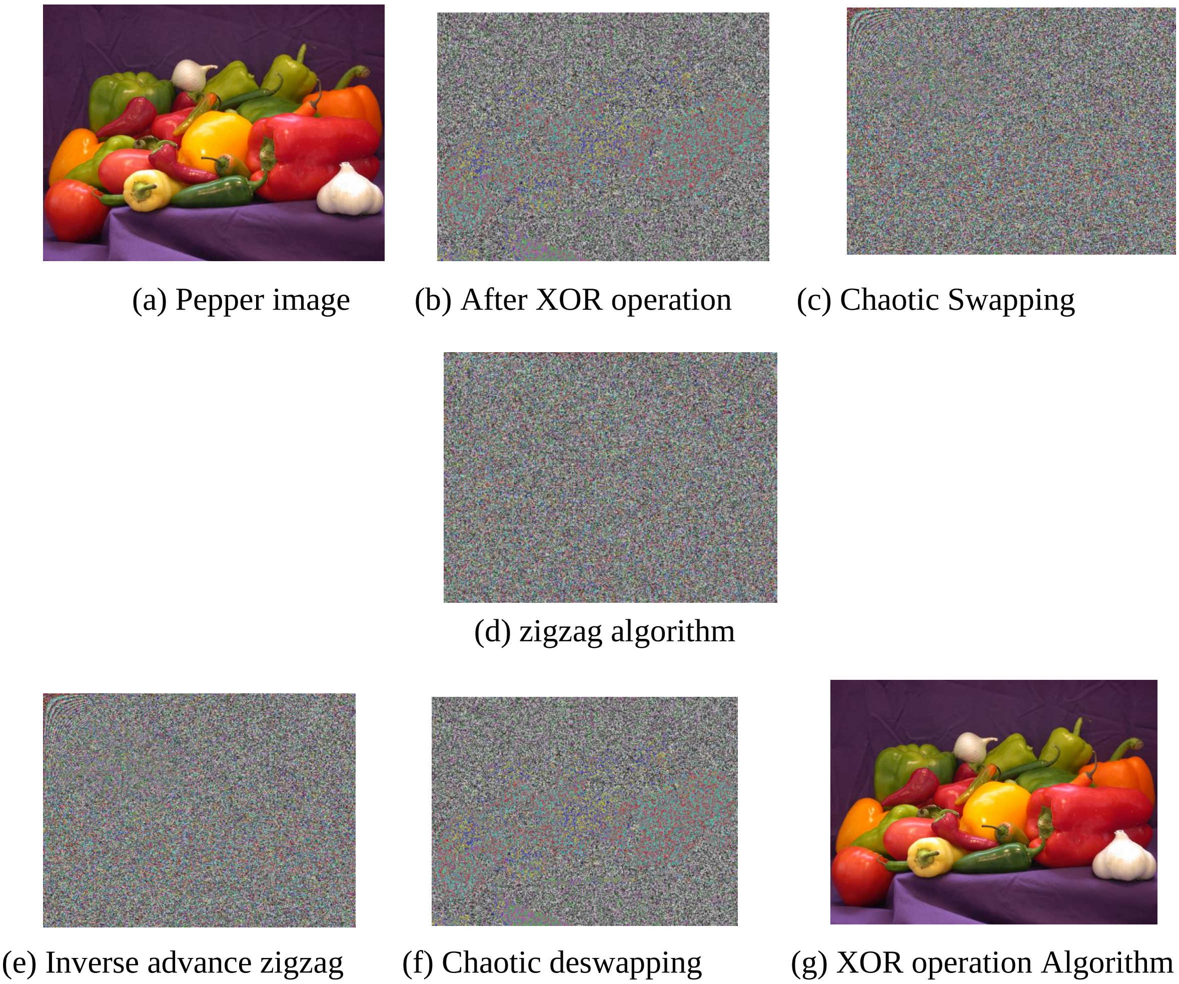
This project is been provided with 512MB of RAM the system is well-suited for handling lightweight applications and processing tasks typical of edge computing things. This memory capacity secures smooth operation of the software system components which do includes the management of data streams and execution of encryption algorithms. The 512MB RAM gives good space for temporary data storage and buffering by having powerful processing without any delays.

The hardware also includes 4GB of eMMC (embedded MultiMediaCard) flash storage. This storage solution has been chosen for its reliability and speed by giving quick read and write operations which is important for data-intensive applications. The 4GB capacity is enough for storing operating system files, application data and encrypted data by securing that the system can perform its tasks without running out of storage space. The combination of the ARM Cortex-A8 processor, 512MB RAM and 4GB eMMC flash storage creates a compact and good hardware solution ideal for edge devices and IoT applications. This configuration supports so many functionalities like data collection, preprocessing and encryption in a resource-constrained environment. The lightweight nature do secures that it can be deployed in a huge range of things from remote sensors to inserted systems in smart devices where space and power things which are important.

5 Implementation

5.1 Implementation of Tinker and Duffing

The implementation of the Tinkerbell and Duffing maps for image encryption do includes using two test images Pepper and Lenna to show the encryption process. The workflow starts by loading the Lenna image from a specified type of file path. Using OpenCV the image is going to read and resized to fit the desired dimensions which are done by scaling the original height and width to maintain the aspect ratio. Once the image is loaded and resized the RGB channels have been extracted. The red, green and blue color channels of the image are separated for individual processing. The next step includes generating a chaotic array using a combination of the Tinkerbell and Duffing chaotic maps. This chaotic array is important for the encryption process as it gives a pseudorandom sequence used to transform the pixel values. For the Tinkerbell map initial values are set and the map is iterated to generate a series of chaotic values. Similarly the Duffing map is been used to produce another series of chaotic values. These two chaotic sequences are then combined to create a final chaotic array that is used for pixel scrambling. The chaotic array has been applied to the RGB channels of the image through an XOR operation which actually modifies the pixel values based on the generated chaotic sequence. This step is going to first encrypts the image by making the pixel values difficult to detect without the correct key. Finally after applying the encryption process the modified image is been saved and analyzed. This implementation has also showed how the Tinkerbell and Duffing maps can be used to achieve secure image encryption using Pepper and Lenna as test cases by showing the practicality and performance of chaotic encryption methods.

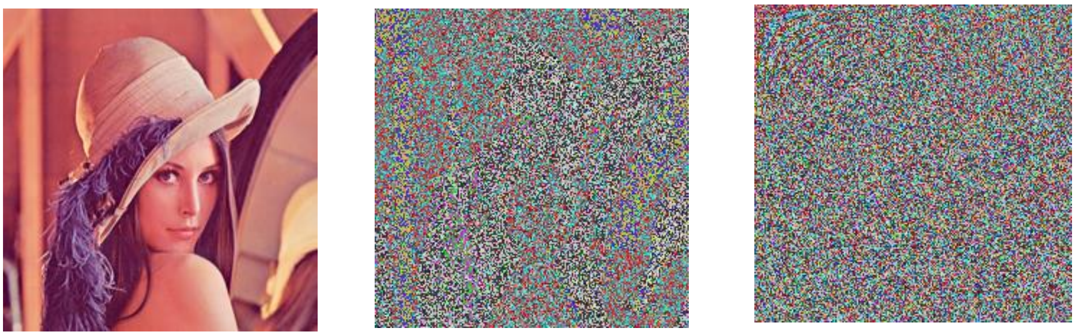


(a) Pepper image (b) After XOR operation (c) Chaotic Swapping

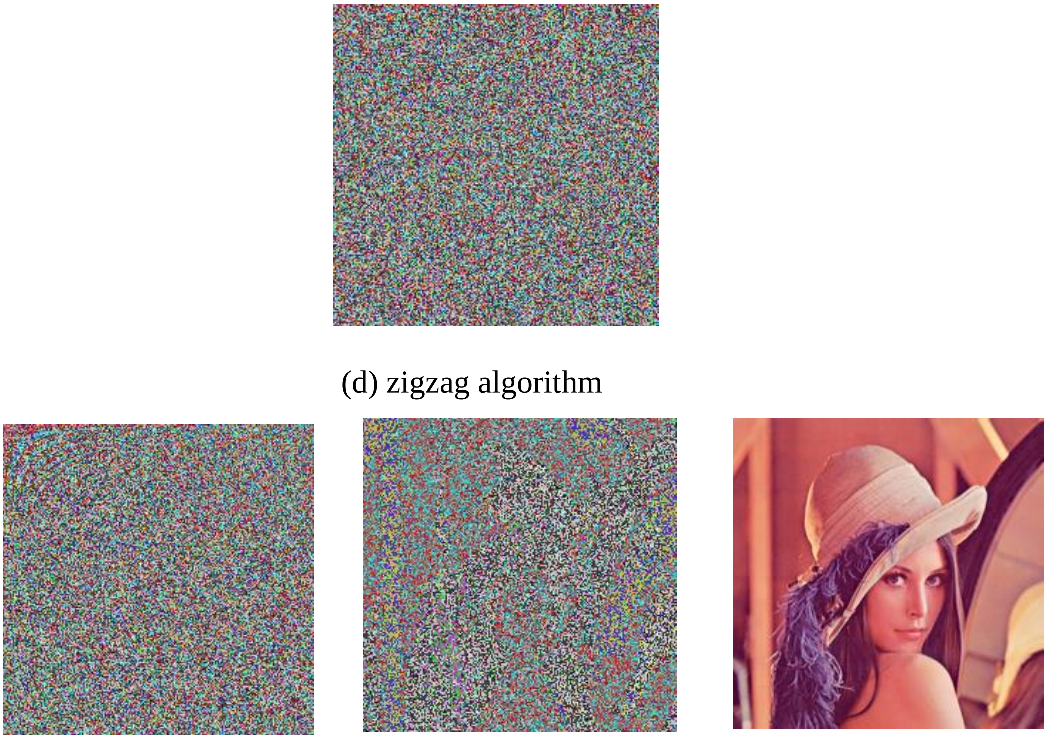
(d) zigzag algorithm

(e) Inverse advance zigzag (f) Chaotic deswapping (g) XOR operation Algorithm

Figure 5.1: Encryption and decryption process applied on peppers image



(a) Lenna image (b) After XOR operation (c) Chaotic Swapping



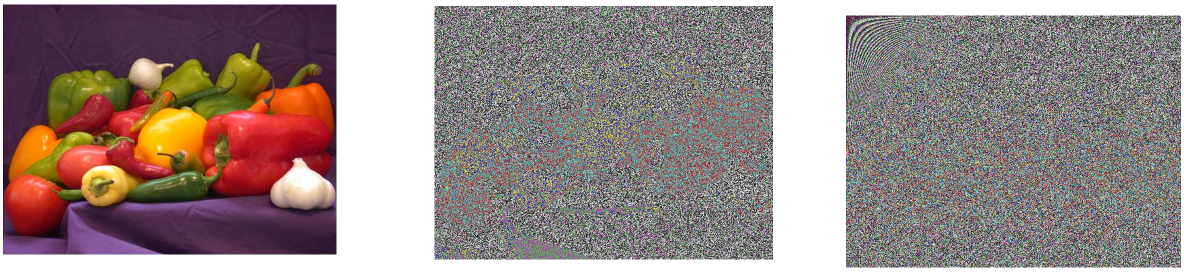
(d) zigzag algorithm

(e) Inverse advance zigzag (f) Chaotic deswapping (g) XOR operation Algorithm

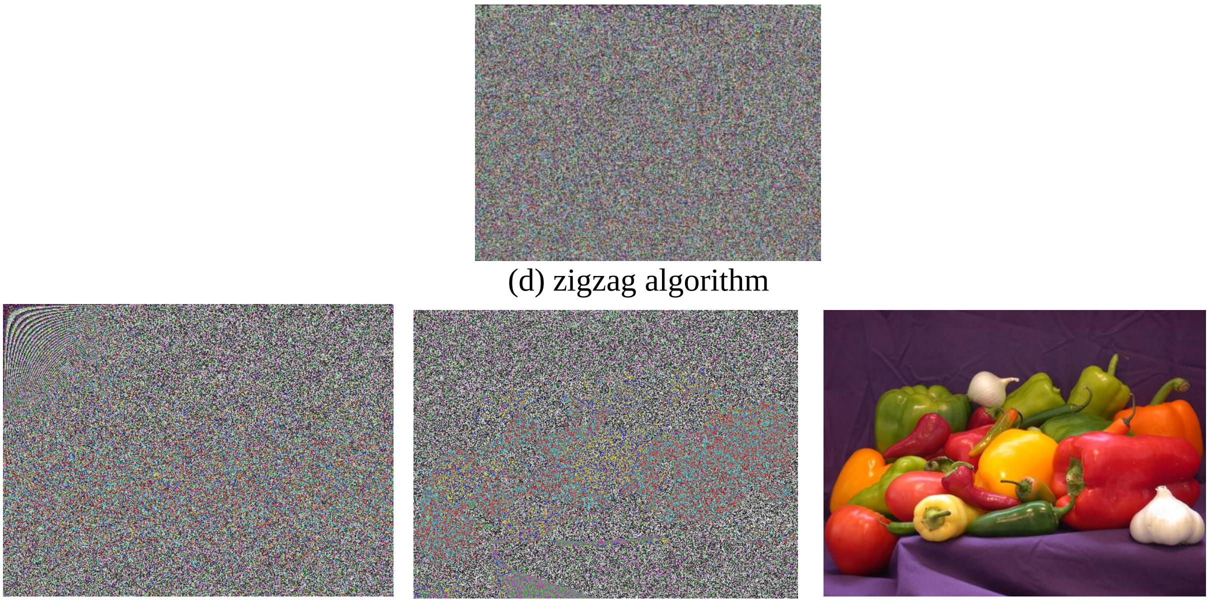
Figure 5.2: Encryption and decryption process applied on Lenna image

5.2 Implementation of Tinker and Henon

In this implementation I have been used the Tinker and Henon maps to encrypt and decrypt two test images which is having pepper and Lenna. The process starts by loading the test images and resizing them to the desired dimensions. For example the pepper image is going to load first and its dimensions are adjusted with help of OpenCV functions. The Tinker map is going to give two sequences x_tinker and y_tinker, while the Henon map generates x_henon and y_henon. These sequences are combined to form a chaotic array in which where each element is a sum of corresponding elements from the Tinker and Henon sequences. This combination will increase the complexity of the chaotic map by obviously making the encryption more strong. The combined chaotic sequences are then scaled and adjusted to secure all values are positive integers within the image dimensions. The encryption process is having three main steps like chaotic scrambling (using the XOR array), chaotic swapping and zigzag scrambling. Whereas decryption is going to reverse these steps. It starts with zigzag descrambling which is been followed by chaotic deswapping and chaotic descrambling.



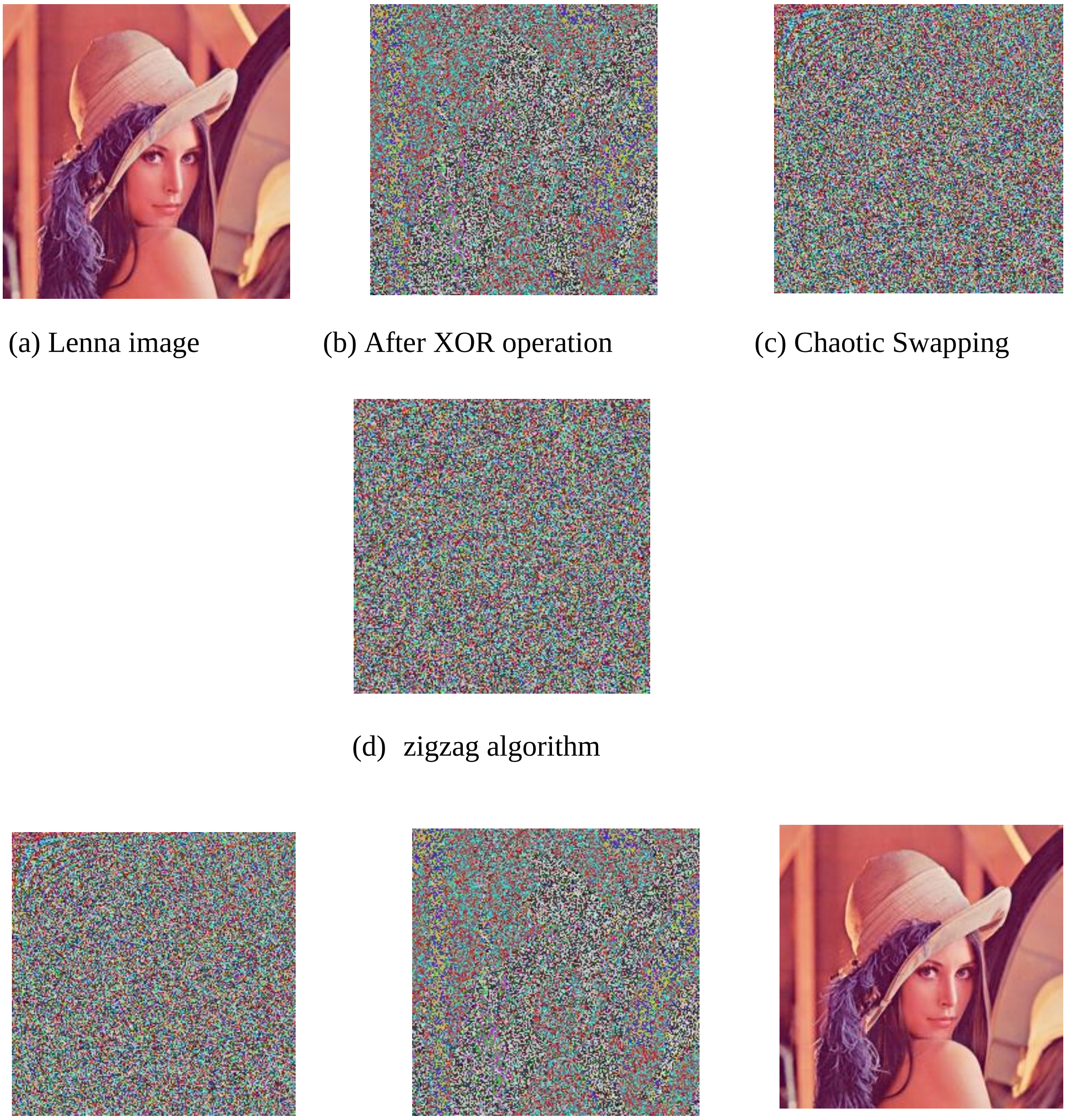
(a)Pepper image (b) After XOR operation (c) Chaotic Swapping



(d) zigzag algorithm

(e) Inverse advance zigzag (f) Chaotic deswapping (g) XOR operation Algorithm

Figure 5.3: Encryption and decryption process applied on pepper image



(a) Lenna image (b) After XOR operation (c) Chaotic Swapping

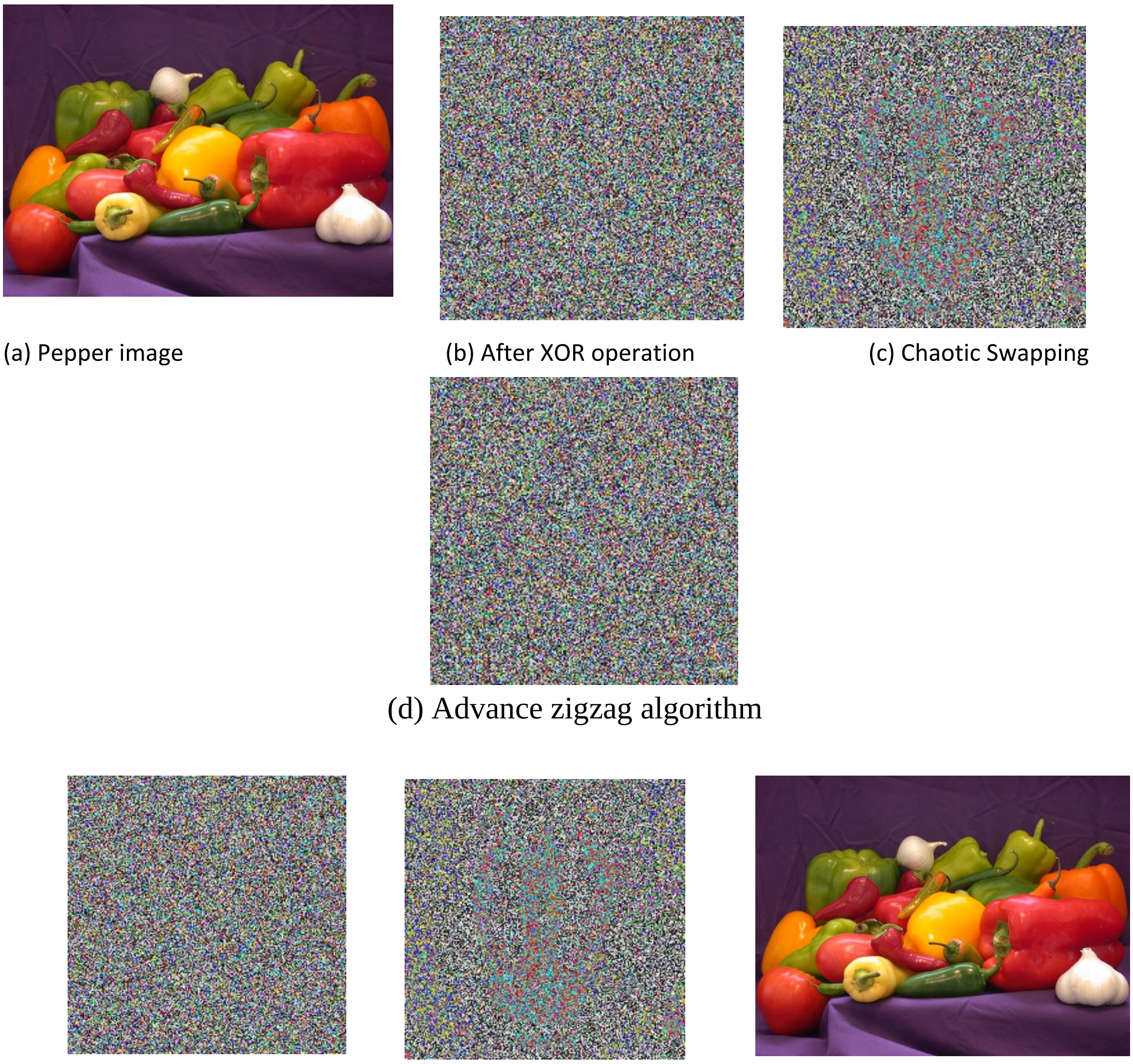
(d) zigzag algorithm

(e) Inverse advance zigzag (f) Chaotic deswapping (g) XOR operation Algorithm

Figure 5.4: Encryption and decryption process applied on Lenna image

5.3 Implementation of Duffing and Henon

In this section I am going to focus on implementing the Duffing and Henon chaotic maps for image encryption and decryption. I have used two test images which have Lenna and pepper to evaluate the performance of this combination technique. The color channels of the image will be having this RGB to use encryption. Among the chaotic combination techniques evaluated the Duffing and Henon combination has been proved to be highly good by showing strong encryption capabilities and strongness. The resulting image encryption with Duffing and Henon showed good improvements in security as compared to other combinations like Tinker + Duffing and Tinker + Henon

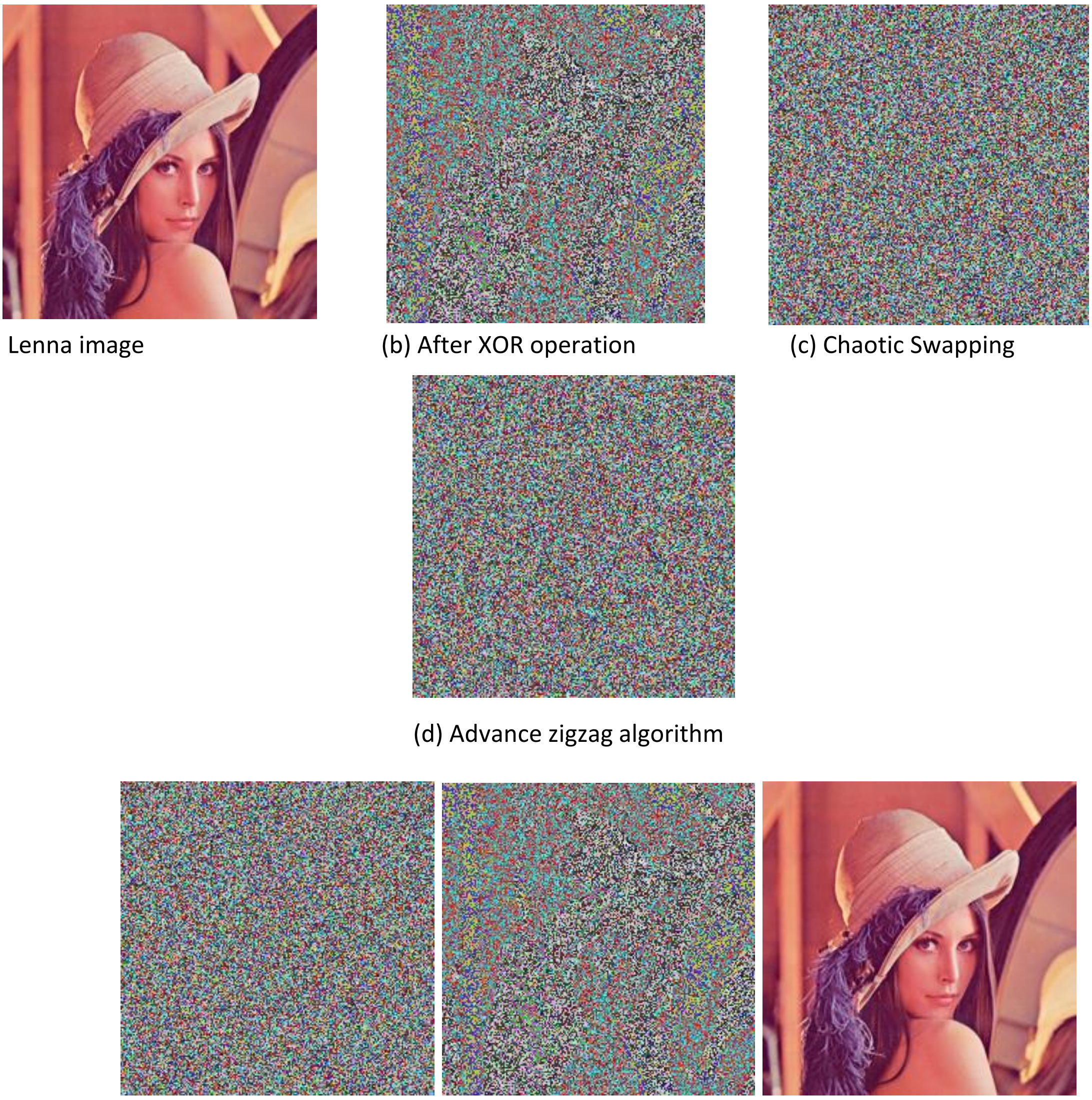


(a) Pepper image (b) After XOR operation (c) Chaotic Swapping

(d) Advance zigzag algorithm

(e) Inverse advance zigzag (f) Chaotic deswapping (g) XOR operation Algorithm

Figure 5.5: Encryption and decryption process applied on Pepper image



(a) Lenna image (b) After XOR operation (c) Chaotic Swapping

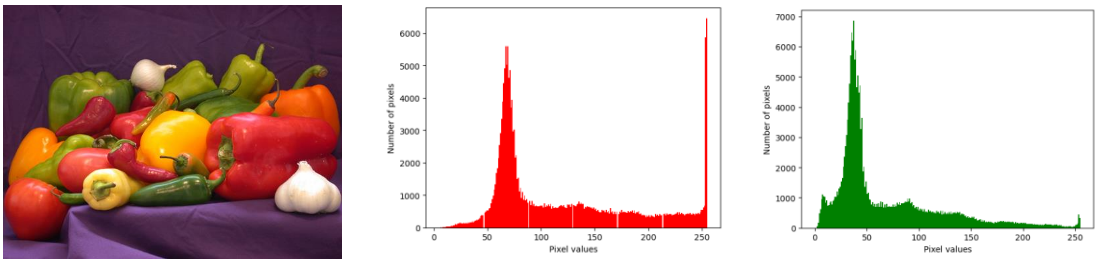
(d) Advance zigzag algorithm

(e) Inverse advance zigzag (f) Chaotic deswapping (g) XOR operation Algorithm

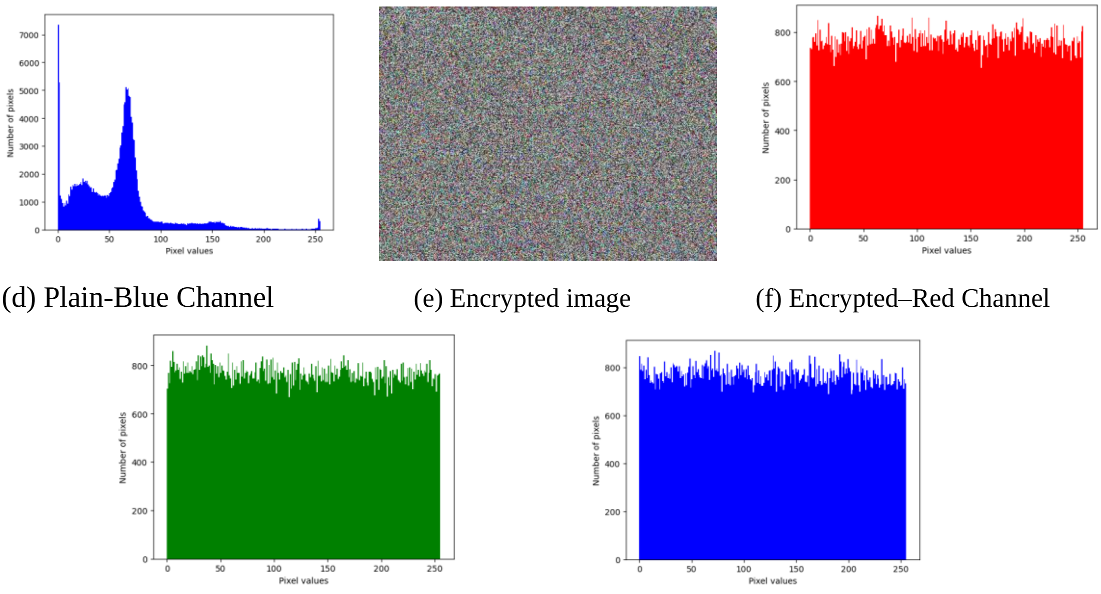
Figure 5.6: Encryption and decryption process applied on Lenna image

6 Evaluation

6.1 Historical analysis of Tinker and Duffin



(a) Original image (b) Plain–Red Channel (c) Plain–Green Channel



(d) Plain-Blue Channel

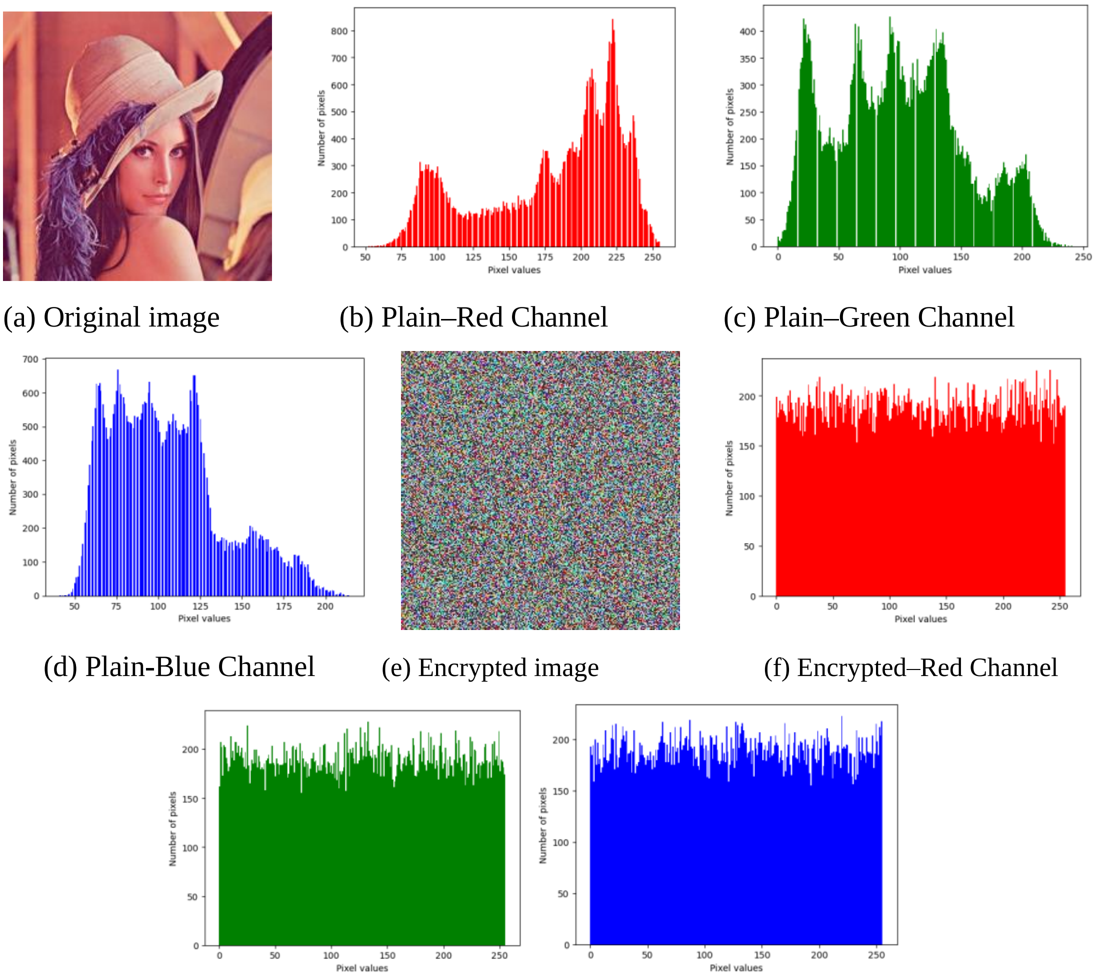
(e) Encrypted image

(f) Encrypted–Red Channel

(g) Encrypted–Green Channel

(h) Encrypted -Blue Channel

Figure 6.1: Histogram of RGB channels of Tinker and Duffin having plain and encrypted pepper image



(a) Original image

(b) Plain–Red Channel

(c) Plain–Green Channel

(d) Plain-Blue Channel

(e) Encrypted image

(f) Encrypted–Red Channel

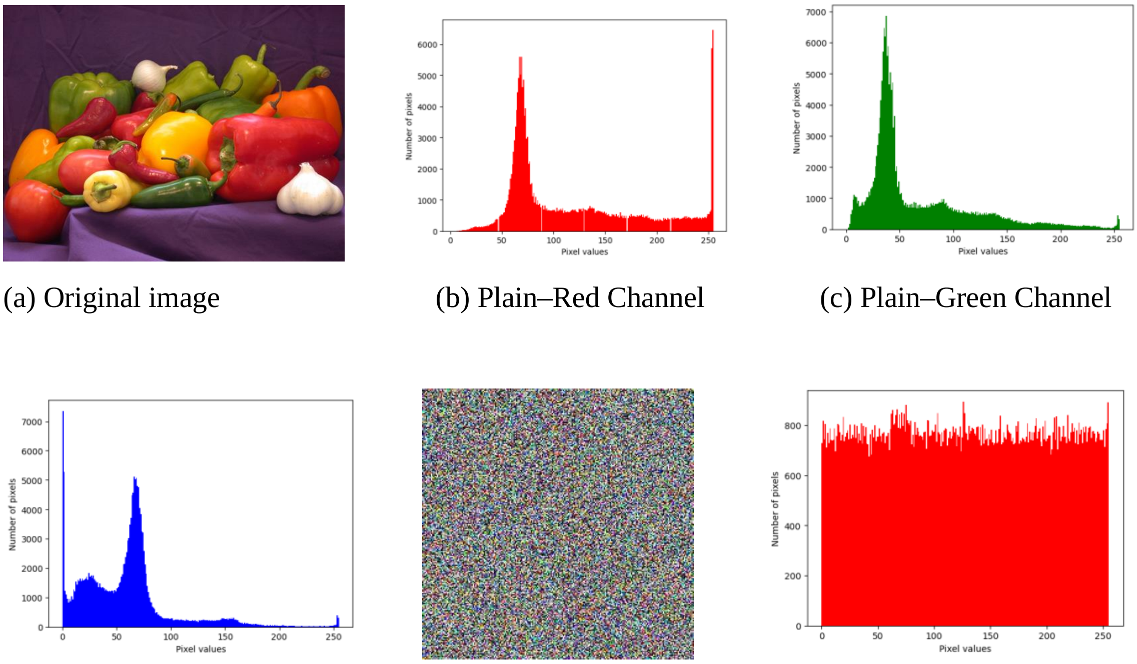
(g) Encrypted–Green Channel

(h) Encrypted -Blue Channel

Figure 6.2: Histogram of RGB channels of Tinker and Duffin having plain and encrypted Lenna image

For the combined Tinkerbell and Duffing chaotic encryption methods applied to the Pepper and Lenna images, the key generation, encryption, and decryption times are notably different between the two images. Key Generation Time: The Pepper image required 1.593 seconds for key generation, while the Lenna image took only 0.241 seconds. This discrepancy is likely due to differences in image complexity or the initial conditions of the chaotic maps. For encryption, the Pepper image experienced a total time of 5.739 seconds, with 2.276 seconds spent on the XOR operation and 0.842 seconds on chaotic map encryption. In contrast, the Lenna image's total encryption time was shorter at 3.602 seconds, with 0.386 seconds for XOR and 0.217 seconds for the chaotic map. The reduced encryption time for Lenna suggests a more efficient processing due to its smaller size or simpler structure. Decryption times followed a similar trend. The Pepper image had a total decryption time of 2.749 seconds, with 0.697 seconds for inverse zigzag and 1.201 seconds for chaotic deswapping. Lenna's decryption was faster at 0.687 seconds total, with 0.287 seconds for inverse zigzag and 0.401 seconds for chaotic deswapping. The reduced decryption time for Lenna indicates a more streamlined process, potentially due to its smaller size or simpler encryption structure.

6.2 Historical Analysis of Tinker and Henon



(a) Original image

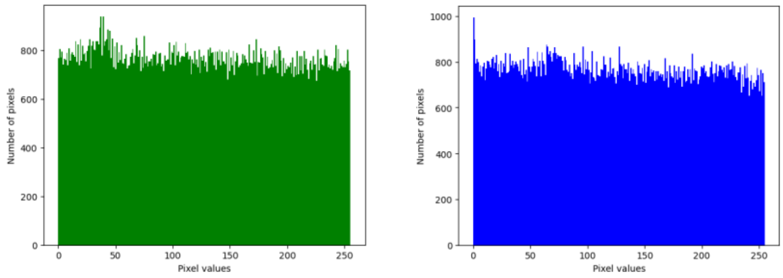
(b) Plain–Red Channel

(c) Plain–Green Channel

(d) Plain-Blue Channel

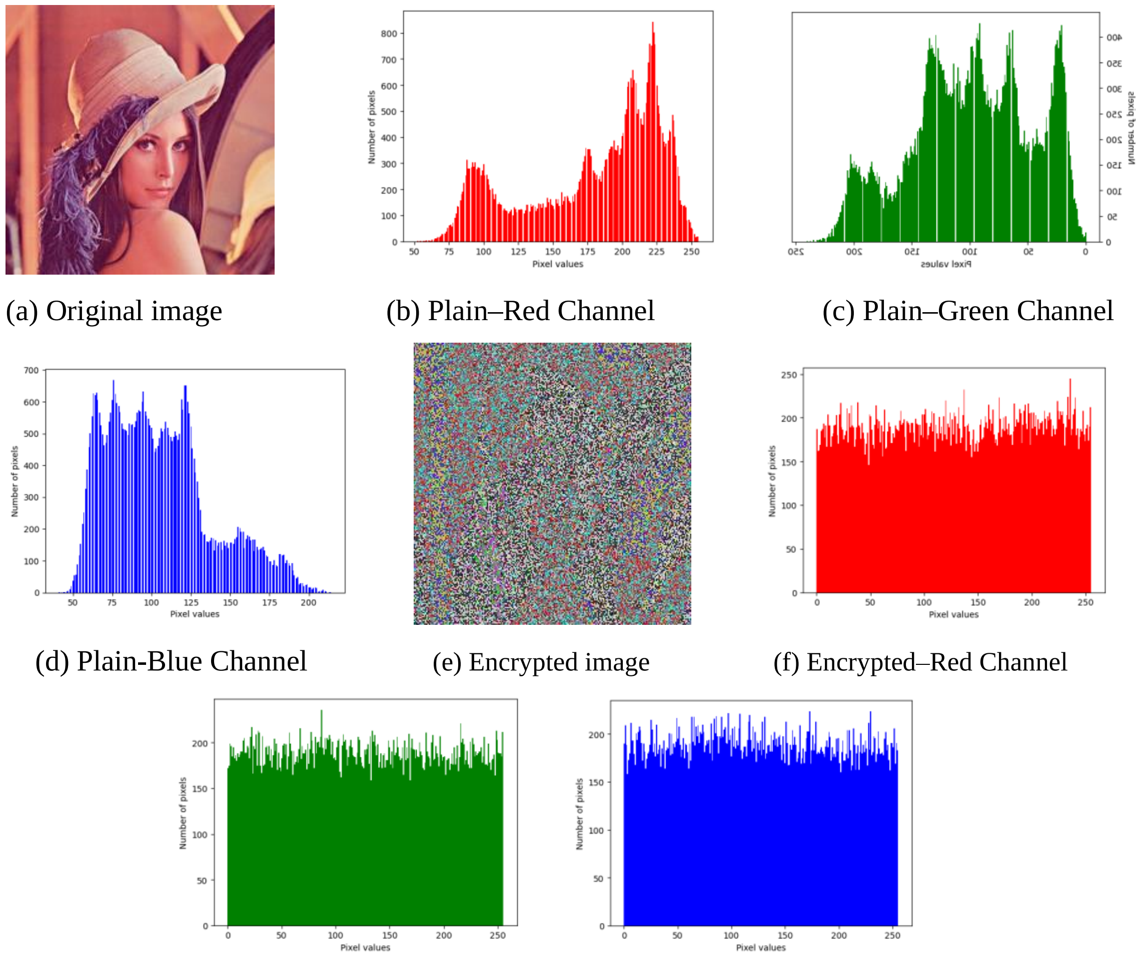
(e) Encrypted image

(f) Encrypted–Red Channel



(g) Encrypted–Green Channel (h) Encrypted -Blue Channel

Figure 6.3: Histogram of RGB channels of Tinker and Henon having plain and encrypted pepper image



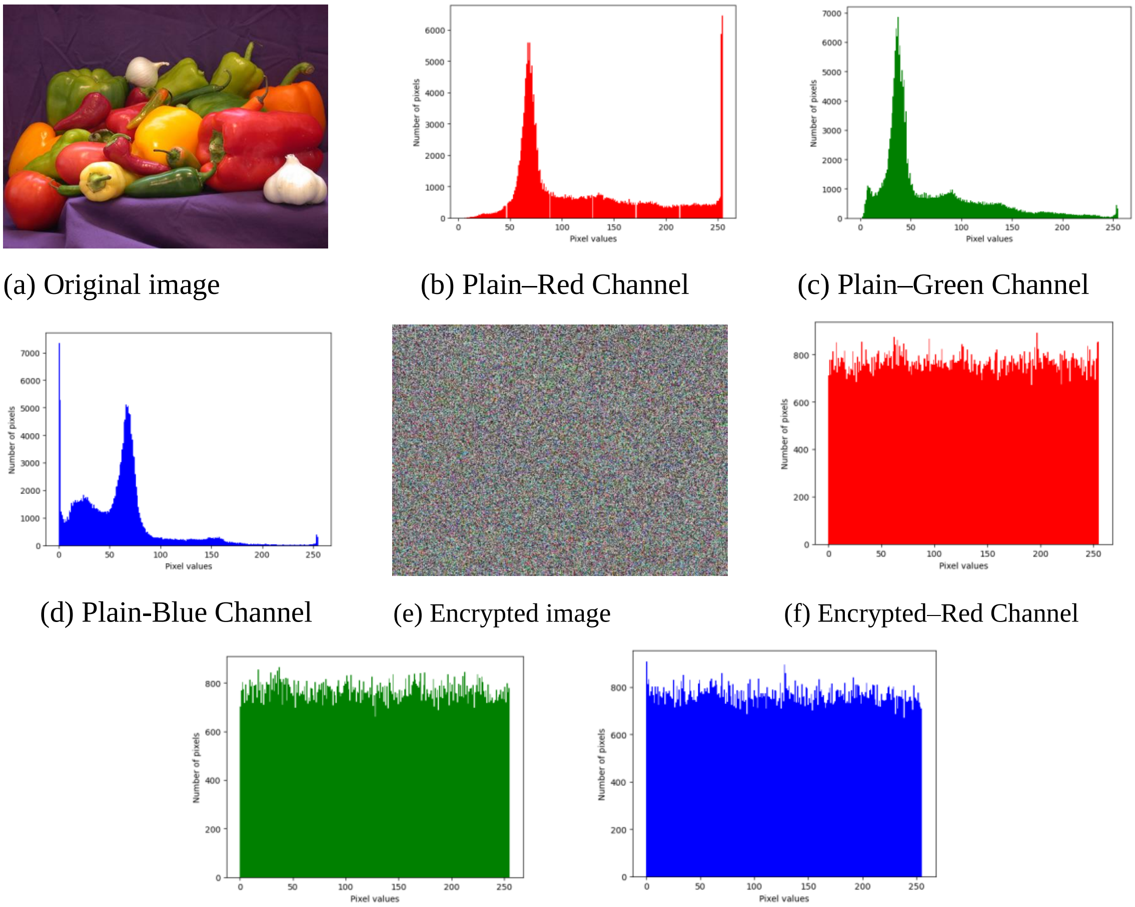
(a) Original image (b) Plain–Red Channel (c) Plain–Green Channel

(d) Plain-Blue Channel (e) Encrypted image (f) Encrypted–Red Channel

(g) Encrypted–Green Channel (h) Encrypted -Blue Channel

Figure 6.4: Histogram of RGB channels of Tinker and Henon having plain and encrypted Lenna image

6.3 Historical Analysis of Duffing and Henon



(a) Original image

(b) Plain–Red Channel

(c) Plain–Green Channel

(d) Plain-Blue Channel

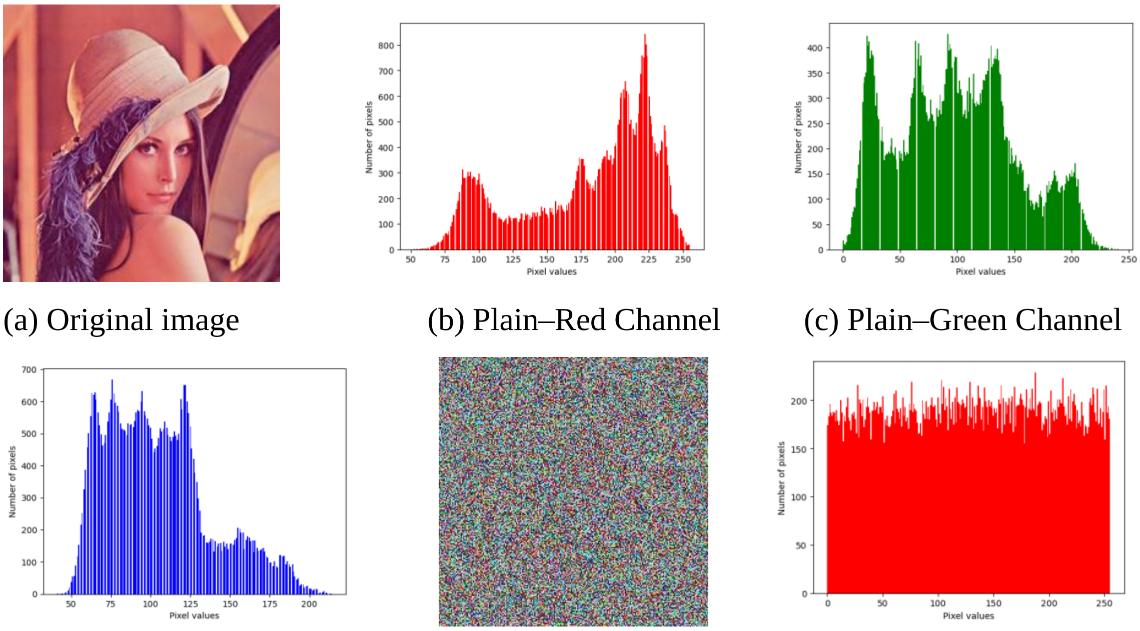
(e) Encrypted image

(f) Encrypted–Red Channel

(g) Encrypted–Green Channel

(h) Encrypted -Blue Channel

Figure 6.5: Histogram of RGB channels of Duffing and Henon having plain and encrypted Pepper image



(a) Original image

(b) Plain–Red Channel

(c) Plain–Green Channel

d) Plain-Blue Channel

(e) Encrypted image

(f) Encrypted–Red Channel

Figure 6.6: Histogram of RGB channels of Duffing and Henon having plain and encrypted Lenna image

6.4 Comparative Analysis of Pepper and Lenna image of all 3 models

The analysis of the both Pepper and Lenna images shows some key differences. The Tinker + Henon model consistently shows the best PSNR values by showing good image quality post-encryption. It also has the lowest encryption time for both images by suggesting performance. The Duffing + Henon model achieves slightly better NPCR and UACI scores by reflecting stronger encryption performance. The Tinker + Duffing model while having higher encryption times and slightly lower NPCR and UACI values which maintains competitive results.

Table 6.1: Comparison Using Pepper Image

Metric	Tinker + Duffing	Tinker + Henon	Duffing + Henon
Image Size	220 x 220	384 x 512	384 x 512
MSE Red Channel	10909.85	10867.93	10901.14
MSE Green Channel	10851.75	10943.96	10925.10
MSE Blue Channel	10900.64	10925.79	10913.91
PSNR Red Channel	7.75	7.77	7.76
PSNR Green Channel	7.78	7.74	7.75
PSNR Blue Channel	7.76	7.75	7.75
Encryption Time	9.51 seconds	6.53 seconds	6.69 seconds
NPCR Red Channel	99.58%	99.60%	99.61%
NPCR Green Channel	99.57%	99.58%	99.60%
NPCR Blue Channel	99.65%	99.57%	99.59%
UACI Red Channel	32.83%	31.94%	31.98%
UACI Green Channel	30.49%	34.46%	34.68%
UACI Blue Channel	27.56%	34.70%	34.98%

Table 6.2: Comparison Using Lenna Image

Metric	Tinker + Duffing	Tinker + Henon	Duffing + Henon
Image Size	220 x 220	220 x 220	220 x 220
MSE Red Channel	10931.71	10931.71	10841.40
MSE Green Channel	10946.84	10946.84	10830.51
MSE Blue Channel	10868.38	10868.38	10792.62
PSNR Red Channel	7.74	7.74	7.78
PSNR Green Channel	7.74	7.74	7.78
PSNR Blue Channel	7.77	7.77	7.80
Encryption Time	4.34 seconds	4.34 seconds	3.05 seconds
NPCR Red Channel	99.67%	99.67%	99.67%
NPCR Green Channel	99.59%	99.59%	99.60%
NPCR Blue Channel	99.55%	99.55%	99.61%
UACI Red Channel	32.73%	32.79%	32.73%
UACI Green Channel	30.56%	30.51%	30.56%
UACI Blue Channel	27.50%	27.32%	27.50%

7 Conclusion and Future Work

7.1 Conclusion

In conclusion this research is going to explore advanced image encryption techniques using chaotic maps to increase security. I have been implemented a combination of Tinkerbell and Duffing maps, Tinkerbell and Henon maps as well as Duffing and Henon maps for encrypting and decrypting images. The test images will use 4 test images which do include Pepper, Lenna, Mandrill and Download. For each combination the workflow will firstly include loading the images by applying chaotic map-based encryption and then conducting decryption processes to get the original images. The Tinkerbell and Duffing combination has been showed strong encryption performance by showing security improvements. So among all tested combinations the Duffing and Henon maps has been proved to be the most best by giving good results in terms of encryption strength. Metrics such as the Number of Changing Pixels Ratio (NCPR) and Unified Average Changing Intensity (UACI) have been used to find encryption performance.

7.2 Limitations and Future Works

This research does have some limitations. Firstly the chaotic maps used Tinkerbell, Duffing and Henon which are based on deterministic chaos which may not fully capture the unpredictability is been required for high-security applications. Also the image encryption process do includes computational complexity which can lead to longer processing times and might not be good or ideal for real-time applications or devices with limited processing power. Future work in this field could focus on solving the limitations which is been identified by exploring other chaotic maps and hybrid encryption techniques to increase security and performance. By combining ML algorithms to adjust chaotic map parameters in response to growing threats could improve security

References

1. Younes, M.A.B., 2019. A SURVEY OF THE MOST CURRENT IMAGE ENCRYPTION AND DECRYPTION TECHNIQUES. *International Journal of Advanced Research in Computer Science*, *10*(1).
2. Muttaqin, K. and Rahmadoni, J., 2020. Analysis and design of file security system AES (advanced encryption standard) cryptography based. *Journal of Applied Engineering and Technological Science (JAETS)*, *1*(2), pp.113-123.
3. Rachmawati, D., Hardi, S.M. and Pasaribu, R.P., 2019, December. Combination of columnar transposition cipher caesar cipher and lempel ziv welch algorithm in image security and compression. In *Journal of Physics: Conference Series* (Vol. 1339, No. 1, p. 012007). IOP Publishing.

4. Veera, D., Mangrulkar, R., Bhadane, C., Bhowmick, K. and Chavan, P., 2024. Modified Caesar Cipher and Card Deck Shuffle Rearrangement Algorithm for Image Encryption. *Journal of Information and Telecommunication*, *8*(2), pp.280-300.
5. Es-Sabry, M., El Akkad, N., Merras, M., Saaidi, A. and Satori, K., 2018. A novel text encryption algorithm based on the two-square Cipher and Caesar Cipher. In *Big Data, Cloud and Applications: Third International Conference, BDCA 2018, Kenitra, Morocco, April 4–5, 2018, Revised Selected Papers 3* (pp. 78-88). Springer International Publishing.
6. Bhandari, N., 2018, December. Iterative Caesar cipher using grayscale image pixel values as keys. In *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 706-711). IEEE.
7. Haryono, W., 2020. Comparison encryption of how to work caesar cipher, hill cipher, blowfish and twofish. *Data Science: Journal of Computing and Applied Informatics*, *4*(2), pp.100-110.
8. Reddy, V.V.K. and Bhukya, S., 2018. Encrypt and decrypt image using vigenere cipher. *International Journal of Pure and Applied Mathematics*, *118*(24), pp.1-8.
9. Ahamed, B.B. and Krishnamoorthy, M., 2020. SMS encryption and decryption using modified vigenere cipher algorithm. *Journal of the Operations Research Society of China*, pp.1-14.
10. Voleti, L., Balajee, R.M., Vallepu, S.K., Bayoju, K. and Srinivas, D., 2021, March. A secure image steganography using improved LSB technique and Vigenere cipher algorithm. In *2021 International Conference on Artificial Intelligence and Smart Systems (ICAIS)* (pp. 1005-1010). IEEE.
11. Arab, A., Rostami, M.J. and Ghavami, B., 2019. An image encryption method based on chaos system and AES algorithm. *The Journal of Supercomputing*, *75*, pp.6663-6682.
12. Hafsa, A., Sghaier, A., Malek, J. and Machhout, M., 2021. Image encryption method based on improved ECC and modified AES algorithm. *Multimedia Tools and Applications*, *80*, pp.19769-19801.
13. Chowdhary, C.L., Patel, P.V., Kathrotia, K.J., Attique, M., Perumal, K. and Ijaz, M.F., 2020. Analytical study of hybrid techniques for image encryption and decryption. *Sensors*, *20*(18), p.5162.
14. Alsaffar, D.M., Almutiri, A.S., Alqahtani, B., Alamri, R.M., Alqahtani, H.F., Alqahtani, N.N. and Ali, A.A., 2020, March. Image encryption based on AES and

RSA algorithms. In *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-5). IEEE.

15. SAHWAL, A.K., KISHORE, B., RATHORE, P.S. and Chatterjee, J.M., 2018. An advance approach of looping technique for image encryption using in commuted concept of ECC. *Eureka*, *2581*, p.477X.
16. Dawahdeh, Z.E., Yaakob, S.N. and bin Othman, R.R., 2018. A new image encryption technique combining Elliptic Curve Cryptosystem with Hill Cipher. *Journal of King Saud University-Computer and Information Sciences*, *30*(3), pp.349-355.