Amrita Vishwa Vidyapeetham
Centre for Excellence in Computational Engineering and Networking
Amrita School of Engineering, Coimbatore

Image Encryption Using Chaos Techniques

Prepared By:
J.R.S. Ajay Surya
V. Mohitha
M. Prasanna Teja
P. Sai Ravula

Supervised by:
Dr. Sunil Kumar
Asst. Professor

An End Semester Project submitted to the CEN department as a part of course evaluations of **"21AIE431 - Applied Cryptography"** for B. tech in **Computer Science Engineering – Artificial Intelligence.**

TABLE OF CONTENTS

Image Encryption Using Chaos Techniques

Image Encryption Using Chaos Techniques

1 Abstract

Images are one of the most important and popular forms of multi-media. Along with being stored on devices like phones, CD's, pen drives etc, images are shared across multiple platforms and across the internet. With this kind of large-scale usage of images, the need for providing a secure and efficient mechanisms for securing the media. The conventional algorithms are not suitable for image encryption as images generally have large data capacity and require large computational volume. An efficient algorithm for image encryption is needed to make it difficult for unauthorised users to view or use the images. This report dives into the usage of chaos-based approaches for image encryption. Specifically, we explore the applications of Arnold and Henon map encryption techniques. These methods leverage the inherent chaos of dynamical systems to transform images into unintelligible ciphertext, ensuring data privacy and protection.

2 Introduction

Chaotic systems are a simple sub-type of nonlinear dynamical systems that exhibit chaotic behaviour which is a phenomenon observed in some complex systems where random and unpredictable outcomes arise from deterministic processes. Chaotic sequences are also extremely sensitive to small changes in the initial condition.

A chaos map is a row of random numbers generated by a mathematical calculation with certain initial values. They dictate how a system evolve over time.

"An n-dimensional map is a function that deals with n features."

The chaos-driven image encryption approach comes with many benefits that takes the advantage of characteristics of chaos theory. Some of the properties associated with Chaos related encryption methods are,

- *Sensitivity to initial conditions*, so small changes in the key generates entirely different images.
- Introduction of *non – linearity* making it difficult for the attacker to predict the algorithm.
- *Pseudo randomness* makes the cipher image look like true random sequences.
- Resistant towards *Cryptanalysis*

With the above-mentioned advantages of chaos theory, it can be inferred that chaos related encryption techniques are well suited for image encryption. With this motivation, we are exploring two different chaos methods for image encryption which are widely used even today. In this project, we will implement these two methods and explain their working along with the corresponding results.

3 Objective

This project aims to demonstrate the application of Chaos Encryption techniques in Image Encryption. We will outline the implementation logic for the proposed methods and conduct a comparative analysis to demonstrate their effectiveness in image encryption. In conclusion, we will provide evidence supporting the efficacy of these encryption methods for images.

4 Proposed methods

In many chaos-based image encryption, two fundamental operations are commonly employed: confusion and diffusion. Confusion involves the rearrangement of pixel positions within an image, while diffusion involves altering the intensity values of pixels. Both operations heavily rely on the dynamics of a chaotic map within the encryption process. This project will focus on implementing two well-established Chaos Encryption methods, which leverage the above-mentioned operations:

1) Arnold Cat Map Encryption
2) Henon Map Encryption

5 Arnold Cat Encryption

Arnold Cat Map is a chaotic model which is used to perform Spatial transformations on an image that involves rearranging the pixels of the image according to the map's iterations without changing the pixel value itself (Confusion).

This transformation is applied using the following equation,

$$x' = (x+y) \bmod N$$
$$y' = (x+2y) \bmod N$$

Here, (x',y') are the new positions of the each pixel (x,y) after performing the transformation and N is the dimension of the image.

5.1 Methodology

The methodology of this process is like every other Encryption and decryption method. Following are the implementation logics for Arnold Cat map encryption,

Our process starts by defining the **Arnold Transformation** Function. This is the core part of the entire methodology since it implements confusion logic that is rearranging the pixel positions of the image for a single iteration.

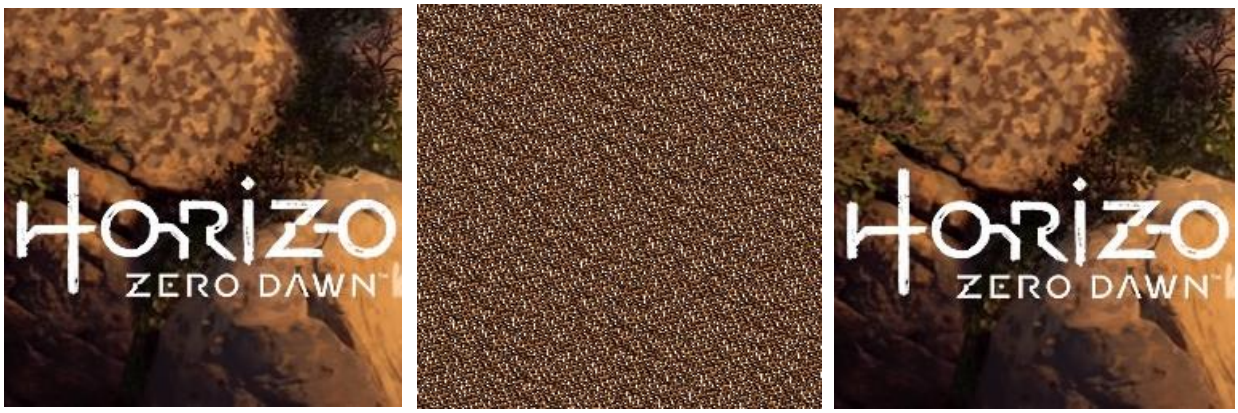
The **encryption function** takes the image and the key as input. This key is the one which denotes the number of iterations of Arnold Transformation to be performed on the image. Now, iterate through the original image by specified number of iterations (key times). Apply the Arnold Transform function in each iteration. Store these new values in a different variable which is our encrypted image.

The **decryption function** takes the encrypted image and the key as input. This involves reversing the transformation applied before. It

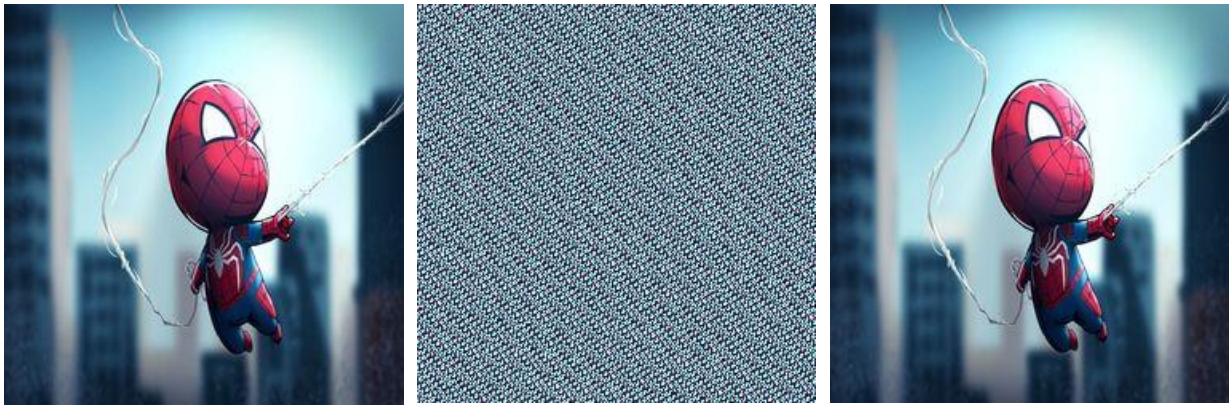
involves calculating the number of decryption iterations based on the image dimension.

5.2 Implementation

Let us see the implementation of the proposed methodology.



Original Image | **Encrypted Image** | **Decrypted Image**



As you can see in the above results, the first image depicts the original image. The middle image clearly depicts the encrypted image that doesn't show any patterns that reveal any information about the original image. This encrypted image illustrates one of the key properties of chaos encryption methods which is pseudo randomness. As you can see the encrypted image is like a complete random

sequence. Also, the decrypted image is as same as that of the original image which proves that our algorithm is working fine.

5.3 Comparison with different key values

As previously discussed, this encryption algorithm should be sensitive to the small changes in the key which means that even a small change in the key should produce an entirely different image. Now, let us test our algorithm by varying the key values.

Key = 19

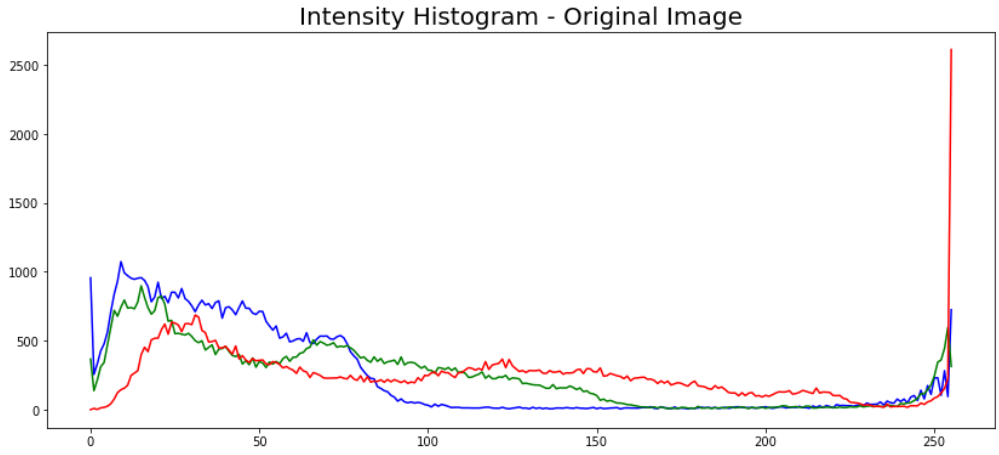
Key = 25

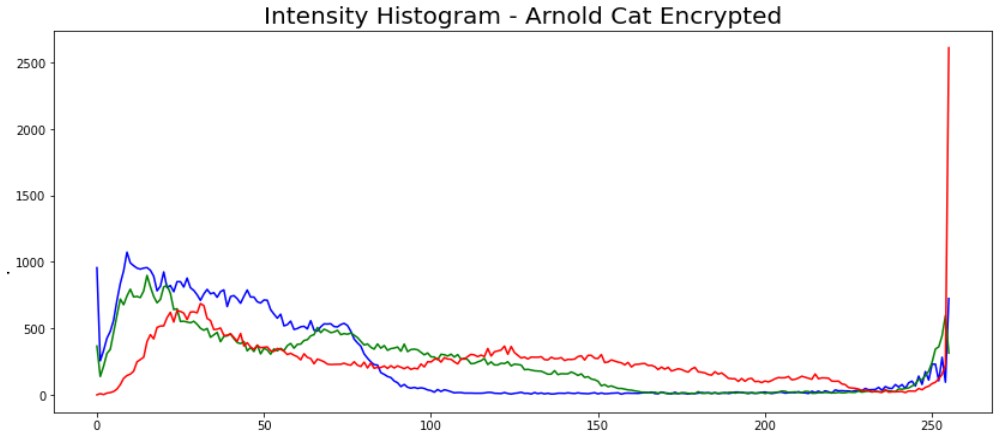
Key = 35

Above are the decrypted images for different key values.

5.4 Histogram Analysis

Histogram analysis on images encrypted using the Arnold Cat Map (ACM) can serve several important purposes in image encryption and security. By analysing the histogram, we can see the intensity distribution of our image and can identify the frequency distribution of our original and encrypted images.





From the above two histograms, we can infer that both the original and encrypted images have the same colour intensity distribution.

5.5 Merits and Demerits of ACM

Some of the merits of the ACM are the simplicity of the algorithm which exhibits chaos behaviour and minimal run time, it does not have complex key management, simple decryption process.

One of the main demerits of the ACM is that this algorithm doesn't change the colour intensity which makes the algorithm vulnerable to Cryptanalysis attacks such frequency analysis. Also, a simple ACM algorithm is vulnerable to brute force attacks since the key value is comparatively small to the keys used in real life scenarios.

So, there is a need for better Encryption algorithm that overcomes the above-mentioned problems.

6 Henon Map Encryption

Henon map encryption is a cryptographic technique that leverages the chaotic behaviour of the Henon map to secure data, particularly images. The Henon map is a nonlinear dynamic system characterized by its chaotic and sensitive-to-initial-conditions nature.

Given initial conditions (x_0,y_0), a Henon map is given by the following equations:

$$x(n+1) = 1 - a * x(n)^2 + y(n)$$
$$y(n+1) = b * x(n)$$

Classical Henon map have values of a = 1.4 and b = 0.3. For the classical values the Henon map is chaotic. The map takes the current state (x(n), y(n)) and maps it to the next state (x(n+1), y(n+1)).

6.1 Methodology

Our methodology starts with defining a function to extract the **image information** that is the pixel values of the original image.

Then we define a function for generating a **transformation matrix** used in Henon map image encryption. The function uses the Henon map equations to produce a sequence of chaotic values. These values are processed into an 8-bit binary sequence, which is then grouped into byte arrays. The function assembles these byte arrays into a transformation matrix, which serves as the core element for encrypting and decrypting images using the Henon map technique. This matrix introduces a pseudorandom, chaotic influence on the image, enhancing its security.

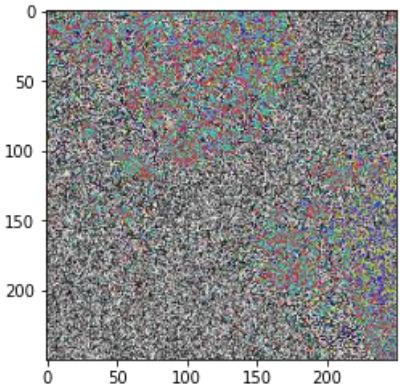
Now we define another function which performs actual **Encryption**. It first retrieves the image matrix that holds the information related to the image. Then, it generates a transformation matrix using the previous function, which is based on the Henon map chaotic system. The function applies a bitwise XOR operation between the transformation matrix and the image matrix, ensuring both diffusion and confusion. This process enhances the security of the image. Finally, the encrypted image is saved in either RGB or grayscale format, depending on the colour information. The function effectively leverages chaos to encrypt the image, providing a robust and pseudorandom encryption method.

Now for the final part, we define another function to perform **Decryption**. It retrieves the encrypted image matrix, its dimension, and colour information. The decryption relies on the same initial conditions or key used during encryption. It reads the encrypted image and generates the Henon map transformation matrix with the specified dimension and key. The function reverses the encryption by applying a bitwise XOR operation between the transformation matrix and the encrypted image matrix. The decrypted image is saved, and its colour format is determined. This function allows the original image to be restored when the correct key is provided, completing the decryption process.

6.2 Implementation

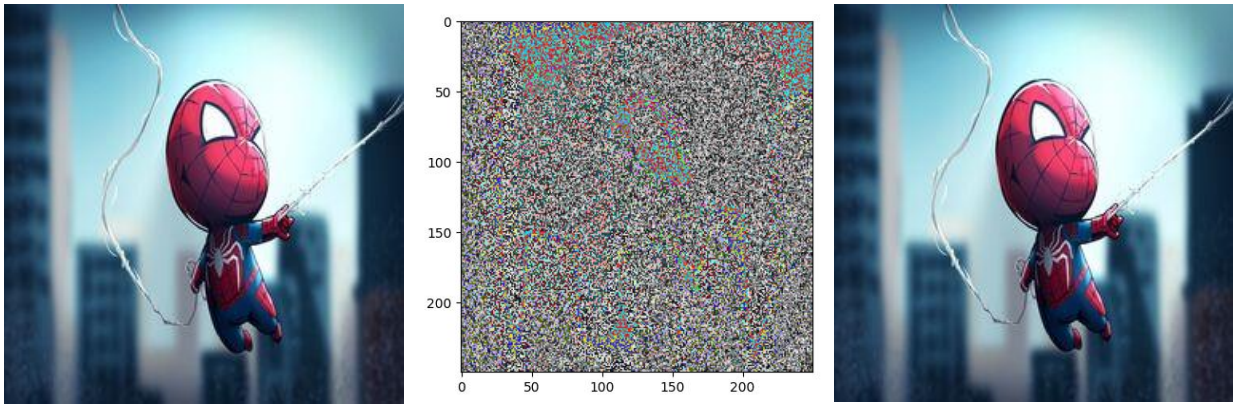
Let us see the implementation of the proposed methodology.

Original Image



Encrypted Image

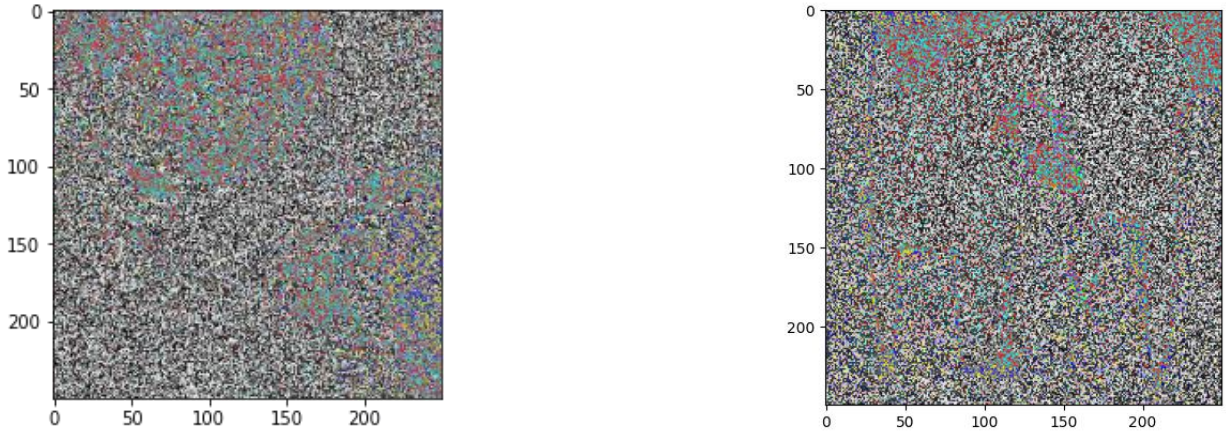
Decrypted Image



As you can see in the above results, the first image depicts the original image. The middle image clearly depicts the encrypted image that doesn't show any patterns that reveal any information about the original image. This encrypted image illustrates one of the key properties of chaos encryption methods which is pseudo randomness.

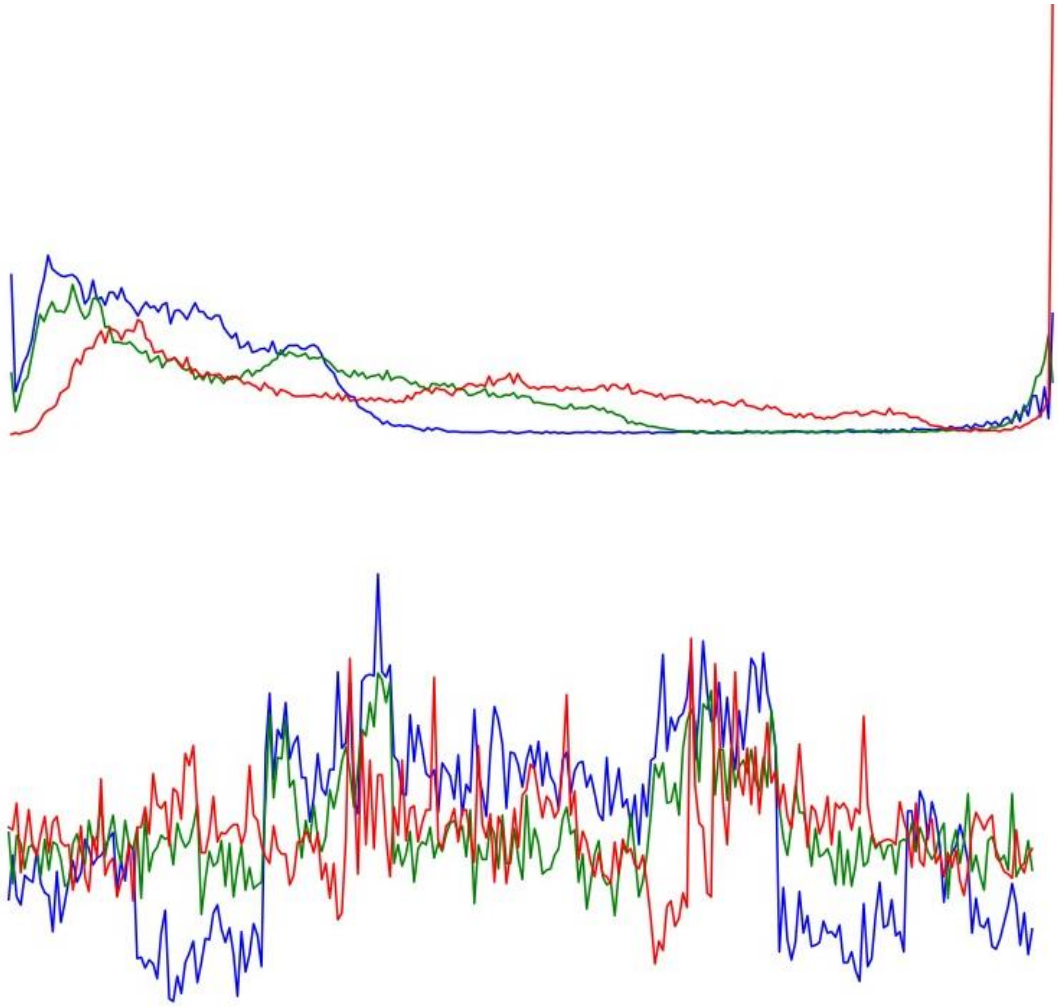
6.3 Comparison with different key values

As previously discussed, this encryption algorithm should be sensitive to the small changes in the key which means that even a small change in the key should produce an entirely different image. Now, let us test our algorithm by varying the key values.



As you can see in the above results, the first image depicts the decrypted image for key (0.1,0.101) and the second image is for the key (0.1,0.104). It is proved that small change in key produce entirely different results.

6.4 Histogram Analysis



The above two histograms are the histograms of original and encrypted image. It is clearly obvious that the encrypted image has very different intensity distribution than that of original image which overcomes the disadvantage of ACM.

6.5 Merits and Demerits of Henon Map

Some of the merits of Henon Map are it provides chaotic behaviour, making it difficult for attackers to predict or reverse the encryption process, it offers a good balance of diffusion and confusion, enhancing security, the method is relatively simple to implement.

Some of the demerits include, Henon map encryption may not provide the same level of security as more complex encryption techniques. The choice of parameters a and b can impact the level of chaos, and selecting appropriate values is critical.

7 Conclusion

In conclusion, the use of chaos-based encryption techniques, specifically Arnold and Henon maps, offers a robust and efficient approach to secure image transmission and storage. These methods provide both diffusion and confusion mechanisms, ensuring the confidentiality and integrity of the data. The Arnold Cat Map rearranges pixel positions, while the Henon Map introduces a colour-shuffling strategy, collectively contributing to the security of the images.

These techniques leverage the inherent properties of chaos, such as ergodicity and non-periodicity, to create pseudorandom properties that enhance encryption strength. Their effectiveness is further underscored by their resistance to cryptanalysis, making them a valuable choice for image encryption.

While Arnold and Henon map encryption techniques exhibit several merits, including simplicity and fast processing, they are not without their limitations, such as the need for secure key management. Nevertheless, their overall effectiveness in securing images makes them compelling options for applications that require robust encryption solutions.