DEERWALK INSTITUTE OF TECHNOLOGY

Tribhuvan University

Institute of Science and Technology

COMPARISON OF DIFFERENT CRYPTOGRAPHIC ALGORITHMS

A PROJECT-II REPORT

Submitted to

Department of Computer Science and Information Technology

DWIT College

In partial fulfillment of the requirements for the Bachelor's Degree in Computer Science and Information Technology

Submitted by

Pradeepti Aryal

20623/075

14th June, 2022

DWIT College

DEERWALK INSTITUTE OF TECHNOLOGY

SUPERVISOR'S RECOMMENDATION

I hereby recommend that this project prepared under my supervision by PRADEEPTI ARYAL entitled **"COMPARISON OF DIFFERENT CRYPTOGRAPHIC ALGORITHMS"** in partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Information Technology be processed for the evaluation.

……

Mr. Bijaya Babu Regmi

Lecturer

DWIT College

Deerwalk Institute of Technology

DWIT College

DEERWALK INSTITUTE OF TECHNOLOGY

STUDENT'S DECLARATION

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

……

Pradeepti Aryal

14th June, 2022

DWIT College

DEERWALK INSTITUTE OF TECHNOLOGY

LETTER OF APPROVAL

This is to certify that this project prepared by PRADEEPTI ARYAL entitled **"COMPARISON OF DIFFERENT CRYPTOGRAPHIC ALGORITHMS"** in partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Information Technology has been well studied. In our opinion it is satisfactory in the scope and quality as a project for the required degree.

……	……..
Mr. Bijaya Babu Regmi Lecturer DWIT College	Mr. Shyam Sundar Khatiwada Year In-charge DWIT College

ACKNOWLEDGEMENT

I would like to express my gratitude to Deerwalk Institute of Technology for providing me this opportunity to explore and work on my concepts. Similarly, I would also like to extend my gratitude to my supervisor Mr. Bijaya Babu Regmi for his encouragement, guidance and support provided during the course of the project.

I would also like to thank my friends for their suggestion and support provided during the development process of the project. Lastly, I would like to thank each and every individual who directly and indirectly helped by providing their suggestions and support in the development process of this project.

Pradeepti Aryal
Roll No.: 20623/075
14th June, 2022

ABSTRACT

Due to increasing use of image in various field, it is very important to protect the confidential image data from unauthorized access. Data Security is primary concern for every communication system. The relentless growth of Internet and communication technologies has made the extensive use of images unavoidable. There are many ways to provide security to data that is being communicated. This Project describes a design of effective security for communication by project in cryptography that involves implementing image encryption using various chaos maps and comparing their merits based on key sensitivity and intensity histograms. The chaos maps implemented were - Arnold cat maps, Henon maps and Logistic chaos maps for encryption and decryption. Chaotic systems are a simple sub-type of nonlinear dynamical systems. They contain a few interacting parts which follow simple rules, but these systems are characterized by a very sensitive dependence on their initial conditions. Despite their deterministic simplicity, over time these systems can display and divergent behavior. Traditional encrypting mechanisms AES and RSA exhibit some drawbacks and weakness when it comes to encryption of digital images and high computing : Large computational time for large images, High computing power for large images. Consequently, there might be better techniques for image encryption.

Keywords: *Chaotic Maps; Arnold cat maps; Henon maps; Logistic Chaos Map; encryption; decryption; images; key*

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1: INTRODUCTION

1.1. Overview

This Project describes a design of effective security for communication by project in cryptography that involves implementing image encryption using various chaos maps and comparing their merits based on key sensitivity and intensity histograms. The chaos maps implemented were - Arnold cat maps, Henon maps and Logistic chaos maps for encryption and decryption.

1.2. Background and Motivation

Cryptography is a method of storing and transmitting data in a form that only those it is intended for can read and process. It is a science of protecting information by encoding it into an unreadable format. It is an effective way of protecting sensitive information as it is stored on media or transmitted through network communication paths. Purpose of cryptography are authentication, integrity, and confidentiality. Traditional encrypting mechanisms AES and RSA exhibit some drawbacks and weakness when it comes to encryption of digital images and high computing. Consequently, there might be better techniques for image encryption.

1.3. Problem Statement

Due to increasing use of image in various field, it is very important to protect the confidential image data from unauthorized access. There is a need for security in digital images, because of faster growth in multimedia technology, internet and cell phones [1]. Image security has become a critical issue. The difficulties in ensuring individuals privacy become increasingly challenging. Various methods have been investigated and developed to protect data and personal privacy. Encryption is probably the most obvious one [2].

1.4. Objectives

The objectives of this project are as follows:

- Encryption of an Image to unreadable format
- Decryption of encrypted image to original image

- Comparison of various chaotic maps algorithms.

1.5. Scope

This helps in sending confidential and sensitive information securely over the internet. Main application of this can be very helpful in Military communication, Forensics, Intelligent systems, Medicine and others.

1.6. Development Methodology

The development methodology used is Iterative model. The iterative methodology starts with a simple implementation of a limited set of software requirements and repeatedly improves the evolving versions until the entire system is built and ready for deployment.

An iterative life cycle model does not try to start with a complete set of requirements. Instead, development begins with the specification and implementation of a small portion of the program, which is then evaluated to discover further needs. This process is then repeated, with each iteration of the model resulting in a new version of the program.

1.7. Outline

The report is organized as follows:

Preliminary Section: This section consists of the title page, abstract, table of contents and list of figures and abbreviations.

Introduction Section: In this section, the background of the project, problem statement, its objectives and scope are discussed.

Requirement and Feasibility Analysis Section: Literature review and Requirement analysis make the bulk of this section.

System Design Section: This section consists of the methodology that was implemented in the project and the system design as well.

Implementation and Testing Section: In this section, the implementation, description of major methods and testing of the system are discussed.

Conclusion and Recommendation: This section consists of the final findings and the recommendations that can be worked on in order to improve the project.

CHAPTER 2: BACKGROUND STUDY AND LITERATURE REVIEW

2.1. Background Study

Chaotic systems are a simple sub-type of nonlinear dynamical systems. They contain a few interacting parts which follow simple rules, but these systems are characterized by a very sensitive dependence on their initial conditions. Despite their deterministic simplicity, over time these systems can display and divergent behavior. Traditional encrypting mechanisms AES and RSA exhibit some drawbacks and weakness when it comes to encryption of digital images and high computing: Large computational time for large images, High computing power for large images. Consequently, there might be better techniques for image encryption. A few chaos based algorithms provide a good combination of speed, high security complexity, low computational overheads.

Moreover, certain chaos-based and other dynamical systems based algorithms have many important properties such as : sensitive dependence on initial parameters, pseudorandom properties and others. The chaos maps implemented in this project are - Arnold cat maps, Henon maps and Logistic chaos maps for encryption and decryption.

2.2. Literature Review

In mathematics, a chaotic map is a map that exhibits some sort of chaotic behavior. Discrete maps usually take the form of iterated functions. Their properties are similar to confusion and diffusion cryptography properties, so they have been used to build good cryptosystems. Furthermore, these properties make chaotic cryptosystems robust against statistical attacks [3]. Several scholars have researched image encryption conduct pixel-shuffling encryption on images by means of encryption algorithm. The method of row, column, and gray-level encrypting enhances encryption security. The security of an image data is different from that of a text file. Because of its intrinsic characteristics, the encryption speed and algorithm simplicity are usually considered to be more important than the absolute security. Chaos theory has already proved that it is an excellent alternative to provide a fast, simple, and reliable image encryption scheme and has ahigh enough degree of security.

The ciphertext image histogram analysis is one of the most straight-forward methods of illustrating the image encryption quality. A good image encryption method tends to encrypt a plaintext image to a random incomprehensible form. Thus, a good image encryption technique generates a cipher image that has a uniformly distributed intensity histogram.

An ideal image encryption algorithm should be sensitive with respect to the secret key i.e., a small change in the key should produce a completely different encrypted image. To test the key sensitivity the we encrypt the plain image with the three algorithms. We then try decrypting them with a slightly changed key.

2.3. Current System

There are many algorithms that can be used for encryption and decryption of images like AES, RSA and these are still being used. But due to some of its drawbacks and weaknesses.

2.4. The problem with Current System

Traditional encrypting mechanisms AES and RSA exhibit some drawbacks and weakness when it comes to encryption of digital images and high computing: Large computational time for large images, High computing power for large images. Consequently, there might be better techniques for image encryption. A few chaos based algorithms provide a good combination of speed, high security complexity, low computational overheads.

CHAPTER 3: SYSTEM ANALYSIS

3.1. Requirement Analysis

The system uses Chaos maps algorithms to encrypt as well as decrypt images. The system encrypts the given image to an unreadable format. The system decrypts the received encrypted image to a readable format. The output of the decrypted image is the same as the original image.

3.1.1. Functional Requirement

The functional requirements are as follows:

- The system shall encrypt the given image to an unreadable format.
- The system shall decrypt the received encrypted image to a readable format.
- The output image shall be same as the original image.

3.1.2. Non-Functional Requirement

The nonfunctional requirements are as follows:

- Encryption should not take a lot of time.
- Decryption should not take a lot of time.
- External factors should not affect the system.

3.2. Feasibility Analysis

3.2.1. Technical Feasibility

The system requires html, css for the front end the python for implementation of algorithms.

3.2.2. Operational Feasibility

A person with basic understanding of computer can easily use this software for encrypting/decrypting image using key.

3.2.3. Economic Feasibility

The webapp will be hosted in localhost i.e., the local machine which will reduce the cost dramatically.

3.2.4. Schedule Feasibility

The project is expected to be completed in the time period of two months.

3.3. Analysis

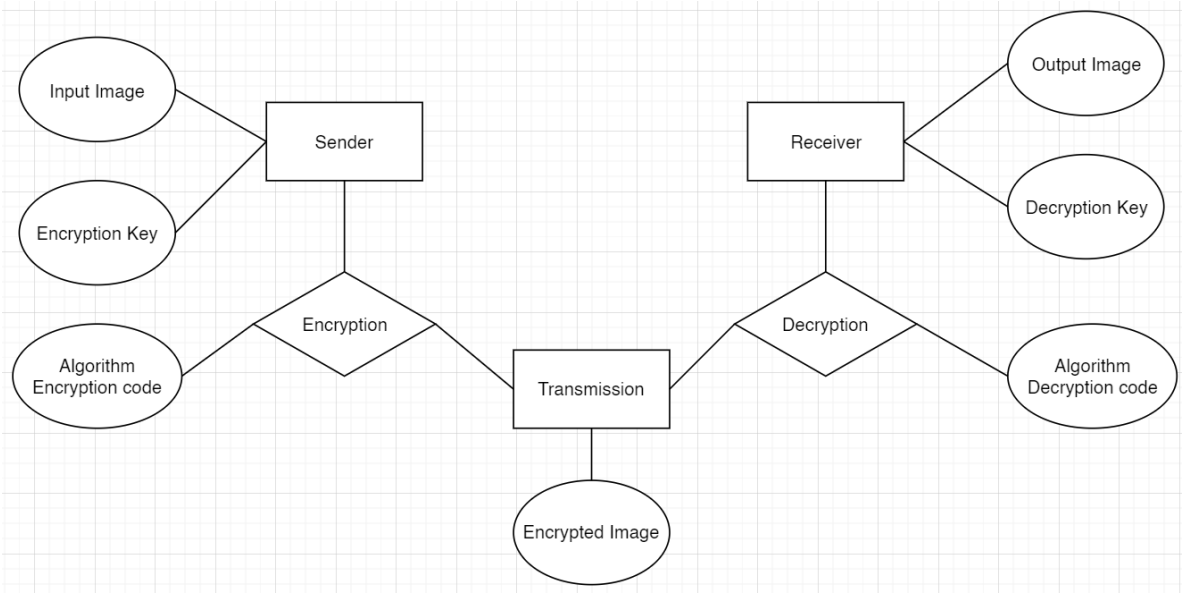

Figure 1 : Data Model represented by ER diagram

REFERENCES

[1] "Image Encryption Using AES Algorithm," Nevon Projects, [Online]. Available: https://nevonprojects.com/image-encryption-using-aes-algorithm/#:~:text=Advantages,encryption%20and%20decryption%20more%20secure..

[2] P. K. P. Radhadevi, "SECURE IMAGE ENCRYPTION USING AES".

[3] R. M. S. S. S. K. Shivangi Das, "A NOVEL ALGORITHM FOR IMAGEENCRYPTION USING LOGISTIC ANDHENON MAPS," [Online]. Available: https://www.academia.edu/6568745/Image_encryption_using_chaotic_maps.