

Enhanced Encryption and Decryption Based On Different Numerical Methods

**Thesis Submitted
in Partial Fulfillment of the Requirements for the
Degree of**

**MASTER OF TECHNOLOGY
in
Software Engineering**

**By
Manish Pandey
(2k22/SWE/10)**

**Under the supervision of
Mr. Sanjay Patidar
Assistant Professor, Department of Software Engineering,
Delhi Technological University**



**Department of Software Engineering
DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Bawana Road, Delhi-110042, India**

May, 2024

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Bawana Road, Delhi-110042, India

CANDIDATE'S DECLARATION

I, Manish Pandey, hereby certify that the work which is being presented in the thesis entitled "Enhanced Encryption And Decryption Based On Different Numerical Methods" in partial fulfillment of the requirements for the award of the Degree of Master of Technology in Software Engineering, submitted in the Department of Software Engineering, Delhi Technological University is an authentic record of my own work carried out during the period from 2022 to 2024 under the supervision of Mr. Sanjay Patidar.

The matter presented in the thesis has not been submitted by me for the award of any other degree of this or any other Institute.

Manish Pandey
Candidate's Signature

This is to certify that the student has incorporated all the corrections suggested by the examiners in the thesis and the statement made by the candidate is correct to the best of our knowledge.

Sanjay Patidar
30/5/24
Signature of Supervisor (s)

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Bawana Road, Delhi-110042, India

CERTIFICATE BY THE SUPERVISOR(s)

Certified that Manish Pandey (2K22/SWE/10) has carried out their search work presented in this thesis entitled "Enhanced Encryption And Decryption Based On Different Numerical Methods" for the award of Master of Technology from the Department of Software Engineering, Delhi Technological University, Delhi, under my supervision. The thesis embodies the results of original work, and studies are carried out by the student himself, and the contents of the thesis do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.


Signature

Mr. Sanjay Patidar

Assistant Professor

Department of Software Engineering

Delhi Technological University

Place: Delhi Technological University, New Delhi

Date: 30/05/2024

ABSTRACT

Encryption is not a novel concept. Instead, it has been in use for thousands of years. The mathematical methods of data security, such as data integrity, secrecy, authentication, and data origin authentication, are studied in this field of study. However, encryption is nothing more than a bundle of methods for encrypting the data, sending it to the right recipient, and allowing this individual to easily decrypt it. In the papers, the methods vary, including numerical, chaos generator, and public key cryptography approaches, while their quality is assessed with statistical tests or through comparison with similar approaches. The articles also discuss the weaknesses and limitations of the methods and claim that some require more exploration to become secure from the attacks.

Keywords: Diffie-Hellman algorithm, encryption, steganography, bisection method, Newton-Raphson method, and fixed point iteration are all examples of cryptography.

DELHI TECHNOLOGICAL UNIVERSITY
(Formerly Delhi College of Engineering)
Shahbad Daulatpur, Bawana Road, Delhi-110042, India

ACKNOWLEDGEMENTS

I would like to express my deep gratitude to my project guide, Mr. Sanjay Patidar, Assistant Professor, Department of Software Engineering, Delhi Technological University, for his guidance, unsurpassed knowledge and immense encouragement. I am also grateful to Prof. Ruchika Malhotra, Head of the Department of Software Engineering, for providing us with the required facilities for the completion of the Dissertation.

I'd also like to thank our lab assistants, seniors, and peer group for their aid and knowledge on a variety of subjects. I would like to thank my parents, friends, and classmates for their encouragement throughout the project period.

Manish Pandey
2K22/SWE/10

Table of Contents

CANDIDATE’S DECLARATION	ii
CERTIFICATE	iii
ABSTRACT	iv
ACKNOWLEDGEMENTS	v
Table of Contents	vi
List of Tables	vii
List of Figures	vii
CHAPTER 1 INTRODUCTION	1
1.1 Overview	1
1.2 Background	1
1.2.1 Cryptography	2
1.2.2 Symmetric / Secret Key Cryptography	2
1.2.3 Asymmetric / Public Key Cryptography	3
1.3 Steganography	4
1.3.1 Text Files	5
1.3.2 Image Files	6
1.3.3 Audio Files	6
1.3.4 Video Files	6
1.3.5 Cryptography vs Steganography	7
1.4 Contributions	8
CHAPTER 2 Literature Review	9
CHAPTER 3 Research Gap	20
CHAPTER 4 Methodology	22
4.1 PROPOSED WORK	22
4.1.2 Decryption algorithm	22
4.1.3 Diffie-Hellman Algorithm	22
4.1.4 Newton-Raphson Method	23
4.1.5 Bisection Method	25
4.1.6 Secant Method	27
4.2 FLOW CHART DIAGRAM	28
CHAPTER 5 Results and Analysis	29
5.1 Results	29
5.2 Time Chart	30
CHAPTER 6 Conclusion and Future Work	33
REFERENCES	34

List of Tables

Table 1: Difference Between Symmetric and Asymmetric Cryptography

Table 2: Difference Steganography and Cryptography

Table3: Summary of literature review

Table 3: Record of Time Taken for Encryption.

List of Figures

Figure 1: Representation of encryption-decryption algorithm

Figure 2: Diffie Hellman Key Exchange

Figure 3: Newton-Raphson Method

Figure 4: Bisection Method

Figure 5: Secant Method

Figure 6: Original Text

Figure 7: Cypher Text

Figure 8 Decrypted Text (Same as original Text)

Figure 9: Time chart for Bisection method.

Figure 10: Time chart for Newton-Raphson method.

Figure 11: Time chart for the Secant method.

Figure 12: Comparison Chart for three methods used

CHAPTER 1

INTRODUCTION

1.1 Overview

Information security is increasingly important in the modern world. With the increasing variety of threats and risks in the digital realm, there is a growing need to find and develop new ways to encrypt sensitive data and information. So, usually, an extra layer of protection is added to the basic encryption/decryption setup with steganography. New transmission technologies, particularly in the field of data communications, necessitate the implementation of a particular security mechanism method. With the volume of data being carried over the Internet, network security is becoming more and more crucial. The most crucial methods for information security are cryptography and steganography. The value of critical data obtained by accessing a system is the main driving force behind attackers' desire to make money from intrusions. Data can be exposed, altered, or tampered with by hackers, or they can utilize it in more complicated attacks.

Combining the advantages of steganography and cryptography into a single system is the answer to this issue. Cryptography is a combination of algorithms indexed by keys and used to encrypt and decrypt messages[1]. From Shannon. Plaintext refers to the original information that is intended to be secured by encryption. The process of converting plaintext into ciphertext, also known as ciphertext occasionally, is known as encryption. The opposite operation, decryption, extracts the text from the encrypted material. The degree of keys required for encryption/decryption is used to characterize encryption techniques, which are then further classified by application and use.

1.2 Background

Information can be protected using cryptography or steganography, which either use keys to encrypt or hide the information. That means the data can be encrypted using steganography or cryptography[2] and then used to protect or hide important data or information. Therefore, various encryption and decryption techniques are essential to protect the data or information in real life. Security is improved when these two methods are used in a single system. It is useful to outline these techniques and go over their benefits.

1.2.1 Cryptography

Cryptography is one of the more well-known methods for safeguarding the confidentiality of communications between parties. This method converts text into ciphertext by encrypting it with a key that is shared between parties over an insecure channel. A valid key is used to decrypt the ciphertext back to the original plaintext. Nobody can access the plaintext unless they know the key. Many of the components required for secure communication via unsecured networks, including B: Data protection, authentication, non-repudiation, and secrecy key exchange. The cryptosystem is visualized in Fig 1.

Mainly there are two types of cryptography for protecting data. Hash functions, public-key cryptography, and private-key cryptography are commonly used techniques to achieve their objective[4]. The kind of encryption algorithm is dependent on the key type and length employed. In the given figure, we can see that the data is transmitted to the receiver through encryption and decryption, and the data is cipher text. When the user transmits data to the receiver, first the user tries to encrypt the data or information into the cipher text, and the user also has keys so that the receiver can decrypt the information with the help of the key, the receiver can easily get the data which the sender sent.

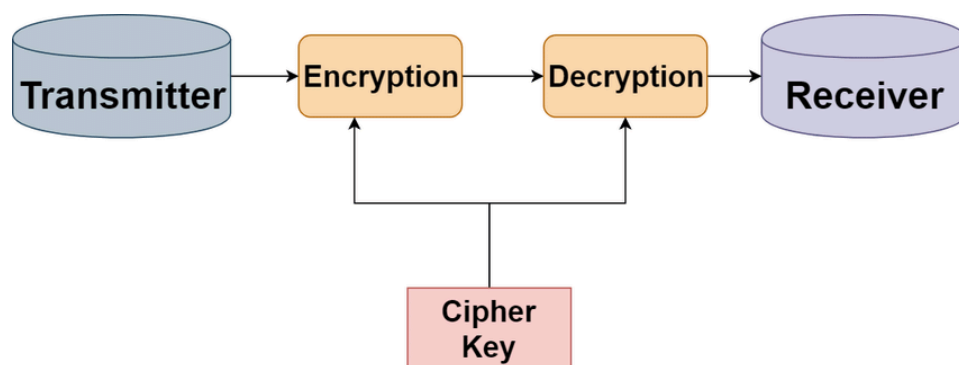


Figure 1: Representation of encryption-decryption algorithm

1.2.2 Symmetric / Secret Key Cryptography

Known also as secret-key cryptography, symmetric-key cryptography, shared-key cryptography, and single-key cryptography. Private key technology is used to encrypt and decrypt private data. The original data, or plaintext, is

encrypted using the sender's key. The recipient decrypts the message and obtains her plain text using a similar key. The key is known only to those authorized to encrypt/decrypt. However, while this technique provides good security for transmission, key distribution is problematic. If someone steals or probes your key, they can easily get your entire data.

In other words, a symmetric key is a type of cryptography where data or information is encrypted and decrypted using one key, or the same key. The key must be securely exchanged by the sender and the recipient. It can handle higher encryption volumes and is faster than asymmetric key cryptography. Popular symmetric/secret key encryption techniques include DES (Data Encryption Standard), 3DES, and AES (Advance Encryption Standard).

It is mostly utilized in situations where data must be encrypted and decrypted, such as storage, database encryption, and secure communication.

1.2.3 Asymmetric / Public Key Cryptography

This technique is sometimes referred to as an asymmetric or public key cryptosystem. Two separately used, mathematically related keys are used for both data encryption and decryption. Once a private key has been used with this method, it is impossible to find the other key or access its contents. All keys are required to operate the technology. The decryption key is kept private and is referred to as the private key, whereas the encryption key is kept openly and is known as the public key.

In other words, an asymmetric key cryptosystem uses two different keys, a public key and a private key. The public key is shared publicly and used to encrypt data, while the private key is kept secret and used to do the exact opposite: decrypt data. In this case, the messages get encrypted using the receiver's public key – but the only key that can decrypt them is the receiver's private key. Asymmetric key cryptography relies on a number of algorithms that are commonly used. These include:

1. RSA(Rivest-Shamir-Adleman): One of the most used public key cryptosystems EFF weighting: it is second in its usefulness today. For information security, high-assurance communications, digital signatures and short informational blocks, This cryptosystem is among the most used.
2. ECC (Elliptic Curve Cryptography) uses elliptic field curves over finite fields. It is more secure than RSA, although it employs shorter key sizes.
3. DSA(Digital Signature Algorithm): These algorithms are used for encryption or decryption and also for digital signatures, which provide confirmation of the integrity and origin of data.

4. Diffie-Hellman: This method is not directly used to encrypt or decrypt data or information; It makes it possible for two people to safely exchange a secret key via an unsecured connection. Symmetric encryption can then be performed using the shared key. This algorithm is also very fast at encrypting data or a very large amount of data, which is better than most algorithms.
5. ElGamal: This algorithm totally depends on Diffie-Hellman and is used for both encryption and digital signatures. It maintains the confidentiality of data or information.

Characteristic	Symmetric Cryptography	Asymmetric Cryptography
Key used for encryption/decryption	Same key is used	One key is used for encryption and another for decryption
Speed of encryption/decryption	Very fast	Slower
Size of resulting encrypted text	Usually same as or less than the original plaintext size	More than the original plaintext size
Known keys	Both parties should know the key in symmetric key encryption	One of the keys is known by the two parties in public key encryption
Usage	Confidentiality	Confidentiality, Digital signature

Table 1 Difference Between Symmetric and Asymmetric Cryptography

1.3 Steganography

It is known as the science of secretly delivering data across ostensibly reliable carriers to cover up its existence. As a result, it is unaware that the message even exists. When a user observes a cover that conceals data, he would not be aware that the cover contains data and would not make an effort to understand it. A Stego system encoder can insert sensitive data onto cover media by using a specific algorithm. A picture, ciphertext, bitstream of plaintext, or any other type of data could constitute a secret message. Once the covert data has been implanted, the covered object is referred to as a stego object. The decoder system uses the same stego procedure to choose the right channel to stego the stego object in order to retrieve the original information. Additionally, the recipient receives it. due to the sender's desire to forward it[9].

Steganography is a technique for concealing information from discovery inside regular files or messages. Secure data can be included in text documents, audio files, video files, and image files. The main goal of steganography is to safeguard the

secret message, which is completely undetectable to anybody but the sender and recipient.

Steganography methods range from very simple, like writing to an invisible file within another file, to more complex methods involving image or video files. It provides an additional layer of encryption of data or information so that the other third parties cannot be involved in this layer. It is commonly used for secure communication and information protection in different fields, including military communication and personal communication.

For example, a secret message or data is hidden in the images, audio files, and video files so that our data will be secure and easily transmitted to the receiver. This makes it different from encryption, which collects a message so it cannot be read or written but does not hide the fact that there is a message. Overall, steganography is a method in which a secret message is hidden on the cover of media or files. It is the idea to prevent secret data by creating suspensions. The forms of steganography are Audio, Video, and images. Steganography is the practice of concealing messages, files or images within another file, messages or image or audio or video. Later, we will extract it at its destination. It is derived from the Greek words *stegano*, meaning covered or hiding, and *graphia* which means writing. Steganography is different from cryptography, but using them together can improve the security of protected data or information and prevent the detection of secret communication. Basically, in Cryptography, we make the data unreadable, and in steganography, we hide the existence of data or information. The user would not be aware that a cover containing data exists and would not attempt to understand it when he saw one. By applying a particular algorithm, a Stego system encoder can inject sensitive data onto cover media. A picture, ciphertext, bitstream of plaintext, or any other type of data could constitute a secret message. There are various types of steganography, including text, image, audio, and video data.

1.3.1 Text Files

Text steganography is the term for the technique of hiding sensitive data inside text. Because this file format can only contain text files, text steganography uses extremely minimal memory. It enables quick file exchange or communication between the sender and receiver. In text steganography, the data or information hidden by text is called text steganography. Let's use an example to better understand. Let's say you have to convey the hello message using text steganography. In such case, you can write it as a poem or as a full text message, with H standing for "hope you are doing well today," e for "everything is good," and y for "you are great."

Overall, The process of disguising data or information in text format so that it can be transferred via a communication channel risk-free is known as text steganography. Text steganography's primary goal is to transfer information covertly and unnoticeably.

1.3.2 Image Files

This is the technique of inserting data into an image's pixel structure, which makes an attacker unable to spot changes to the cover image. Popular image steganography algorithms include the LSB technique. In image steganography, the data or information hidden by image files is called image steganography. There are a few techniques which are used in image steganography:

1. Least Significant Bit (LSB): This is a very important technique used in image steganography. It changes the last bits of some of the pixels in an image to encode private data or information.

2. Masking and Filtering: This is a very important technique used in image steganography. It changes the data or information into some watermark pattern. This method is very difficult to detect and remove.

3. Redundancy-Based Techniques: This is a very important technique used in image steganography. It changes the secret data or information into a redundant pattern of colours. This method is very secure and difficult to detect and remove.

The above techniques are very useful for image steganography. All these methods are used in real-life problems to efficiently protect data or information.

1.3.3 Audio Files

This is how information is hidden in the voice. Confidential information can be hidden in audio recordings in a number of ways. Consider phase coding. In this steganography, the data or information is converted into an audio or recorded form. Audio steganography is a very important technique for protecting data or information.

1.3.4 Video Files

It is a method for encrypting private data included within a video file's frames. In this steganography technique, data or information changes to video format

or picture video format so that it is secure or protected from unauthorized persons. So, this method is very useful in steganography.

1.3.5 Cryptography vs Steganography

Table 2 illustrates the distinctions between cryptography and steganography based on many criteria. The basis for comparisons is definitions, targets, carriers, input files, keys, visibility, security services offered, attack kinds, attacks, repercussions, and applications.

Criteria/Method	Steganography	Cryptography
Definition	Cover writing	Secret writing
Objective	Maintaining existence of a message secret ,Secret communication	Maintaining contents of a message secret ,Data protection
Carrier	Any digital media	Usually text based
Input file	At least two	One
Key	Optional	Necessary
Visibility	Never	Always
Security services offered	Authentication, Confidentiality, Identification	Confidentiality, Identification, Data Integrity and authentication Non- repudiation
Type of Attack	an aim of finding whether it is stego file or not	Cryptanalysis
Attacks	Broken when attacker reveals that steganography has been used. known as Steganaly- sis.	Broken when attacker can understand the secret message. known as Cryptanalysis
Result	Stego file	Ciphertext
Applications	Used for securing information against potential eavesdroppers	Used for securing information against potential eavesdroppers

Table 2 Differences Steganography and Cryptography

The basic difference between Cryptography and Steganography is that cryptography is used for secret writing, and Steganography is used for cover writing. Cryptography means changing normal text into cipher text so that third parties cannot detect the actual data or information. In steganography, the data is converted into different forms, such as an audio file, a text file, a video file, or an image file.

Cryptography is used to secure information against potential eavesdroppers, and steganography is used to secure information or data against potential eavesdroppers.

Encryption Cryptography is one of the more well-known methods for safeguarding the confidentiality of communications between parties. Using a shared key that is encrypted across an unsecure channel, this method turns text into ciphertext. With a functional key, the ciphertext can be decoded and returned to the original plaintext. Steganography is a method used to hide data from being found in ordinary files or messages. Secure data can be included in text documents, audio files, video files, and image files.

Stated differently, the main goal of steganography is to safeguard the secret message, which is completely undetectable to anybody but the sender and recipient.

1.4 Contributions

1. The function $f(x)$ used to generate the ciphertext is only used to illustrate the use of numerical methods. In practice, much more complex one-way functions are used.
- 2 . Intended for communication between two users only. Conveniently, this algorithm can be run in a circular fashion for multiple users.
3. Tolerance is assumed to be 0.001 for all numeric methods.
4. This work aims to investigate Secant, Bisection, and Newton Raphson's numerical root-finding model for data encryption and decryption.
5. Compare and find the best one of the three root-finding methods.
6. Overall, this study's primary goal is to numerically apply the secant, bisection, and Newton Raphson methods. From there, it will identify the root of the provided equation—which represents the messages' ciphertext—and compare the approaches to determine which one will provide the fastest encryption.
7. In general we are comparing all these three numerical methods.

CHAPTER 2

LITERATURE REVIEW

In this section, we describe the various studies done by researchers in numerical-based encryption-decryption methods.

Abdelrahman Karawia et al.[1] presents a new image encryption technique that makes use of the General Bischi-Naimzadeh Duopoly System and the Newton-Raphson method. The Newton-Raphson procedure is used in the algorithm to shuffle plain images in rows and columns, while the dispersed image pixels are implemented using General Bischi-Naimzadeh Duopoly System. Therefore, this paper offers a viable image encryption method that can be utilized to secure personal image data.

D.I. George et al.[2] The article discusses the challenges of image encryption. It offers a new secure and efficient algorithm for encrypting and decrypting images using public key cryptography based on Magic Rectangle (MR). Instead, the proposed technique splits the original image into single-byte parts, which MR then replaces. The process of encryption involves several public key encryption methods like RSA El Gamal, among others, with randomly selected MR control scenarios. From the test results, this method of encryption is viable and can correctly encrypt and decrypt images through multiple secret keys. This method will produce ciphertext that is safe to send over the internet and is entirely different from the original image file.

Priyajit Biswas et al. [3] propose a non-chaotic picture encryption technique in their study that defines a pseudo-random sequence with a polynomial. There are two stages to the suggested approach: distraction and spread. Using the created pseudo-random sequence, rows and columns shift in a cyclical confusion phase. Value station adjustments to the pixel intensity values are made during the diffusion phase, and then repetitive XOR operations take place. The final step involves creating the encrypted image using a pseudo-random series masking technique. The security and computing complexity of the proposed method are compared with a few different approaches. The presented findings demonstrate that the suggested approach to fighting against differential assault performs better than earlier methods. The paper also discusses potential flaws and downsides in the suggested method, like its sensitivity towards the size of the key space and potential attacks on the polynomial equation that generates the pseudo-random series. All these things

considered, this study report offers a straightforward and efficient non-chaotic picture encryption method that works with a variety of picture formats. More research is required to address potential flaws and enhance its resilience against attacks.

Aesha N et al.[4] used a 1-D piecewise chaotic map and a bisection method which is based on image/picture encryption attacking approach. The bisection method algorithm is primarily used during the shuffling stage of line shuffling when chosen spots are filled with polynomial values to produce a pseudorandom series. Diffusion and permutation are the two stages of this method-based encryption attack, which is based on the permutation-substitution model. A single series is used to frequently update the susceptible picture. A bitwise XOR operation is used to apply a mask created using a Tent chaotic map to the modified object to obtain the image and enhance its information security. The experimental outcome demonstrated the model's efficacy in preventing attacks.

Following the same approach, Inaam Razzaq et al. [5] used a strategy based on the permutation-substitution paradigm. It is divided into two phases. The first one is diffusion, and the second one is a permutation. The permutation phase used the bisection approach. It produces a random sequence when specific polynomial values are placed at particular spots. The basic image is generated using this random sequence. Through a bitwise XOR operation that originates from the tent, the X-axis of the tent's chaotic map creates a mask that is utilized in an XOR operation with the shuffled image. To improve the method's security, any one of the two values derived from the formula can be altered using a chaotic mapping process.

Keyvan et al. [6] also worked on the same strategy of the bisection method and 1 D piecewise chaotic map. Intervals from the bisection approach are periodically applied to polynomial values at precise positions in the permutation stage to generate a pseudo-random sequence. Then, simple images are combined using this sequence. To increase the method's security, the shuffled picture is put to a bitwise XOR operation at the diffusion step using a mask created from the Tent chaotic map. Experimental results and numerical simulations validate the algorithm's resilience to attacks; additionally, its efficacy is evaluated statistically and contrasted with competing algorithms.

Akif Akgul et al. [7] introduced a novel encryption method for text. It was based on chaos generators and chaotic nonlinear equations, which increased communication security. Three sophisticated and efficient 1-D chaos generators that generate the cypher required for encryption and decoding are the Logistic Map, Pinchers Map, and Sine-Circle Map. The encryption technique's effectiveness was evaluated using

Shannon entropy and time. The findings of the experiment indicate that the encrypted content's entropy value rises.

Arab A et al. [8] introduced a novel image encryption method. The advanced encryption algorithm, or AES, and the chaos system served as its foundations. This work generates the encryption key using the Arnold chaos sequence. Next, the principal image is encrypted using state-of-the-art encryption standards utilising the round keys produced by the chaotic system. Basically what has happened in AES is that column substitution and integration operations have been changed to become linear conversion and pixel values summing, respectively, resulting in an AES with ten rounds of encryptions in total. These techniques reduce the time complexity of CCAES making it stronger against differential attacks while at the same time enhancing its diffusion capabilities.

In [9], Yin Q et al. developed a novel image encryption algorithm. In this case study, we propose a more sensitive chaotic image cryptosystem for improving security as well as sensitivity through dynamic diffusion and breadth-first search. A breadth-first search is used to browse the plain image during the permutation phase. In his article, he looks at the challenges associated with photo encryption.

It presents a novel algorithm for security. During the permutation phase, a breadth-first search is used to navigate the plain image. The entire permutation is then carried out to provide a shuffled sequence. Similar to this, breadth-first search is used to rearrange the diffusion key stream. Moreover, a dynamic diffusion method is proposed to encrypt the shuffled sequence at the diffusion step. This can increase the cryptosystem's sensitivity and ensure that every encrypted pixel is linked to every other encrypted pixel. This method's hyper-chaotic mechanism generates pseudorandom sequences at every stage. The performance study and simulation results show how effective the recommended scheme is as well as how safe it is from brute-force, statistical, and differential attacks.

Askar, S et al. [10] Various techniques that are structured to encrypt and decode images have been presented in the literature. This work proposes a robust method based on pixel shuffling and a one-dimensional chaotic economic map for picture encryption and decryption. The suggested method is constructed from multiple photographs. The security and effectiveness of the proposed method are evaluated in terms of key space, key sensitivity, correlation between two neighbouring pixels, information entropy, contrast, and differential attack. Not many of them are based on chaotic systems with chaotic bifurcation paths. They have benefits and drawbacks in terms of security and processing speed. The observed experimental data indicates that the proposed method has a large key space, high sensitivity to the secret key, very low correlation coefficients, strong information entropy, and high contrast. In

the end, the experiments confirm that the proposed approach is highly effective in defending against statistical and differential attacks. The obtained results of our proposed algorithm have shown how sensitive the algorithm is to initial conditions. This indicates that the picture is negatively impacted by the chaotic map's parameters that were utilized in the method. A decrypted picture that lacks information about the original plain image results from even little adjustments to certain settings. Additionally, the method has demonstrated a good level of security against many kinds of attacks using huge space keys.

Karawia A. et al. [11] came up with a new image encryption method. In order to improve encryption efficiency and enable the secure transmission of many images inside a single band through the use of a spatial scanning mechanism, this work presents an encryption technique for multiple photos that combines a two-dimensional economic map with a mixed image element (MIES). It can prevent hackers from succeeding because of its enormous number of key space sizes. In addition, the suggested technique outperforms all existing algorithms in the literature in terms of encryption results. Similar algorithms are compared with the proposed algorithm. The results of the experiment demonstrate the safety and efficiency of the recommended algorithm. Initially, the original images are grouped into a single large image that is further divided into multiple pure image elements (PIES); subsequently, the logistic map is used to shuffle the PIES; third, it is combined with the sequence produced by the two-dimensional economic map to obtain MIES; and finally, the MIES are gathered into a single large encrypted image that is further divided into multiple images of the same dimensions as the original images. Numerous sectors, including weather forecasting, the military, engineering, health, science, and personal concerns, can benefit from its use. This study presents a simulation of the suggested concept using identically sized grayscale photographs. The suggested concept will be used on grayscale photos of various sizes in the future.

Askar S et al. [12] introduced a novel image encryption method. Numerous picture encryption techniques have been developed based on various chaotic maps in the literature. Even if such algorithms perform well in the cryptographic process, further advancements are still required to raise the level of security that they enable. This work presents a novel encryption technique that relies on a two-dimensional chaotic economic map that is logistic in nature. Part of the implementation and security of the method is investigated through statistical studies, including sensitivity to the key space, pixel correlation, the entropy process, and contrast analysis. Based on the study findings and comparisons made, we have determined that the provided approach is characterized by a vast space of key security, sensitivity to the secret key, few coefficients of correlation, a high contrast, and acceptable information of entropy. Moreover, experimental results show that our suggested method is resilient

to statistical, brute-force, noise, and differential attacks. By applying the proposed approach to a variety of picture types, its resilience is demonstrated. The results of using the proposed method show that the ciphered image appears to be random since the 256x256 cypher image's information entropy is almost equal to the theoretical value of eight, its RSA is almost 99.6%, and its RSA is almost 33.4%. As such, our system becomes extremely sensitive to even the smallest change to the original image. The results collected imply that the proposed system has a high level of security and can withstand attempts by hackers to compromise it.

Karawia A et al.[13] introduced an innovative method of image encryption. For picture encryption techniques, some researchers employed different chaotic economic maps (CEMs). The simple image's rows and columns are first shuffled using it. Second, the shuffled image's pixels are confused during the substitution step by using the 3DCEM. The suggested technique is used with a variety of picture formats. To verify the suggested algorithm's performance and security, several measurements are made. Furthermore, experimental findings and numerical simulations have been used to confirm that the suggested method is capable of withstanding various forms of assault. It gives the E-FYS-3DCEM algorithm priority in order to repel attacks. Based on the simulation findings, it can be concluded that the E-FYS-3DCEM approach has a high sensitivity for the security keys. This means that any small adjustment or consideration of the actual value of the security keys will not be able to restore the plain picture. Additionally, the E-FYS-3DCEM technique indicates that the cypher image has information entropy close to 8, NPCR, and UACI close to 99.6 and 33.4%, respectively.

Wu X et al. [14] introduced a novel image encryption method. The four processes that make up the picture cryptosystem that is being given are the pixel-level diffusion process, the DNA sequences diffusion process, the confusion process for DNA sequences, and the key stream generation process. The pseudorandom key streams are generated in the first step by combining the information entropy of the plain image with two straightforward enhanced chaotic systems. The third step diffuses the jumbled DNA matrices in a row and column pattern using key streams and DNA XOR. After the DNA matrices are transformed into the encrypted image using the DNA decoding rules, a ciphertext diffusion in a crisscross pattern is further used to further boost the security and sensitivity of the cryptosystem. After the DNA grids are converted into an encoded image by using DNA rules, we utilise a crisscross pattern to further jumble the secret code in order to increase the security and sensitivity of the cryptosystem. To make the picture secret, we make key codes using messy systems and regular pictures. This keeps the secret picture and the keys very secret. According to the DNA rules, the first picture changes into DNA grids. Then, the key codes mess up the DNA grids. After that, the mixed-up DNA grids spread

out by rows and columns by blending in the key codes. In the end, the DNA rules turn the spread-out DNA grids into the secret picture. This way of making the picture secret holds onto the picture's good quality as it gets encoded. So, we think this way of making a picture secret is perfect for sending pictures in real-time.

Wu, X and others [15] made a new way to hide images. In this study, a new way to hide color pictures is put forward. It uses the 2D wavelet change and a 6D wild system. Unlike other picture hiding ways, our plan uses the 6D wild idea and 2D wavelet change in both sound and space parts, where the secret streams rely on the plain picture and the wild system. Using the 2D wavelet change, the plain picture is first cut into four picture parts in the plan. Then, a secret stream changes the parts and a number makes them smaller. After that, the four hidden picture parts use the 2D back change to make a middle image. Lastly, another secret stream is used to change the middle image's dots to make it safer. First, the plain picture is cut into its parts using the 2D Haar wavelet change. Next, a secret stream mixes these parts and makes them smaller. In the next part, we use the 2D back Haar wavelet change to get a middle picture. To further improve security, another key stream modifies the intermediate image's pixel values. The results of the performance study and testing have shown how effective and safe the recommended encryption system is. Our tactic also involves resistance against cropping attacks. Thus, using the recommended technology for real-time encryption and transmission is secure.

Ivanov, G. et al. [16] introduce a novel cryptography encryption method. In the last several years, a great deal of research has been done on the cryptographic characteristics of S-boxes and their many designs. Algebraic constructs, pseudo-random generation, and heuristic methods are methods for generating S-boxes. In this paper, we propose an S-box generation technique that combines a special kind of artificial immune system known as the clonal selection algorithm with a slightly modified version of the hill-climbing method for S-boxes. With our original method, we generate large sets of highly nonlinear bijective S-boxes with poor differential uniformity in a reasonable amount of time.

Jia N et al. [17] introduce a novel encryption method Based on Chaos and ECC. A novel encryption method with reduced memory use and processing time is represented by the chaotic encryption algorithm. However, because of the computational precision of hardware processing, chaotic sequences will result in a short-lived event, which raises security concerns. In this study, we use the one-dimension Logistic Sequence to process the plaintext and provide the first degree of security. Next, we provide the second level of protection using the optimised ECC encryption approach. The experiment can demonstrate that the encryption/decryption system is feasible and that, following the decryption

procedure, the message remains impartial and identical to the input. It can guarantee data integrity and demonstrate the algorithm's viability. The approach we suggested takes a bit longer to complete than a single ECC, but it offers a greater level of security with the same key size. By making the key larger, it prevents resource use. Therefore, as compared to a single ECC, we believe it saves time while maintaining security.

Hayat U et al. [18] introduce a brand-new elliptic curve-based encryption method. There are two goals for this paper. First, we present new methods for constructing substitution boxes (S-boxes) and generating pseudo-random numbers (PRN) by using a total order on an elliptic curve (EC) over a prime sector. Rather than using the computationally expensive group law that is more conventional, an efficient search approach is employed to create an EC. The S-box generation approach uses the x-coordinates of the points on an ordered elliptic curve (OEC), and an OEC's points are utilized to generate PRN by means of a generalization of the Frobenius map and the n-norm. Second, a two-phase picture encryption approach is proposed based on the recently developed PRN-generating and S-box methods. This article proposes a hybrid picture encryption method using an ordered elliptic curve (OEC) and pseudo-random numbers (PRN) based on a dynamic S-box. S-boxes are produced using the OEC's x-coordinates and the modulo 256 operation, whereas PRN is built on an OEC using the n-norm and ideas from a generalized Frobenius map. Developing a method to employ the suggested technique to encrypt a colour image in a single round without increasing computer complexity.

A unique encryption strategy based on a new hyperchaotic finance system is introduced by Tonga X et al. [19]. Based on a chaotic financial system, this work provides a novel four-dimensional hyperchaotic finance system. The key sequence is produced by comparing chaotic sequences, which are generated using the Runge–Kutta technique. Regarding plaintext, the key sequence is utilized for picture encryption. Numerous evaluations of the encrypted image's histogram, unpredictability, and information entropy reveal that the novel hyperchaotic system is extremely sophisticated and secure. In this study, we build a novel four-dimensional hyperchaotic system by adding a nonlinear term to the chaotic financial system. Next, we examine the fundamental dynamic features of the system and employ the Runge–Kutta technique to produce a chaotic sequence. In picture encryption, the sequence linked to the plaintext is utilized. Many security checks are carried out. The test results demonstrate the algorithm's ability to withstand differential, known plaintext, and statistical attacks. The ciphertext sequences are very secure and passed the SP 800-22 tests. Furthermore, there is adequate room in the key area to fend off brute-force attacks.

Guo H et al. [20] The proposed system is based on a pipeline design of an Analog-to-Digital converter (ADC) modified to operate as a set of piecewise-linear chaotic maps. The evolution of each map is monitored and quantized to provide a random bit stream. The suggested circuit can be readily created by rearranging an existing pipeline ADC, making it ideal for embedding in cryptographic systems such as smart cards. The two prototypes had throughputs of 40 Mbit/s and 100 Mbit/s, respectively, and were designed in 0.35- μm and 0.18- μm CMOS technology. The measurements demonstrate orders of magnitude faster operating speed at the same quality level when compared to similar high-end commercial systems.

TABLE 3
SUMMARY OF LITERATURE REVIEW

AUTHOR NAME AND REFERENC E	DATE OF PUBLICATI ON	ADVANTAG ES	DISADVANT AGES	METHOD USED
Abdelrahman et al.[1]	Dec'2020	sensitive image content.	Taking more time.	Newton-Raph son Method and General Bischi-Naimz adah Duopoly System
D.I. George et al.[2]	Oct'2015	Efficient, secure image	No comparison to existing methods	Cryptography based on MR
Priyajit	Aug'2020	Better	Sensitivity to	Bisection

Biswas et al.[3]		immunity against differential attack.	the key space size and vulnerability to attacks on the polynomial function.	method
Aesha et al.[4]	Mar'2021	Secure algorithm based on bisection and chaotic map	Limited evaluation and comparison with existing algorithms.	Bisection Method and One-Dimensional Piecewise Chaotic Map.
Inaam Razzaq et al.[5]	Nov'2017	Enhanced security applicable to various networks	Limited applicability	Bisection Method
Keyvan Derakhshan et al.[6]	Mar'2014	Provides a useful introduction to essential concepts in information security and includes a case study.	Lacks in-depth analysis and maybe too basic for advanced readers.	Newton-Raphson Method
Akif Akgul et al.[7]	2015	New method proposed for text encryption using Chaos generators.	no real-world implementation example.	One-Dimensional Chaos Generators and Nonlinear.
Arab A et al.	May'2019	Strong	More	Chaos

[8]		Against Variational Assaults	Complexities. In implementation.	Sequence and AES Algorithm.
Yin Q et al. [9]	2018	High security and high sensitivity	More Complexities. In implementation	Dynamic Diffusion and BFS.
Askar, S et al. [10]	Jan '2018	Very Strong entropy.	Maintenance complexities.	1-D chaotic economic map.
Karawia A. et al. [11]	Oct'2018	Very large key space and more security to protect the data and information	More Complexities. In implementation	2-D chaotic economic map.
Askar S et al. [12]	Jan' 2019	High security, high sensitivity, and Very large key space and more security to protect the data and information	More Complexities. In implementation.	2-D logistic chaotic economic map.
Karawia A et al. [13]	Seot'2019	Very large key space and more security to protect the data and information	Sensitivity to the key space size and vulnerability to attacks on the polynomial function.	3-D chaotic economic map and CEMs.

2.1 CONCLUSION OF LITERATURE REVIEW

1. There are many algorithms to enhance encryption, but my project aims to implement a symmetric encryption-decryption algorithm. As we have mentioned above, the one-way function does encryption, and Diffie-Hellman is used to exchange the symmetric key. Our basic idea for the project is to apply three methods to find the solution of polynomials and find an approach with the least time taken.
2. Overall, The main purpose of this study is to implement the secant method, the bisection method, and Newton Raphson method numerically and then find the root of the given equation, which is the ciphertext of the messages and then compare that method that which methods will give the fastest encryption.
3. In the real world, The easiest functions to compute are one-way functions. It's like finding $f(x)$ given the value of x , but talking about images, it's hard to get an image from random input. A one-way function is used to assign a unique address to the input, but there is no way back to get the original input. One-way functions are, therefore, naturally used in cryptography to encode messages.
4. We can also check or verify whether they are accurate or not by knowing the input and output from the original phase. For this project, we have approximated the one-way function's root in cryptography using three distinct numerical techniques. We have contrasted the iterations and outcomes of each approach from the standpoint of the conclusion.

CHAPTER 3

RESEARCH GAPS

1. Enhancement of Sensitivity and Key Space:

There are many numerous techniques that depend on the economic and chaotic image, which are useful but can yet be enhanced for better key space and sensitivity to enhance security.

2. Strongness Against All Forms of Attack:

A general technique that gives good security against all types of attack is still necessary, even though many algorithms are immune to certain kinds of attack, such as statistical or differential.

3. Real-Time Application:

Some methods are not suitable for real-world applications, so algorithms that can efficiently encrypt or decrypt the message and image are needed.

4. Efficiency and Speed:

There are some encryption methods or techniques which are effective but may slow and require more computational space. There is a need for more algorithms which are more efficient and suitable.

5. Complexity and implementation:

Some methods or techniques take more time to implement the encryption and description algorithms and are also difficult to implement practically. Enhancing these methods or algorithms without losing security is an ongoing challenge.

6. Managing various text or image formats:

Numerous methods are tested on particular kinds or formats of images or text. So, there is need of good Techniques that work well with a range of image formats and resolutions are required.

7. Combining techniques:

Combining different encryption methods may enhance security, but more research is needed to enhance the security of text or images.

8. Adaptive Methods:

We need techniques for adaptive encryption: algorithms that can be altered dynamically depending on the type of data being used or the environment.

9. Initial Conditions Sensitivity:

Some schemes would be highly sensitive at the first stage, and that can be a double-edged sword, so we need more robust methods that enable high security without extreme sensitivity

10. Validation and Testing:

There are too many studies with limited scope that don't scrutinize the shortcomings and practical limitations of the methods they propose, and there are fewer studies that test and validate the novel techniques of encryption.

The existence of these gaps highlights that more research is needed to go around these limitations and to propel computer vision from its current status as research to more efficient and practical solutions, benefiting both practical applications and theoretical studies, allowing us to study new systems and, as a result, fortify our cryptography, our encryption and/or decryption algorithms, and focusing on areas where existing methods need to be improved for better performance, security, and practical usability.

CHAPTER 4

METHODOLOGY

4.1 PROPOSED WORK

4.1.1 Encryption algorithms

Let's first understand what encryption algorithms are.

The Encryption algorithm converts plain text into ciphertext so that an unauthorized person cannot read it, which means only an authorized person can read it.

The following steps are given below for the encryption:

1. Converts text messages to decimal numbers (the ASCII values of characters).
Use the Diffie-Hellman algorithm to obtain the one-way function $f(x)$ and the private key.
2. required by the user and recipient.

Once you have the function $f(x)$, use one of the numeric methods to resolve the ASCII text message value of $f(x) = x$. The root of this equation is the ciphertext.

3. You now have an array of equation solutions representing the encrypted data.

4.1.2 Decryption algorithm

Let's first understand what encryption algorithms is.

So, the decryption algorithm is a method to convert ciphertext into plain or main text.

The encryption algorithm is exactly what the decryption method is not. It goes like this:

1. The equation representing encrypted data has several solutions. We can
2. put these values into the equation to get the value of $f(x)$.
3. The value of $f(x)$ is equal to the ASCII value of the text message.
4. From this, we can get back to the original message.

4.1.3 Diffie-Hellman Algorithm

This method is not directly used to encrypt or decrypt data or information; It enables the safe sharing of a secret key between two people over an unsecured route or media. The shared key can then be used for symmetric encryption. Also, this

algorithm is very fast at encrypting data or a very large amount of data, which is better than most algorithms.

The following steps for Diffie-Hellman Algorithm:

1. Both the sender and the recipient agree to use the same base g and prime number p .
2. The sender selects an integer secret key, a , and sends the recipient the value $k = g^a \text{mod}(p)$.
3. Similarly, the receiver chooses a secret key(integer) b and sends the sender a value $m = g^b \text{mod}(p)$.
4. The sender finds $s = g^m \text{mod}(p)$, while the receiver finds $s = g^k \text{mod}(p)$.
5. Both the sender and the recipient now share the secret key.

For instance, let us assume that the public keys p and g in the Diffie-Hellman algorithm are, respectively, 14 and 7. Private keys $a = 5$ are assigned to the sender, Alice, and $b = 3$ to the recipient, Bob. Everyone else cannot see the private keys.

4.1.4 Newton-Raphson Method

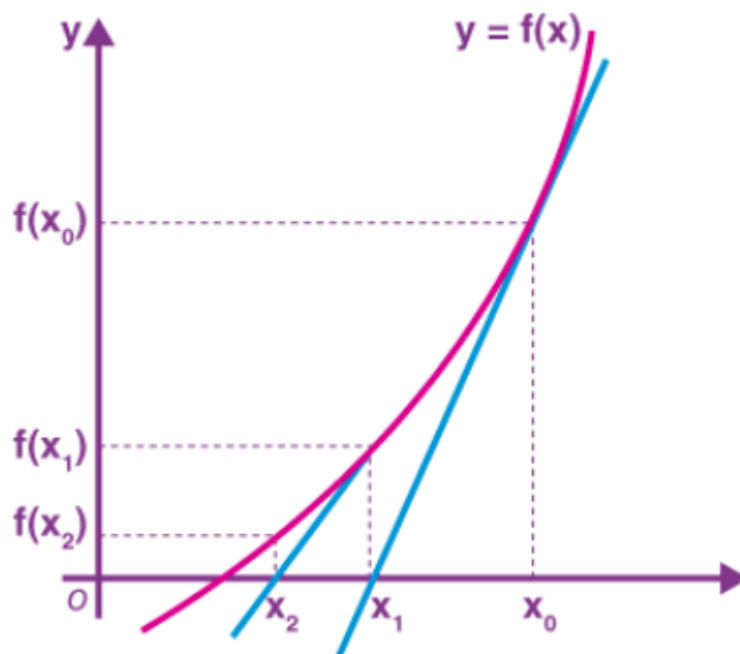


Figure 2: Newton-Raphson Method[1]

Newton-Raphson Method, simply called Newton's method, is a numerical method where we try to find the root of a function using an initial guess of x_0 and approximating the function by its tangent line.

Stage 1: We consider an initial guess $x = x_0$ as the root of the function $f(x)$.

Stage 2: The approximation of the root at the $(i+1)^{\text{th}}$ iteration is given by:

$$x_{i+1} = x_i - \frac{f(x_i)}{f'(x_i)}$$

Equation 1

Stage 3: While coding, we stop the iterations when the error at that stage. The error at the $(i+1)^{\text{th}}$ stages is given by:

$$E_a^{(i+1)} = \left| \frac{x_m^{(i+1)} - x_m^{(i)}}{x_m^{(i+1)}} \right|$$

Equation 2

Stage 2: We then compute $f(x_m)$ and check for sign change between x_1 and x_m or x_2 and x_m . One of the intervals will be discarded.

- When $f(x_1)f(x_2) = 0$, the root is x_m . Next, stop the iterations.
- The root is located in the interval (x_1, x_m) if $f(x_1)f(x_m) < 0$. Do Step 1 again using $x_2 = x_m$.
- The root is located in the interval (x_m, x_2) if $f(x_m)f(x_2) < 0$. Iterate Step 1 using $x_1 = x_m$.

This is repeated at every stage until the iterations are stopped.

Stage 3: While coding, we stop the iterations when the error at that stage. The error at the $(i+1)^{\text{th}}$ stage is given by:

$$E_a^{(i+1)} = \left| \frac{x_m^{(i+1)} - x_m^{(i)}}{x_m^{(i+1)}} \right|$$

4.1.6 Secant Method

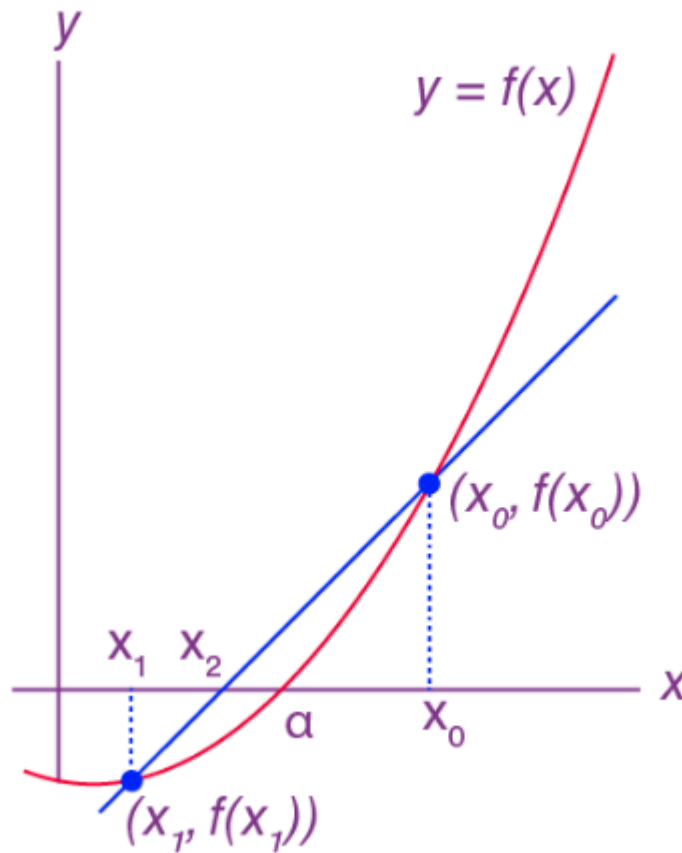


Figure 4: Secant method

The secant method is a recursive technique that uses consecutive approximations to discover the root of polynomials. By using a secant line or chord to the function $f(x)$, we can roughly represent the neighbourhoods of the roots in the secant technique.

Stage 1: We consider two initial guesses, $x = x_0$ and $x = x_1$, as the neighbourhoods of the roots of the function $f(x)$.

Stage 2: The approximation of the root at the $(i+1)^{\text{th}}$ iteration is given by:

Stage 3: While coding, we stop the iterations when the error at that stage. The error at

$$x_{i+1} = x_i - \frac{(x_{i+1} - x_i)f(x_i)}{f(x_{i+1}) - f(x_i)}$$

the $(i+1)^{\text{th}}$ stage is given by:

equation 4

$$E_a^{(i+1)} = \left| \frac{x_m^{(i+1)} - x_m^{(i)}}{x_m^{(i+1)}} \right|$$

4.2 FLOW CHART DIAGRAM

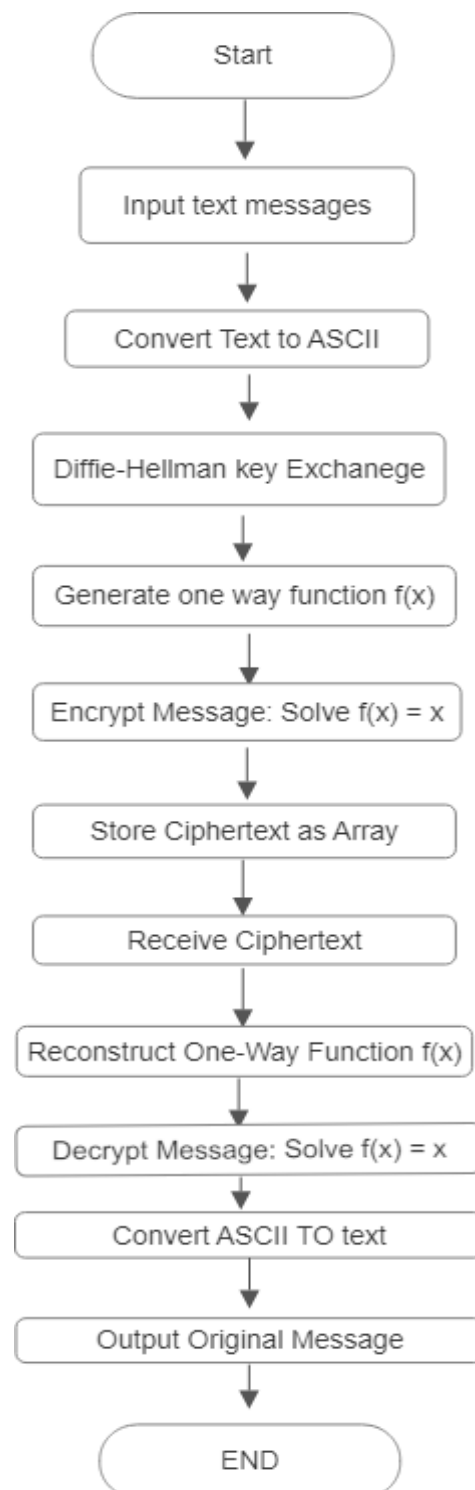


Figure 5: Flow chart diagram for the implementation.

CHAPTER 5

Results and Analysis

5.1 Results

As an example, we have used the following plain text:

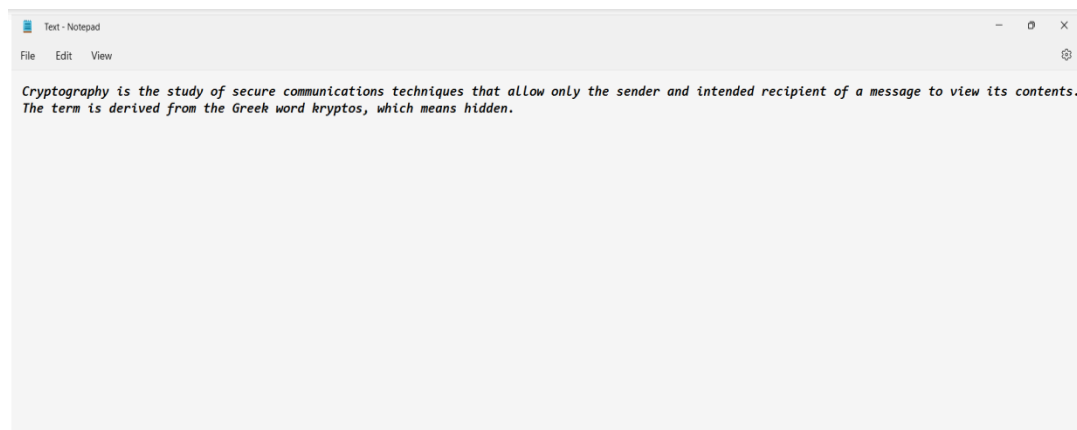


Figure 6: Original Text

The encrypted text (that is, the cipher text) that we obtained after using function $f(x)$ as $(\text{Secret Key})x^3 - 2.7x - (\text{ASCII}) = 0$ is shown below:

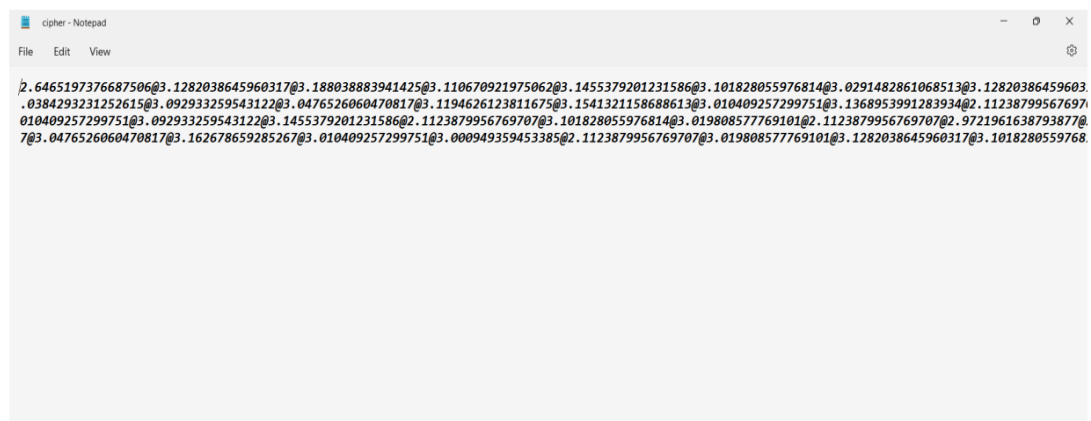


Figure 7: Cypher Text

The decrypted text that we obtained using the decryption code is shown below:

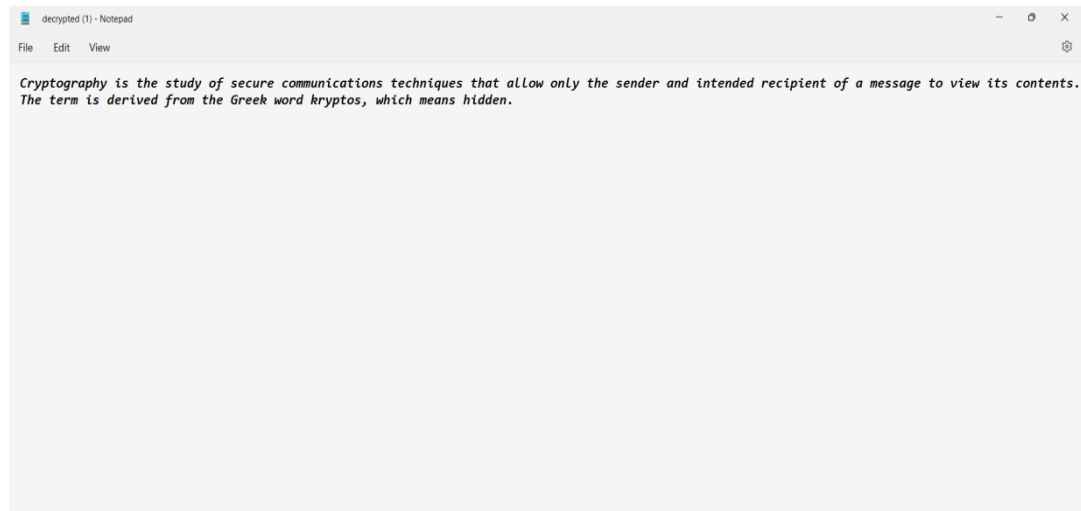


Figure 8. Decrypted Text (same as original)

5.2 Time Chart

	Secant Method	Bisection Method	Newton's Method
	8 Iterations	17 Iterations	9 Iterations
Number of Characters	Time(1)	Time(2)	Time(3)
100	0	0	0
200	0.015738	0.015085	0.015888
300	0.027568	0.015085	0.027888
400	0.027568	0.029569	0.027888
500	0.027568	0.029569	0.027888
600	0.027568	0.029569	0.027888
700	0.027568	0.031291	0.027888
800	0.027568	0.031291	0.027888
900	0.031487	0.031291	0.031567
1000	0.031487	0.031291	0.031567
1100	0.031487	0.031291	0.031567
1200	0.04268	0.031291	0.04567
1300	0.04268	0.047349	0.04567
1400	0.04268	0.047349	0.04567
1500	0.04268	0.047349	0.04567
1600	0.04268	0.047349	0.04567
1700	0.04268	0.047349	0.04567
1800	0.058501	0.060308	0.058832
1900	0.058501	0.060308	0.058832
2000	0.058501	0.060308	0.058832

Table 4. Record of Time Taken for encryption

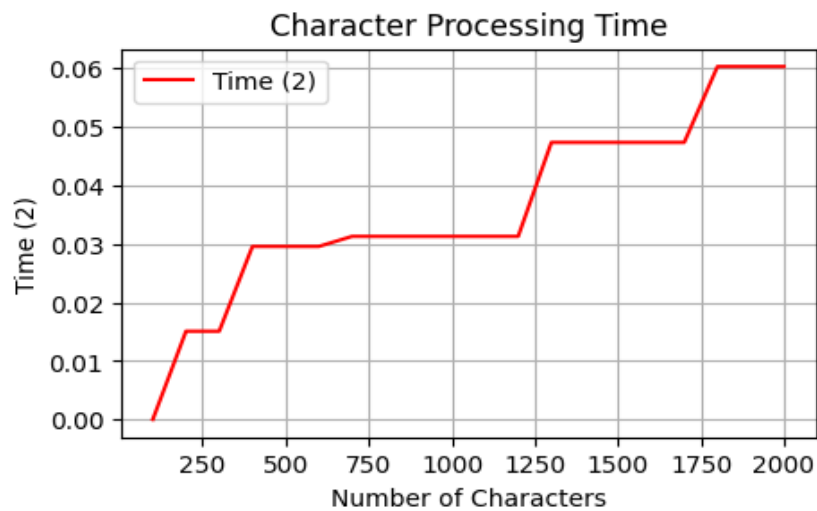


Figure 9: Time chart for Bisection method.

In Figure 9, the time chart for the bisection method shows that if 500 words are given, it takes a total of 0.2988. If it contains 1000 words, it takes 0.3167, and so on. Based on the given number of characters, the bisection method will take time.

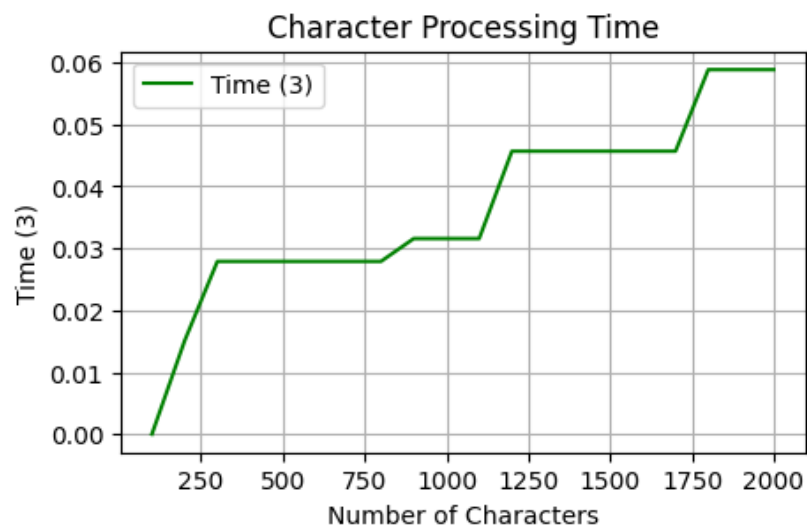


Figure 10: Time chart for Newton-Raphson method.

In Figure 10, the time chart for the bisection method shows that if 500 words are given, it takes a total of 0.0256. If it contains 1000 words, it takes 0.031568, and so on. Based on the given number of characters, the bisection method will take time.

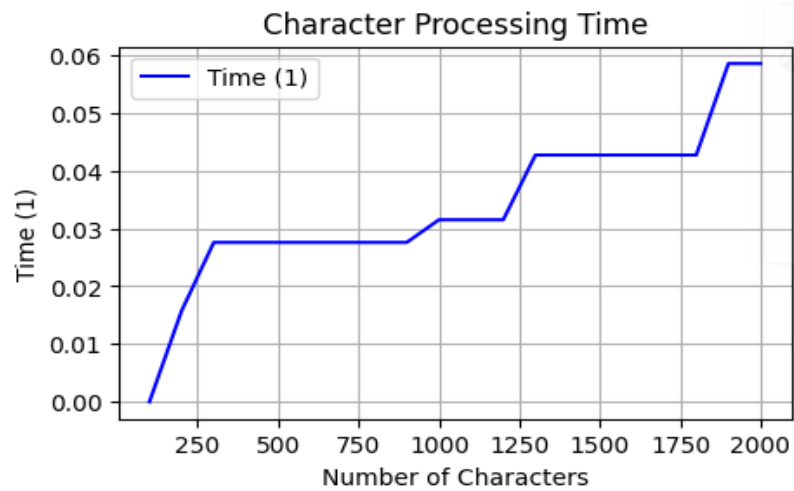


Figure 11: Time chart for the Secant method.

In Figure 11, the time chart for the bisection method shows that if 500 words are given, it takes 0.2766. If it contains 1000 words, it takes 0.031568, and so on. Based on the given number of characters, the secant method will take time.

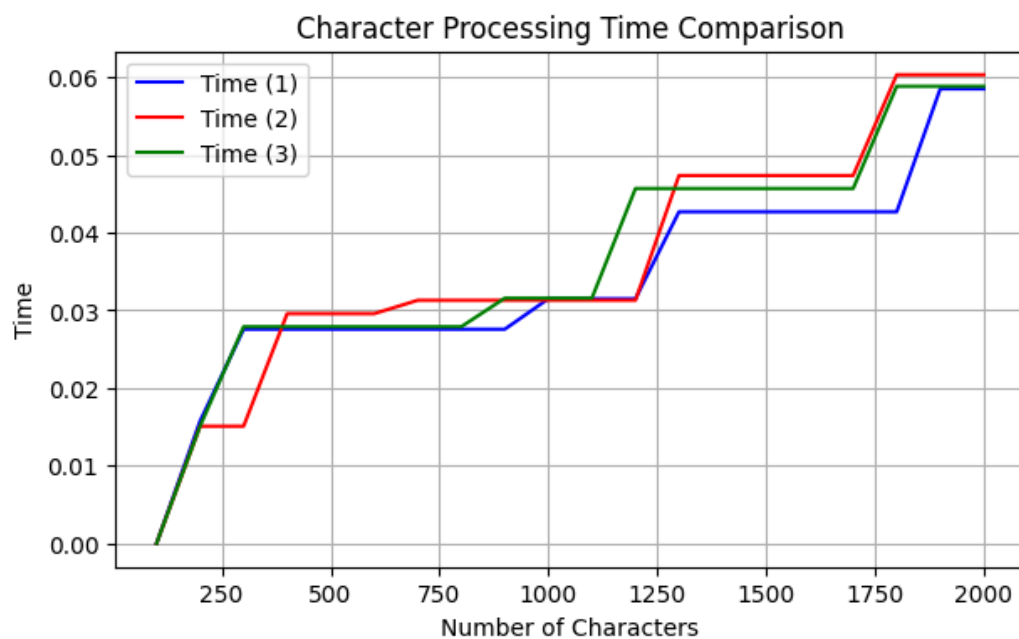


Figure 12: Chart for comparing three methods used.

Figure 12 shows a graph comparing the three methods. It also shows that Newton and Secant perform faster encryption than bisection methods, but overall, Newton and Raphson's methods are faster than both methods.

CHAPTER 6

Conclusion and Future Work

The results of the comparison show that the Newton-Raphson method and Secant method are quite efficient, while methods like the Bisection method do not work very efficiently for a larger length of text. It is evident that the Newton-Raphson and Secant methods use little time and iterations to encrypt an identical text message. Overall, the findings we received support the general expectation that the Secant approach and the Newton-Raphson method require less time to converge.

We have used text-to-text encryption, which means we are encrypting the required text in some other non-susceptible text. This encryption can be extended to more complex steganography techniques, such as encrypting text in an image or even more complex techniques, such as encrypting an image in a video file.

Further, we can extend the study to compare the results for other numerical methods as well, such as Brent's method, Runge-Kutta method, etc. In the current world, there is a possibility of the insecurity of the data through encryption. Researchers are still looking for more secure encryption. There may exist some futuristic encryption methods like Honey Encryption, in which information is created by wrong guess that looks accurate. Restricted secret keys are used in functional encryption to only teach the keyholder about a certain function of encrypted material. Quantum atoms are used in quantum key encryption to protect the data.

REFERENCES

- [1] A. Karawia, "Cryptographic Algorithm Using Newton-Raphson Method and General Bischi-Naimzadah Duopoly System," *Entropy*, vol. 23, no. 1, p. 57, Dec. 2020.
- [2] D. I. G. Amalarethinam et al. "Image encryption and decryption in public key cryptography based on MR," in 2015 International Conference on Computing and Communications Technologies (ICCCT), 2015, pp. 133–138.
- [3] P. Biswas et al. "An image encryption scheme using sequence generated by interval bisection of a polynomial function," *Multimedia tools and applications*, vol. 79, no. 43–44, pp. 31715–31738, Aug. 2020.
- [4] A. N. Elghandour et al. "An image encryption algorithm based on bisection method and one-dimensional piecewise chaotic map," *IEEE Access*, vol. 9, pp. 43411–43421, 2021.
- [5] IR Al-Siaq "Public Key Cryptosystem Based on Numerical Methods" *Global Journal of Pure and Applied Mathematics*, 2017.
- [6] Keyvan Derakhshan Nik, "CRYPTOGRAPHY, ENCRYPTION/DECRYPTION AND STEGANOGRAPHY," *Indian Journal of Fundamental and Applied Life Sciences* ISSN: 2231– 6345 (Online)2014 Vol. 4 (S4), pp. 646-651/Nik.
- [7] A. Akgul et al. "Text encryption by using one-dimensional chaos generators and nonlinear equations," in 2013 8th International Conference on Electrical and Electronics Engineering (ELECO), 2013, pp. 320–323.
- [8] A. Arab, M. J. Rostami, and B. Ghavami, "An image encryption method based on chaos system and AES algorithm," *The Journal of Supercomputing*, vol. 75, no. 10, pp. 6663–6682, May 2019.
- [9] Q. Yin and C. Wang, "A New Chaotic Image Encryption Scheme Using Breadth-First Search and Dynamic Diffusion," *International Journal of Bifurcation and Chaos*, vol. 28, no. 04, p. 1850047, Apr. 2018.
- [10] S. S. Askar, A. A. Karawia, and F. S. Alammam, "Cryptographic algorithm based on pixel shuffling and dynamical chaotic economic map," *IET Image Processing*, vol. 12, no. 1, pp. 158–167, Jan. 2018.

- [11] A. Karawia, "Encryption Algorithm of Multiple-Image Using Mixed Image Elements and Two Dimensional Chaotic Economic Map," *Entropy*, vol. 20, no. 10, p. 801, Oct. 2018.
- [12] S. S. Askar, A. A. Karawia, Abdulrahman Al-Khedhairi, and F. S. Al-Ammar, "An Algorithm of Image Encryption Using Logistic and Two-Dimensional Chaotic Economic Maps," *Entropy*, vol. 21, no. 1, pp. 44–44, Jan. 2019.
- [13] A. Karawia, "Image encryption based on Fisher-Yates shuffling and three-dimensional chaotic economic map," *IET Image Processing*, vol. 13, no. 12, pp. 2086–2097, Oct. 2019.
- [14] X. Wu, K. Wang, X. Wang, and H. Kan, "Lossless chaotic colour image cryptosystem based on DNA encryption and entropy," *Nonlinear Dynamics*, vol. 90, no. 2, pp. 855–875, Aug. 2017.
- [15] Wu, X.; Wang, D.; Kurths, J.; Kan, H. A novel lossless colour image encryption scheme using 2d dwt and 6d hyperchaotic system. *Inf. Sci.* 2016, 349, 137–153.
- [16] G. Ivanov, N. Nikolov, and Svetla Nikova, "Cryptographically Strong S-Boxes Generated by Modified Immune Algorithm," *Lecture notes in computer science*, pp. 31–42, Jan. 2016.
- [17] N. Jia, S. Liu, Q. Ding, S. Wu, and X. Pan, "A New Method of Encryption Algorithm Based on Chaos and ECC," vol. 7, no. 3, 2016, Accessed: May 21, 2024.
- [18] U. Hayat and N. A. Azam, "A novel image encryption scheme based on an elliptic curve," *Signal Processing*, vol. 155, pp. 391–402, Feb. 2019, doi: 10.1016/j.sigpro.2018.10.011.
- [19] Tonga, X.; Zhanga, M.; Wang, Z.; Liu, Y.; Ma, J. An image encryption scheme based on a new hyperchaotic finance system. *Optik* 2015, 126, 2445–2452.
- [20] Guo, H.; Zhang, X.; Zhao, X.; Yu, H.; Zhang, L. Quadratic function chaotic system and its application on digital image encryption. *IEEE Access* 2020, 8, 55540–55549.

PAPER NAME

thesis.pdf

WORD COUNT

8693 Words

CHARACTER COUNT

46077 Characters

PAGE COUNT

35 Pages

FILE SIZE

1.2MB

SUBMISSION DATE

May 30, 2024 11:11 AM GMT+5:30

REPORT DATE

May 30, 2024 11:12 AM GMT+5:30

● 10% Overall Similarity




The combined total of all matches, including overlapping sources, for each database.

- 6% Internet database
- 7% Publications database
- Crossref database
- Crossref Posted Content database
- 5% Submitted Works database

● Excluded from Similarity Report

- Bibliographic material
- Quoted material
- Cited material
- Small Matches (Less than 8 words)

Safari.pdf

 My Files My Files Delhi Technological University

Document Details

Submission ID

trn:oid::27535:60488889

Pages

Submission Date

Jun 1, 2024, 1:32 PM GMT+5:30

Words

Download Date

Jun 1, 2024, 2:11 PM GMT+5:30

Characters

File Name

Safari.pdf

File Size

1.2 MB

How much of this submission has been generated by AI?

0%

of qualifying text in this submission has been determined to be generated by AI.

Caution: Percentage may not indicate academic misconduct. Review required.

It is essential to understand the limitations of AI detection before making decisions about a student's work. We encourage you to learn more about Turnitin's AI detection capabilities before using the tool.

Frequently Asked Questions

What does the percentage mean?

The percentage shown in the AI writing detection indicator and in the AI writing report is the amount of qualifying text within the submission that Turnitin's AI writing detection model determines was generated by AI.

Our testing has found that there is a higher incidence of false positives when the percentage is less than 20. In order to reduce the likelihood of misinterpretation, the AI indicator will display an asterisk for percentages less than 20 to call attention to the fact that the score is less reliable.

However, the final decision on whether any misconduct has occurred rests with the reviewer/instructor. They should use the percentage as a means to start a formative conversation with their student and/or use it to examine the submitted assignment in greater detail according to their school's policies.

How does Turnitin's indicator address false positives?

Our model only processes qualifying text in the form of long-form writing. Long-form writing means individual sentences contained in paragraphs that make up a longer piece of written work, such as an essay, a dissertation, or an article, etc. Qualifying text that has been determined to be AI-generated will be highlighted blue on the submission text.

Non-qualifying text, such as bullet points, annotated bibliographies, etc., will not be processed and can create disparity between the submission highlights and the percentage shown.

What does 'qualifying text' mean?

Sometimes false positives (incorrectly flagging human-written text as AI-generated), can include lists without a lot of structural variation, text that literally repeats itself, or text that has been paraphrased without developing new ideas. If our indicator shows a higher amount of AI writing in such text, we advise you to take that into consideration when looking at the percentage indicated.

In a longer document with a mix of authentic writing and AI generated text, it can be difficult to exactly determine where the AI writing begins and original writing ends, but our model should give you a reliable guide to start conversations with the submitting student.

Disclaimer

Our AI writing assessment is designed to help educators identify text that might be prepared by a generative AI tool. Our AI writing assessment may not always be accurate (it may misidentify both human and AI-generated text) so it should not be used as the sole basis for adverse actions against a student. It takes further scrutiny and human judgment in conjunction with an organization's application of its specific academic policies to determine whether any academic misconduct has occurred.

