Novel Encryption System Using Knight's Tour Algorithm And Logistic Map Function

Submitted by

Khandoker Wakib Rashad

181-35-2288

Department of Software Engineering

Daffodil International University

Supervised by

Syeda Sumbul Hossain

Former Lecturer (Senior Scale)

Department of Software Engineering

Daffodil International University

This Project report has been submitted in fulfillment of the requirements for the Degree of Bachelor of Science in Software Engineering

APPROVAL

This thesis titled on "**Novel Encryption System Using Knight's Tour Algorithm And Logistic Map Function**", submitted by **Khandoker Wakib Rashad (ID: 181-35-2288)** to the Department of Software Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of Bachelor of Science in Software Engineering and approval as to its style and contents.

BOARD OF EXAMINERS

---------- **Chairman**

Dr. Imran Mahmud
Head and Associate Professor
Department of Software Engineering
Faculty of Science and Information
Technology Daffodil International University

---------- **Internal Examiner**

Kaushik Sarker
Associate Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

---------- **Internal Examiner**

Dr. Md. Fazla Elahe
Assistant Professor
Department of Software Engineering
Faculty of Science and Information Technology
Daffodil International University

---------- **External Examiner**

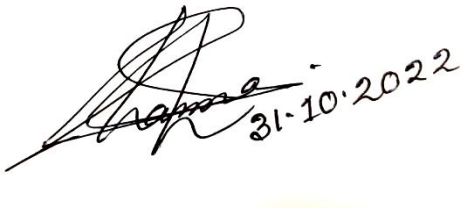
Mohammad Abu Yousuf, PhD.
Professor
Institute of Information Technology
Jahangirnagar University

DECLARATION

It's been declared that this thesis including all the research-based experimental works has been completed by me under the supervision of Syeda Sumbul Hossain (Former Lecturer), Department of Software Engineering of Daffodil International University.

I also declare that neither this thesis nor any part of this whole research-based experiment has been submitted elsewhere for the award of any degree.

Khandoker Wakib Rashad
181-35-2288
Department of Software Engineering
Daffodil International University



Syeda Sumbul Hossain
Former Lecturer(Senior Scale)
Department of Software Engineering
Daffodil International University

ACKNOWLEDGEMENT

We are very grateful to our supervisor Ms. Syeda Sumbul Hossain, Lecturer at the Department of Software Engineering, at Daffodil International University. Behind the thesis, we had to deal with some implementation issues, and the encouragement and guidance of our supervising teacher in those moments were truly unparalleled. His excellent scholarly guidance and encouragement and enthusiastic supervision have made the completion of this thesis possible. It would not have been possible without his endless cooperation. Thanks a lot, to my classmates who have been helping me and encouraging me during this thesis. finally, and most importantly, our hearts are grateful for this blessing of God Almighty. And a lot of respect for our parents for their heartfelt support.

ABSTRACT

The Internet is developing faster than any other preceding technology. The security for the transmission of messages has now been elevated to the top priority status as the Internet has emerged as the primary means for exchanging sensitive information. Image steganography has become a premier method for information concealment in order to protect the security of transmitted data. Steganography is the technique of covert communication, which is to hide the existence of a secret text within any computer-based media to keep away from recognition, the restricted information is then separated into its previous form. Steganography can also be used in addition to encryption to further conceal or safeguard the secret data. The abstract of this paper means to propose another technique for information concealing in view of a matrix based way to deal with the concealing of the secret information in variety of color images using warnsdorff's knight's tour algorithm. The logistic map function, a type of chaotic algorithm that exhibits the butterfly effect, is also used to construct the cover image's pixels. The advantage of this method over the traditional LSB method is that we do not need to encrypt the data before beginning the primary steganography process because the data is scrambled in the image in such a way that makes unintentional decryption via steganalysis assaults nearly impossible. To evaluate our tool, we use a different type of ASCII value and embed it into a randomly generated image. And we successfully, extract the data from the stego image with data loss. This tool can hide data more securely and extract data more efficiently. The results show that the proposed method has achieved MSE 39.307 and PSNR 32.186 DB. This means that compared to other methods(LSB for example) ours have a correlation between pixels in the encrypted image which is negligible compared to the original image.

Keywords: Knight tour, Steganography, data hiding, encryptio

TABLE OF CONTENT

CHAPTER 1: INTRODUCTION 1

1.1 Background 1

1.2 Motivation of the Research 3

1.3 Problem Statement 3

1.4 Research Questions 3

1.5 Research Objectives 4

1.6 Research Scope 4

1.7 Thesis Organization 4

CHAPTER 2: LITERATURE REVIEW

2.1 Background 5

2.2 Related paper review 1 6

2.3 Related paper review 2 7

2.4 Summary 7

CHAPTER 3: METHODOLOGY

3.1 Solution overview 8

3.2 Preparing the hidden message..... 9

3.3 Random image generation using chaotic LMF..... 9

3.4 Key generation using the Warnsdorff algorithm..... 10

3.5 Encode secret message into a randomly generated image..... 11

3.6 Decode secret message from an image using key 12

CHAPTER 4: IMPLEMENTATION AND EVALUATION

4.1 Implementation Overview 14

4.2 Processing the secret message..... 14

4.3 Random image generation using chaotic LMF..... 14

4.4 Key generating using knight's tour algorithm..... 15

4.5 Encode secret message into random image..... 16

4.6 Decode secret message from the image using key..... 17

4.7 Results 17

4.7.1 Environment 18

CHAPTER 5: CONCLUSIONS AND RECOMMENDATIONS

5.1 Findings and Contributions …… 19
5.2 Recommendation and Future works ……... 19
REFERENCES ……. 20

LIST OF FIGURES

Figure 1.1 Image steganography …….. 2
Figure 3.1 Block diagram of the methodology …… 8
Figure 3.2 Knight's tour move ……. ……. 10
Figure 3.3 Stego image generator ……. ……. 11
Figure 3.4 Extract data from the stego image ..…….. 13
Figure 4.1 User interface ……..... 14
Figure 4.2 Embedded data ……..……..... 15
Figure 4.3 Randomly generated image …….. 15
Figure 4.4 Stego image ……..…… 16
Figure 4.5 Extract the message from the image ……..17

ABSTRACT

The Internet is developing faster than any other preceding technology. The security for the transmission of messages has now been elevated to the top priority status as the Internet has emerged as the primary means for exchanging sensitive information. Image steganography has become a premier method for information concealment in order to protect the security of transmitted data. Steganography is the technique of covert communication, which is to hide the existence of a secret text within any computer-based media to keep away from recognition, the restricted information is then separated into its previous form. Steganography can also be used in addition to encryption to further conceal or safeguard the secret data. The abstract of this paper means to propose another technique for information concealing in view of a matrix based way to deal with the concealing of the secret information in variety of color images using warnsdorff's knight's tour algorithm. The logistic map function, a type of chaotic algorithm that exhibits the butterfly effect, is also used to construct the cover image's pixels. The advantage of this method over the traditional LSB method is that we do not need to encrypt the data before beginning the primary steganography process because the data is scrambled in the image in such a way that makes unintentional decryption via steganalysis assaults nearly impossible. To evaluate our tool, we use a different type of ASCII value and embed it into a randomly generated image. And we successfully, extract the data from the stego image with data loss. This tool can hide data more securely and extract data more efficiently. The results show that the proposed method has achieved MSE 39.307 and PSNR 32.186 DB. This means that compared to other methods(LSB for example) ours have a correlation between pixels in the encrypted image which is negligible compared to the original image.

Keywords: Knight tour, Steganography, data hiding, encryption

CHAPTER 1
INTRODUCTION

1.1 Background

Modern technology has made it simple to share computer-based media such as audio, photos, and recordings on the internet. Because of the enormous advancements in digitization and personal computers as well as the tremendous growth in the usage of Internet networks for the transmitting and receiving of data, the digital media protection on the Internet has become a crucial concern. In order to prevent hackers and intruders from accessing the information and data, the researchers focused on developing techniques to protect it and make it more private.

Information is secured using cryptography, a method that encrypts data in a way that only the trusted person who has the secret key may decipher it and read it. The process of concealing various information or data inside different media is known as steganography. Steganography's objective is to obscure other "harmless" computerized media communications in unthinkable ways for anyone to even notice the presence of a hidden message. There are many ways to encrypt and decrypt data, but they all lost their effectiveness with the advent of the Internet, necessitating the search for new methods of data concealment. As a result, steganography as a concept was created [1, 2, 3]. A knight's tour [4, 5, 6] is a set of movements on a chessboard where the knight only travels to each square once. When pixels are chosen properly, data can be hidden with great quality and robustness[7, 8].

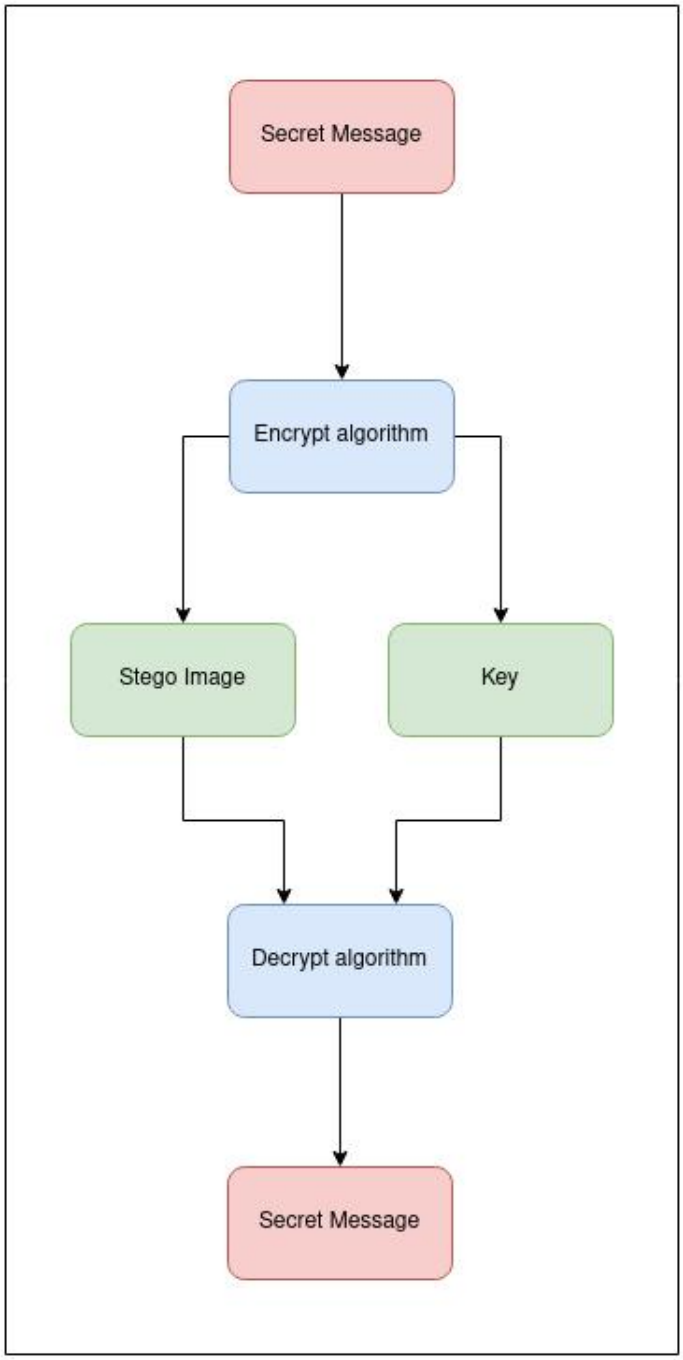


Figure 1.1: Image Steganography

In this contribution, another method of image steganography for uncoded images is presented. It combines the mostly used bit replacement method with the generalized knight's your algorithm.

1.2 Motivation for the Research

Steganography, the art, and science of invisible communication conceal the existence of the communicated information by enclosing it in other ways so that no one other than the intended recipient is aware of its presence.

Image steganography is one of the popular ways of hiding secret messages. Many researchers research this topic but there is more room for improvement on this topic. The most popular way is Least Significant Bit. In this process, secret messages can easily be extracted from images.

That is why in this article we suggested using the Generalized Knight's Tour algorithm for encoding secret messages inside images.

1.3 Problem Statement

There are much research has been conducted on image steganography topics but there is a lot of room for improvement.

First of all, a secret message is encoded inside the image in a sequential way from start to end. So any unauthorized user or hacker can extract the secret message from the stego image because data is embedded in a sequential way.

1.4 Research Question

What kind of process or step need to embed a secret message inside the image?

1.5 Research Objectives

This paper's aims and objectives are listed as follows.

- Generate a random 8x8 image
- Encode data using knight’s tour algorithm
- This system is built as an Image Steganography tool.
- This tool can generate stego images and keys.
- From the stego image and key, it can extract secret data.

1.6 Research Scope

Image Steganography is always a popular way of hiding secret messages and transferring them from one user to another. The use of image steganography is increasing day by day. And Hackers are finding new ways to extract data from image steganography. That’s why the Image Steganography tool is the most demandable tool for generating strong stego images.

1.7 Thesis Organization

This thesis is organized as follows: Chapter 1 outlines the thesis background, motivation of the research, problem statement, research questions, research objectives, research scope, and thesis organization. Detailed reviews are provided from previous studies in chapter 2 and divided into the background, related paper review 1, related paper review 2, and summary. Chapter 3, details of methodology such as solution overview, information gathering, attack generation, analysis response, and report generation. Chapter 4 includes implementations and evaluation. Chapter 5 includes findings and contributions and future work.

CHAPTER 2
LITERATURE REVIEW

2.1 Background

It can be extremely difficult to encrypt computer-based media and incorporate a hidden text in a single photo. There are numerous tried-and-true methods for securely transferring the data contained in photographs, including steganography and watermarking. Steganography can also stop unauthorized parties from using hidden messages for illicit purposes. Scientists in the field of image steganography have presented a wide range of methodologies and techniques. Getting precise results is the main goal of these strategies and tactics.

Steganography, according to Johnson and Jajodia [9], conceals the hidden message inside a medium rather than changing its structure, making the alteration invisible. Therefore, steganography keeps unapproved beneficiaries from associating the presence of information inside a particular media. The security of steganographic frameworks relies upon the secrecy of the information encryption system, according to Conway [10].

In their proposed image encryption algorithm, Manpreet et al. [11] used Euler's solution to scramble the image using the usual chessboard knight's tour strategy. By modifying the filter template matrix and utilizing Knight's tour matrix and slip filter convolution technique, Jiang et al. [12] devised an encryption algorithm.

The knight's tour matrix algorithm, which divides the image into m x n block sizes, was proposed by Kanchan et al [13]. To obtain the encrypted image, Knight's tour matrix neighborhood addition modulo encryption is used twice. Said et al [14] .'s proposed utilizing DNA encoding Choquet's integral sequences as image encryption and steganography technology. Utilizing Choquet's method, four random sequences are encoded, and four coded images are created using DNA bases and integral sequences. To create an encrypted image, a wavelet fusion approach is used.

The two primary categories of image steganography techniques are spatial domain techniques and frequency domain approaches. While in frequency domain approach, the picture is first changed utilizing a discrete wavelet change, and afterward an implanting procedure is finished to conceal the message, in spatial space methods, picture pixels are modified to store the secret message. Each method has benefits and drawbacks of its own.

However, the steganography technology is quickly overcome once the encoding method is understood. Therefore, it is crucial to protect the mentioned steganographic procedure from various assaults from an attacker. The flexibility, reliability and security of the encrypted steganographic picture are two of the most urgent variables [15] that may be used to assess the effectiveness of different steganography techniques. Proposes a DCT-based image steganography technique [16]. On a block image of size 8 by 8, two-dimensional DCT is applied without overlapping. Discusses the procedure for compressing the secret image before it is put in the cover image [17].

The least significant bit manipulation is a common and popular technique to hide text inside an image. But there are some disadvantages such as huge file size, therefore someone can suspect about it. Easily crackable if the cover image is found. The thought behind LSB embedding of pixels is that in the event that we change the last two bit of a pixel, there won't be a lot of noticeable change in the color variety. Possibly single encryption methods are utilized and in the event that keys are not overseen really there are possibilities of leakage of keys.

The widely popular Bit replacement technique along with the logistic map function(LMF) and the Knight Tour Algorithm are combined in this research to create a novel method for picture steganography on non-encoded pictures. The advantage of this bit replacement technique over the others is that we do not have to encrypt the data prior to the main steganography process as the information is mixed in the picture in such a way that it becomes almost impossible to unintended decryption via steganalysis attacks.

2.2 Related paper review 1

In this paper, Nie proposes image steganography of the cover image using the LSB method and the Knight’s Tour Algorithm. The primary goal is to raise the security level of the stego

picture. The sender and receiver sides make up the main components of the suggested technique. Then, by statistically analyzing the pixel values, steganalysis, a type of assault on the stenographyic algorithm, is used to find the secret message in the cover picture [18].

2.3 Related paper review 2

In this paper, Elmarsy proposed an image steganography method using LSB-based color images. Comparative performance tests against other spatial picture steganographic techniques are conducted to assess the proposed method using some of the well-known image quality parameters [19].

2.4 Summary

Image Steganography is always a popular way of hiding secret messages and transferring them from one user to another. The use of image steganography is increasing day by day. And Hackers are finding new ways to extract data from image steganography. That's why the Image Steganography tool is the most demandable tool for generating strong stego images.

In this paper, we proposed a method to hide data using the knight's tour algorithm.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Solution Overview

The essential target of our approach is to conceal a lot of information with an excellent steganographic method and achieve high security for the data concealing inside the cover image. In this paper, we proposed another way to deal with accomplishing higher security by utilizing the Knight`s Tour Algorithm & Chaotic Logistic Map to get arbitrary moves of the knight's tour. The two principal stages are the installing stage for the cover picture and the getting stage for the steganographic picture.

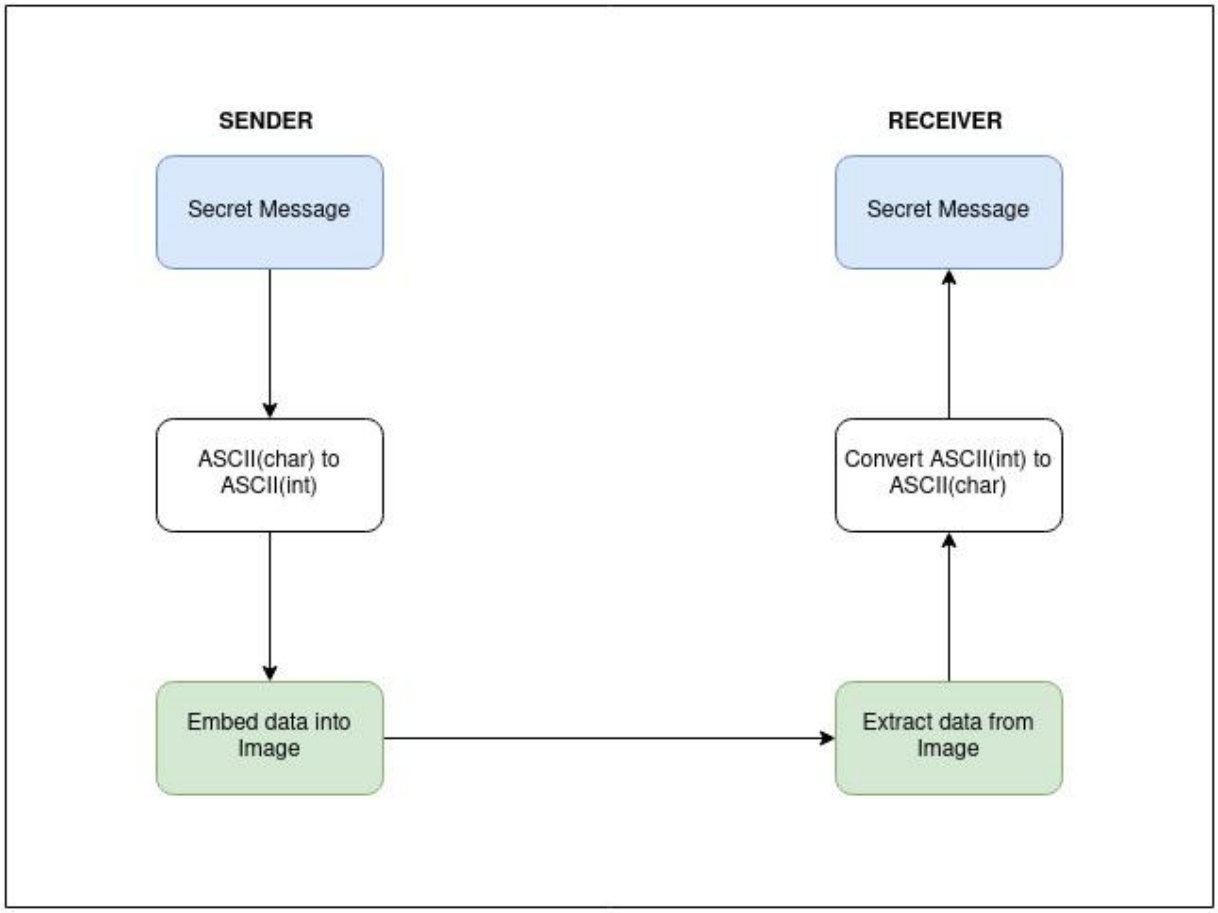


Figure 3.1: Block diagram of the methodology

In this paper, to hide secret messages just run the program and enter the secret message that’s all you need. To extract secret messages you need the encrypted image and the key.

This paper proposes methods that have four phases.

- **Secret Message:** This is the input from a user. The secret message length must be less than 64 characters.
- **ASCII(char) to ASCII(int):** Convert secret characters into ASCII int so that they can easily embed into images.
- **Embed data into an image:** Using knight's tour algorithm data will be embedded into the image.
- **Extract data from the image:** Data will be extracted from the image using a key generated in the embedded data process.
- **Convert ASCII(int) to ASCII(char):** Extract data will be in integer format. Then the integer will be converted into ASCII(char).

3.2 Preparing the Hidden Message

To start with, the mystery message should be written in the English letters in order and the length of the hidden message must be under 64 characters. Because we take an 8x8 chess board which means 64 moves and we put one character in one point. Then the letter will be converted to binary.

3.3 Random Image generation using chaotic Logistic Map Function (LMF)

One of the simplest non-linear recursive equations with chaotic behavior is the logistic map. The polynomial of degree 2 that makes up this dynamical equation was first made popular by Robert May. In this paper, the chaotic logistic map function is used for random data. The logistic map has pathological issues because a value of $r > 4$ will produce some unfavorable outcomes.

To generate an 8x8 random image we used a python library name Pillow. The Python interpreter gains the ability to process images thanks to the Python Imaging Library name Pillow. First, we need to specify what kind of image you want, in this paper we use RGB

images. Then we use a loop and generate random values using a chaotic logistic map function in the range of 0 to 255 and put the value into an 8x8 image.

3.4 Key generation using the Warnsdorff's Algorithm

The "Knight's Tour" Algorithm was first examined by Euler in 1759 and is a reasonable strategy to figure out the grouping of the mystery bit stream inside the picture pixels. The Knight Visit calculation is a self-created calculation in view of the knight visit numerical issue. Furthermore, is a reasonable strategy to form the grouping of the mystery bit stream inside the picture pixels.

The knight's tour algorithm is a self-created calculation in view of the knight's tour promlem in 8x8 chessboard. It has the upper hand over the Pseudo Random Number Generator (PRNG) strategy in that it can't be recognized by accidental recipients. The Knight Visit calculation isolates the chessboard into blocks.

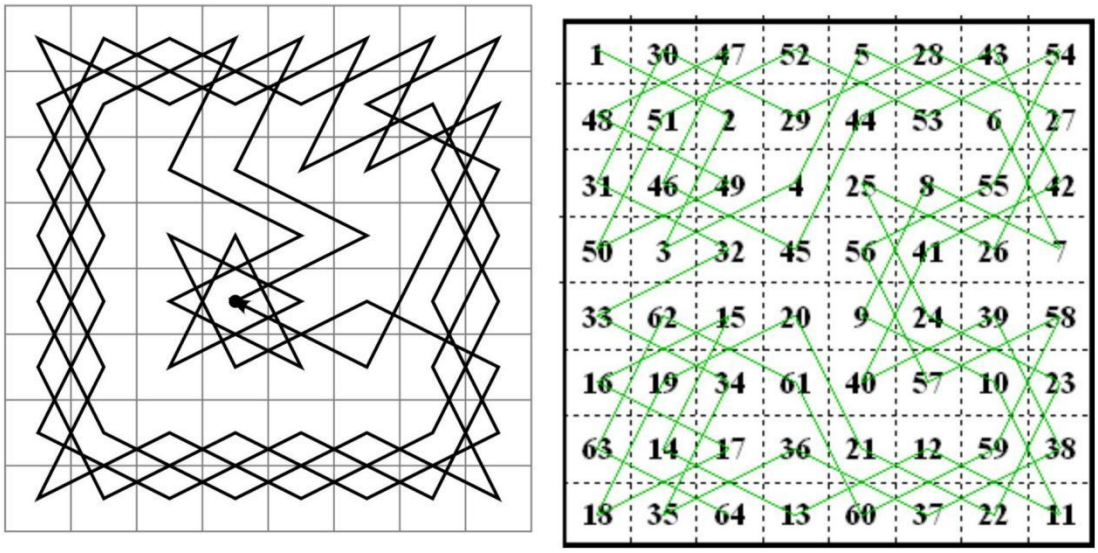


Figure 3.2: Knight's tour move

There are only two types of knight's tour, they are open tour and closed tour. The combination of closed tours is 26,534,728,821,064 and the open tours combination is infinity. That's why we choose the knight tour algorithm to generate a random tour which is completely random to generate the key. Numerous mathematicians have proposed exceptional techniques for finding the knight's tour, yet we have found an overall strategy for Hamiltonian path in 8x8 matrix and an overall technique for knight visits on a matrix of any shape and size.

3.5 Encode secret message into a randomly generated image

As mentioned above, at first the Knight's Tour Algorithm divides the chess board into 8x8 matrix.

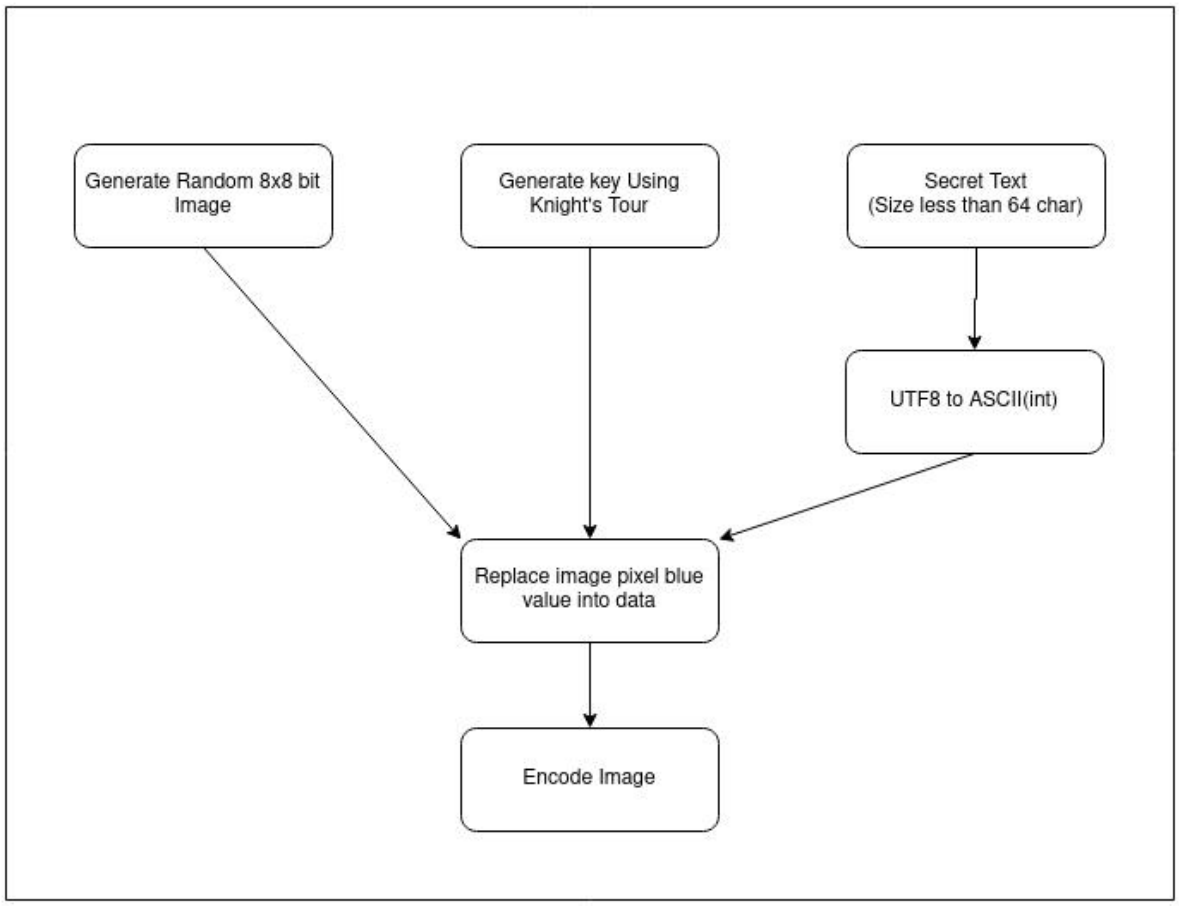


Figure 3.3: Stego Image generates

First, generate a random image as explained in figure **3.3.** Then generate a key using the knight's tour as explained in figure **3.4**. And process the secret message as explained in figure **3.2**.

Following the selection of the frame's pixels using the Knight Tour method. Then replace the pixel's blue value with data. Then our steganography is ready.
The steps of the embedding process are:

Input: Secret message
Output: Stego image

Step 1: Generate a random image
Step 2: Generate a key using knight's tour
Step 3: Convert the secret message into ASCII(int)
Step 4: Replace the image pixel blue value with data
Step 5: Stego image

3.6 Decode secret message from the image using key

In this stage after the embedding process is completed, the sender sends the stego image to the recipient and the key.

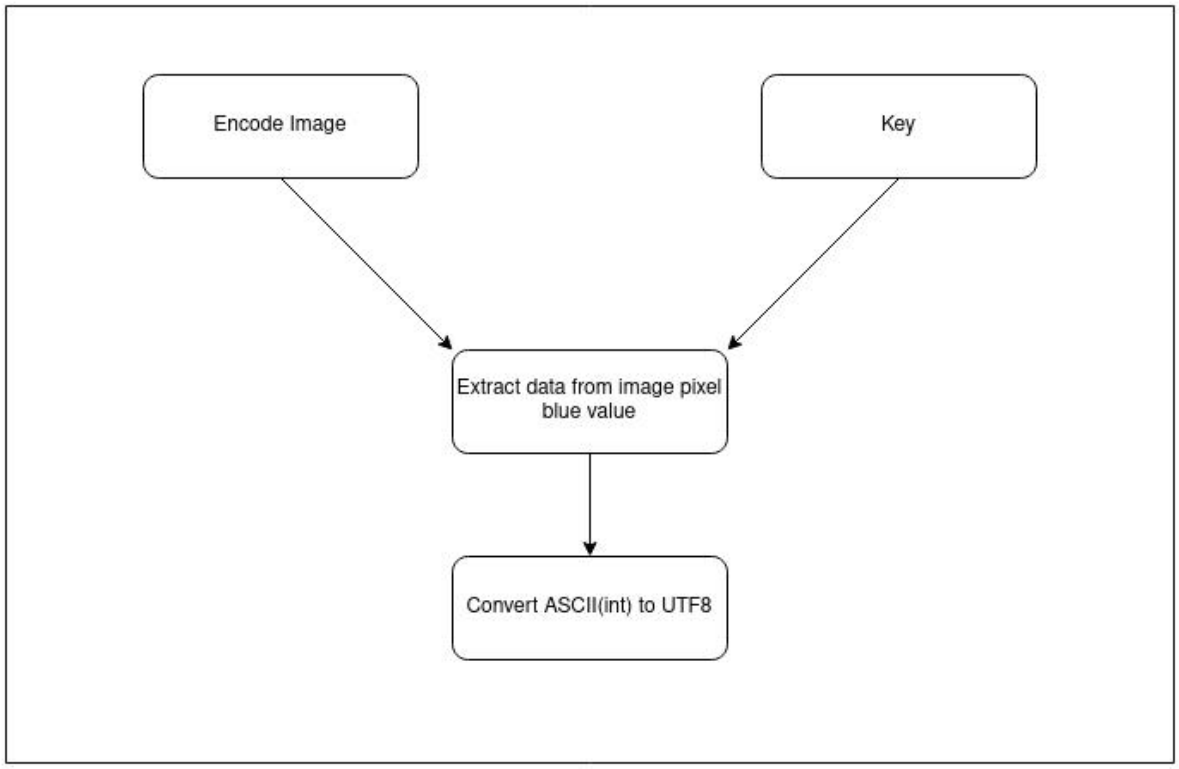


Figure 3.4: Extract data from the stego image

First, take the embedded image and the key then extract data from the image pixel blue value. After extracting the data convert the data into UTF8.

The steps of the extraction process are:

Input: Stego image and Key
Output: Secret message

Step 1: Search pixel using key
Step 2: Extract the value from the pixel blue value
Step 3: Combine the data
Step 4: Convert into UTF8
Step 5: Secret message

CHAPTER 4
IMPLEMENTATION AND EVALUATION

4.1 Implementation Overview

In this paper, we implement an Image Steganography tool. This tool has Command Line Interface (CLI). In this chapter, we discuss the implementation of all modules of the Image Steganography tool in brief. In this paper, our tool is divided into six modules such as data preparation, random image generation, data embedding, data extraction, and finally secret data.

Figure 4.1: User interface

4.2 Processing the Secret Message

First, the secret message should be written in English alphabets and the length of the secret message should be less the 64 characters. Because we take an 8x8 chess board which means 64 moves and we put one character in one point. Then the letter will be converted to binary.

4.3 Random Image generation using chaotic LMF

In this module, we generate a random image using the chaotic logistic map function. First, we create an RGB image using the Python Pillow library.

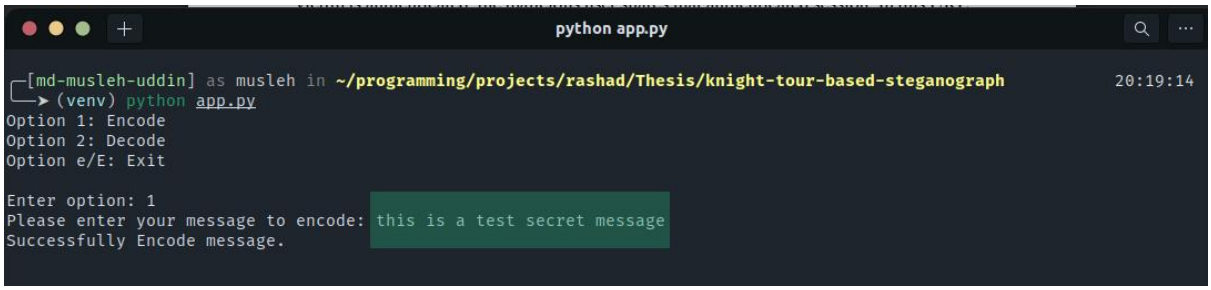


Figure 4.2: Embed data

Then we change every pixel of the image with random values generated using the chaotic logistic map function.

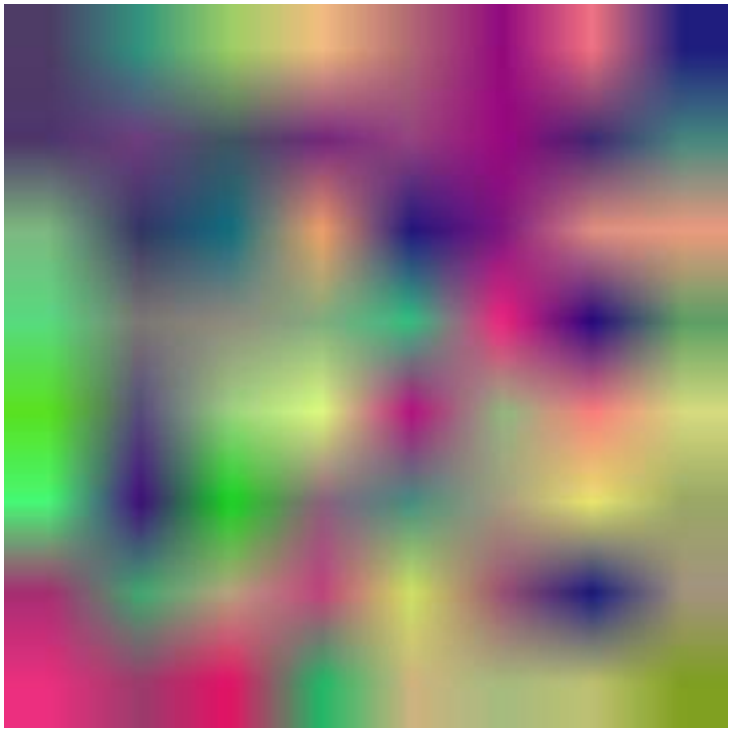


Figure 4.3: Randomly generated image

The image size should be 8x8. Then the image will be saved in PNG format. This is how an image will be generated.

4.4 Key generation using knight’s tour algorithm

In this module, we generate a key. The key will be every move of the knight’s tour. The Knight's Visit calculation is a self-created calculation in light of the knight visit numerical issue. It has the upper hand over the Pseudo Arbitrary Number Generator (PRNG) procedure in that it can't be distinguished by accidental collectors. The Knight Visit Calculation partitions the chess board into blocks.

4.5 Encode secret message into random image

In this module, the Algorithm for Knight’s Tour first divides the chess board into 8x8 matrix. Then manipulates the image pixel and changes the blue value with data.

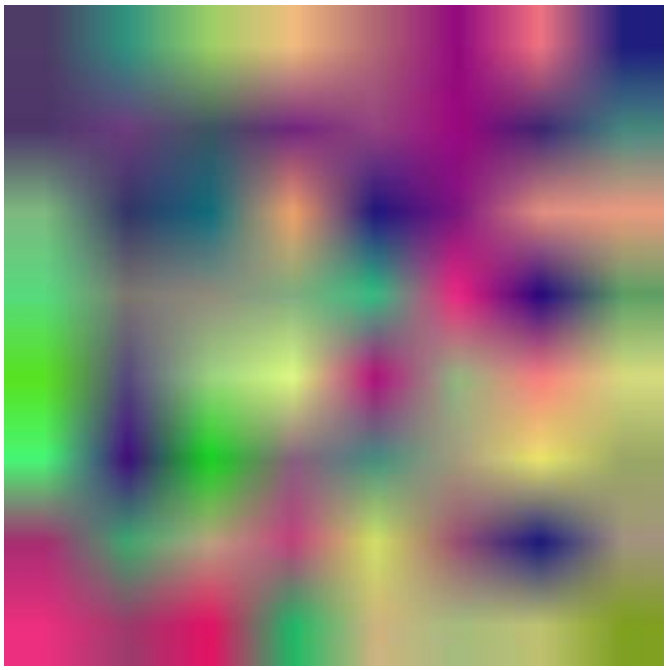


Figure 4.4: Stego Image

The processed secret data will be embedded into the randomly generated image.

4.6 Decode secret message from the image using key

In this module, the stego image, and key will be input by a user. The data will be extracted from the stego image using the key.

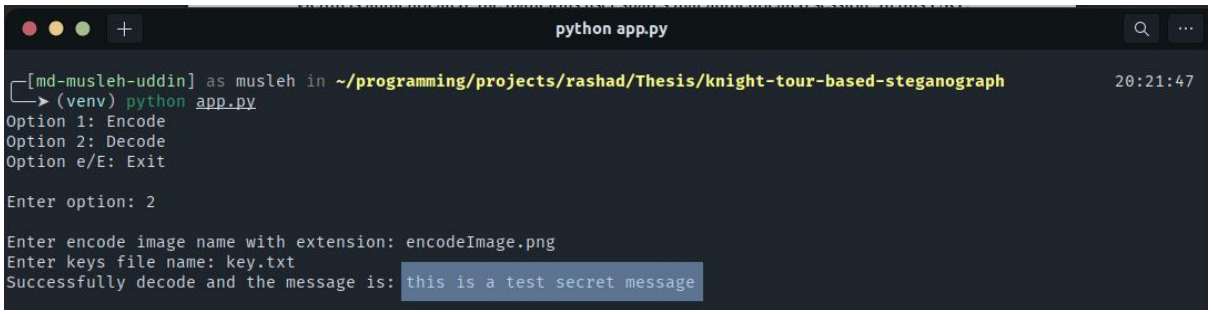


Figure 4.5: Extract the message from the image

First, take the embedded image and the key then extract data from the image pixel blue value. After extracting the data convert the data into UTF8.

4.7 Results

There are several ways to assess the effectiveness of image steganography.
Each of these techniques evaluates a unique component of the steganographic outcome. Known techniques include firstly Mean Square Error (MSE) and then Peak Signal Noise Ratio (PSNR).

The average square of the pixel value difference between the actual image and the steganographic image is known as the mean square error. It provides us with a gauge of the inaccuracy of the data embedding method caused in the cover image. In our tool, **MSE is 39.307**.

Another well-liked benchmark for determining How much the inserting contorted the cover photograph is the PSNR. It is the proportion of the greatest worth of the sign to its twisting

noise power (MSE) calculated in dB. Higher PSNR values mean better embedding and distortion of image. In our tool, **PSNR is 32.186 DB**.

4.7.1 Environment

For the first test, we use Pillow == 9.2.0 version. which is a python library for image manipulation. In the future, this tool can be accessed publicly. The Image Steganography tool tries on Ubuntu(22.04) operating system with 8GB RAM and core i3 4th generation four processing cores.

CHAPTER 5
CONCLUSIONS AND RECOMMENDATIONS

5.1 Findings and Contributions

This paper suggested an improved method to replace the widely used Knight Tour Algorithm and chaotic LMF. RGB images that were created randomly were used to evaluate the suggested method. We took into account the stability and security of the stego image.
However, the size of the picture that can be utilized as the cover is a deadly shortcoming in the Knight's Tour Algorithm. The algorithm can walk through all of the image's pixels for encoding because only 8x8 images with no remnant are allowed.

5.2 Recommendations for Future Works

In this proposed method we tried to create a steganographic system without the need for prior encryption as the data is scrambled in the image in such a way that it becomes almost impossible to unintentional decryption. We achieved this in an efficient manner than the usual LSB technique for steganography. However, this can be further improved if we are able to use all the color values(RGBA) of a color image.

REFERENCES

1. Elmasry, W. (2018). New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check. *Sādhanā*, *43*(5), 1-14.

2. Kumar, V., & Kumar, D. (2019). Performance evaluation of modified color image steganography using discrete wavelet transform. *Journal of Intelligent Systems*, *28*(5), 749-758.

3. Thanikaiselvan, V., Arulmozhivarman, P., Amirtharajan, R., & Rayappan, J. B. B. (2012). Horse riding & hiding in image for data guarding. *Procedia Engineering*, *30*, 36-44.

4. Ghosh, D., & Bhaduri, U. (2017, September). A simple recursive backtracking algorithm for knight's tours puzzle on standard 8× 8 chessboard. In *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 1195-1200). IEEE.

5. Bai, S., Zhu, G. B., & Huang, J. (2013, December). An intelligent algorithm for the (1, 2, 2)-generalized Knight's tour problem. In *2013 Ninth International Conference on Computational Intelligence and Security* (pp. 583-588). IEEE.

6. Younus, Z. S., & Younus, G. T. (2020). Video steganography using knight tour algorithm and LSB method for encrypted data. *Journal of Intelligent Systems*, *29*(1), 1216-1225.

7. Elzbieta, Z., Wojciech, M., & Krzysztof, S. (2014). Trends in steganography. *Commun. ACM*, *57*, 86-95.

8. Nipanikar, S. I., & Deepthi, V. H. (2018). A multiple criteria-based cost function using wavelet and edge transformation for medical image steganography. *Journal of Intelligent Systems*, *27*(3), 331-347.

9. Johnson, N. F., & Jajodia, S. (1998). Exploring steganography: Seeing the unseen. *Computer*, *31*(2), 26-34.

10. Conway, M. (2003). Code wars: steganography, signals intelligence, and terrorism. *Knowledge, Technology & Policy*, *16*(2), 45-62.

11. Singh, M., Kakkar, A., & Singh, M. (2015). Image encryption scheme based on Knight's tour problem. *Procedia Computer Science*, *70*, 245-250.

12. Delei, J., Sen, B., & Wenming, D. (2008, December). An image encryption algorithm based on knight's tour and slip encryption-filter. In *2008 International Conference on Computer Science and Software Engineering* (Vol. 1, pp. 251-255). IEEE.

13. Bisht, K., & Deshmukh, M. (2020, February). Encryption algorithm based on knight's tour and n-neighbourhood addition. In *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)* (pp. 31-36). IEEE.

14. El-Khamy, S. E., Korany, N. O., & Mohamed, A. G. (2020). A new fuzzy-DNA image encryption and steganography technique. *IEEE Access*, *8*, 148935-148951.

15. Rai, P., Gurung, S., & Ghose, M. K. (2015). Analysis of image steganography techniques: a survey. *International Journal of Computer Applications*, *114*(1).

16. Zhang, X., Peng, F., & Long, M. (2018). Robust coverless image steganography based on DCT and LDA topic classification. *IEEE Transactions on Multimedia*, *20*(12), 3223-3238.

17. Pal, A. K., Naik, K., & Agrawal, R. (2019). A steganography scheme on JPEG compressed cover image with high embedding capacity. *Int. Arab J. Inf. Technol.*, *16*(1), 116-124.

18. Nie, S. A., Sulong, G., Ali, R., & Abel, A. (2019). The use of least significant bit (LSB) and knight tour algorithm for image steganography of cover image. *International Journal of Electrical and Computer Engineering*, *9*(6), 5218.

19. Elmasry, W. (2018). New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check. *Sādhanā*, *43*(5), 1-14.

