UNIVERSITY OF GHANA, LEGON

DEPARTMENT OF COMPUTER SCIENCE

FINAL YEAR PROJECT

IMAGE ENCRYPTION ALGORITHM

BY

NAME: KONADU KOFI AMPONSAH (10809563)

NAME OF SUPERVISOR: PROF. YAOKUMA WINFRED

A THESIS SUBMITTED TO THE

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF A BACHELOR OF SCIENCE (BSC) DEGREE IN INFORMATION TECHNOLOGY.

AUGUST 2023

DECLARATION

I hereby declare that the project entitled “IMAGE ENCRYPTION” submitted is a record of an original work done by me under the guidance of Prof. Yaokuma Winfred, and this project work is submitted in the partial fulfilment of the requirements for the award of the bachelor of science degree in information technology. The results of embodied in this thesis has not been submitted to any other University for the award of any diploma.

……... ……

Konadu Kofi Amponsah Date

10809563

CERTIFICATION

I hereby certify that this thesis was supervised in accordance with procedures laid down by the University

……. ...……

Prof. Yaokuma Winfred Date

(Supervisor)

DEDICATION

This work is dedicated to the Almighty God who gave me life, strength, and knowledge to enable me do this research. I also dedicate it to my parents, siblings and all my family who helped me reach this far either directly or indirectly.

ACKNOWLEDGEMENT

The success and final completion of this project required a great deal of guidance and assistance from my supervisor, and I consider myself quite fortunate to have received this support. Whatever I have done is only due to such guidance and assistance, for which I am grateful.

Prof. Yaokuma Winfred is someone I admire and thank for giving me the opportunity to work on my project and for providing me with the support and advice I needed to finish it on time. I am incredibly grateful to him for offering such wonderful help and guidance despite his hectic schedule.

I am grateful and fortunate to have received consistent encouragement, support, and advice from everyone of the Department of Computer Science's teaching staff, which assisted me in successfully completing my project work. Thank you very much.

ABSTRACT

Image encryption is the process of converting a digital image into a format that cannot be easily understood by unauthorized users. This is performed by applying a mathematical transformation to the image data, such as a cipher or a hash function. The encrypted image can then be transmitted or stored without fear of unauthorized access. The choice of picture encryption technique is determined by a variety of criteria, including the sensitivity of the data being protected, the computational resources available, and the application's security requirements.

This project will look into how image encryption techniques can be used to protect sensitive image data. It will focus on creating a secure, efficient, and simple image encryption technique. It will also assess the security of existing image encryption techniques and identify areas for improvement. The results of this project will be of interest to information security researchers and developers. The project will also provide useful information to organizations who need to protect sensitive image data.

Table of Contents

TABLE OF FIGURES

CHAPTER ONE: INTRODUCTION

1.1 Introduction

Digital images are gaining importance in today's society. The growing significance of digital images in a variety of applications, including medical imaging, military imaging, and financial imaging, has increased the need for secure image transmission and storage. Sensitive images can be compromised readily if they are not properly encrypted, which can have severe repercussions. For instance, medical images could be used to identify patients or to plan medical procedures, military images could be used to plan military operations and financial images could be used to commit fraud.

In recent years, cybersecurity threats have grown in complexity and prevalence. As the rate of digitization increases, images have become an essential component of communication and storage. As they can be intercepted and altered by unauthorized parties, the transmission and storage of photographs may pose significant security risks. When intimate photographs are intercepted, they are frequently used to blackmail and extort substantial sums of money from victims. Occasionally, the amount requested by the interceptors is so high that the victim is unable to pay, causing the interceptors to release the photographs and damage the victim's reputation. Encrypting images can assist in mitigating these security threats by preserving the confidentiality and integrity of image data. Image encryption is the process of converting an image into an unintelligible format for the purpose of preventing unauthorized access.

This introduction sets the tone for my exploration into the field of image encryption by outlining the background of my project and image encryption, my research problem statement,

research aims and objectives, the limitations or scope of the study, my research methodology and the organization of my thesis.

1.2 Background

The importance of image encryption has increased considerably in recent years due to the widespread use of digital images. Images are being shared across networks as the internet and digital communication become more popular, raising the risk of interception and tampering. Images contain highly sensitive and confidential information. Because images play such an important part in many applications, it is critical to protect sensitive and proprietary data from unauthorized use and modification. Encryption is one of the greatest approaches for accomplishing this goal among information-concealing methods. Image encryption addresses these security concerns by guaranteeing the confidentiality and integrity of image data.

The evolution of image encryption is linked to the advancement of information security and cryptography. As digitization progressed, so did the complexity of image threats. Encryption techniques were first centred on text, but as digital images became more popular, there was a need for specialized encryption methods to be developed. With time, these methods progressed from substitution ciphers to more complicated algorithms using mathematics and advanced cryptography ideas.

In order to apply image encryption to digital images, the image's original pixel values must be converted into ciphertext. Using a confidential key, this transformation is accomplished. The resultant cipher-text image appears as a scrambled variation of the original image, rendering it unreadable and incomprehensible to unauthorised parties. The cipher-text image can only be decrypted and restored to its original form by those who possess the correct key.

The Python programming language, which is open-source and widely used, will be utilized to implement the method. The algorithm's advantages include safe image transmission and storage, open-source implementation, robust encryption capabilities, and efficiency.

1.3 Research Problem Statement

In spite of the security of the image encryption, image encryption still faces a number of research challenges that need to be addressed. One challenge is to improve the efficiency of image encryption. Image encryption algorithms are efficient algorithms, but large images can still cause it to be slow. The trade-off between security and computational efficiency is another primary concern. The application of image encryption can be computationally intensive because digital images consist of vast amount of data, potentially causing performance bottlenecks in real-time image processing applications. In image encryption, striking the right balance between security and computational efficiency is a significant research problem

Another challenge is improving the security of image encryption against new and various attacks including chosen-plaintext attacks, known-plaintext attacks, and differential attacks. While image encryption has earned a reputation of securing images, its implementation may introduce certain vulnerabilities that require in-depth analysis and effective countermeasures. It is essential to address these vulnerabilities and strengthen the resilience of image encryption to ensure the security of digital image transmission and storage. Also, image encryption methods should be flexible to a variety of fields, including medical imaging, multimedia sharing, e-commerce, and others, while security measures should be tailored to individual use cases. It is critical to highlight that when new threats are created, image encryption algorithms must be updated to increase their security.

1.4 Research Questions

To start with, I would like to explain a few terminologies used in encryption. They are:

- Plain Image: It is the image that requires protection when being transmitted over a public network. It is often referred to as the original or input image.
- Cipher image or encrypted image: It is the plain image turned into an unreadable format after encryption.
- Encryption: It is the procedure of converting a plain image to a cipher image through the use of an encryption method and a secret key.
- Decryption: This is when the encrypted image is turned to a plain image at the receiver's end using a decryption method and a secret key.
- Key: It is the numerical, alphabetical, or pin code used to encrypt or decrypt the image.

The research questions for this project are as follows:

1. What are the best practices and approaches in image encryption?

   There are many approaches but I would like to talk about only three of them.

   i. Using a strong encryption algorithm: The encryption algorithm should be sufficiently robust to withstand possible intrusion attempts. Commonly employed image encryption techniques include Advanced Encryption Standard (AES), Data Encryption Standard (DES), and Rivest-Shamir-Adleman (RSA).

   ii. Using a strong encryption key: The encryption key should be strong enough to withstand brute-force attacks.

   iii. Using a different key for each image: Using the same key for many photos is risky because if one key is hacked, all images encrypted with that key can be decrypted.

2. How can an image encryption algorithm based on be implemented using the Python programming language?

   To do this:

   i. Install the necessary libraries needed: tkinter library is needed. To install, I will run “pip install tk” in my command prompt and also install the hashlib library.

   ii. Import the necessary libraries: I will import the file dialog from the tkinter library by typing “from tkinter import filedialog”. I will also import message box from the tkinter library using “from tkinter import messagebox”

   iii. Generate a secret key: I will generate a secret key to help in encryption and decryption of the image.

   iv. Open the image file: To encrypt the image, you must first open it with the Pillow library by doing this: “from PIL import Image”.

   v. Save the encrypted image: You must convert the ciphertext and tag to bytes and save them to a file in order to save the encrypted image.

      “with open(file1, ‘wb’) as fi:

      fi.write(encrypted_image)

   vi. Decrypt the image: type in the secret code.

   vii. Save the decrypted image

1.5 Research Aims & Objectives

My research aims to investigate the application of image encryption by examining the strengths and weaknesses of image encryption. My research aims to improve our understanding of its ability to protect the privacy and integrity of digital images. My research seeks to accomplish the following goals:

1. Evaluate the security strength of image encryption: Assessing the cryptographic robustness of image encryption when applied to image data is the purpose of this objective. The research will examine the image encryption algorithm's resistance to brute-force, statistical, and known-plaintext attacks.
2. Analyse the performance of image encryption: This objective examines the computational complexity and performance of image encryption when encrypting large image datasets. The research will examine the processing speed and resource utilization of image encryption to determine its practical viability for real-time image encryption applications.
3. Assess the impact of image encryption on image characteristics: This objective seeks to study the effects of image encryption on a variety of image characteristics, including image quality, compression efficacy, and resistance to lossy compression techniques. This study will analyse the trade-offs between encryption strength and the preservation of visual information within encrypted images.
4. Explore potential enhancements or modifications to image encryption: This objective entails examining potential modifications or enhancements to the image encryption to resolve any limitations identified in the context of image encryption. The research will investigate techniques such as adaptive encryption schemes, key management strategies, and hybrid encryption approaches in order to enhance the security and efficiency of image encryption for image data.

1.6 Limitations/ Scope of the Study

Image encryption have certain limitations and scope that need to be considered. The limitations or scope of image encryption are as follows:

i. Computational Complexity: When applied to large images or real-time applications, image encryption can be computationally intensive. Encryption and decryption demand significant computational resources, which may limit the applicability of image encryption in certain situations, particularly those with limited processing capacity or time-sensitive requirements.

ii. Vulnerability to Side-Channel Attacks: Implementation of image encryption are susceptible to side-channel attacks, in which an attacker exploits information released via power consumption, electromagnetic radiation, or timing analysis. These assaults have the potential to disclose information about the encryption keys, compromising the security of the encrypted images.

iii. Implementation and Key Management: Image encryption requires a secure implementation and appropriate key management to be effective. The security of encrypted images can be compromised by inadequate implementation or poor key management, such as improper key generation, storage, or sharing.

iv. Data Privacy and Confidentiality: The foundation for maintaining data privacy and confidentiality is image encryption. It protects private photos, private medical images, exclusive design blueprints, and other intrinsically valuable visual content. This scope is very important as the digital era blurs the boundaries between private and public spaces.

v. Secure Communication: Image encryption ensures the secure transmission of visual data across networks, preventing interception and eavesdropping. It is very important for ensuring that only authorized recipients can access and interpret sensitive information shared via multimedia channels.

vi. Authentication and Integrity: Image encryption techniques make image authenticity and integrity checks easier. It is now possible to validate the validity of visual data and detect any tampering or adjustments that can jeopardize its trustworthiness by adding digital signatures or watermarks within encrypted images.

vii. Multimedia Protection: Image encryption goes beyond traditional images to include multimedia content. Videos, audio files, and other multimedia elements frequently contain sensitive data that must be encrypted to prevent unauthorized access or manipulation.

1.7 Research Methodology

My research seeks to investigate the application of image encryption algorithms to image data, with an emphasis on determining its effectiveness and limitations in protecting the confidentiality and integrity of digital images. To accomplish this objective, a comprehensive research methodology comprising several key components will be employed.

1. Literature Review: The research will begin with a comprehensive literature review to obtain a thorough understanding of the existing knowledge and research on image encryption. This review will involve exploring academic papers, conference proceedings, and relevant publications to understand the developments, advancements, challenges, and best practices in the field.

2. Theoretical Analysis: A comprehensive understanding of the image encryption and its underlying principles is essential. This research will entail an in-depth study of image encryption, including the deciphering of its mathematical foundations, key generation, encryption, and decryption processes, and any applicable modes of operation. This theoretical analysis will form the foundation for future research and experimentation.

3. Algorithm Implementation: An implementation of the image encryption will be developed in order to evaluate the performance and security of image encryption. This implementation will require programming and software development to create a system capable of encrypting and decrypting digital images. Python programming languages will be used.

4. Experimental Evaluation: A systematic experimental evaluation will be used to assess the efficacy and limitations of image encryption. This evaluation will employ diverse image datasets and metrics to determine the effect of image encryption on image characteristics such as visual quality, compression efficiency, and attack resistance. Experiments will examine the trade-offs between encryption strength and image usability.

5. Performance Analysis: The practicality of image encryption is determined primarily by its computational complexity and efficacy. The research will measure the processing time and resource consumption of image encryption for images of varying sizes through performance analysis. This analysis will give insight into the algorithm's suitability for real-time applications and environments with limited resources.

1.8 Organization of Thesis

In summary, the increasing significance of digital images in a variety of fields has increased the need for secure image transmission and storage. Encryption is essential for preventing unauthorized access and manipulation of sensitive images. Image encryption is extensively used in military, medical, and financial applications and is renowned for its resistance to a variety of attacks. My project's goal is to develop an image encryption algorithm that converts images into unintelligible formats to prevent unauthorized access and protect images before transmission and storage. Images will be encrypted using a key.

To begin, I established in the introduction the project's background by underlining the importance of image encryption in today's digital society. It recognizes the rising cybersecurity dangers as well as the critical importance of images in communication and storage, making their protection critical. The importance of encryption in protecting the confidentiality and integrity of image data is explored. This transformation makes the image unreadable to unauthorized parties, and only those with the correct key can decrypt and restore the original image. I will use Python programming language to implement the image encryption algorithm.

From the project’s background in the introduction, I delve into the background or history of image encryption, following it from text-based encryption technologies to the requirement for specialized ways to secure digital images. The section underlines the importance of using confidential keys to convert images into an unreadable format, with decryption available only to those who have the correct key.

The research's problem statement is presented, emphasizing the difficulties that picture encryption faces, such as efficiency optimization, security against multiple attacks, and adaptability to different use cases. The study's scope and limitations, including computational complexity, susceptibility to side-channel attacks, and the significance of good implementation

and key management, are acknowledged. The research questions section defines essential terms in cryptography and explains the questions that the project intends to answer. These inquiries centre on picture encryption best practices and methodologies, the concepts of constructing an image encryption algorithm in Python, and the necessity for adaptable security measures.

To conduct the research, a methodology comprising literature review, theoretical analysis, algorithm implementation, experimental evaluation, performance analysis, and comparative analysis will be employed. This will provide insights into the security, performance, and usability of Image encryption, aiming to enhance the understanding and effectiveness of image encryption in protecting digital images.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

Image encryption is a process that uses a secret key to convert a plain image into an encrypted image. It is essential that no one gets access to the content without a key for decryption. With the advancement of information technology, image information has become the primary content of network information transfer. In recent years, with the rapid promotion and popularization of network technology and digital communication technology around the world, digital images and digital video-based digital images have become an important medium for information storage and transmission in computer networks in both civil and military fields.

Information transmission and sharing based on digital images frequently encounter issues such as data theft, tampering, deletion, and attack, which have resulted in significant losses for digital image owners or publishers. Digital images are shared across different types of networks, and a large amount of this digital content is either classified or private. Encryption technology is a widely used technique and practice in digital information security systems. If the security and reliability of the encryption method is high enough, then the security of digital information can be protected (Hailan Pan, 2018). Therefore, the research into digital image encryption technology and method is an important direction for digital image security protection.

In general, encryption technology or encryption system is mainly based on the requirements of text encryption. At present, the more common encryption system cannot achieve better results in terms of compatibility and encryption quality of digital image encryption. Although digital images can be processed as a two-dimensional data set, cryptographic systems that directly use text-encryption techniques often face problems of inefficiency in encryption and decryption, low practicability, and low security (T. Caulfield; Z.

Cai; Sun Y Q; S.W. Lee). Image data contains distinct features such as redundancy and high pixel correlation. Also, they are typically large in scale, making standard encryption techniques impossible to implement and slow to process. Furthermore, the decrypted content must be the same as the original text, although this criterion is insufficient for image data, because a because a slightly distorted decrypted image is typically accepted as a feature of human insight. Therefore, algorithms designed for textual data cannot be optimised for multimedia data. While the Triple Data Encryption Standard (T-DES) and the International Data Encryption Algorithm (IDEA) provide high security, they may not be suitable for multimedia applications. As a result, well-known encryption algorithms such as the Data Encryption Standard (DES), the Advanced Encryption Standard (AES) and the International Data Encryption Standard (IDEA) have been developed for text data rather than multimedia data

The image encryption algorithms are divided into three categories: position permutation algorithms, value transformation algorithms, and visual transformation algorithms. (Komal D Patel, 2011). In encryption, a plaintext is the original message, ciphertext is the coded message, encryption is the process of converting plaintext to ciphertext, decryption is the process of converting ciphertext to plaintext, and cryptography refers to the many encryption schemes. Cryptography is classified into two types: secret key cryptography and public key cryptography. Secret key cryptography, also known as symmetric key cryptography, is a type of cryptography in which both the sender and the receiver know the same secret code, known as the key. In this sort of cryptography, messages are encrypted by the sender using the key and decrypted by the receiver using the same key. Public key cryptography, also called asymmetric key cryptography, uses a pair of keys for encryption and decryption. With public key cryptography, keys work in pairs of matched public and private keys (Manjit Kaur, 2018).

2.2 Materials and Methods

Various image encryption approaches have been developed so far. With the passage of time, researchers have also applied different types of concepts to improve the security of images. The traditional approaches such as DES, AES, and IDEA, have been obsolete in the case of images but I am going to use the XOR image encryption method in my project. Because the images have different properties as compared to text, many image encryption approaches have been developed during the last few decades.

The preferred reporting items for systematic reviews and meta-analyses (PRISMA) method is used to obtain accurate results in order to summarize the existing work in image encryption. The method consists of four phases: identification, screening, eligibility, and inclusion, that provide the accurate report for the analysis. The PRISMA method ensures that the final outcome is free of review study biases; yet, most reviews may suffer from selective outcome reports. Furthermore, a large number of sources can be used by providing relevant Boolean queries to eliminate items that are irrelevant. The model starts with identifying the sources of the articles, followed by screening to eliminate duplicates and irrelevant articles by going through the titles and abstracts. Following that, the remaining papers will be screened further by reading the entire paper, and any articles that are irrelevant to the subject will be excluded from the review studies.

2.3 Evaluation Parameters

Evaluation parameters are used to evaluate or assess the performance of image encryption. There are many security attacks performed by the attacker to break the encryption approach and find the key. Cryptanalysis is mainly used by attackers to study the encryption approach (C. Zhu; S. Zhu). Therefore, the plaintext statistics and the secret key must be hidden.

Image encryption strength can be assessed using security and quality analyses. The quality analysis evaluates the image quality of decrypted image by using peak signal-to-noise ratio, mean square error, among others. Statistical analysis, differential analysis, and key analysis are all part of the security analyses. Since the key determines the performance of the image encryption, it is best to use a large key so that it cannot be guessed easily.

The purpose of the evaluation of the encryption algorithm is mainly to assess the security of the encryption algorithm. The security evaluation of this study is mainly analysed from the randomness of the sequence and the effect of mapping scrambling. The number of random sequences has a significant impact on digital image encryption security. The chaotic system generates a pseudorandom signal with high initial sensitivity, randomness, and unpredictability. It is well suited for application in the encryption system. Therefore, the encryption system based on chaotic system is very widely used in practical applications. Practically, chaotic sequences are created and generated by using chaotic systems, and then chaotic sequences and encrypted data are fused or coded to obtain the encrypted ciphertext sequence. The chaotic encryption system is a type of symmetric encryption system. In the process of data decryption, the same chaotic system and initial value are required to generate the pseudorandom sequence number, and then the ciphertext is calculated correspondingly to acquire the plaintext sequence. It is very efficient and fast to encrypt data by using chaotic map's pseudorandom sequence number. However, with the development and advancement of information security technology, the challenge of key sequence security in an encryption system based on a single chaotic map has become gradually convex. Because the chaotic encryption sequence is generated by chaotic mapping and there are only 10 types of chaotic systems, the attacker can analyse the chaotic system utilized in the encryption process based on the item space construction method. Unless the entire encryption process is completely secure, the attacker can crack the parameter values and initial values of the chaotic sequence

using certain plaintext and ciphertext pairs, hence, breaking the encryption algorithm (Hailan Pan, 2018).

2.4 Image Encryption Approaches

There are different types of image encryption approaches. They include: spatial, transform, optical and compressive sensing based image encryption approaches.

Spatial domain approaches are those that directly manipulate the pixels of the image. There are several spatial domain-based image encryption described in the literature. However, we have considered the most well-known approaches such as chaotic-based, elliptic curve-based, fuzzy-based, DNA, and Metaheuristics-based approaches. Chaotic maps are extremely important in the field of encryption. These maps generate random numbers that are used as encryption keys (M. Kaur, 2018). The reason is its properties such as dynamic and deterministic nature, sensitive to initial conditions, and ergodicity. There are different types of chaotic maps but the main ones are: one-dimensional and higher-dimensional chaotic maps. Chaotic maps help in performing the confusion and diffusion operations in the encryption process (J. Liu). Elliptic curve cryptography (ECC) uses the least amount of memory and has a tiny key size (S. Toughi). Optical image encryption approach is widely utilized in the field of cryptography due to its good computational speed and parallel processing. In this, a double random-phase encoding (DRPE) approach is used to convert the plain image into stationary white noise (Y. Qin, 2014).

2.5 Literature Survey

Cryptography is necessary when transferring secret information over a public network. Confidentiality, authentication, key exchange, integrity, and digital signature are the major security services required in communication currently. Hongjun Liu et al. (Honjun Liu, 2012) proposed an image encryption method based on confusion and diffusion techniques. The method permutes the pixels by randomly changing the nucleotide into its base pair, while the other generates new keys based on the plain image and the common keys, which can cause the initial conditions of the chaotic maps change automatically in every encryption process. After permuting the rows and columns using the arrays generated by piecewise linear chaotic map (PWLCM), each pixel of the original image is encoded into four nucleotides using deoxyribonucleic acid (DNA) coding.

Maniccam and Bourbakis (S. S Maniccam, 2001) developed a method for both lossless compression and encryption of binary and grayscale images. An overview of SCAN, compression and decompression algorithms, encryption and decryption algorithms and the test results of the methodology are presented. Maniccam and Bourbakis (S.S Maniccam, 2004) introduced an image and video encryption system based on SCAN patterns. The image is encrypted using SCAN-based pixel permutation and a substitution rule to create an iterated product cypher.

Khaled Loukhaoukha et al. (Khaled Loukhaoukha, 2012) proposed an image encryption technique based on the principle of Rubik’s cube. The pixel positions are reordered using the Rubik’s cube principle to produce a scrambled version of the original image. To obtain the cipher image, the bitwise XOR operation is applied to the scrambled image's odd rows and columns first, and subsequently to the even rows and columns using secret keys.

Avi Dixit et al. (Avi Dixit, 2012) proposed an image encryption technique based permutation and rotational XOR techniques. Here, the pseudorandom index generator is used to generate the 8 bit key. The pixel decimal value is converted into an 8-bit binary stream. Each pixel of the original image is permuted based on the 8 bit key. Then the entire image is divided into blocks of size 8×8 pixels and the blocks are permutated using same 8 bits key. The binary stream is then transformed to a decimal value and used as the cipher image.

2.6 Related Works

Image encryption has sparked the interest of both scholars and practitioners due to its critical role in protecting the security and integrity of visual data in an increasingly linked and data-driven society. This literature review's related works section delves into the rich tapestry of research, approaches, and breakthroughs that have shaped the landscape of image encryption. This section attempts to provide a complete overview of the various approaches and insights that have contributed to the evolution of image encryption systems by examining the existing body of knowledge.

Deng and Zong (Z. Deng, 2019) introduced a chaotic map-based digital picture encryption algorithm. The algorithm has sensitive key, large key space, and uniform pixel distribution after encryption, so it can effectively protect the security of encrypted images. However, because the technique uses image scrambling to achieve encryption and ignores the choice of plaintext attack, the algorithm is vulnerable to the choice of plaintext attack. The results show that the technique can effectively resist plaintext selection attacks, is particularly sensitive to minor changes in the plaintext, and the encrypted image entirely completely the image of the original image.

Wu et al. (X. Wu, 2016) introduced a new greyscale image technique. In this technique, Pascal's matrix of order 4 is paired with a seven-dimensional hyperchaotic system. They generated random sequences using a seven-dimensional hyperchaotic system, and we chose three of these sequences to shift the pixel position. The diffused grayscale image is divided into four sub-blocks, and the pixel values for each sub-block are modified using Pascal's matrix. To increase security, confusion and dispersion techniques are used twice. The proposed technique's security and robustness testing revealed excellent sensitivity to any pixel or key change and robustness in the face of all common attacks.

Ye et al. (X. Ye, 2020) proposed a technique using a new mixed chaotic circuit with memristors. The mathematical model was created using the circuit equations, and the system's equilibrium point was calculated. The NIST successfully tested the chaotic system's sequences. After then, the memristive chaotic system was used to create a novel encryption technique. The security was assessed using the grey histogram, correlation, NPCR, UACI, and information entropy; the results indicate that the new encryption technique has very high security. This new mixed memristive chaotic circuit model has a complete RLC structure as well as a number of memristors.

Khan et al. (S. Khan, 2019) proposed a new image encryption algorithm for classified or personal images to prevent the images from being stolen or exploited. Even if hackers succeed in stealing them, their approach ensures image security and distinguishes itself from others in the following ways. To begin, the binary form of image is subdivided, and a new Feistel-based rapid bit inversion algorithm is used to modify the pixel values and reduce the correlation impact. Second, after reviewing past research, they discovered that the DNA encoding rules are mainly fixed and are sometimes used as a key, which is a shortcoming of any algorithm since relevant information from the ciphered image can be recovered faster than the algorithm in which unfixed rules. Third, the Moore neighbourhood local rule structure is

used in the 2D-CA component, which implies that a unique mix of neighbours is used for each matrix, which improves performance while decreasing complexity. Furthermore, a strategy based on local rules (LR) determines how many, which, and whose cells will participate in the next matrix update process. Finally, we used the secure hash (SHA-256) technique to extract the secret key from the plain image, while the double hash function allows us to transfer the secret key over standard channel. As a result, their proposed encryption technique is more secure and sensitive to the plain image. While our technique has substantial limitations, such as only working with grayscale images, it can be implemented for colour images in the future, despite the difficulties of dealing with the RGB channel of a coloured image.

2.7 Relevance

The first relevance of image encryption is to protect personal privacy and security. The widespread availability of smartphones, social media and digital cameras has resulted in an unprecedented flow of digital images. Though this exposure has been good, it has also introduced new dangers. In an era where images in the wrong hands can be used to damage the someone's reputation, it is essential to safeguard it from falling into the wrong hands, and even if they fall into the wrong hands, the third party must not be able to access the image's contents. Image encryption provide services that ensure that personal images are not understood if they fall into the wrong hands. Image provides these services to address vulnerabilities by converting the original image into a form incomprehensible using complex mathematical techniques. It does this using a key that encrypts the image into an incomprehensible form. The encryption simply creates a protective barrier around the image by prohibiting unauthorised access and ensuring the remains incomprehensible. The encrypted image can only be decrypted to a comprehensible form using a decryption key possessed by the authorised recipient.

In conclusion, in a world where digital images play an important part in communication, it critical to prioritise the safety of images by employing image encryption to assure image security and security. Image encryption is a powerful technique that allows people to safeguard their personal images while also preserving their personal privacy and security.

2.8 Conclusion

In this comprehensive literature review, we have embarked on a journey through the introduction, materials and methods, evaluation parameters, the image encryption approaches, literature survey, related works, and the relevance of image encryption across various fields. It is very clear that the importance of image encryption goes beyond algorithms and codes. In other words, image encryption reflects our connection with digital information and the need for the protection of digital information such as images. It is also clear that the journey of image encryption does not end where it is now. The field of image encryption will continue to evolve as a result of technological advancements. As we draw the curtains on this study, it becomes evident that image encryption is not only a technological endeavour but a critical aspect of modern digital existence, playing a pivotal role in protecting the confidentiality, integrity, and authenticity of visual information in an increasingly interconnected world.

CHAPTER THREE: SYSTEM ANALYSIS AND DESIGN

3.1 Methodology

In my project titled “Image Encryption”, I used the agile methodology. Agile methodology is a project management technique that involves breaking down projects into phases and emphasizes continuous collaboration and improvement. In other words, agile methodology is an iterative approach to managing software development projects that focuses on continuous releases and customer feedback. Agile methodology been applied in software development has shown its effectiveness in a wide range of projects by emphasizing collaboration, flexibility, and incremental progress. Agile methodology consists of a cycle of planning, executing and evaluating. Using this method, I broke down the project development into small iterations or sprints, with defined goals for each enabling continuous improvement of the encryption process.

The first step I took in the process was creating a backlog. A backlog is a build-up of work that needs to be completed. But under agile methodology, a backlog is a list of deliverables that should be implemented as part of a project or product development. This allows me to identify the tasks required to complete the project. Identifying the tasks involved in the project’s development simplifies things. I began by designing a small Graphical User Interface (GUI) that will help me input the encryption key. Creating a backlog helped me understand the project and what needs to be done to get a good outcome.

The second step I took was planning the small iterations also known as sprints in the project. Sprint planning is intended to define what can be delivered in the sprint and how they will work. It is an important step in agile methodology. In this stage, I first did a detailed breakdown of the tasks required to finish my project. After the break down, I assigned a goal

to each task. That is, I outlined what every task was supposed to accomplish and what it is expected from each task.

After planning the sprints, I moved on to the development of the algorithm and the encryption implementation. In this step, the conceptual aspects of my image encryption project came to life through coding, execution , and the creation of software components. At this point, I wrote the code for the encryption algorithm. This is the point at which I transitioned the process from theoretical concepts into actual lines of code. After finishing the code, I made sure the encryption algorithm was correctly implemented. Another important step I took here was making sure not to forget about the encryption key. This is because, without an encryption key, the algorithm losses its purpose.

I then moved to the testing phase after the encryption development and implementation. I performed an extensive testing to make sure the algorithm executes as expected. I ran various tests on the algorithm to make sure the vulnerability was little. I tried decrypting it using a key other than the one used for the encryption, and it worked as expected because the wrong key did not decrypt the encrypted image. I then evaluated the effectiveness and speed of the encryption process to check the algorithm's efficiency and how it responds to images especially large images. I made sure there were no bugs in code that might hinder or slow the performance of the algorithm. I fixed any bugs that I found in order to increase the algorithm's performance.

I began my project documentation after completing the encryption development and implementation. Documentation is also essential in agile methodology. It is essential because it captures the complex inner workings of the encryption process and lays the foundation for the project's longevity. It offers a thorough examination of the project, explaining its components and methodologies. Documentation in agile methodology bridges the gap between the abstract concepts and the practical implementation in the project. Though agile

methodology prioritises software development over documentation, it does not dismiss the importance of documentation.

In conclusion, the successful completion of my "Image Encryption" project work using Agile methodology showcases the importance of an iterative, collaborative, and adaptable approach in software development. Agile methodology's values of continuous improvement and flexibility harmonize perfectly with the complexities of encryption projects, resulting in an encryption solution that is both robust and user-centric. Through my agile journey of planning, executing, testing, and documenting, the project not only achieved its technical goals but also demonstrated a methodology that can be applied effectively to a wide range of software development endeavours.

3.2 Requirement Analysis

1. Functional Requirements: In software engineering, Functional requirements are product features or functions that developers must implement to enable users to accomplish their tasks. Here are some of my project's functional requirements:
    i. Image Selection: Users must be able to select and encrypt an image file in the JPG or PNG formats.
    ii. Key Input: The algorithm must permit users to enter a secret key for encryption.
    iii. Encryption Process: The algorithm must be able to perform encryption on the selected image using the provided key.
    iv. Saving Encrypted Image: The system must allow users save the encrypted image back to the same location as the original image file.
    v. User Feedback: The system must display a success message when the encryption process is completed.

2. Non-functional Requirements: Non-Functional Requirement is a requirement that does not relate to functionality, but to attributes such as reliability, efficiency, usability, maintainability and portability. Here are some of my project's non-functional requirements:
    i. Security: The image encryption algorithm should be to able provide basic protection against attackers, preventing the original image from being easily recognised.
    ii. Usability: The user interface should be simple to use. That is, it must be simple enough to allow users to select images easily.
    iii. Performance: The algorithm must be capable of efficiently handling encryption for images of various sizes and formats.
    iv. Compatibility: The algorithm must be compatible with common image formats such as JPG and PNG. Also, the Graphical User Interface (GUI) must be compatible with the user's system and screen resolution.
    v. Maintainability: The code should be well-structured and simple to understand, making future updates or changes simple.

3.3 Flowchart/ Use Case Diagrams

A flowchart is a graphical representation of a process, system, or computer algorithm. They are widely used in a variety of fields to document, study, plan, improve, and communicate often complicated processes in clear, simple diagrams. My project's flowchart is shown below:

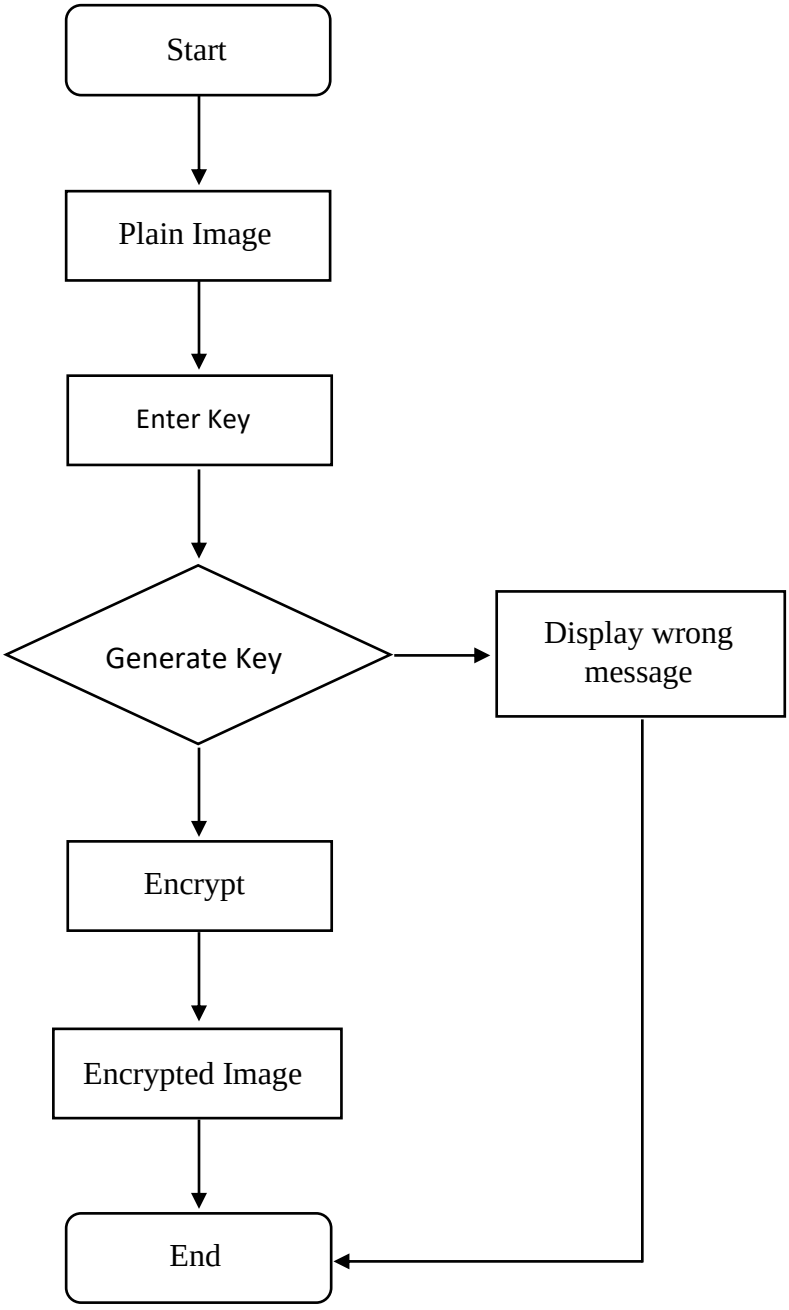


Figure 1: Flowchart Diagram

A use case diagram is used to describe a system's high-level functionality and scope. These diagrams also show how the system and its actors interact with one another. In use-case diagrams, the use cases and actors describe what the system does and how the actors interact with it, but not how the system runs internally.

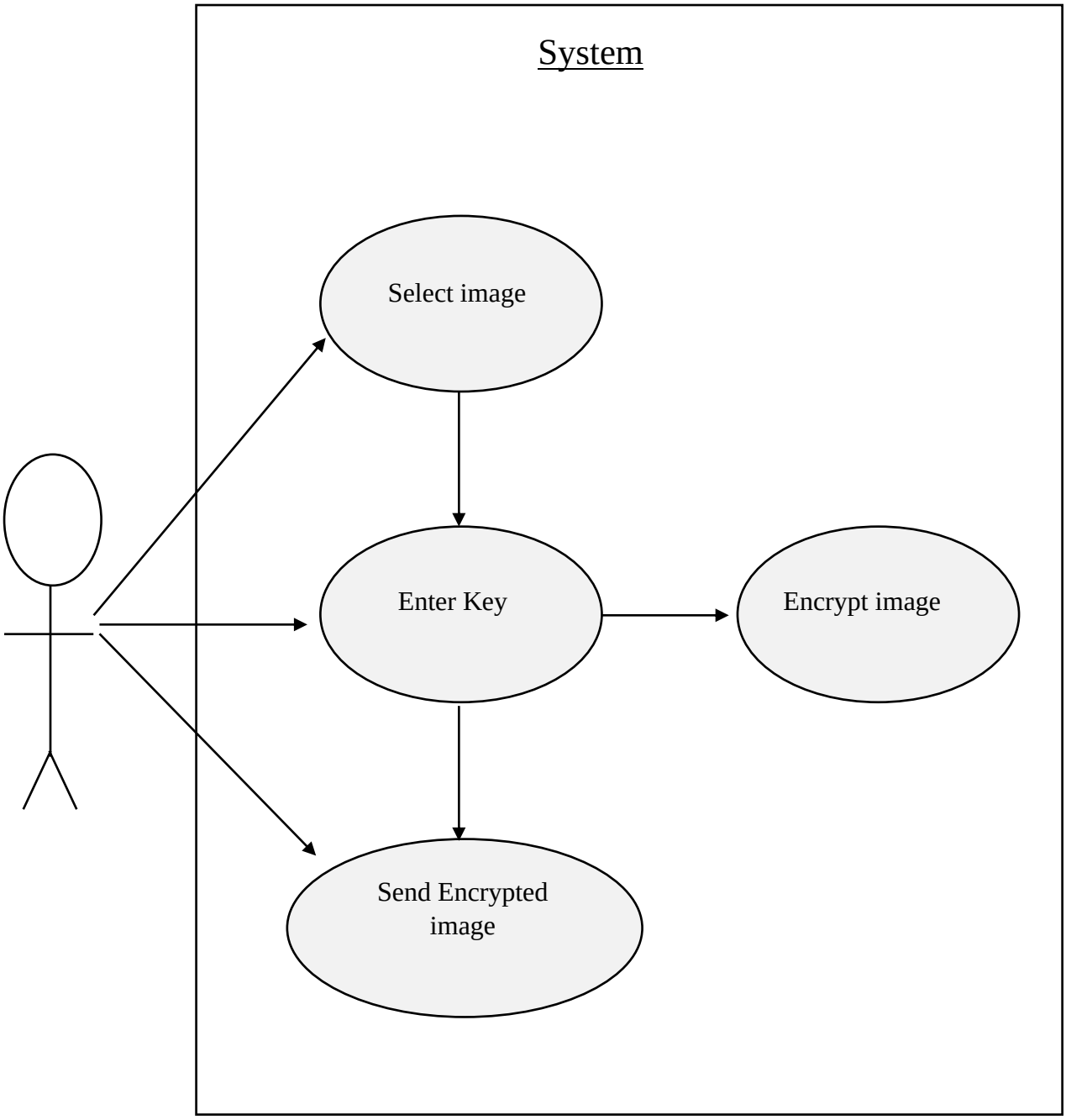


Figure 2: Use Case Diagram

CHAPTER FOUR: IMPLEMENTATION AND EVALUATION

4.1 Introduction

This chapter delves into the project's implementation and evaluation phases. It is focused on the implementation, presentation, performance and testing of the system before it is released.

4.2 Implementation

Implementation is the process of carrying out the plan. That is, it is the process of converting the virtual design of the system into an actual design. It is a critical component of the system's overall security. A well-implemented image encryption algorithm can provide a high level of security for the data being protected. This image encryption algorithm was created with the use of virtual studio code and the Python programming language. The images below demonstrate how the system or algorithm works:

I'm about to encrypt this image.

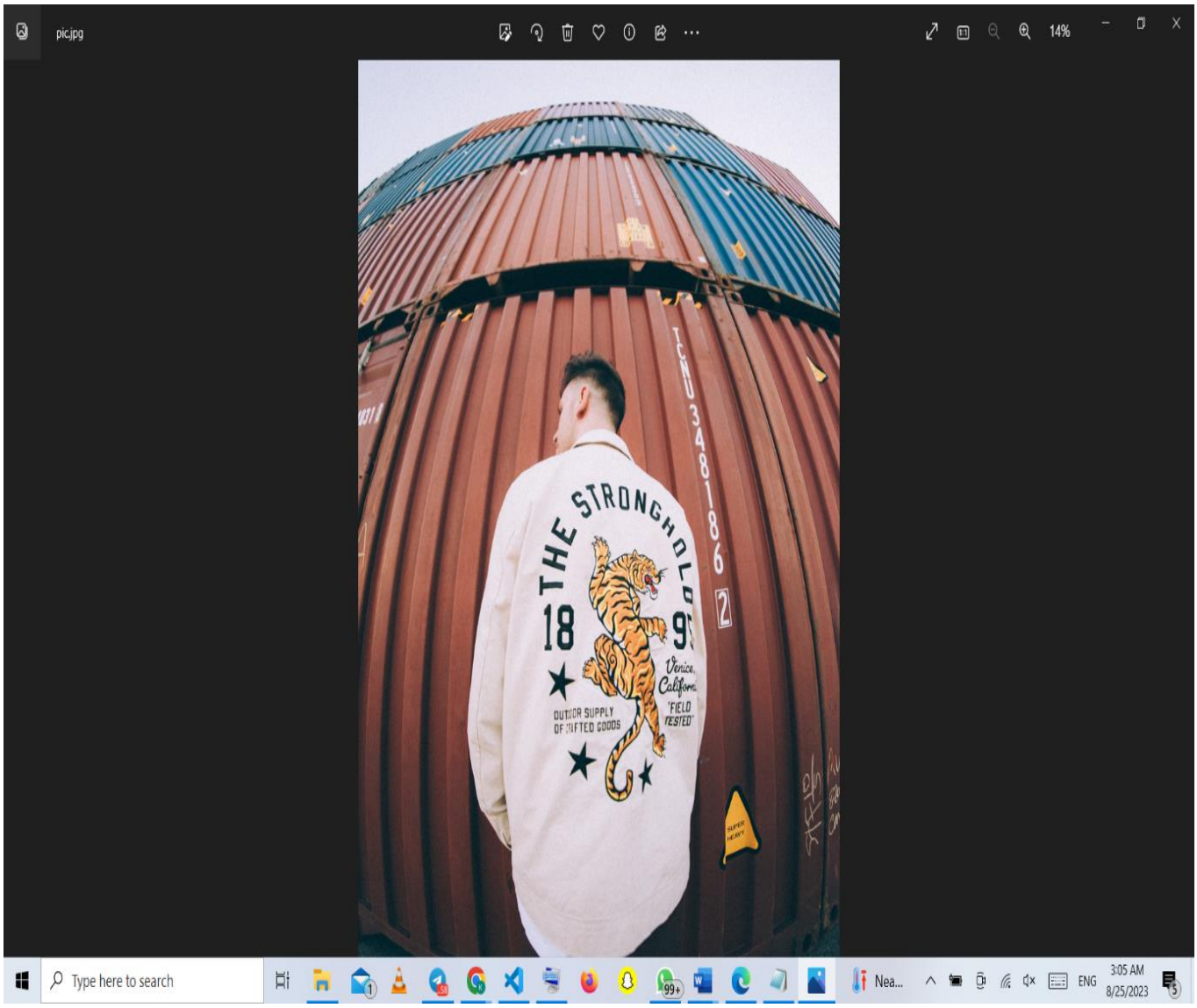


Figure 3: Image before Encryption

This is the Graphical User Interface (GUI) after you run the code

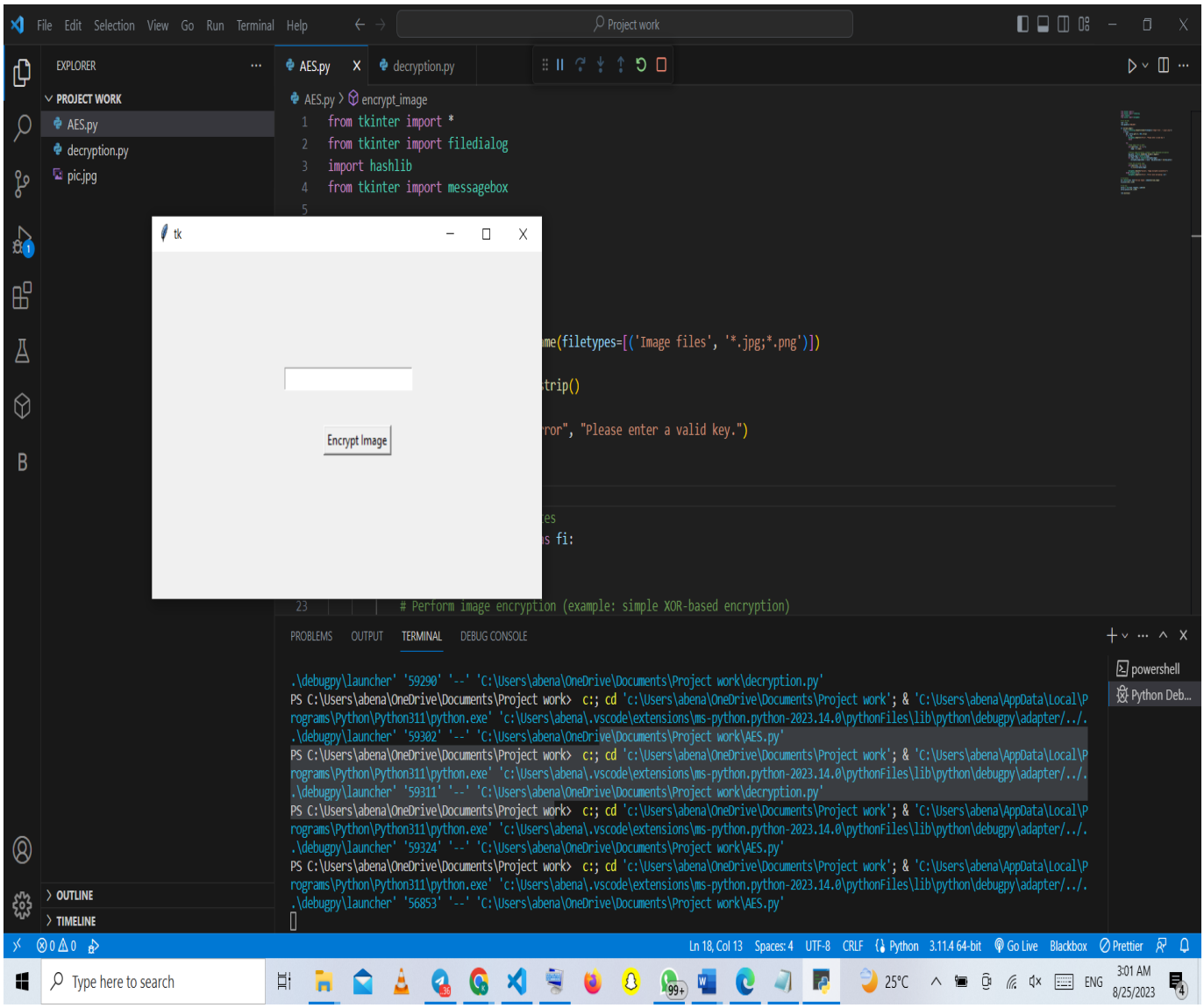


Figure 4: Simple GUI of the Algorithm

You enter your secret key before you select the image you want to encrypt

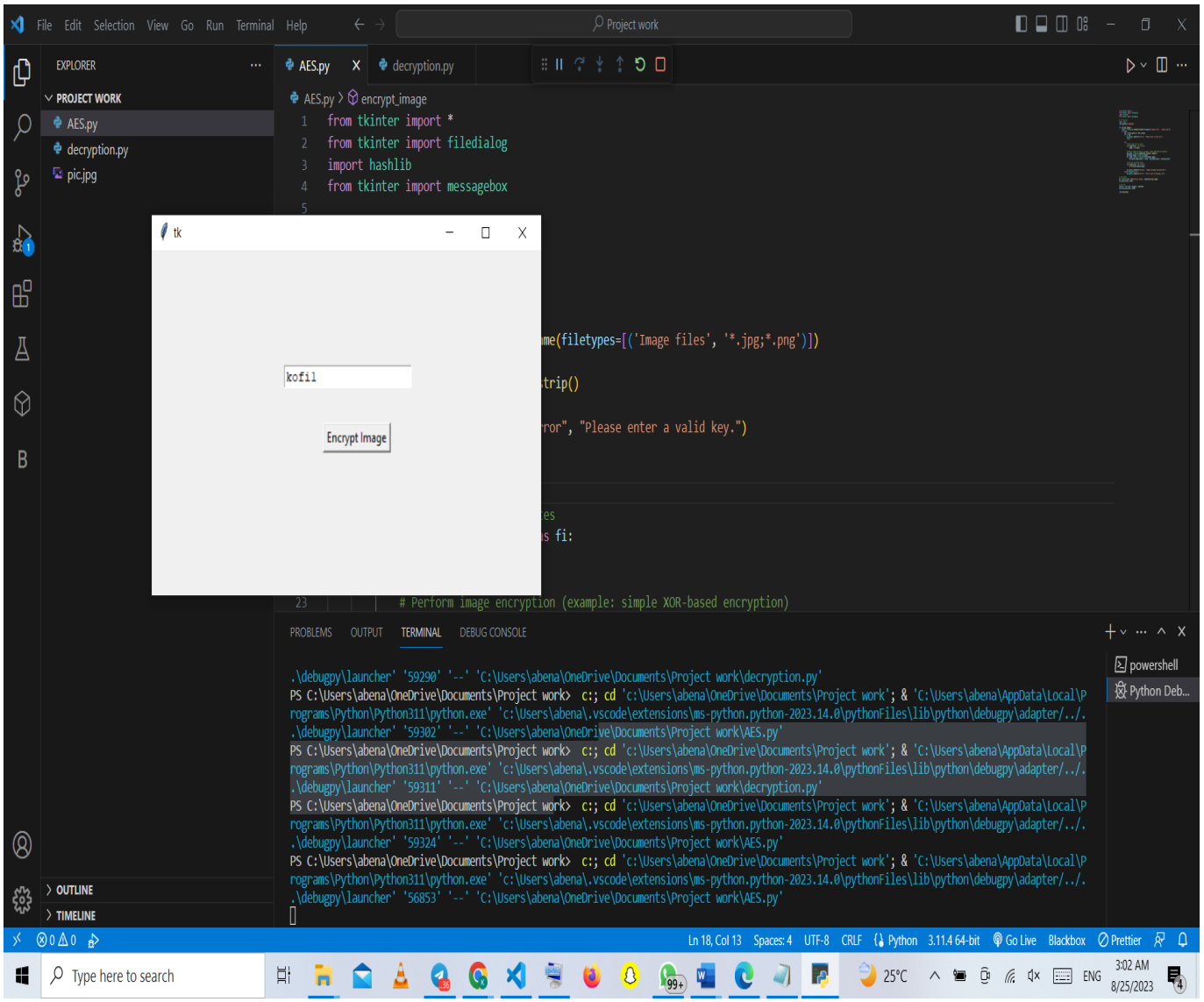


Figure 5: Encryption Key

In the image above, the key entered is “kofi1”,but you can type in any key you want. The larger the key, the more difficult it is to breakdown the secret if intercepted by attackers. Click on the “Encrypt image” button to move to the next phase after typing the key.

Select the image you want to encrypt and click on open.

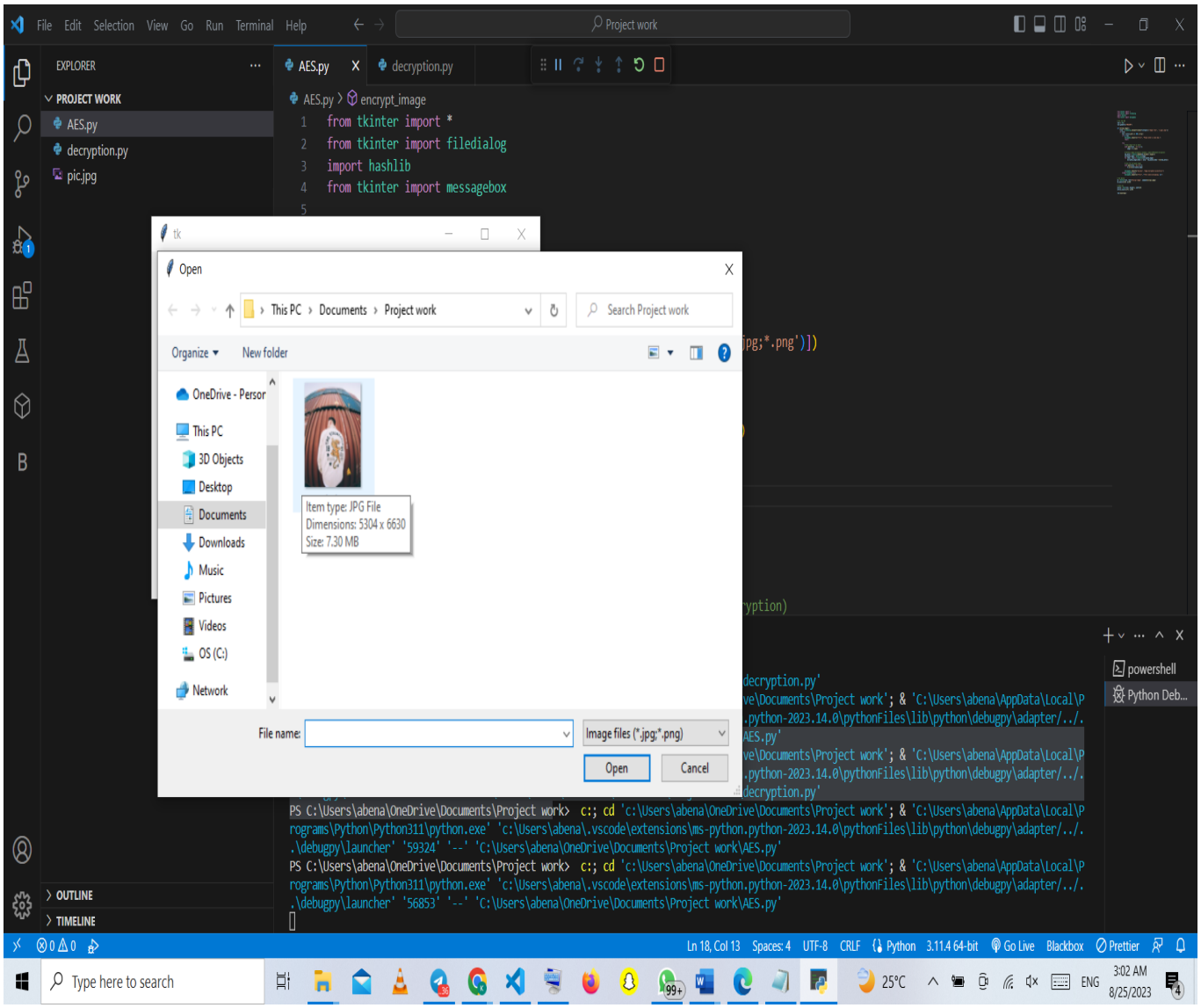


Figure 6: Image Selection Window

You will get a message reading “Image encrypted successfully!”

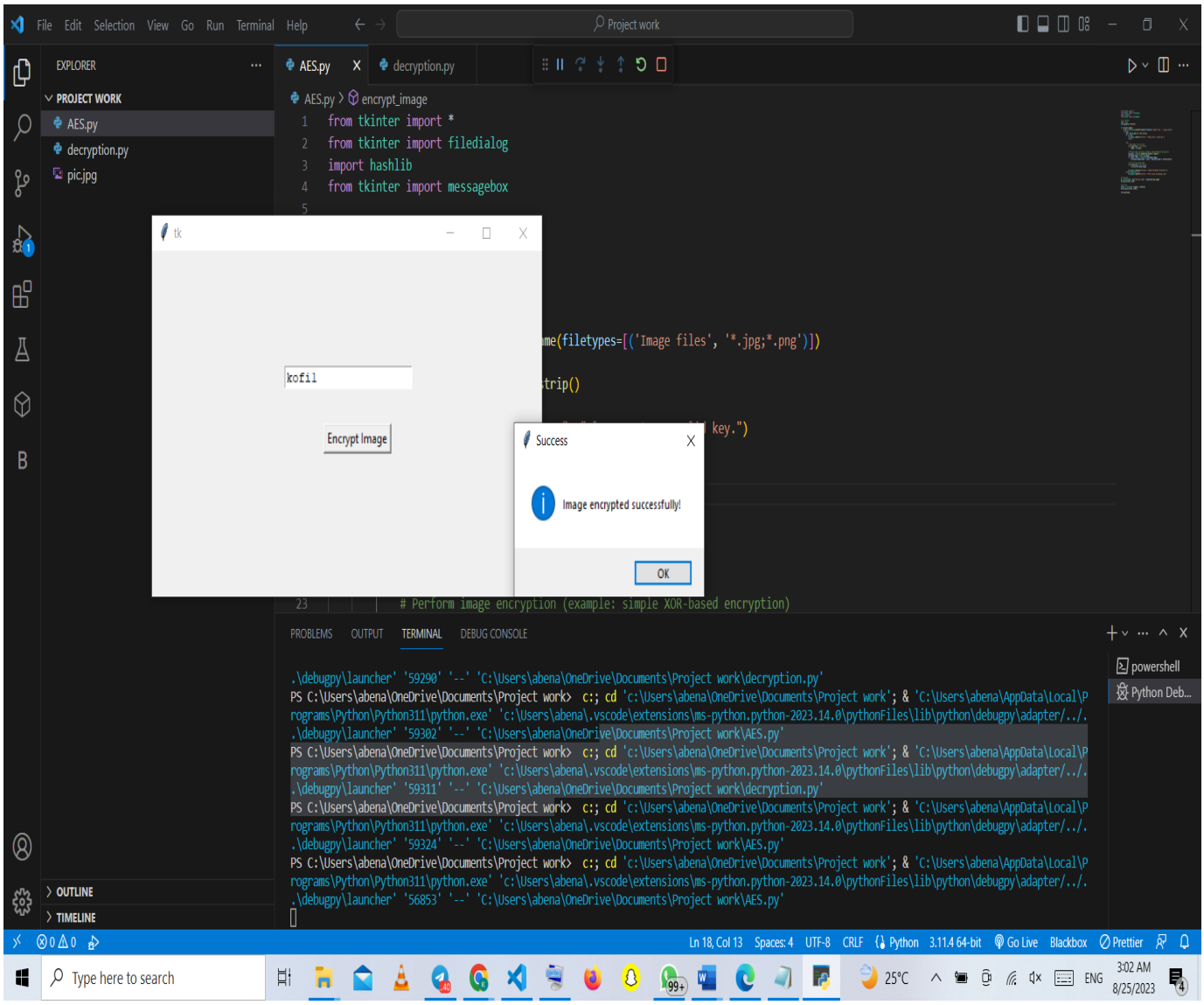


Figure 7: Encryption Successful Message

This is the image after encryption

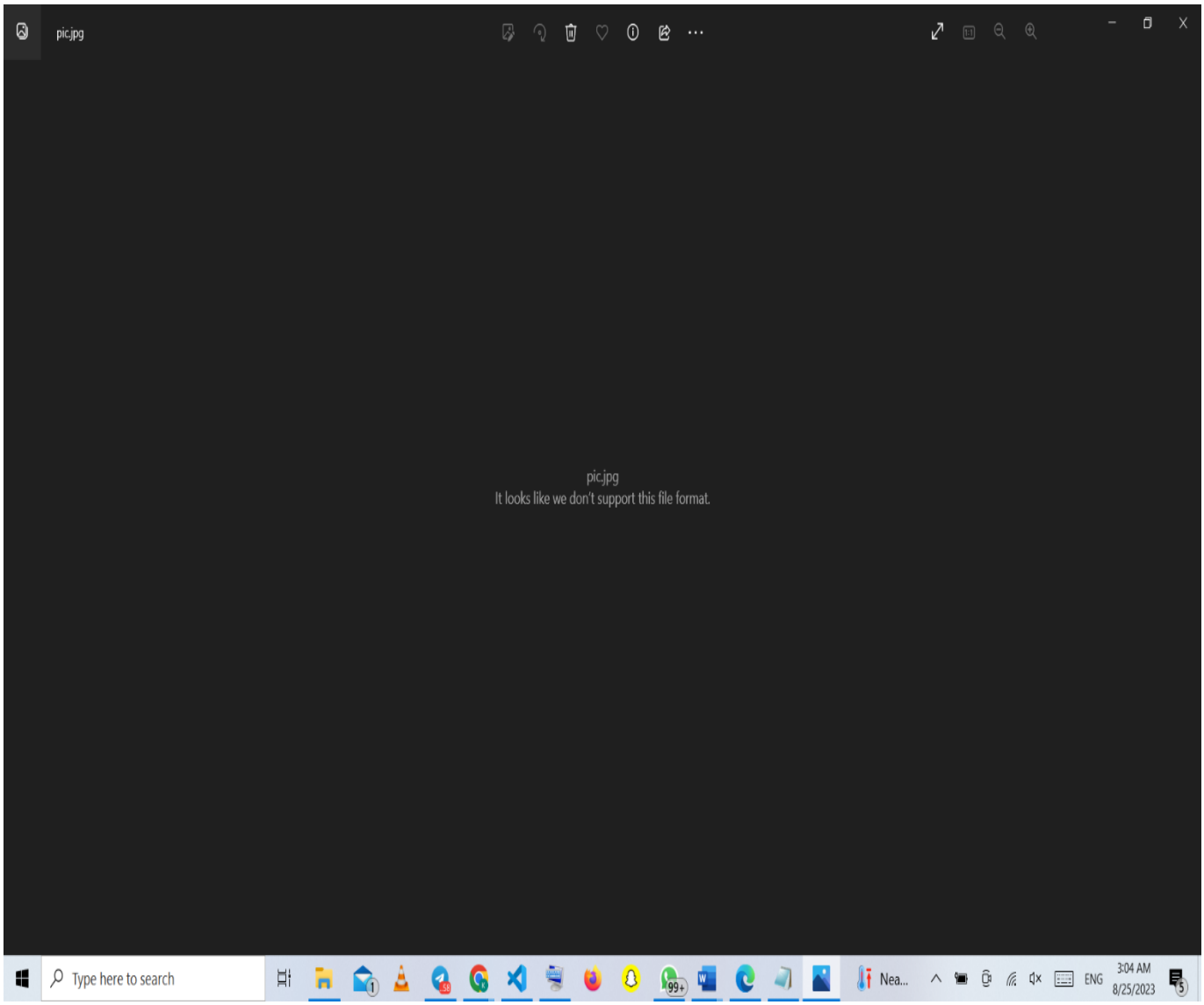


Figure 8: Image after Encryption

This is the message you get if you don’t type a code before selecting an image and try to encrypt

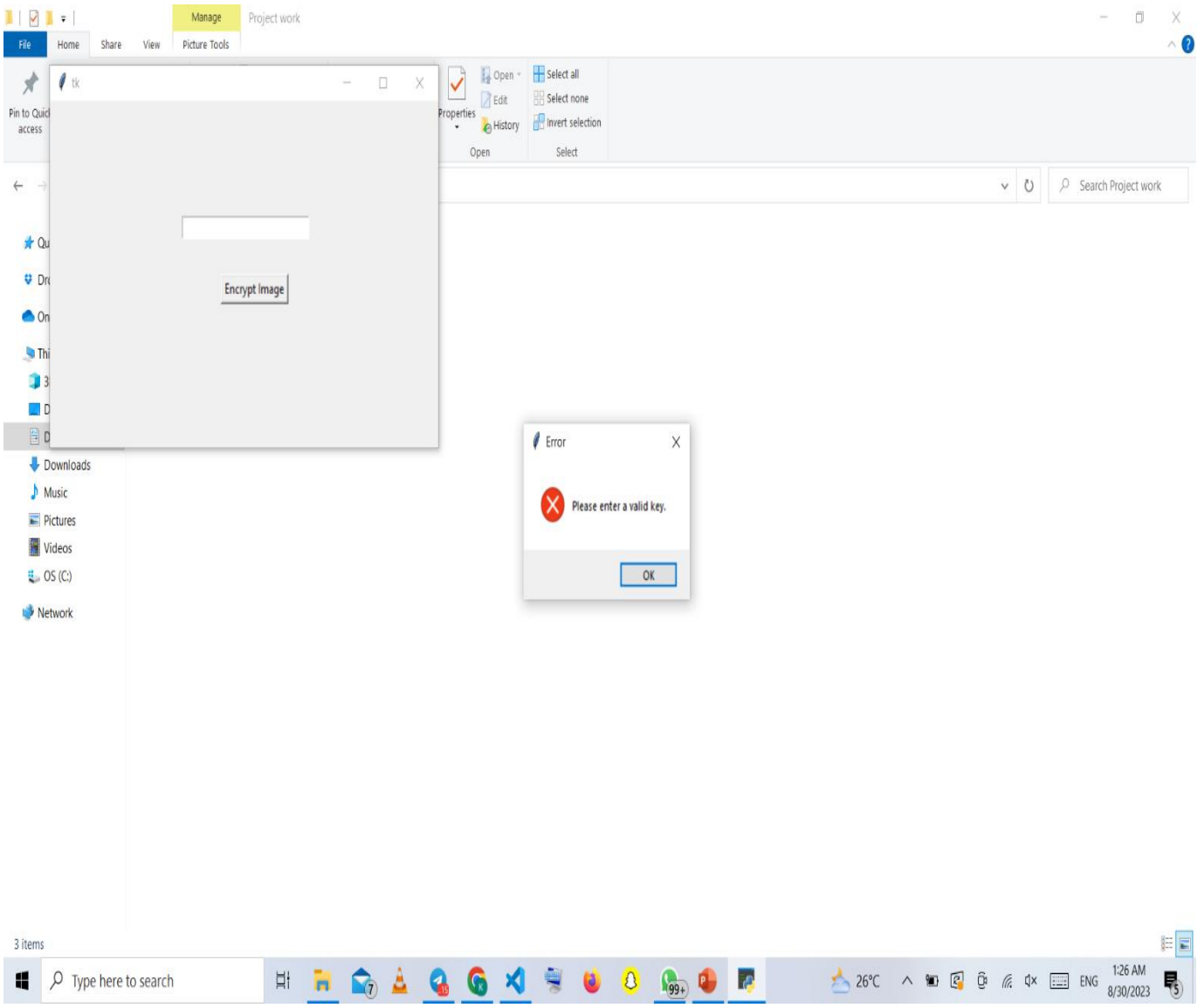


Figure 9: Error Message

4.3 Testing

Testing is the process of evaluating and verifying that a software application does what is designed to do. This helps in the prevention of bugs, reduction of development costs and the improvement of software application performance. It also ensures the application's functionality, security, and reliability. This essay delves into the testing process, looking into functional testing, security analysis, and efficiency testing.

Functional testing is used to ensure that the code works as it should. This can be done by encrypting a simple image to test that the algorithm is valid and functions as expected. I also tested the button and textbox in the Graphical User Interface (GUI) to ensure they functioned properly. After that, I tested the algorithm's file selection part. There were no issues, so I proceeded to the next section of the algorithm, which is the success and error message. There were no issues there either. So, I went to check if the image selected had been encrypted and it was indeed encrypted.

Security analysis is the second step in testing the algorithm. Given the nature of image encryption, security analysis is crucial. To test the algorithm's security, I encrypted the image without a secret key to see if it would work, but it didn't. Then, without knowing the secret key, I attempted to decrypt the encrypted image. I was unable to decrypt, indicating that the algorithm is secure.

The code's efficiency is tested as the last step I used in the testing process. This can be accomplished by analysing the time it takes to encrypt an image. The more efficiently the code can encrypt images, the faster it is. I measured the time it took to encrypt a basic image to assess the code's efficiency. The code encrypted the image in a matter of seconds. This shows that the code is effective.

Finally, evaluating the image encryption algorithm gave me insight into the algorithm's functionality, security, and efficiency. This procedure helped me in developing a robust and secure algorithm capable of protecting digital images from unauthorised access and tampering.

4.4 Video Pitch

https://www.loom.com/share/c5fdd94859ce4de1acec385429fa100b

CHAPTER FIVE: CONCLUSION AND FUTURE WORKS

5.1 Chapter Overview

Digital images tend to be kept or exchanged across insecure channels, exposing them to unauthorised access. Image encryption is a technique for protecting the secrecy of digital images by converting them into a format that unauthorised users cannot easily understand. A variety of methodologies can be used to evaluate the security and effectiveness of image encryption methods. A security analysis, which identifies potential attack vectors and assesses the likelihood of successful attacks, can be used to assess security. Performance analysis can be used to assess efficiency by measuring the time and resources required to encrypt and decrypt images. Image encryption is an important technique for keeping digital images private. Developers can build image encryption solutions with a high level of security by carefully picking an encryption method and effectively implementing it.

5.2 Summary of Work

My project looks deeply into the subject of image encryption. To create the picture encryption algorithm, I used the Python computer programming language and Visual Studio code. The project includes a number of libraries that enabled the encryption to be implemented. In summary, my project employed a Graphical User Interface (GUI) that makes it possible for users to encrypt images without much difficulty. The GUI was implemented using the “tkinter” library.

My project also focuses on the encryption procedure. After running the code, the user will be provided with a graphical user interface (GUI) that includes a textbox and a button. The textbox receives or helps the user input the secret key used to encrypt the image. The "Encrypt

image" button also assists in moving the user to the next phase of the encryption procedure. That is, the button takes the user to the image selection phase. My project supports image files with the "JPG" and "PNG" file extensions. The algorithm obtains the key to encrypt the image when you enter the key and select the image. If you don't provide any secret key, you'll get an error message. However, if you enter a code before picking an image, it will encrypt the image and display the message "Image encrypted successfully!".

In conclusion my project work provides a simplified implementation of image encryption that is user friendly because of the Graphical User Interface (GUI) feature it has.

5.3 Future Work

This study looked at an image encryption algorithm that used the XOR encryption method. I built the project in Python and used the "tkinter" library to create a basic Graphical User Interface (GUI) for encrypting the images. While the current algorithm is functional, there are several future improvements or updates that can be made to improve its functionality and usability.

The first thing I'd like to do or address is improving the user interface. The existing user interface is really good and could be improved. As a result, I'll endeavour to improve the user interface. I will improve the interface's visual design. To make the user interface more fascinating, I will improve or adjust the interface's appearance or visual design to make it more professional and attractive. During the encryption process, I will also include a progress bar feedback element. This allows the user to track the encryption's progress.

In addition, I'd like to use a more secure algorithm, such as the Advanced Encryption Standard (AES). Though the current algorithm is secure, it employs a basic XOR encryption algorithm, which is not as secure as other algorithms such as Data Encryption Standard (DES)

and AES. As a result, it is preferable to explore the possibility of using a more secure algorithm in the future.

Finally, I would change the algorithm to support multiple image formats. At the moment, the algorithm only supports JPEG and PNG image formats. In future works or enhancements, I would like to extend the algorithm's image support formats to include more formats such as GIF, BMP, and TIFF, among others.

In conclusion, while the existing code offers a foundation for image encryption, there is much potential for future work and modifications to increase its functionality, security, and usability. The direction of these future works should be driven by the application's specific demands and aims.

References

Avi Dixit, P. D. (2012). Image encryption using permutation and rotational XOR technique. 1-9.

C. Zhu, G. W. (2018). Improved cryptanalysis and enhancements of an image encryption scheme using combined 1d chaotic maps. 843.

Hailan Pan, Y. L. (2018, December 13). *SpringerOpen.* Retrieved from SpringerOpen: https://jivp-eurasipjournals.springeropen.com/articles/10.1186/s13640-018-0386-3#ref-CR1

Honjun Liu, X. W. (2012). Image encryption using DNA complementary rule and chaotic maps . 1457-1466.

J. Liu, S. T. (2019). A novel fourth order chaotic system and its algorithm for medical image encryption. 1637-1657.

Khaled Loukhaoukha, J.-Y. C. (2012). A secure image encryption algorithm based on Rubik's cube principle . 1-13.

Komal D Patel, S. B. (2011, November). Retrieved from https://www.researchgate.net/profile/Sonal-Belani/publication/279206672_Image_Encryption_Using_Different_Techniques_A_Review/links/5590ff9508aed6ec4bf685ab/Image-Encryption-Using-Different-Techniques-A-Review.pdf

M. Kaur, V. K. (2018). Efficient image encryption method based on improved Lorenz chaotic system. 562-564.

Manjit Kaur, V. K. (2018). *SpringerLink.* Retrieved from https://link.springer.com/article/10.1007/s11831-018-9298-8

S. Khan, L. H. (2019). A new hybrid image encryption algorithm based on 2D-CA, FSM-DNA rule generator, and FSBI. 81333-81350.

S. S Maniccam, N. B. (2001). Lossless image compression and encryption using scan patterns . *Pattern Recognition* , 1229-1245.

S. Toughi, M. H. (2017). An image encryption scheme based on elliptic curve pseudo random and advanced encryption system . 217-227.

S. Zhu, C. Z. (2019). Plaintext-related image encryption algorithm based on block structure and five-dimensional chaotic map. 147106-1477118.

S.S Maniccam, N. B. (2004). Image and video encryption using scan patterns. 725-737.

S.W. Lee, S. P. (2017). Smart Door Lock Systems using encryption technology [J]. 27(1), 65–71.

Sun Y Q, W. X. (2017). Information encryption technology with strong robustness based on QR code and matrix mapping [J]. *Packaging Engineering*, 38, 194-199.

T. Caulfield, C. I. (2016, February). Discrete Choice, Social Interaction, and Policy in Encryption Technology Adoption (Short Paper). *In International Conference on Financial Cryptography and Data Security*, 271-279.

X. Wu, D. W. (2016). A novel lossless color image encryption scheme using 2d dwt and 6d hyperchaotic system. *Information Sciences, vol. 349-350*, 137-153.

X. Ye, X. W. (2020). A new chaotic circuit with multiple memristors and its application in image encryption. 1489-1506.

Y. Qin, Q. G. (2014). Multiple-image encryption in an interference-based scheme by lateral shift multiplexing . 220-225.

Z. Cai, D. H. (2017). Research on DES Data Encryption Technology in Network Information Security [J]. *Computer Measurement & Control*, 25, 241-247.

Z. Deng, S. Z. (2019). A digital image encryption algorithm based on chaotic mapping . *Journal of Algorithms and Computational Technology, vol. 13*.

APPENDIX A: Figures

Figure 1: Flowchart Diagram of the image encryption algorithm…….....Chapter 3.3

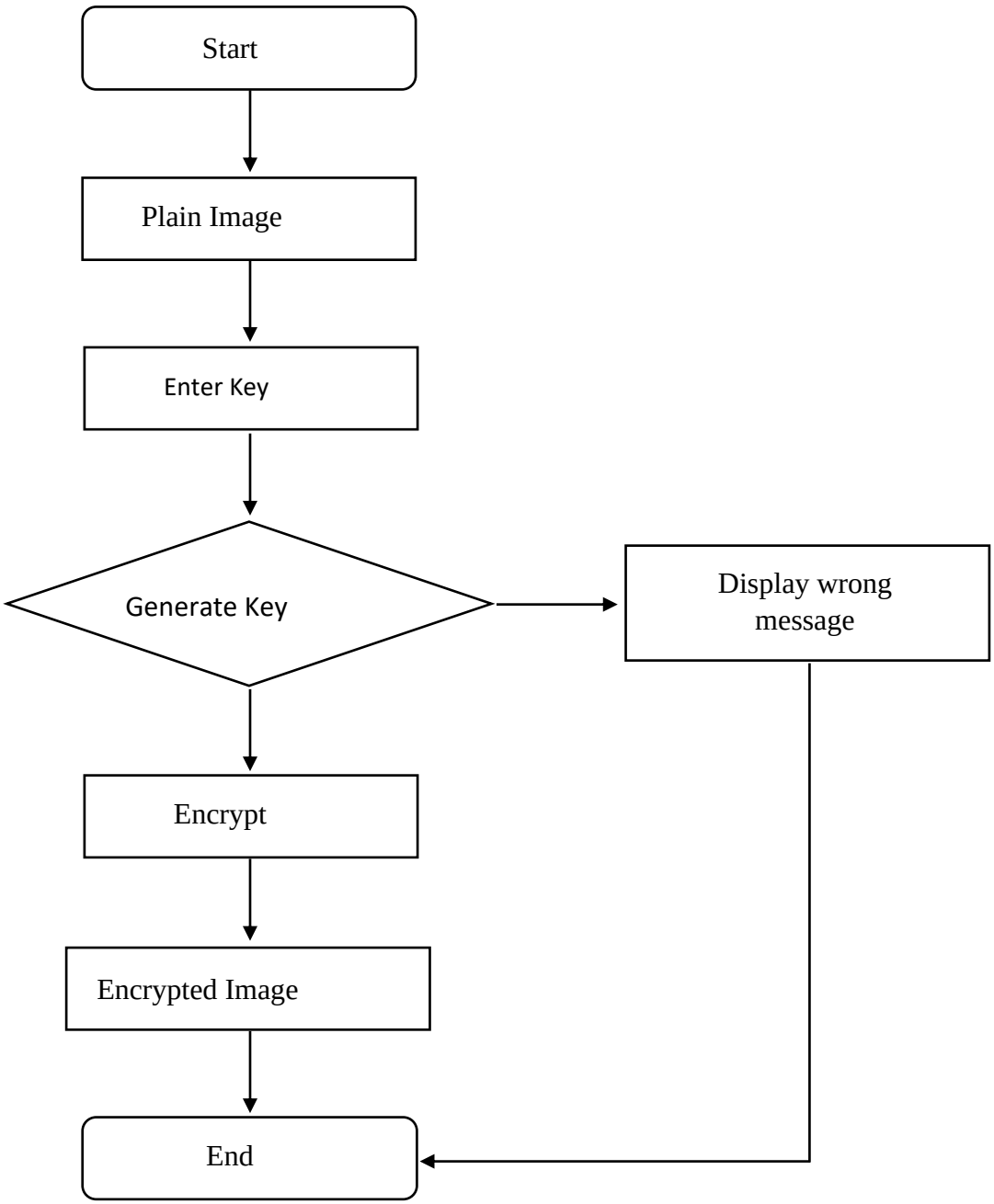
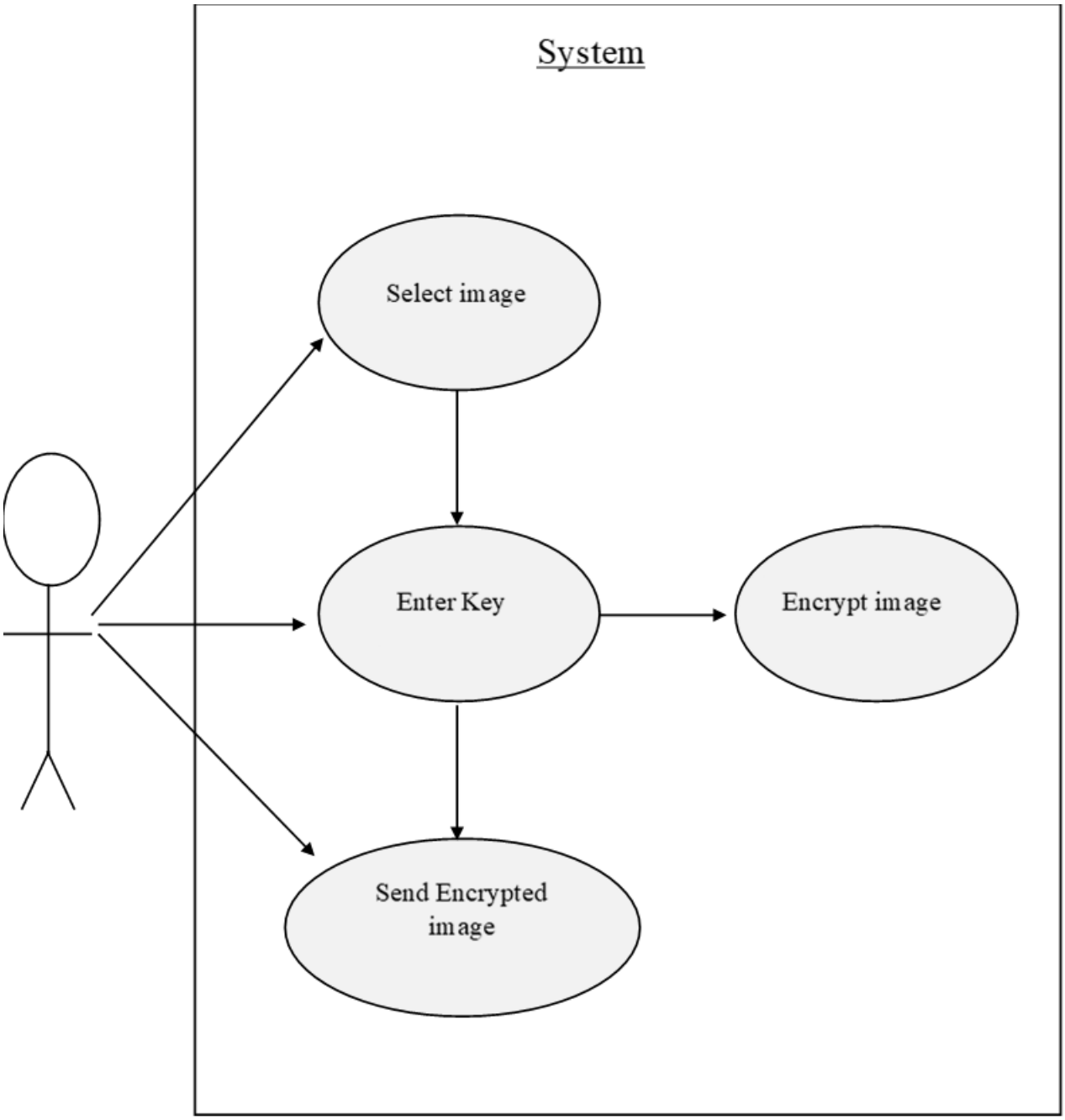


Figure 2: A Use Case Diagram of the image encryption algorithm…….....Chapter 3.3



APPENDIX B: Codes

Image Encryption Python Codes

```
from tkinter import *
from tkinter import filedialog
import hashlib
from tkinter import messagebox

# for the GUI
root = Tk()
root.geometry("500x300")

def decrypt_image():
    file1 = filedialog.askopenfilename(filetypes=[('Image files', '*.jpg;*.png')])
    if file1:
        key = entry1.get(1.0, END).strip()
        if not key:
            messagebox.showerror("Error", "Please enter a valid key.")
            return

        try:
            # Read encrypted image file as bytes
            with open(file1, 'rb') as fi:
                encrypted_image = fi.read()

            # Perform image decryption (reverse the encryption process)
            key_bytes = hashlib.sha256(key.encode()).digest()
            decrypted_image = bytearray(encrypted_image)
```

```
        for index, value in enumerate(decrypted_image):
            decrypted_image[index] = value ^ key_bytes[index % len(key_bytes)]

        # Save the decrypted image
        with open(file1, 'wb') as fi:
            fi.write(decrypted_image)

        messagebox.showinfo("Success", "Image decrypted successfully!")
        except Exception as e:
        messagebox.showerror("Error", f"Error while decrypting: {e}")

# The Button
b1 = Button(root, text="Decrypt Image", command=decrypt_image)
b1.place(x=220, y=150)

# Text box
entry1 = Text(root, height=1, width=20)
entry1.place(x=170, y=100)

root.mainloop()
```