ENHANCING SECURITY OF IMAGE STEGANOGRAPHY USING VISUAL CRYPTOGRAPHY

A PROJECT REPORT

Submitted by

SANAL MOHAN (TKM21MCA-2032)

to

The APJ Abdul Kalam Technological University

In partial fulfillment of the requirements for the award of the degree of

MASTER OF COMPUTER APPLICATION

Thangal Kunju Musaliar College of Engineering
Kerala

DEPARTMENT OF COMPUTER APPLICATION

MAY 2023

DECLARATION

I undersigned hereby declare that the project report on **ENHANCING SECURITY OF IMAGE STEGANOGRAPHY USING VISUAL CRYPTOGRAPHY**, submitted for partial fulfillment of the requirements for the award of degree of Master of Computer Application of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by me under supervision of Prof. Jasmin M R. This submission represents my ideas in my own words and where ideas or words of others have been included,I have adequately and accurately cited and referenced the original sources. I also declare that I have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. I understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University..

Kollam

16-05-2023

SANAL MOHAN

DEPARTMENT OF COMPUTER APPLICATION

TKM COLLEGE OF ENGINEERING, KOLLAM

2021 - 23

CERTIFICATE

This is to certify that the report entitled **ENHANCING SECURITY OF IMAGE STEGANOGRAPHY USING VISUAL CRYPTOGRAPHY** submitted by **SANAL MOHAN** (TKM21MCA-2032) to the APJ Abdul Kalam Technological University in partial fulfillment of the Masters degree in Computer Application is a bonafide record of the project work carried out by him under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Internal Supervisor Head of the Department External Examiner

Acknowledgement

First and foremost I thank GOD almighty and my parents for the success of this project. I owe sincere gratitude and heart full thanks to everyone who shared their precious time and knowledge for the successful completion of my project. I am extremely grateful to **Dr. Fousia M Shamsudeen**, Head of the Department, Department of Computer Application, for providing me with best facilities. I would like to express my sincere gratitude to the project coordinator, **Prof. Vaheetha Salam**, Department of Computer Applications, for their invaluable guidance, support, and encouragement throughout the entire duration of this project. I would like to thank my project guide **Prof. Jasmin M R**, Department of Computer Applications, who motivated me throughout the project. I would like to express my heartfelt gratitude to the advisor, **Prof. Natheera Beevi M**, Department of Computer Application for the unwavering support throughout this project. I profusely thank all other faculty members in the department and all other members of TKM College of Engineering, for their guidance and inspirations throughout my course of study. I owe my thanks to my friends and all others who have directly or indirectly helped me in the successful completion of this project.

SANAL MOHAN

ABSTRACT

ENHANCING SECURITY OF IMAGE STEGANOGRAPHY USING VISUAL CRYPTOGRAPHY, provides way to increase the security of Image Steganography by combining with Visual Cryptography. Steganography is the technique of hiding secret information within a cover image to ensure secure communication. Visual cryptography is a method of encrypting secret images into multiple shares, which are then distributed among different parties. By overlapping the shares, the original secret image can be reconstructed. This project propose a novel approach to enhance the security of image steganography using visual cryptography. The proposed method employs a combination of LSB-based steganography and visual cryptography to hide a secret image within a cover image. The LSB-based steganography technique is used to embed the secret image in the cover image, and visual cryptography is applied to encrypt the secret image into multiple share.

The proposed method enhances the security of image steganography by providing a double layer of encryption. The secret image is encrypted using visual cryptography, and the cover image is used to hide the encrypted shares. As a result, even if the steganographic communication is detected, the attacker will not be able to extract the secret image without having all the shares. Experimental results demonstrate that the proposed method provides higher security than conventional steganography techniques while maintaining the visual quality of the cover image. Therefore, the proposed method can be used for secure communication of sensitive information over public networks.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Information security has grown in importance in the modern world with the rise of digital communication. A common method for concealing sensitive information in an image, audio, or video file is steganography. However, traditional steganography techniques have a number of flaws, making it frequently easy for an attacker to find the hidden information or even extract it.

To address these issues, researchers have proposed various advanced steganography methods that can enhance the security of hidden information. One such method is visual cryptography, which involves splitting a secret picture into multiple shares and distributing them among different parties. The secret image can only be revealed by stacking the shares together; each share stands alone and conceals nothing about the original picture.

The project's objective is to use visual cryptography to increase the security of image steganography. This entails creating a cutting-edge method that fuses visual cryptography and steganography techniques to conceal sensitive information within images while maintaining its security and integrity. By using visual cryptography systems, which disperse the secret information over numerous shares to increase resistance against unauthorised access and detection, the project seeks to deliver an enhanced level of security.

1.1 Existing System

To maintain secure communication, the current approach of image steganography entails concealing sensitive information within an image. However, it has several drawbacks in terms of robustness and security. The previous approaches often rely on transformation-based or LSB (Least Significant Bit) replacement techniques, which are vulnerable to detection and removal by attackers.

The suggested study seeks to improve the security of image steganography through the use of visual cryptography in order to address these constraints. Visual cryptography is a method of encrypting data that distributes secret information over a number of shares or layers without revealing any valuable information on its own. These shares only reveal hidden information when they are superimposed. The project seeks to increase security and attack resistance by adding visual cryptography to image steganography. The method will require breaking up the secret information into shares and employing steganography to put each share in a new cover image. Attackers will see these resultant stego-images as harmless because they don't contain any valuable information without the right sharing and decoding steps. The proposed study will look into and put into practise several visual cryptography algorithms, assess their effectiveness, and contrast them with current steganography methods. The goal is to create a more advanced system that offers strong security and secrecy for the transmission of critical information within images.

1.2 Problem Statement

The development of image steganography techniques is a result of the widespread usage of digital photographs and the requirement for secure communication. The security of the hidden data is jeopardised by the attack and detection susceptibilities of current steganography techniques. This study proposes a novel method that fuses image steganography with visual cryptography in order to address these security issues. By distributing the secret information among numerous shares and using visual cryptography techniques to ensure robustness against attacks and preserve the confidentiality of the hidden data, the objective is to make image steganography more secure.

1.3 Proposed System

The proposed system aims to increase image steganography's security through the integration of visual cryptography techniques. Image steganography is a widely used method of hiding secret information within an image to ensure confidentiality. However, traditional image steganography techniques have vulnerabilities that can be exploited by attackers. Therefore, the incorporation of visual cryptography techniques offers an additional security measure to safeguard the secret data.

The selection of a cover image, which will be used to conceal the secret information, is the first step in the suggested system. Prior to merging the cover image with the hidden image, an appropriate encryption procedure is utilized to encrypt it. The encrypted image is divided into numerous portions using visual cryptography techniques to ensure increased security. These shares don't each include any details about the original picture; instead, a particular combination is needed to decrypt the hidden image. The shares collected by visual cryptography are then inserted into various cover image pixel positions. By making the modifications to the cover image invisible to the human eye, the embedding procedure makes it harder for attackers to recognise the existence of hidden information. Since the hidden image can only be obtained by using the right combination of shares during the decryption process, the sharing system employed in visual cryptography offers robustness.

1.4 Objective

The goal of this project is to use visual cryptography to increase the security of image steganography. The intention is to create a reliable and effective algorithm that can use visual cryptography to add an extra layer of protection and steganography to conceal information in cover images. The secret image must only be recovered from the stego-image by authorised users in order to maintain the confidentiality and integrity of the hidden data.

The goal is to accomplish the following:

- To comprehend the idea of visual cryptography and image steganography.
- To review the existing methods of image steganography and visual cryptography.
- To analyze the limitations of the existing methods and propose a solution to enhance security using visual cryptography.

- To implement the proposed method for image steganography using visual cryptography.
- To assess how well the suggested method performs in terms of security and image quality.
- to assess the suggested method's security and image quality in comparison to current methods.
- To discuss the applications and future scope of the proposed method.
- To offer suggestions for additional visual cryptography and image steganography research.

Chapter 2

Literature Survey

Literature review is that the comprehensive study and interpretation of literature that relates to a selected topic.When doing a literature review, research questions are defined, and then relevant literature is sought for and analysed to address these issues. By reanalyzing the study's data, it is possible to acquire fresh insights, which is an advantage of literature reviews. A literature review is both a summary and an explanation of the complete and current state of information on a topic as contained in academic books and journal articles. There are two types of literature reviews you may be required to write in college: one is written as a stand-alone assignment in a course, while the other is done as an introduction to or preparation for a longer piece of writing, typically a thesis or research report. The primary objective and perspective of your review, as well as the hypothesis or thesis argument you develop, depend on the type of review you are writing. You can learn the distinctions between these two types by reading published literature reviews or the introductory chapters of theses and dissertations in your subject area. Note the framework of their arguments and the manner in which they approach the issues.

2.1 Purpose of the Literature Review

1. It chooses top-notch research papers or studies that are pertinent, significant, important, and valid and summarises them into a single comprehensive report to provide readers with quick access to information on a certain issue.

2. By requiring them to describe, assess, and compare original research in this particular field, it gives researchers who are starting their research in a new area a great place to start.

3. It makes sure that researchers don't repeat already completed studies.
4. It can indicate potential directions for future research or suggest topics to concentrate on.
5. It emphasises the important findings.
6. It points up gaps, discrepancies, and inconsistencies in the literature.
7. It offers a helpful critique of the methods and strategies used by other researchers.

2.2 Related Works

2.2.1 Image Steganography

Image steganography is a widely studied field in information security, with numerous techniques proposed to hide secret information within images. In conventional methods, the secret information is immediately included into the pixels' least important bits. However, these methods may suffer from various vulnerabilities, such as visual detectability and statistical analysis attacks. Researchers have explored different algorithms and strategies to address these issues and improve the security and robustness of image steganography.

In this study, a brand-new steganography technique intended exclusively for halftone photographs is presented. In order to provide secure communication, steganography is a crucial technique used to conceal sensitive information within the carrier medium. Due to their binary character and restricted colour palette, halftone images, which are frequently employed in printing and digital imaging, present special challenges for steganographic algorithms. When used with halftone photographs, existing steganography techniques frequently have poor visual quality or a low embedding capacity. In the suggested strategy, it take advantage of the halftone images' natural properties to create a strong and effective steganographic approach. The system embed confidential information into the least significant bit (LSB) planes of particular dot clusters by taking advantage of the halftone dots' spatial distribution. The system use a statistical model to select the best embedding locations and precisely tune the LSB values to ensure imperceptibility and defend against visual attacks. The study offers a novel method for steganography in halftone photos that may have benefits like increased resilience and security. A high level of undetectability is ensured by the proposed approach, which could offer increased hiding capability while keeping visual quality. The research also makes a

contribution to the area by presenting a novel algorithm that could broaden the selection of steganography methods accessible for halftone photos. The new steganography technique for halftone photographs that is presented in this paper might have some drawbacks. It is crucial to take into account any difficulties that might occur when implementing the suggested approach, such as computational complexity or performance problems. The document should also go through the method's potential flaws or shortcomings, such as potential detection strategies or assaults that might undermine the concealed data. The credibility of the strategy would be improved by additional empirical analysis and comparison with current approaches. [1]

This paper introduces a novel steganography method that employs an image-hiding pixel-based algorithm. The art of steganography involves concealing private information on an apparently irrelevant cover medium. The suggested technique makes use of the intrinsic properties of pixels to smoothly incorporate information into an image while guaranteeing that it is invisible to the human eye. The algorithm's capacity to selectively alter pixel values based on the secret message while utilising a safe encryption method to maintain data integrity is the algorithm's major innovation. The algorithm exhibits robustness against various steganalysis techniques while keeping high capacity for concealed data after considerable experimentation and analysis. In comparison to existing strategies, the proposed strategy also performs better in terms of embedding speed and extraction accuracy. The outcomes highlight the effectiveness and promise of the pixel-based algorithm in boosting the safety and effectiveness of steganography applications. The research offers a reliable and safe technique for obfuscating information in photographs. The pixel-based algorithm also ensures high-speed operations by enabling effective encoding and decoding procedures. Thirdly, the method demonstrates resistance to diverse attacks on image processing, increasing its dependability. Finally, this context's usage of steganography makes it possible for covert communication and data protection. The introduction of hidden data, however, could result in a reduction in image quality, which would be one of this method's possible drawbacks. The efficiency of the algorithm may also differ based on the qualities of the image and the level of examination used by potential attackers. Its performance in real-world circumstances needs to be determined through additional analysis and testing. Additionally, care should be made to guarantee that the concealed data is safe and resistant to any threats. [2]

In order to achieve high capacity and security, this research suggests a revolutionary image steganography technique that combines LSB replacement with modified Huffman

encoding. The proposed technique is evaluated on various standard test images, and the results demonstrate its effectiveness and robustness against various attacks.The proposed technique leverages LSB (Least Significant Bit) substitution and modified Huffman encoding to achieve both high capacity and enhanced security. The least significant bits of the cover image pixels are effectively inserted with the LSB substitution method, while the modified Huffman encoding algorithm optimizes the data compression and embedding process. Utilising a variety of common test photos, the proposed technique's effectiveness is assessed., and the results demonstrate its effectiveness and robustness against common steganalysis attacks. To achieve large capacity image steganography, the suggested technique combines LSB substitution and modified Huffman encoding. It increases the total capacity for information hiding by enabling the insertion of a significant amount of hidden data into the image. Additionally, by eliminating redundancy, the updated Huffman encoding improves the security of the embedded data. The method offers a fresh perspective that may work well for secret communication or information concealment. However, the paper might not give thorough explanations of any potential restrictions or downsides of the suggested method. To assess its resistance to different steganalysis approaches and potential flaws, more investigation is required. To evaluate the technique's viability and effectiveness in practical applications, it should also be taken into account for its computing complexity.[3]

In-depth research and analysis of reversible image steganography techniques are presented in this publication. Reversible image steganography is the practise of concealing information while preserving the capacity to reconstruct the original image without losing any data. The purpose of this study is to examine multiple reversible image steganography techniques and weigh the benefits and drawbacks of each. The basic ideas and principles of reversible picture steganography are first introduced in this study, followed by a review and categorization of current techniques based on their methodology, such as spatial domain, transform domain, and prediction-based approaches. High data hiding capacity, imperceptibility of the embedded information, and resistance against multiple attacks are advantages of reversible picture steganography algorithms. However, there are several drawbacks and restrictions to take into account, such as higher processing complexity, decreased stego picture visual quality, and vulnerability to detection by sophisticated steganalysis algorithms.[4]

The practise of steganography involves concealing information in digital media to ensure secrecy and confidentiality. The focus on the possibilities of utilizing the LSB technique in

RGB images for embedding secret data. The LSB method alters an image's least significant bits of pixel values, which are generally less perceptible to the human eye. By replacing these bits with secret data bits, it can conceal information within the image. The objective of this research is to assess the capacity and robustness of LSB steganography in RGB images. Through experimental analysis and evaluation, the paper investigate the trade-off between the amount of secret data that can be embedded and the resulting impact on image quality. Additionally, the reaearch explore various LSB embedding strategies and assess their effectiveness in terms of data capacity and security. The findings of this research contribute to enhancing the understanding and potential applications of LSB steganography in RGB images. In this study, the potential for LSB (Least Significant Bit) steganography in RGB photographs is examined. On the plus side, LSB steganography offers a simple and effective way to conceal information within images, making it appropriate for a variety of applications. There may be certain restrictions, though, such as increased assault susceptibility and limited payload capacity. Despite these shortcomings, the research offers insightful information about the potential application of LSB steganography in RGB photos and provides a solid framework for further investigation in this area.[5]

2.2.2 Visual Cryptography

Visual cryptography is a cryptographic technique that utilizes visual information to distribute and reveal secret images or messages. It provides a secure mechanism to encrypt and decrypt data without the need for complex cryptographic algorithms. Visual cryptography has been extensively studied for its applications in various domains, including authentication, privacy protection, and information hiding. In visual cryptography, a secret image is divided into shares or layers, which individually appear as random patterns but collectively reveal the original image when combined.

Visual cryptography is a method of distributing secret information among a number of shares, with the original information only becoming visible when the shares are superimposed. This study presents a random grid-based visual cryptography method that makes use of a shared secret. Using a specified set of patterns, the suggested approach creates random grids and encodes the secret information into these grids. The participants are given the common share along with the random grids. The secret information is made visible by superimposing the common share with any of the random grids. Benefits of this approach include ease of use,

greater security provided by the randomization of grids, and flexibility in pattern selection. But it also has drawbacks, such as larger shares compared to conventional visual cryptography systems and the risk of data leakage in the event that the common share is compromised. The suggested scheme offers a viable strategy for secure secret exchange and may find use in a number of areas, including secure image transmission and authentication systems.[6]

The secure visual secret sharing (VSS) technique presented in this study is a revolutionary method created especially for colour photographs. The proposed method combines the principles of visual cryptography (VC) and digital watermarking to ensure secure and reliable sharing of sensitive color image information. An encryption method known as ”visual secret sharing” separates a secret image into many shares, known as shadow images, which, taken alone, offer little insight into the original picture. The original image can only be reconstructed by combining a predefined number of shares. In this plan, each color pixel in the original image is transformed into a set of subpixels, and these subpixels are encrypted using a modified VC algorithm. Then, to give an extra level of protection and authentication, a digital watermark is integrated into the shares. This watermarking technique ensures that the shares remain robust against various attacks and tampering attempts. Experimental results demonstrate the effectiveness of the proposed scheme in terms of visual quality, security, and resistance to common attacks. The proposed method offers a reliable and efficient solution for secure sharing of color images, making it suitable for applications in areas such as secure communication, image authentication, and copyright protection. The advantages of this plan include improved security because it guarantees the shared secret's privacy and secrecy and the capacity to recreate the original image without distortion. The embedding of watermarks could result in a loss of visual quality, an increase in computational complexity, and a potential vulnerability to sophisticated attacks.[7]

Visual cryptography is an emerging field that aims to secure confidential information by transforming it into visual images that can be easily deciphered by the visual system of humans. This paper propose a novel visual cryptography scheme that enhances the security and efficiency of information encryption and decryption processes. This system utilizes the principle of pixel expansion and image decomposition to generate shares, which are individual images containing encrypted fragments of the original information. The decryption process requires a simple visual superposition of the shares, ensuring that the original information can only be revealed when the shares are properly aligned. Experimental findings show how

successful and reliable this plan is, making it suitable for applications where secure visual information transmission is paramount, such as secure document sharing and biometric data protection. The proposed system offers a high level of security. The benefits and security of fundamental systems are enhanced by visual cryptographic encryption. The best use for it is in the transfer of financial documents because it offers higher security. It is also possible to create more apps that demand a high level of security. This approach also has flaws because the image that is revealed is of poor quality. [8]

This paper dives into the field of visual cryptography, which is a promising technique for secure information transmission. Without using complicated cryptographic techniques, visual cryptography tries to encrypt a secret picture into a set of shares that can be visually deciphered by human perception. This research provide a brand-new technique for extracting useful shares from the hidden image. The shares preserve relevant visual information by using the pixel expansion technique, allowing for human interpretation without the need for computing. To secure the privacy and validity of the secret image, the system also look into the security features of the suggested scheme, such as the expansion factor for pixels and contrast improvement. The efficiency of the suggested technique and its potential use in secure image sharing, visual authentication, and watermarking are demonstrated by experimental findings. The findings contribute to the development of visual cryptography techniques and their practical implementation in various domains requiring secure information transmission. Its ability to offer aesthetically beautiful encryption algorithms without requiring complicated mathematics is one of its advantages. Additionally, it provides a high level of security because it is virtually impossible to decode data without the necessary shares. However, given the necessity for many shares, its principal disadvantage is the additional storage and transmission requirements. The quality of the image is also diminished by the fact that the decrypted version's resolution is lower than the original. [9]

This paper introduces an enhanced method for secret sharing through the utilization of XOR-based Visual Cryptography (VC). Secret sharing is a prominent technique that aims to distribute a confidential message among multiple participants in such a way that collaboration is necessary to disclose the original content. Visual Cryptography (VC) involves the encoding of secret images into shares, which are given out to the participants. The original secret can be visually obtained by stacking these shares together. However, existing VC schemes have limitations, including low contrast of reconstructed images and inefficient pixel expansion.

To overcome these issues, this paper proposes an improved secret sharing approach based on XOR operations. The shares are subjected to XOR operations, which considerably improves the contrast of the rebuilt image, resulting in a clearer and more accurate representation of the secret. Moreover, the proposed scheme ensures pixel expansion efficiency by minimizing the number of additional pixels required. Experimental findings show that the suggested procedure is more successful than current ones and is therefore superior, making it a promising solution for secure secret sharing applications. The advantages of the study include the use of XOR-based approaches to boost security, straightforward implementation, and the ability to reconstruct the hidden image without the need for complicated calculations. However, drawbacks could include the secret image's size restrictions and vulnerability to specific attackers. [10]

2.2.3 Combining Image Steganography and Visual Cryptography

To enhance the security of image steganography, researchers have proposed integrating visual cryptography with steganographic techniques. This combination offers a promising solution to overcome the limitations of traditional steganography methods. By leveraging visual cryptography, the secret information might be split up into several shares and incorporated into several cover photos. These shares can be distributed among different channels or recipients, making it extremely challenging for an adversary to get the original secret information without having all the shares.

This paper presents a novel approach to visual cryptographic steganography in images, combining the techniques of visual cryptography and steganography. Visual cryptography involves the encryption of secret information into shares, which can then be visually decoded by overlaying the shares. Steganography, on the other hand, focuses on concealing information within cover objects to achieve covert communication. By integrating these two methods, the paper propose a robust and secure scheme for hiding secret messages within digital images. This approach utilizes a pixel-level manipulation technique to integrate the cover image with the secret information, ensuring imperceptibility and resistance to statistical analysis. The embedded information is then transformed into shares using visual cryptography, ensuring that the secret message remains hidden even if part of the image is compromised. The decoding process involves the superposition of the shares, revealing the original secret message. Experimental results demonstrate the effectiveness and efficiency of the proposed method, showcasing its resistance to various attacks, including steganalysis. Furthermore, this scheme

maintains high image quality and avoids visual artifacts, making it suitable for practical applications requiring secure and covert communication through images. The study's benefits include improved security achieved by combining cryptography with steganography, as well as the capacity to conceal private data within images. Due to the complexity of the procedure, the method may, however, suffer from lower data storage capacity and increased attack risk. [11]

Image steganography is a widely used technique for hiding secret information within digital images. However, the security of steganographic systems has become a significant concern due to the advancement of digital forensic tools. This paper propose a novel approach for enhancing the security of image steganography by integrating neural networks and visual cryptography. This method leverages the power of neural networks to incorporate cover image with hidden data using a robust and imperceptible manner. By training the neural network on a large dataset of cover images and secret data, the paper ensure the embedding process is optimized for both security and visual quality. Additionally, the employ visual cryptography techniques to further increase the stego pictures' security. The proposed system achieves enhanced security by providing a dual-layer protection mechanism that combines the strength of neural network-based steganography and visual cryptography. Experimental findings show how effective the strategy is in terms of imperceptibility and resistance against various steganalysis techniques. The proposed method offers a practical solution for secure information hiding, with potential applications in data transmission and covert communication channels. The suggested method combines the benefits of visual cryptography and neural networks to increase the security of image steganography. Robust embedding and extraction of hidden data are made possible by neural networks, and visual cryptography adds another level of protection by dividing the secret image into shares. By combining these methods, you can increase your defences against attacks and detection, making it more difficult for unauthorised users to access information that is being kept secret. Despite its benefits, this strategy could have some drawbacks. Using neural networks exclusively for embedding and extraction could result in computational overhead and longer processing times. Additionally, the formation of additional shares as a result of the integration of visual cryptography may increase storage demand. Furthermore, a complete evaluation of this strategy's effectiveness in thwarting sophisticated steganalysis methods is still needed. [12]

2.2.4 Python

This paper presents a survey on the role of Python in the IT world. Python has become one of the most popular programming languages, and its popularity continues to grow due to its simplicity, versatility, and wide range of applications. The survey investigates the reasons behind the increasing adoption of Python in the IT industry and the specific use cases where it is being used. The study also analyzes the challenges faced by developers when using Python, such as performance limitations and the need for additional libraries and frameworks. The survey results indicate that Python is being used in a variety of applications, including web development, scientific computing, machine learning, and data analysis. Moreover, the study found that Python's ease of use and extensive libraries and frameworks make it an attractive choice for developers. Overall, this survey highlights the significance of Python in the IT industry and its potential to continue to grow in popularity.[13]

Python has emerged as a powerful and versatile programming language that caters to the needs of data analytics, scientific research, and technical applications. This paper explores the various features and libraries in Python that make it an ideal choice for these domains. Python's simplicity and readability, combined with its extensive ecosystem, enable researchers and practitioners to efficiently handle complex data analysis tasks. The paper discusses the use of Python's data manipulation libraries such as NumPy and pandas, which provide efficient data structures and tools for data cleaning, transformation, and analysis. Furthermore, Python's integration with visualization libraries like Matplotlib and Seaborn allows for the creation of insightful visual representations of data. Overall, this paper emphasizes Python's relevance and effectiveness in data analytics, scientific research, and technical applications, making it a valuable tool for researchers and practitioners in these fields.[14]

2.2.5 Flask

In this research, a unique method for creating a multi-disease prediction model using machine learning algorithms and a Flask API is presented. The proposed model aims to predict the occurrence of multiple diseases based on various patient attributes such as age, gender, medical history, and symptoms. To achieve this, a comprehensive dataset comprising medical records from diverse patients was collected and preprocessed. To create precise prediction models for various diseases, machine learning methods such as decision trees, random forests, and

support vector machines were trained on the dataset. Furthermore, a Flask API was developed to facilitate seamless integration of the prediction model into existing healthcare systems. The API allows for efficient data transmission between the user interface and the machine learning model, enabling real-time predictions. Results from experiments show that the suggested multi-disease prediction model is reliable and useful. The utilization of Flask API ensures scalability, flexibility, and ease of deployment, making it a promising solution for disease prediction in healthcare settings.[15]

This paper presents an innovative approach for developing a face recognition-based attendance system by integrating Flask, a micro web framework, with Python programming language. The system aims to automate the attendance process in educational institutions or organizations, reducing the need for manual record-keeping and increasing efficiency. Flask provides a lightweight and flexible framework for building web applications in Python. By leveraging Flask's capabilities, a user-friendly interface that allows users to register and enroll their faces, capture real-time images, and perform attendance verification is created. The integration of Flask with Python's face recognition libraries enables the system to accurately identify and match faces against a pre-registered database. The proposed system addresses the challenges of traditional attendance systems, such as proxy attendance and inaccurate record-keeping. By utilizing Flask's features, such as routing, templates, and request handling, the system ensure a smooth and interactive user experience. Additionally, Flask's extensibility allows for easy integration with other technologies and systems, enabling future scalability and customization. Experimental results demonstrate the system's effectiveness in achieving accurate and efficient attendance management through face recognition. The integration of Flask and Python enhances the system's performance, reliability, and usability, making it a viable solution for attendance management in various domains.[16]

Chapter 3

Methodology

ENHANCING SECURITY OF IMAGE STEGANOGRAPHY USING VISUAL CRYPTOGRAPHY aims to improve the security of image steganography techniques through the implementation of visual cryptography. Image steganography is the practise of securely transmitting confidential information by enclosing it within an image. The confidentiality of the hidden data, however, may be threatened by attacks on conventional steganography techniques.

To address these vulnerabilities, the project proposes the utilization of visual cryptography, which is a cryptographic technique that splits a secret image into shares. These shares, when combined, reveal the original secret image. Visual cryptography utilizes visual perception properties to ensure that the secret information remains hidden until the shares are properly combined. The methodology involves implementing and enhancing existing image steganography techniques by incorporating visual cryptography.

3.1 Introduction to Image Steganography

Image steganography is a method for concealing sensitive information in digital photos without drawing attention to it. Its main goal is to guarantee confidential treatment of sensitive data and safe communication. This project concentrate on integrating visual cryptography, a cryptographic method that permits secure transmission and display of secret information, to increase the security of image steganography.

The currently available approaches for image steganography, like LSB embedding and spatial domain techniques, are frequently used. These methods are vulnerable to unauthorised access and detection due to a number of flaws and limitations. In order to strengthen the security

of image steganography and defend against future attacks, it is important to investigate fresh ways.

3.2 Visual Cryptography

A cryptographic method known as ”Visual Cryptography” uses visual perception to share and reveal confidential information. Binary images, which individually reveal nothing about the original secret, are used as shares. The hidden data is only visible when the shares come together or are stacked. Due to this characteristic, visual cryptography is a desirable option for increasing the security of image steganography.

The fundamental idea behind visual cryptography is to randomly distribute a number of shares of the secret image. Once given to the various participants, these shares can then be combined to reveal the hidden image. The main aim is to add another level of security to the concealment and retrieval of sensitive information by combining visual cryptography with image steganography.

3.3 Module Description

3.3.1 Module I (Encryption)

- Selecting Secret Image: Select and load the image that needs to be encrypted.
- Random share generation: According to the size of the chosen secret image, a random image is created and saved as share-1 image.
- Encryption of the image: The encrypted image is created by conducting an XOR operation on the share-1 picture, which results in the creation of the share-2 image, which is the next share to be broadcast.
- Image Steganography: With the use of LSB-based image steganography, the created share-2 picture was then concealed inside a cover image.

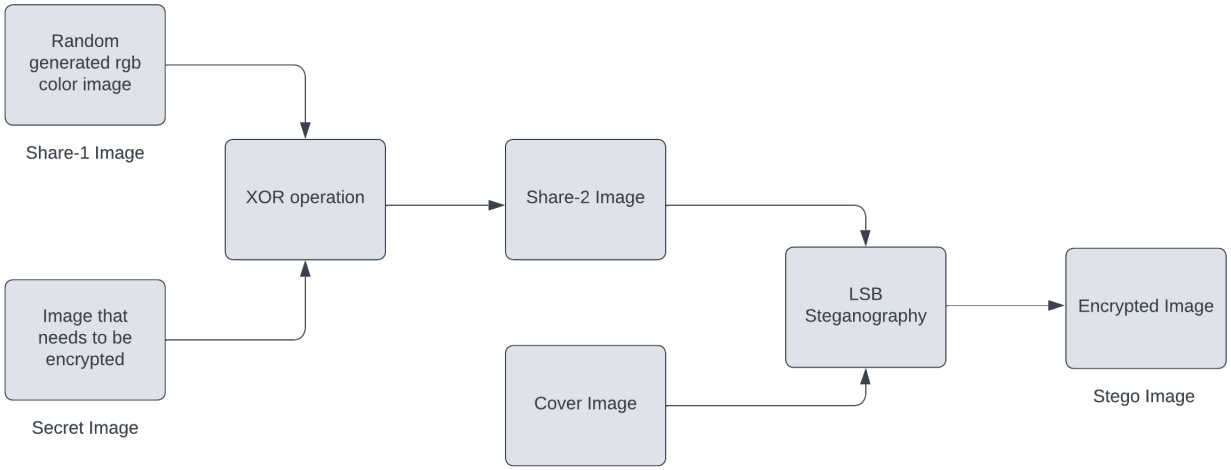


Figure 3.1: Encryption flow chart

3.3.2 Module II (Decryption)

- Selecting encrypted Image and share-1 image: Share-1 and the encrypted picture have been chosen and loaded.
- Regenerating Share-2 image: By combining the least significant bits of the encrypted image, the Share-2 image is recreated.
- XOR operation: The created share-2 image and the chosen share-1 image are put through an XOR operation to recover the secret image.

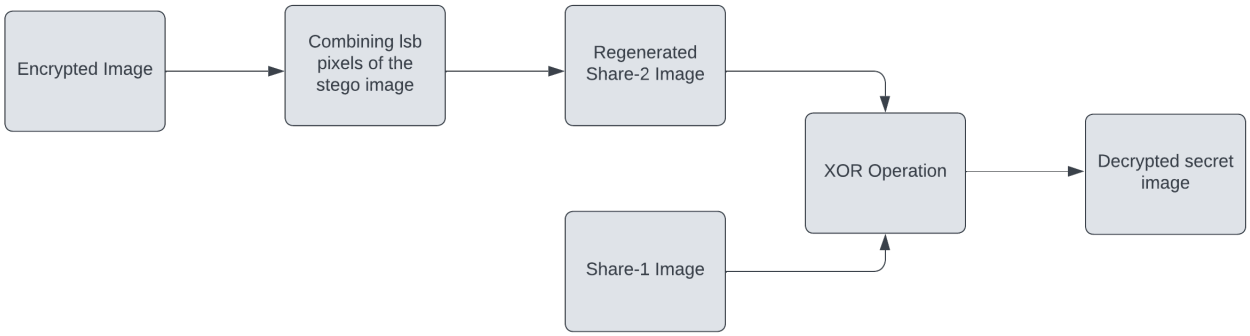


Figure 3.2: Decryption flow chart

3.4 Software Requirements and Specifications

The software requirements for the project includes:

- Python
- Anaconda
- Flask framework
- HTML and CSS

3.4.1 Python

Python is a popular high-level programming language that is renowned for being straightforward and readable. Python was developed by Guido van Rossum in the late 1980s, and because of its concise and clear syntax, which emphasises code readability, it is a well-liked choice among both novice and seasoned coders. Because of its versatility, Python can be used for a wide range of applications, including web development, data analysis, scientific computing, artificial intelligence, and automation. The broad ecosystem of third-party packages and its extensive standard library give developers access to a wide range of tools and resources. The emphasis on productivity in Python is one of its main advantages. Developers are freed from low-level details by its dynamic typing and automatic memory management, which enable them to concentrate on problem-solving. Python's interpreted nature also makes it possible for quick prototyping and development. Python has a thriving ecosystem of libraries, frameworks, and resources because of its community-driven development and open-source philosophy. Due to its simplicity, adaptability, and broad community support, it is becoming increasingly popular and is a great option for both inexperienced and seasoned programmers.

3.4.2 Anaconda

Anaconda is a well-liked and powerful Python distribution that is frequently used in applications for data science and machine learning. Many data scientists and researchers rely on it because it offers an extensive package management system and a stable environment for scientific computing. One of Anaconda's main benefits is the large selection of pre-installed libraries and tools, which include, among others, NumPy, SciPy, Pandas, and Scikit-Learn. These libraries are crucial for manipulating, analysing, and visualising data, enabling

users to finish challenging jobs quickly. Jupyter Notebook, an online interactive computing environment that enables users to create and share documents with live code, equations, visualisations, and explanatory writing, is also a component of Anaconda. Additionally, by including the Conda package manager, Anaconda makes package administration simpler. It enables users to quickly install, update, and manage packages across several operating systems as well as their dependencies. Reproducibility and project collaboration are made simple by this. Overall, Anaconda acts as a thorough and user-friendly platform that equips data scientists and researchers with the tools they need to efficiently design and deploy data-driven applications.

3.4.3 Flask Framework

Python web application development can be done with the Flask microweb framework. Being known as a micro-framework is a result of the fact that it does not need specific tools or libraries. It is well-liked by newcomers to web programming because of its lightweight design, simplicity of usage, and ease of learning. Routing, templating, and request handling are some of the fundamental capabilities offered by Flask. Developers can also apply extensions to it to increase its capabilities. Authentication, database integration, and testing are just a few of the extensions that Flask can support. Flask is flexible and may be used for a range of web development projects, from small to large. It is renowned for being straightforward and minimalist, which makes it the perfect option for creating simple web apps or APIs. To build more complicated web applications, Flask can also be used in conjunction with other Python modules and frameworks. Overall, Flask is an easy-to-use web framework that gives programmers the flexibility they need to swiftly and effectively build web applications.

3.4.4 HTML and CSS

CSS (Cascading Style Sheets) and HTML (Hypertext Markup Language) are two essential technologies used in web development. The markup language used to create the structure and content of web pages is called HTML. To specify elements like headings, paragraphs, photos, links, and more, it makes use of tags. These tags give the webpage a logical structure and make it possible for browsers to appropriately comprehend and display the content. The visual design and layout of web pages are defined by CSS, which contrasts with HTML. It

enables programmers to style HTML components with things like colours, fonts, margins, and positioning. It is simpler to maintain and alter the appearance of a website when the design and content are separated by CSS. Web pages can be made visually beautiful and interactive by combining HTML and CSS. While CSS takes care of the styling and layout, HTML concentrates on the structure and semantics. Developers may create interesting websites that offer a fantastic user experience on a variety of devices and browsers by skillfully utilising these technologies.

Chapter 4

RESULT AND DISCUSSION

The primary quality control method used in software development is testing. Following the coding stage, testing purposes are served by running the accessible computer programmes. Testing must find flaws made during the earlier phase as well as those introduced during development. So, the purpose of testing is to find programme requirements, design, or coding flaws.

- A programme is tested by being run with the goal of identifying any errors.
- A excellent test case is one that has the highest chance of spotting an error that hasn't been identified yet.
- A test that finds an error that hasn't been found yet is successful.

The objective is to develop tests that systematically uncover many sorts of issues with minimal time and effort. Testing indicates that software functionalities appear to operate as expected and that performance criteria appear to have been met. The information acquired during testing is an excellent predictor of programme reliability and a partial indicator of software quality as a whole. Testing has one drawback, however: it can only demonstrate the presence of software defects, not their absence.

4.1 Testing and it's types used

The main task following software development is to determine whether the experimental results and the actual results agree. Testing is the process in question. It is employed to ensure that the created system is free from errors.Testing's primary purpose is to find errors and missing

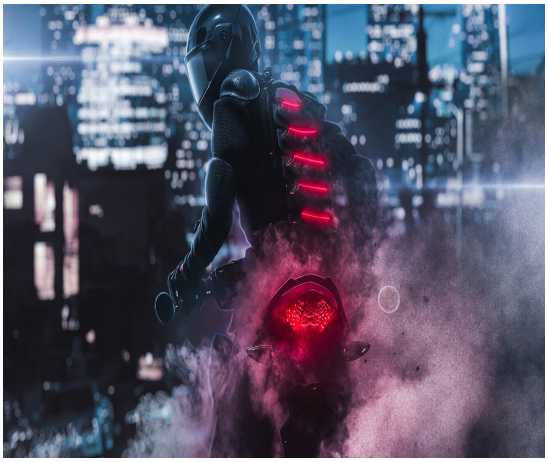
operations by running the software. Additionally, it makes sure that the developer satisfies all of the project's goals. Testing's objective is to determine is to identify defects in the developed software as well as ways to increase its correctness, usability, and efficiency. It seeks to gauge a software program's performance, functionality, and specification. The developed programme is put through tests, and the outcomes are compared to the required documentation. Debugging is carried out when there are too many faults that have happened. After debugging, the software is once more tested to make sure there are no errors. Unit testing, integration testing, and system testing are the main testing methodologies used in this project.

- In unit testing, tested to each distinct piece of software. It ensures that the software's many components all function as intended.
- In integration testing, the integrated distinct components are examined to see whether or not the intended purpose was accomplished. It helps us find any problems that might appear after the units are combined.
- The entire piece of software is evaluated during system testing to make sure it meets all the requirements.

4.1.1 Peak Signal-to-Noise Ratio (PSNR) Calculation

Peak Signal-to-Noise Ratio, or PSNR, is a popular metric for assessing the efficacy or precision of picture compression or restoration methods. By contrasting the pixel values of two images, it offers a quantitative assessment of how similar the images are.The mean square error (MSE) between the original image and the reconstructed or compressed image is used to determine the PSNR value. The difference between the matching pixels in the two images, squared, is what determines the MSE. The PSNR is then calculated by taking the square root of the MSE and dividing it by the logarithm of the maximum allowable pixel value squared (typically 255 for 8-bit grayscale images or 65535 for 16-bit images). A higher PSNR value indicates a better quality or accuracy of the reconstructed or compressed image, as it means the pixel differences between the original and processed images are smaller. In contrast, a lower PSNR value denotes a more pronounced divergence between the two images.

(a) Rose



(b) Bike

Figure 4.1: Cover Images used

(a) Tree

(b) Dog

Figure 4.2: Secret Images used

Inorder to perform LSB-Steganography number of pixels of the cover image must be larger than the number of pixels of the secret image.

The below table shows the PSNR value for the original cover image and the image after encryption and also the PSNR value for the original secret image and the decrypted image for different combinations of cover and secret images.

4.2 Output Screens and Results

1. Home page:

   This is the main landing page. wo buttons are included on it—one for encryption and the

Slno	Cover Image	Secret Image	PSNR (in dB) for Cover Image	PSNR (in dB) for Secret Image
1	Rose	Tree	30.48dB	34.41dB
2	Rose	Dog	30.48dB	35.25dB
3	Bike	Tree	30.1dB	34.46dB
4	Bike	Dog	30.1dB	35.22dB

Table 4.1: PSNR Evaluation Table

other for decryption. Cover picture and the secret image are used as input for encryption, and encrypted image and share-1 image are used as input for decryption.

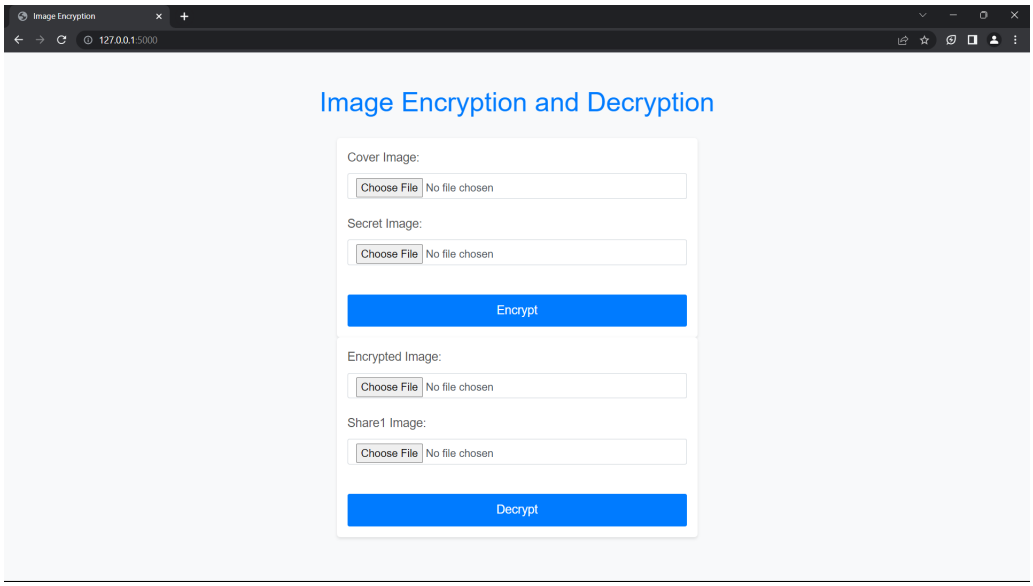


Figure 4.3: Home Page

2. Secret Image

   The image that needs to be encrypted.

Figure 4.4: Secret Image

3. Cover Image

   Image that is used to hide the encrypted share image.

Figure 4.5: Cover Image

Share-1 Image

This is the random generated image based on the size of the secret image.

Figure 4.6: Share-1 Image

4. share-2 Image

   This is the image that is obtained after performing XOR operation between share-1 image and secret image.

Figure 4.7: Share-2 Image

5. Encrypted Image

   This is the image that is obtained after hiding the share-2 image inside the cover image using lsb-steganography.

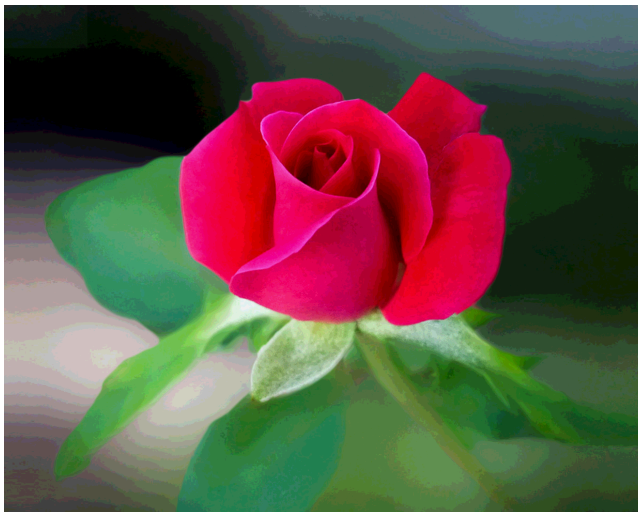


Figure 4.8: Encrypted Image

6. Decrypted Image

   This is the secret image that is obtained back after extracting the lsb pixels of the encrypted image and then performing XOR operation between the extracted image and share-1 image

Figure 4.9: Decrypted Image

Chapter 5

CONCLUSION

Through the use of visual cryptography techniques, the project ”Enhancing Security of Image Steganography Using Visual Cryptography” aims to increase the security of image steganography. The effort improved the security of image steganography by providing an additional layer of security through the use of visual cryptography. Visual cryptography separated the secret image into shares, which individually seemed like random patterns but when stacked up disclosed the secret information. This guaranteed that the hidden data would remain unintelligible even if an attacker managed to access one share. The study put the suggested method into practise and carried out a thorough evaluation utilising a variety of images. The outcomes demonstrated the system's better security and sturdiness. By using this method, the secret information was successfully hidden within the cover image, making it difficult for unauthorised individuals to find or access the hidden data. In conclusion, by combining visual cryptography, the system was able to successfully address the drawbacks of conventional image steganography techniques. It offered a novel method that improves the safety and privacy of sensitive information contained in photographs. The results of this study offer up fresh possibilities for applications requiring secure communication and data concealment while laying the foundation for more investigation in the areas of image steganography and visual cryptography.

5.1 Future Enhancement

The incorporation of machine learning techniques to enhance the detection and prevention of steganography attacks is one potential future improvement for the ”Enhancing Security of Image Steganography Using Visual Cryptography” project. Machine learning algorithms can be trained to recognise the existence of hidden information in photographs by examining the statistical characteristics of those images. By identifying attacks and limiting unauthorised access to the concealed information, this may enhance the steganography system’s overall security. The creation of a mobile application that uses the steganography technique is another potential improvement. A mobile application could offer a practical and safe platform for users to encrypt and decrypt their messages using visual cryptography techniques as the use of mobile devices for communication and data sharing increases. This would necessitate both the creation of an application’s user-friendly interface and the customization of the steganography algorithm to operate on mobile platforms.

REFERENCE

[1] Efe Çiftci, Emre Sümer, *"A Novel Steganography Method for Halftone Images," 2022 30th Signal Processing and Communications Applications Conference (SIU)" , 2022, DOI:10.1109/SIU55565.2022.9864763.*

[2] Jawwad A R. Kazi, Gunjan N. Kiratkar, Sonali S. Ghogale, Atiya R. Kazi, *"A novel approach to Steganography using pixel-based algorithm in image hiding," 2020 International Conference on Computer Communication and Informatics (ICCCI), 2020, DOI:10.1109/ICCCI48352.2020.9104072*

[3] K. Anitha, S. Selvakumar,*"A High Capacity Image Steganography Technique Using LSB Substitution and Modified Huffman Encoding," IEEE International Conference on Computer Communication and Informatics (ICCCI) in 2017, 2017, DOI: 10.1109/CCCI.2017.8117486.*

[4] Malarvizhi. N, Priya. R, *"A Comprehensive Study and Analysis of Reversible Image Steganography Techniques,"2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2021, DOI: 10.1109/ICECA52323.2021.9676053*

[5] Rutvik Dumre, Aashka Dave, *"Exploring LSB Steganography Possibilities in RGB Images," 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2021, DOI: 10.1109/ICCCNT51525.2021.9579588*

[6] Sruthy K Joseph, Ramesh R, *"Random grid based visual cryptography using a common share," 2015 International Conference on Computing and Network Communications (CoCoNet), 2015, DOI: 10.1109/CoCoNet.2015.7411259.*

[7] Jitendra Saturwar, D.N. Chaudhari,*"Secure visual secret sharing scheme for color images using visual cryptography and digital watermarking," 2017 Second International*

Conference on Electrical, Computer and Communication Technologies (ICECCT), 2017, DOI: 10.1109/ICECCT.2017.8117849.

[8] Debasish Jena, Sanjay Kumar Jena,*"A Novel Visual Cryptography Scheme," 2009 International Conference on Advanced Computer Control, 2009, DOI: 10.1109/ICACC.2009.109.*

[9] Ashutosh, Sayan Dev Sen, *"Visual Cryptography," 2008 International Conference on Advanced Computer Theory and Engineering, 2008, DOI: 10.1109/ICACTE.2008.184.*

[10] Vandana Purushothaman, Sreela Sreedhar, *"An improved secret sharing using XOR-based Visual Cryptography," 2016 Online International Conference on Green Engineering and Technologies (IC-GET), 2016, DOI: 10.1109/GET.2016.7916633.*

[11] Piyush Marwaha, Paresh Marwaha,*"Visual cryptographic steganography in images," 2010 Second International conference on Computing, Communication and Networking Technologies, 2010, DOI: 10.1109/ICCCNT.2010.5591730*

[12] K.S. Seethalakshmi, Usha B A, Sangeetha K N,*"Security enhancement in image steganography using neural networks and visual cryptography," 2016 International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS), 2016, DOI: 10.1109/CSITSS.2016.7779393*

[13] Arun Kumar, Supriya.P. Panda N,*"A Survey: How Python Pitches in IT-World," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, DOI: 10.1109/COMITCon.2019.8862251*

[14] Abhinav Nagpal, Goldie Gabrani,*"Python for Data Analytics, Scientific and Technical Applications," 2019 Amity International Conference on Artificial Intelligence (AICAI), 2019, DOI: 10.1109/AICAI.2019.8701341*

[15] Akkem Yaganteeswarudu,*"Multi Disease Prediction Model by using Machine Learning and Flask API," 2020 5th International Conference on Communication and Electronics Systems (ICCES), 2020 DOI: 10.1109/ICCES48766.2020.9137896*

[16] Claudia Audia Trianti, Budhi Kristianto, Hendry,*"Integration of Flask and Python on The Face Recognition Based Attendance System," 2021 2nd International*

Conference on Innovative and Creative Information Technology (ICITech), 2021 DOI: 10.1109/ICITech50181.2021.9590122

APPENDIX

Screenshots

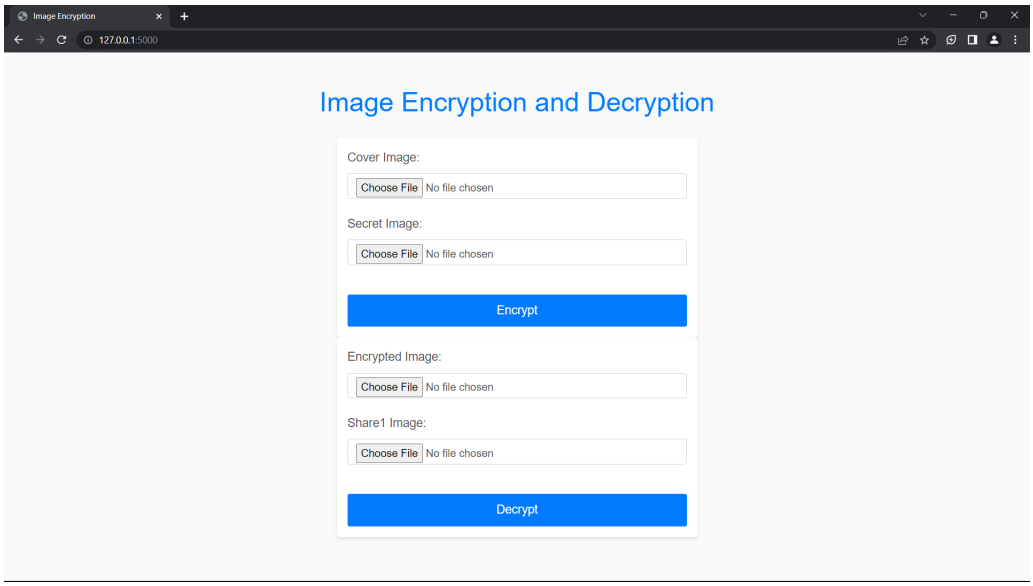


Figure A.1: Home Page

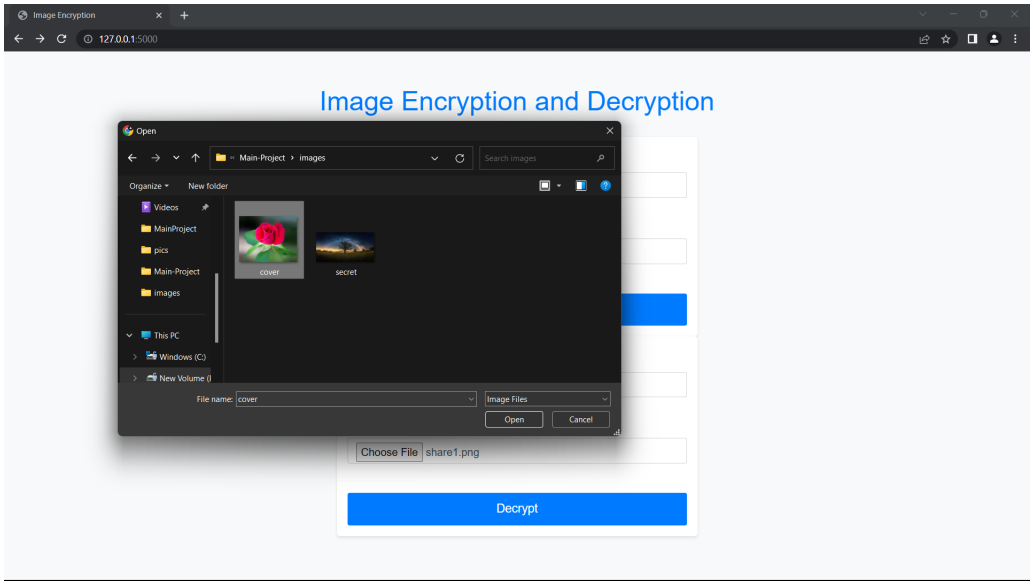


Figure A.2: Selecting Images

Figure A.3: Secret Image

Figure A.4: Cover Image

Figure A.5: Share-1 Image

Figure A.6: Share-2 Image

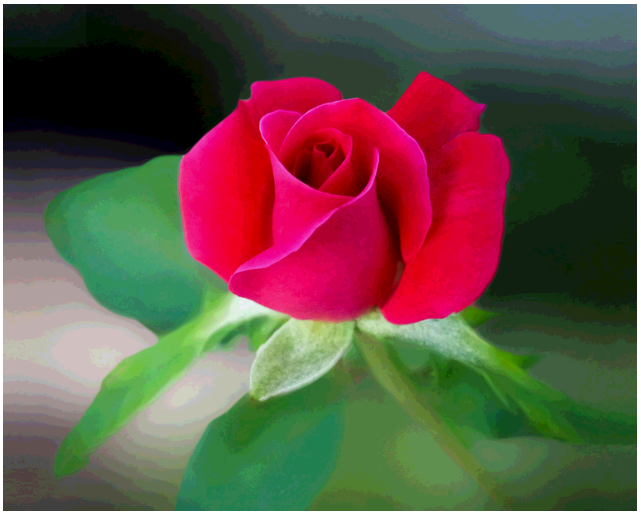


Figure A.7: Encrypted Image

Image Successfully Encrypted!

Figure A.8: Encryption Success Message

Figure A.9: Decrypted Image

Image Successfully Decrypted!

Figure A.10: Decryption Success Message