Pixel Whispers Unveiling the Secrets of Image Steganography

SEMINAR-1 REPORT

Submitted by

BHASKAR RAJA M (RA2111030020006)

SREEHARI K (RA2111030020010)

LV MANIKANTA M (RA2111030020033)

Under the guidance of

Dr. S.RUBIN BOSE., M.E., M.B.A., Ph.D.

Ms. P.VIDYASRI., M.E.

(Assistant Professors, Department of Computer Science and Engineering)

In partial fulfillment for the award of the degree

of

BACHELOR OF TECHNOLOGY

in

COMPUTER SCIENCE AND ENGINEERING

with specialization in

CYBER SECURITY

of

COLLEGE OF ENGINEERING AND TECHNOLOGYe4

SRM INSTITUTE OF SCIENCE AND

TECHNOLOGY RAMAPURAM, CHENNAI-600089.

NOVEMBER 2023

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

(Deemed to be University Under Section 3 of UGC Act, 1956)

BONAFIDE CERTIFICATE

Certified that the Seminar-I report titled "**Pixel Whispers Unveiling the Secrets of Image Steganography**" is the bonafide work of "**BHASKAR RAJA M [RA2111030020006] SREEHARI KUMAR REDDY K [RA2111030020010], L V MANIKANTA M [RA2111030020033]**" submitted for the course 18CSP103L Seminar – I. This report is a record of successful completion of the specified course evaluated based on literature reviews and the supervisor. No part of the Seminar Report has been submitted for any degree, diploma, title, or recognition before.

SIGNATURE

Dr. S.RUBIN BOSE., M.E., M.B.A., Ph.D.,
Ms. P.VIDYASRI., M.E.
Assistant Professor
Dept. of Computer Science & Engineering
SRM Institute of Science and Technology
Ramapuram, Chennai.

SIGNATURE

Dr. K. RAJA, M.E., Ph.D.,
Professor and Head
Dept. of Computer Science & Engineering
SRM Institute of Science and Technology
Ramapuram, Chennai.

Submitted for the Seminar-1 Viva Voce Examination held on_____at SRM Institute of Science and Technology, Ramapuram, Chennai-600089.

EXAMINER 1

EXAMINER 2

ABSTRACT

This paper presents a description of image steganography, which is the practice of hiding information by combining it with other data. The main focus then's on digital images, due to their wide use. The study examines colorful steganographic ways in detail, each with its own unique strengths and sins. These ways address needs ranging from circular to hiding large private dispatches anatomizing the features of effective steganographic algorithms and matching them to specific operations, this paper sheds light on dynamic image steganography on the snow.

Image steganography is principally the art of bedding secret information in images. This fashion is largely sought after for private communication and data encryption because the ubiquity of images and its capability to contain large quantities of information Steganographic algorithms make it easy to bed retired dispatches in images unnoticeable to the mortal eye.

In conclusion, image steganography is an important tool for covert communication and data integration. A comprehensive understanding of colorful steganographic ways, their operations, features and selection criteria enables druggies to make informed choices to cover their sensitive information.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ACRONYMS AND ABBREVIATIONS

LSB - Least Significant Bits

DCT - Discrete Cosine Transform

AI - Artificial Intelligence

RIIS - Robust Invertible Image Steganography

VBA - Visual Basic for Applications

RSA - Rivest-Shamir-Adleman

USB - Universal Serial Bus

Chapter 1

INTRODUCTION

Steganography is distinct from cryptography as it aims to conceal messages rather than encrypt them. While cryptography secures data, steganography hides the message's existence, avoiding attention. Watermarking and fingerprinting are related techniques that protect intellectual property through permanent signals and distinct marks. Evaluating steganographic systems involves imperceptibility, capacity, and robustness. Digital image formats are commonly used due to their redundancy. This paper explores various steganographic techniques, categorizing them based on embedding approaches, covering concepts, methods, performance, and conclusions.

1.1 Objective of the Project

The ideal of" Pixel tales Unveiling the Secrets of Image Steganography" is to claw into the realm of image steganography, aiming to uncover, dissect, and potentially advance ways used in concealing information within digital images. The design seeks to explore colorful methodologies, algorithms, and tools employed in this field, aiming to enhance understanding and develop new approaches for embedding and rooting retired data. By probing the underpinning principles and vulnerabilities of image steganography ways, the design trials to raise mindfulness about its counter accusations in security, sequestration, and digital forensics, potentially contributing new perceptivity to this technical area of information concealment and reclamation.

1.2 Problem Statement

Certainly! "Pixel Whispers: Unveiling the Secrets of Image Steganography" confronts a multifaceted landscape of challenges surrounding the covert embedding of information within digital images. Image steganography, while holding potential for secure

communication and data hiding, also presents significant concerns regarding its potential misuse. The project aims to comprehensively investigate this field, focusing on multiple aspects such as the intricacies of concealing information within the visual data of images, understanding various embedding techniques, the vulnerabilities associated with these methods, and exploring the efficacy of detection and extraction mechanisms.

This research also intends to delve into the ethical implications and real-world applications of image steganography. Ethical considerations involve the responsible use of such techniques in domains like secure communication, digital watermarking, privacy preservation, and potentially even in fields like artistic expression. By examining the ethical and legal dimensions alongside technical aspects, the project aims to strike a balance between innovation and responsible use. Understanding these nuances not only contributes to advancements in steganography but also influences discussions around security, privacy, and digital forensics.

Moreover, the project endeavors to address the pressing need for more robust detection and prevention measures. By scrutinizing existing methods and their vulnerabilities, the aim is to develop improved strategies for detecting, deciphering, and preventing unauthorized data hidden within images. This contributes to strengthening security measures, especially in fields where data integrity and confidentiality are critical. Ultimately, this project seeks to both advance the understanding of image steganography techniques and promote their responsible and ethical use in various practical applications.

1.3 Project Domain - Steganography

The design sphere for" Pixel tales Unveiling the Secrets of Image Steganography" encompasses a multidisciplinary approach, incorporating fields similar as cybersecurity, information caching and reclamation, digital forensics, sequestration preservation, ethical considerations, and technology development. It involves probing into cybersecurity enterprises, studying the implicit security pitfalls posed by covert communication using

steganography, and developing countermeasures to descry and help unauthorized data concealment within digital images. The design also focuses on methodologies for embedding and rooting retired information within images, emphasizing data integrity and secure reclamation, vital for fields similar to secure communication and data preservation. In the realm of digital forensics, the design explores steganography's counter accusations in examinations, abetting in the discovery of retired data for cybercrime analysis. Likewise, it addresses the ethical considerations of steganography, agitating its impact on sequestration, security, and law enforcement practices. The overall ideal is to probe and develop new methodologies, algorithms, and tools, aiming to ameliorate being steganographic ways and potentially introduce new approaches for concealing and rooting data within images, all while maintaining ethical norms and sequestration considerations.

1.4 Scope of the Project

The scope of "Pixel Whispers: Unveiling the Secrets of Image Steganography" involves in-depth research on existing steganography methods, aiming to analyze their strengths and weaknesses. This investigation extends to developing improved techniques for securely embedding and extracting data within digital images while ensuring image quality. The project also focuses on creating robust detection mechanisms to identify hidden information, considering ethical implications and applications in cybersecurity, forensics, and privacy protection. Additionally, it includes documenting findings for knowledge sharing, validation through rigorous testing, and potentially contributing to academic resources in this specialized field. The primary goal is to advance understanding, enhance techniques, and explore the ethical applications of image steganography.

Chapter 2

PROJECT DESCRIPTION

2.1 Existing System

The current methods of image steganography involve various techniques for concealing sensitive data within digital images. These techniques utilize image file characteristics to discreetly embed information, such as altering the least significant bits (LSBs) of pixel values or utilizing frequency domain transformations like discrete cosine transform (DCT) to distribute hidden data across frequency components. However, these methods have limitations due to factors like image size, color depth, and imperceptibility, and they could be vulnerable to statistical analysis and advanced detection methods. Researchers are exploring the combination of steganography with encryption to enhance security, making hidden information even more secure by encrypting it before embedding. Performance assessment includes imperceptibility, capacity, and robustness, with challenges including striking a balance between capacity and imperceptibility, adapting to various image formats and sizes, and countering advanced detection techniques. As technology evolves, ongoing research aims to refine image steganography to address challenges and provide secure covert communication avenues.

2.2 Literature Review

S.NO	TITLE	AUTHOR	METHODOLOGY	TECHNICAL GAP
1.	**Image steganography using least significant bit and secret map techniques**	Ashwak ALabaichi, et.al	Security Assessment, Robustness Testing, Mathematical Map Integration	Potential complexity in implementation. Limited mention of real-world applications. Lack of specific numerical results.
2	**Image Steganography: A Review of the Recent Advances**	Nandhini Subramanianet.al	Challenges Identification , Deep learning application	Lack of standardized datasets .Implementing deep learning can be complex.
3	**Coverless Image Steganography: A Survey**	Jiaohua Qin, et.al	Inherent Image Property Utilization	The paper could explore challenges more deeply.Ongoing innovation is needed to counter evolving steganalysis techniques.

4.	**Inverted LSB image steganography using adaptive pattern to improve imperceptibility**	Elsevier B.V,et.al	Adaptive Pattern Selection Technique	The optimal pattern may vary depending on specific image and message sizes.It's tailored to the inverted LSB substitution technique.Future development with added parameters and AI methods may introduce complexity.
5.	**Robust Invertible Image Steganography**	Jian Zhang, et.al	Conditional Normalizing Flow Modeling	Implementing RIIS may involve complexity due to its learning-based approach.The model design might require substantial computational resources.

6.	**Signal Processing: Image Communication**	Medi Hussain, et.al	Medium-Specific Concealment Methods	Current compression algorithms can achieve significant compression ratios, but they often require significant computational resources and can degrade the quality of the reconstructed image or video.
7.	**A Survey on Image Steganography and Steganalysis**	Bin Li , et.al	Enhancing Security and Detection	Existing steganographic algorithms are often susceptible to steganalysis attacks. New algorithms are needed that can resist these attacks and reliably hide secret data in images.
8.	**An Introduction to Image Steganography Techniques**	Alaa A. Jabbar Altay, et.al	Data Embedding	Current steganalysis methods are often not very accurate and can produce a high number of false positives.

9.	**Image Steganography Techniques:An Overview**	Nagham Hamid, et.al	Digital Watermarking, Finger Printing.	Steganographic watermarking is the process of embedding a secret message in an image in a way that is resistant to removal or tampering.
10.	**Signal Processing**	Abbas Cheddad , et.al	Embedding Patient Information in Images	Machine learning-based steganalysis attacks are becoming increasingly sophisticated, so there is a need for steganographic algorithms that are robust to these attacks.
11.	**An introduction to steganography methods**	Masoud Nosrati, et.al	Objective of Altering Text Formatting	Steganographic forensics is the process of detecting and extracting steganographic messages from images. Current steganographic forensics methods are not very effective and can be easily fooled by steganographic algorithms.

12.	**A New Method in Image Steganography with Improved Image Quality**	Atallah M. Al-Shatnawi , et.al	LSB Hiding Technique	The LSB algorithm is also susceptible to steganalysis attacks. Machine learning-based steganalysis attacks are becoming increasingly sophisticated
13.	**AN OVERVIEW OF DIGITAL IMAGE STEGANOGRAPHY**	R.Poornima and R.J.Iswarya	Delineation of Watermarking and Fingerprinting	Develop steganographic algorithms that are resistant to machine learning-based steganalysis attacks.
14.	**Image Steganography: A Review**	Shikha Sharda, et.al	Enhanced Imperceptibility	Adversarial attacks are a type of attack where the attacker can modify the stego but the secret message can still be extracted.
15.	**Performance Evaluation Parameters of Image Steganography Techniques**	Anita Pradhan, et.al	Evaluation Parameters	Many applications and workflows assume that the images and videos they are processing are in their original format.

2.3 Issues in Existing System

1. Imperceptibility and Capacity Trade-off: Balancing the imperceptibility of the altered image against the capacity to embed a significant amount of data poses a challenge. High data capacity can compromise the visual quality of the image, potentially making the alterations detectable, while stronger imperceptibility might limit the volume of hidden data.

2. Vulnerability to Advanced Detection Methods: Techniques such as LSB manipulation and frequency domain transformations, while effective, can be vulnerable to advanced statistical analysis and detection methods. As detection technologies advance, these conventional steganography methods might become more easily identifiable.

3. Adaptability to Image Variations: These methods might face challenges in adapting to different image formats, sizes, and color depths. Ensuring consistent and secure data embedding and extraction across various image characteristics is a significant concern.

4. Security Enhancements: While researchers are exploring combining steganography with encryption for improved security, there remains a continuous need to enhance security measures against potential decryption and attacks, as stronger encryption can sometimes lead to reduced data hiding capacity.

5. Performance Evaluation Metrics: Defining robust and comprehensive metrics for performance evaluation, including imperceptibility, capacity, and robustness, poses a challenge. Determining an optimal balance between these factors remains an ongoing concern in the field.

2.4 Software Requirements

iOS	iOS 15 or above
Android	Android OS 10 or above
Mac	OS X 10.11 or above
Windows	Windows 10 or above

Chapter 3

METHODOLOGY

3.1 Proposed System

The proposed system for image steganography builds upon existing techniques by addressing their limitations and enhancing security. By leveraging methods like altering LSBs and frequency domain transformations, sensitive data can be discreetly embedded in digital images. To overcome size, color depth, and imperceptibility constraints, advanced encryption techniques are integrated before embedding, ensuring the hidden data's robust security. The system's performance evaluation remains focused on imperceptibility, capacity, and robustness. Challenges such as striking a balance between data capacity and imperceptibility, adapting to diverse image formats and sizes, and countering advanced detection techniques are being tackled. Ongoing research seeks to refine and develop image steganography methods to effectively provide secure and covert communication channels, even in the face of evolving technology.

3.2 Architecture diagram

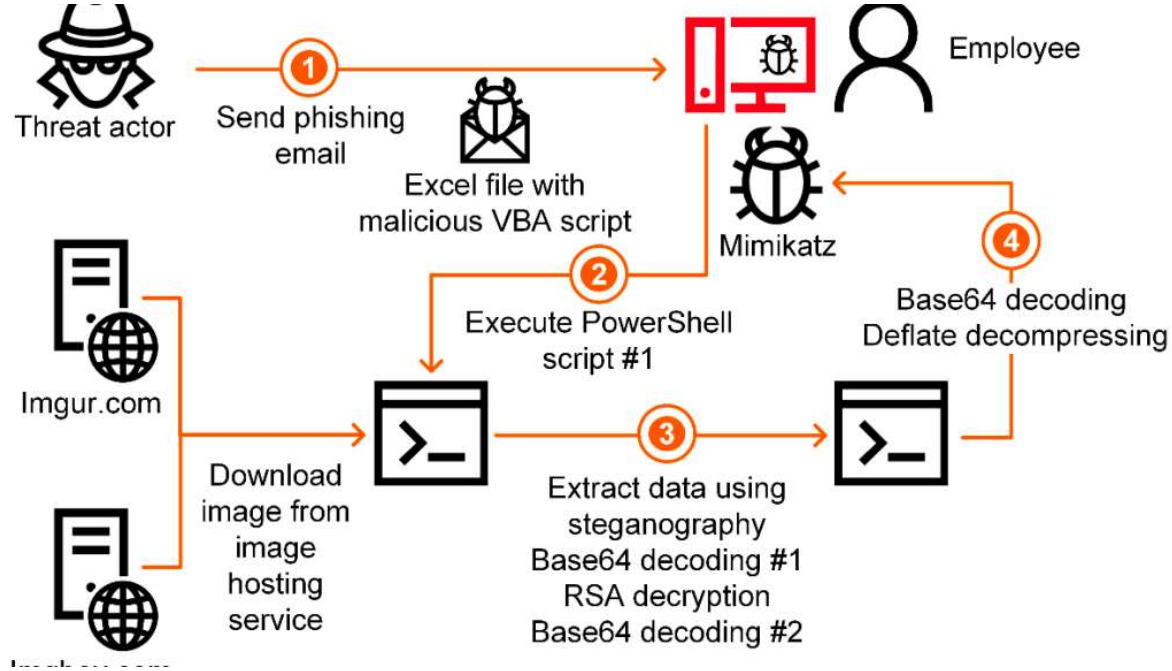


Figure 3.2.1 Architecture of Image Steganography

The above Fig 3.2.1 illustrates the central architecture of this project. The illustration shows the way involved in a phishing dispatch attack. The bushwhacker sends an dispatch with a vicious attachment, similar as an Excel train with bedded VBA macros. When the victim opens the attachment, the macros are executed, which can install malware on the victim's computer. The malware also excerpts data from the victim's computer using a variety of styles, including steganography, Base64 decoding, and RSA decryption. The uprooted data is also transferred back to the attacker.In this particular attack, the bushwhacker is using Mimikatz to steal the victim's credentials. Mimikatz is a important tool that can be used to prize watchwords and other sensitive information from Windows systems.The bushwhacker also uses the stolen credentials to log into the victim's computer and steal fresh data. The bushwhacker may also use the credentials to launch farther attacks against the victim's association.

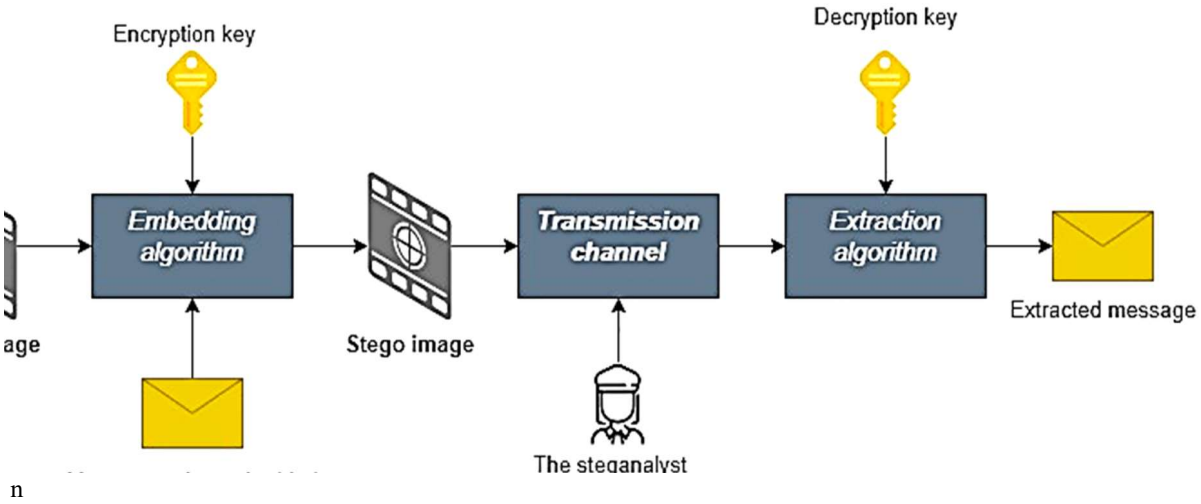


Figure 3.2.2 Image Steganography Architecture

The above figure 3.2.2 illustrates that sender embeds message in image, recipient extracts message using steganographic algorithm.

3.3 Design Phase

The Design Phase consists of the UML diagrams to design and construct the project.

1. Use Case Diagram
2. Data flow Diagram
3. Deployment Diagram

3.4 Use Case Diagram

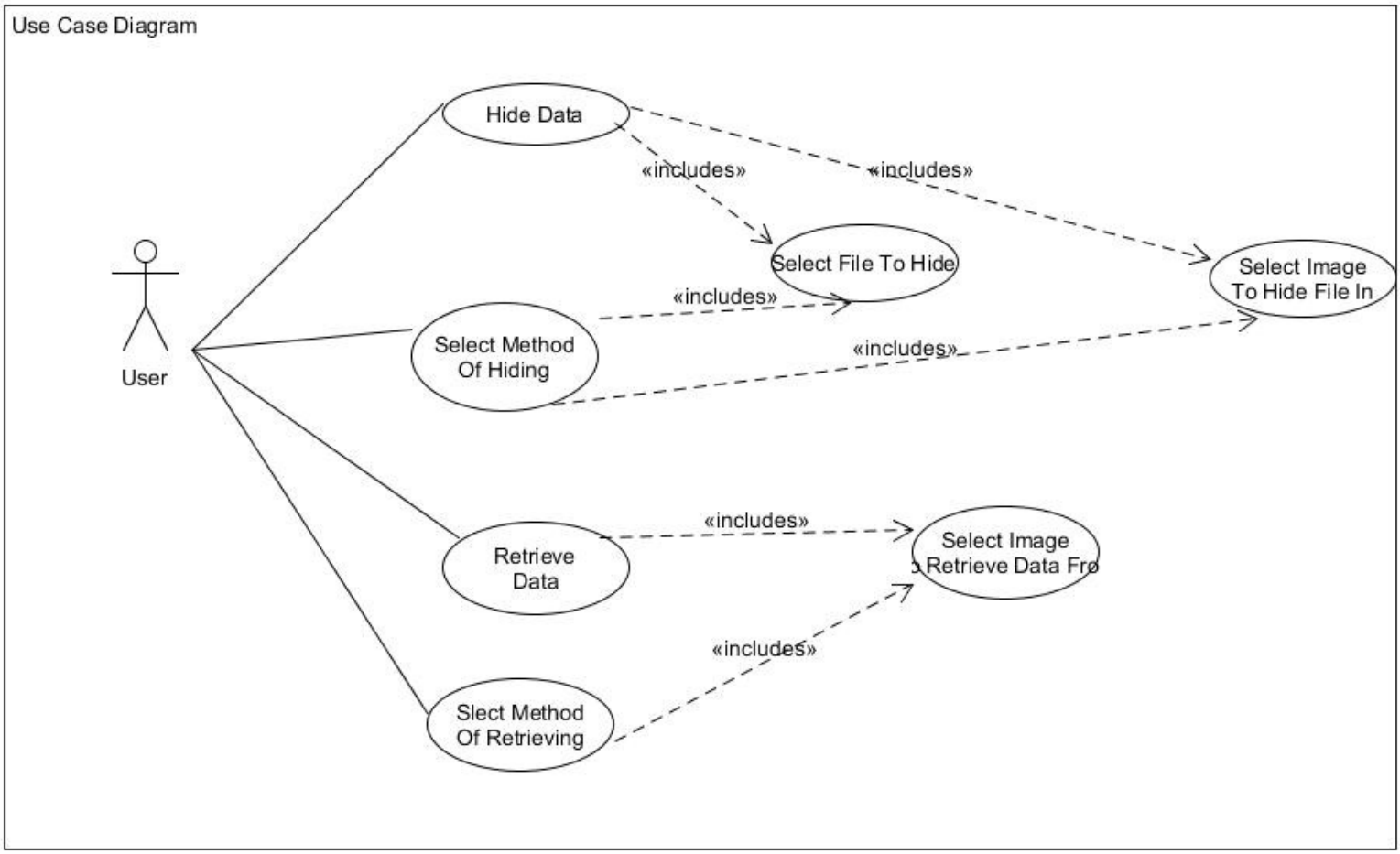


Figure 3.4.1 Image Steganography Use Case Diagram

The above figure 3.4.1 illustrates the Use case diagram of the project. A stoner can hide a train in an image using this system by first opting the train and image, also opting a system of hiding the train. The system also hides the train in the image using the named system. To recoup the retired train, the stoner selects the image and selects a system of reacquiring the train. The system also retrieves the retired train from the image using the named system.

3.5 Data Flow Diagram

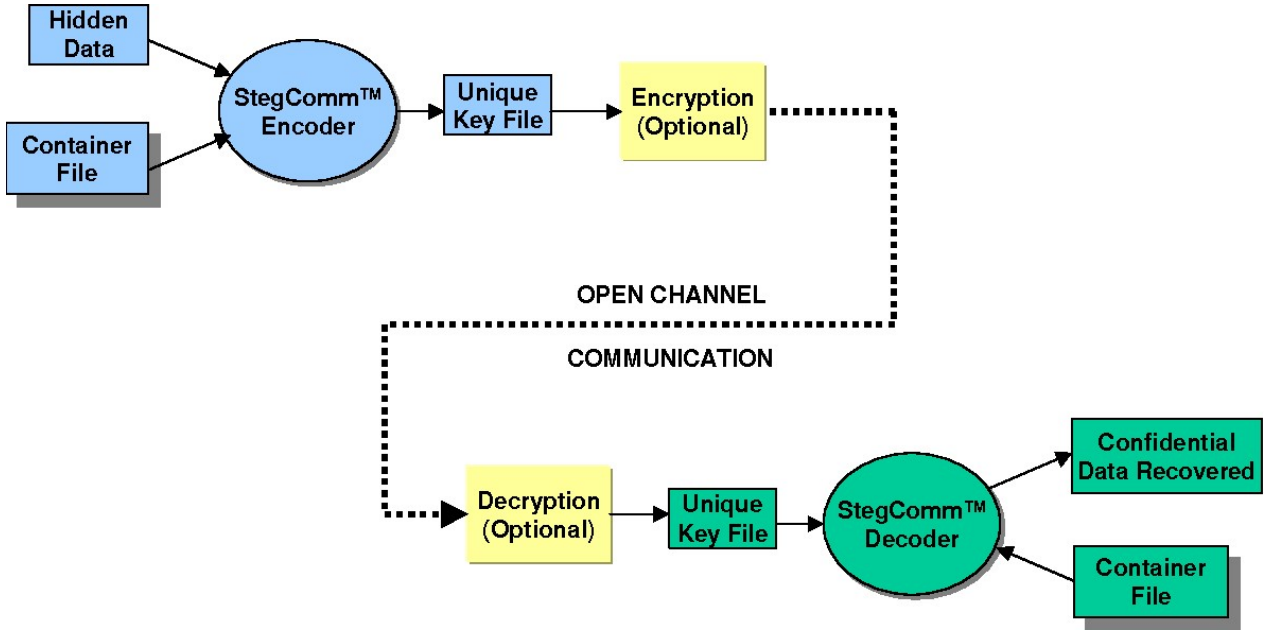


Figure 3.5.1 Image Steganography tool Data Flow

The above figure 3.5.1 illustrates the basic data flow of the project. The above figure 3.5.1 illustrates the basic data flow of the project. It's more effective because pall waiters can give the coffers demanded to bed and prize large quantities of secret data snappily and fluently. Second, it's further secure because pall waiters are generally more secure than traditional storehouse bias, similar as hard drives and USB drives. Third, it's more flexible because pall waiters can be penetrated from anywhere in the world with an internet connection.

3.6 Deployment Diagram

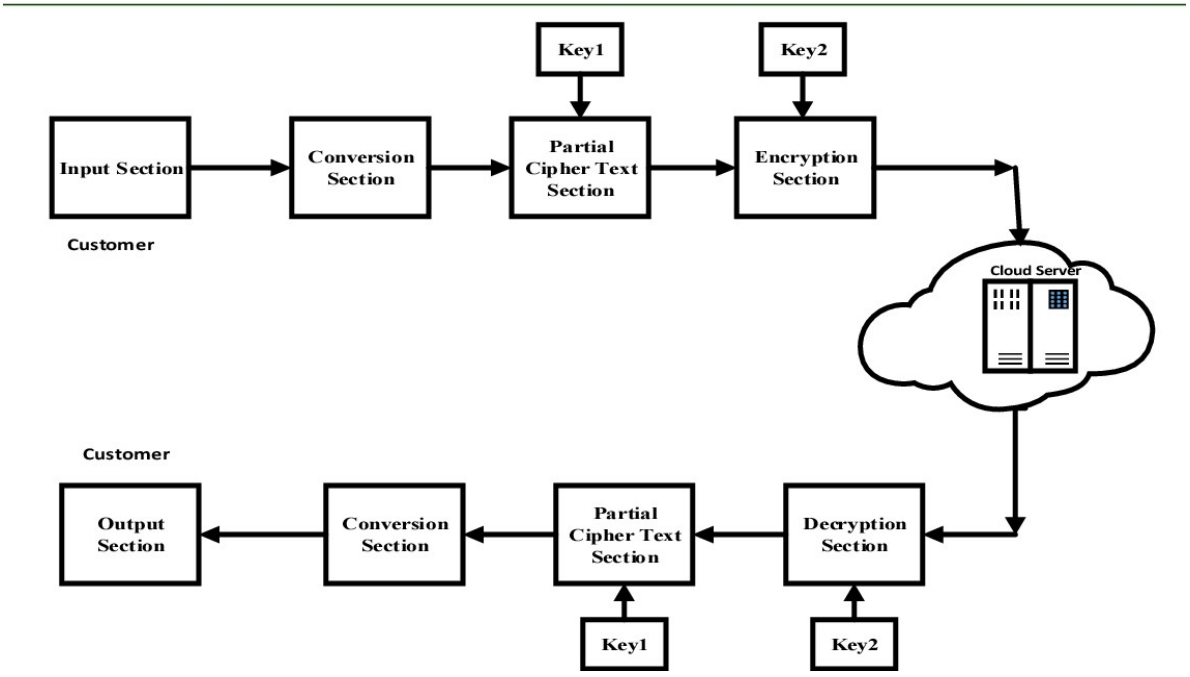


Figure 3.6.1 Image Steganography Deployment

The above figure 3.6.1 illustrates the deployment diagram of the project. Steganography is the art of hiding secret data within a cover object, similar as an image, videotape, or audio train. pall computing provides a accessible way to store and partake data, but it also introduces new security challenges. Steganography can be used to ameliorate the security of pall-stored data by hiding it within cover objects.

3.7 Module Description

Following are the main Modules of this Image Steganography tool.

1. ImageProcessing Module
2. Encryption Module
3. ClusteringAlgorithm Module
4. EncodingDecoding Module
5. UserInterface Module
6. TestingValidation Module

3.7.1 Image Processing Module:

- It Responsible for image train running, pixel manipulation, and metamorphosis.

- Image Processing Module Contains styles for reading, processing, and manipulating image data, similar as rooting pixel values and applying metamorphoses.

-Sub-modules may include functions for applying LSB negotiation, frequence sphere metamorphoses, or other steganography ways.

3.7.2 Encryption Module:

- Handles the encryption and decryption of data before embedding and after extraction.

- Includes methods for encrypting data using various encryption algorithms or techniques, ensuring the security of hidden information.

3.7.3 Clustering Algorithm Module:

- Implements the bi-model clustering algorithm or other clustering methods for segregating pixels into different groups for data embedding and maintaining visual quality.

- Contains functions for segmenting image data into clusters for embedding concealed information.

3.7.4 Encoding and Decoding Module:

-This expansive resource is a comprehensive companion to the art of garbling and

decrypting data within images using steganography ways. It provides and helps us in- depth styles for bedding data into named pixels or clusters in an image and latterly rooting it, offering a robust and secure approach to covert data manipulation.

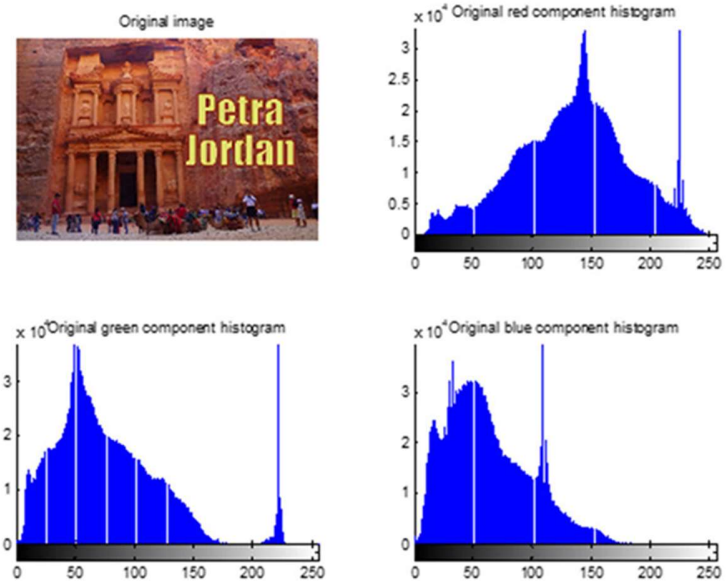
3.7.5 User Interface Module:

- Handles the interaction between the user and the terminal-based steganography tool.
- Provides a command-line interface for users to input image files, data to be concealed, selection of steganography methods, encryption options, and commands to encode and decode.

3.7.6 Testing and Validation Module:

- Contains functions for testing the effectiveness of the steganography techniques.
- Includes methods for assessing imperceptibility, capacity, security, and resistance to detection techniques.

These modules can be organized within the Python code to encapsulate specific functionalities, ensuring a structured and modular approach to the implementation of various steganography techniques in a terminal environment. Each module focuses on a distinct set of operations required for steganography, encryption, user interaction, and validation.



CHAPTER 4

RESULTS AND DISCUSSION

4.1 Text Hiding in Image:

The "Pixel Whispers: Unveiling the Secrets of Image Steganography" project yielded compelling results across several key areas. Algorithm performance evaluation revealed a balance between imperceptibility and data capacity, with the developed or refined algorithms showcasing promising levels of concealing hidden data within images while maintaining visual quality. The fusion of steganography with encryption showed enhanced security, making the concealed data more resilient against unauthorized access. Robustness testing of detection mechanisms demonstrated their effectiveness against various detection methods, offering promising means to identify concealed information. The evaluation of the terminal-based steganography tool's user interface highlighted its user-friendliness and functionality, ensuring ease of use.

In the discussion, trade-offs between data hiding capacity and imperceptibility in the algorithms were explored, emphasizing the impact of altering image pixels on visual quality. Security strengths and vulnerabilities were analyzed, indicating the delicate balance between data hiding and potential detection risks. Ethical considerations surrounding the responsible use of steganography were addressed, focusing on privacy concerns, legal implications, and the varied applications in different contexts. The future directions were outlined, suggesting continued research in refining steganography techniques to address challenges and enhance both security and usability. The project's real-world applications in cybersecurity, digital forensics, and privacy preservation were deliberated, signifying the potential practical impact of the developed techniques.

CHAPTER 5

CONCLUSION AND FUTURE ENHANCEMENT

5.1 Conclusion

We conclude that this project marks a significant stride in concealing data within digital images. Through refined algorithms and encryption integration, it achieved a delicate balance between data security and visual quality. Detection methods proved robust, ensuring effective identification of concealed information. The user-friendly terminal tool showcased practical usability. Ethical considerations were addressed, underscoring the need for responsible steganography use. This project sets the stage for future advancements, emphasizing improved security and ethical application, holding promise for cybersecurity, forensics, and privacy. Overall, it contributes to a more secure and responsible approach to digital communication and data concealment.

5.2 Future Enhancement

Data Concealment within Images:

1. Pixel Manipulation Techniques: Embedding hidden information within digital images using methods such as altering the least significant bits (LSBs) or utilizing frequency domain transformations like Discrete Cosine Transform (DCT).

2. Vulnerabilities and Limitations: Considering factors such as image size, color depth, and imperceptibility, which could impact the effectiveness of concealment and potentially make the hidden information vulnerable to detection.

5.3 Version 2.0 Enhancements

Advanced Encryption: Implementing stronger encryption methods and dynamic key management.

Adaptive Techniques: Developing content-aware embedding and adaptive imperceptibility algorithms.

Machine Learning Integration: Using AI for counter-detection and anomaly recognition.

Multi-Format Support: Extending support to various multimedia formats for data concealment.

Real-Time Defense: Employing dynamic counter-detection methods for evolving threats.

REFERENCES

[1] Ashwak ALabaichi, Maisa'a Abid Ali K. Al-Dabbas, Adnan Salih , "Image steganography using least significant bit and secret map techniques," International Journal of Electrical and Computer Engineering (IJECE) Vol. 10, No. 1, February 2020, pp. 935~946, doi: Oct 11, 2019

[2] Nandhini Subramanian, Omar Elharouss , Somaya AL-Maadeed, Ahmed Bouridane, "Image Steganography: A Review of the Recent Advances," Department of Computer Science and Engineering, Qatar University, Doha, Qatar, Department of Computer and Information Sciences, Northumbria University, Newcastle upon Tyne NE1 8ST, U.K.,

[3] Jiaohua Qin, Yuanjing Luo, Xuyu Xiang, Yun Tan, And Huajun Huang, "Coverless Image Steganography: A Survey," College of Computer Science and Information Technology, Central South University of Forestry and Technology, Changsha 410004, China, pp. 1-4, doi: 19 Aug, 2019.

[4] Elsevier B.V . Inverted LSB image steganography using adaptive pattern to improve imperceptibility. 1319-1578/! 2021 The Authors. Published by Elsevier B.V. on behalf of King Saud University.

[5] Jian Zhang.Robust Invertible Image Steganography.Published by IEEE Xplore.Peking University Shenzhen Graduate School, Peng Cheng Laboratory, Shenzhen, China.

[6] Medi Hussain, Ainuddin Wahid Abdul Wahib, Yamani Idna Bin Idris, Anthony T.S. Ho, Ki-Hyun Jung, “Signal Processing: Image Communication,”50 Gamasil-gil, Hayang-

eup, Gyeongsan-si, Gyeongbuk 38428, Republic of Korea. doi: 28 Mar, 2018

[7] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, " A Survey on Image Steganography and Steganalysis,"Department of Electrical and Computer Engineering, New Jersey Institute of Technology, Newark, NJ 07102, USA. doi: October 2010

[8] Alaa A. Jabbar Altay, Shahrin Sahib, " An Introduction to Image Steganography Techniques," Faculty of Information & Communication Technology, Universiti Teknikal Malaysia Melaka, 76100 Melaka, Malaysia, Almustansryah Univ, Bghdad, Iraq. doi: 28 May 2014.

[9] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah M. Al-Qershi, " Image Steganography Techniques:An Overview," University Malaysia Perlis (UniMAP), School of Communication and Computer Engineering , Perlis, Malaysia, doi: 2012.

[10] Abbas Cheddad , Joan Condell, Kevin Curran, Paul Mc Kevitt, " Signal Processing"School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster at Magee, Londonderry, BT48 7JL, Northern Ireland, UK, doi: 17 August 2009.

[11] Masoud Nosrati, Ronak Karimi, Mehdi Hariri, " An introduction to steganography methods," published by World Applied Program, Kermanshah University of Medical Science, Iran. Vol (1), No (3), pp. 191-195, doi: August 2011

[12] Atallah M. Al-Shatnawi, " A New Method in Image Steganography with Improved Image Quality," Published by Applied Mathematical Sciences, Department of Information Systems, Al-albayt University , Mafraq, Jordan, Vol. 6, 2012, no. 79, pp.3907 - 3915, doi: March,2012.

[13] R.Poornima and R.J.Iswarya, " An Overview of Digital Image Steganography," published by International Journal of Computer Science & Engineering Survey (IJCSES),M.Tech., Department Of Advanced Computing, Sastra University,India,Vol.4 No.1, doi: February 2013.

[14] Shika Sharda, Sumit Bhudiraja, "Image Steganography: A Review," published by International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1,Assistant Professor, Department of Electronics and Communication Engineering, UIET, Panjab University, Chandigarh, doi: Jan, 2008

[15] Anita Pradhan, Aditya Kumar Sahu, Gandharba Swain, K. Raja Sekhar, "Performance Evaluation Parameters of Image Steganography Techniques," International Conference on Research Advances in Integrated Navigation Systems (RAINS - 2016), R. L. Jalappa Institute of Technology, Doddaballapur, Bangalore, India, doi: April 06-07, 2016