National College of Ireland

Securing secret data using an enhanced Camellia encryption with steganography using pixel indicator technique

Academic Internship
MSc in Cybersecurity

Bharat Moganti
Student ID: x22150935

School of Computing
National College of Ireland

Supervisor: Dr.Vanessa Ayala-Rivera

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: Bharat Moganti

Student ID: x22150935

Programme: MSc Cyber Security **Year:** 2023-2024

Module: Academic Internship

Supervisor: Vanessa Ayala-Rivera

Submission Due Date: 31/01/2024

Project Title: Securing secret data using an enhanced Camellia encryption with steganography using pixel indicator technique

Word Count: 7615 **Page Count** 21

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Bharat Moganti

Date: 31/01/2024

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Securing secret data using an enhanced Camellia encryption with steganography using pixel indicator technique

Bharat Moganti
x22150935

Abstract

Data privacy in the digital realm faces escalating threats necessitating innovative protective measures beyond conventional encryption. Information can be made more secure by the practice of steganography, which involves hiding data through unrelated cover material. This study explores the fusion of advanced Camellia encryption with steganography employing the Pixel Indicator Technique, aimed at fortifying information security within visual data. The research delves into the efficacy of this hybrid approach in concealing sensitive information within images while preserving statistical integrity and imperceptibility to visual inspection.

The Pixel Indicator Technique, a robust method examined in this investigation, seamlessly integrates pixel value concealment with encryption to create imperceptible yet secure steganographic images. The study rigorously assesses various image quality indicators such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and Mean Squared Error (MSE) to ensure minimal alteration to original images while maintaining consistent pixel luminosity distribution. Visual inspection via histogram analysis confirms the technique's imperceptibility and successful integration of concealed data without noticeable anomalies. This research offers insights into the robustness of combining Camellia encryption with Pixel Indicator Steganography, suggesting promising directions for future research and advancements in secure data communication.

Keywords: Steganography, Pixel indicator technique, Camellia encryption, cryptography, Peak Signal-to-Noise Ratio, Structural Similarity Index Measure, and Mean Squared Error

1 Introduction

The increasing dependence on digital platforms for information sharing highlights how critical it is to protect people's security and privacy in today's communication environment. While there are benefits and drawbacks to technology's widespread use, companies and educational institutions will always need to produce creative ways to safeguard student information. By incorporating hidden layers into digital photos, this study tries to investigate the relationship between cryptography and steganography and offers a fresh and efficient method for data transmission that is safe. Ensuring the highest level of security in communication techniques is crucial in the 21st century, since digital communication plays a pivotal role.

Unauthorized access to transmitted content is a problem that is increased by the growing digital footprint. The suggested strategy combines the security of the Camellia encryption technique with the efficacy of steganography to increase the degree of secrecy for encoded communications concealed inside digital photographs. Camellia, which is renowned for its strong encryption methods, offers a high degree of protection for encrypted communications, rendering them unintelligible to outside parties trying to decipher them. Steganography and cryptography together can increase the effectiveness of security systems by strengthening their resistance to intrusions.

Considering the absolute necessity of total communication concealment, steganography becomes indispensable. Data transit security is improved with the cooperation of steganographic technology and the Camellia algorithm. This integration makes it feasible to encrypt messages and then hide them behind innocent digital images. By keeping steganographic images from being easily recognized, subtle changes provide security by impeding visual identification. To evaluate the efficacy of the approach, appropriate statistical tests and analyses must be conducted. The picture quality is evaluated using a variety of criteria, including the structural similarity index, entropy difference, average and maximum differences, normalized cross-correlation, and others. The validity and security of the pictures are verified by comparing them through these tests with the matching steganographic coverings.

Furthermore, this study explores the visual implications of the suggested method, stressing the attainment of a smooth merging of cover and steganographic pictures wherever feasible. Empirical studies indicate that the steganographic picture is hidden because the human visual system cannot distinguish between the two. Analyzing histograms yields important information that protects picture features from possible steganography assaults. The suggested method is highly valuable since it complies with the CIA Triad framework and guarantees the privacy, accessibility, and accuracy of information. Up to a maximum of 10,000 characters, the steganographic picture deftly combines words of different lengths while maintaining its aesthetic appeal.

Subsequent research endeavors might delve into additional file types, including video, audio, and networking protocols, with the aim of expanding the range of potential uses for image-based steganography. This growth is warranted by the significant and quick developments in technology, which emphasize the continuous difficulty of data security in a society that is becoming more networked by the day. A notable development that demonstrates the ongoing quest for improved data security is the fusion of steganography with encryption methods.

1.1 Research questions

1. How the Camellia encryption algorithm can be strengthened to increase the security of confidential data while employing the Pixel Indicator Technique for image steganography?
2. What is the best way to combine the Pixel Indicator Technique with Camellia encryption to strike a balance between security, capacity, and imperceptibility?

2 Related Work

Researchers in the evolving portion based on information security have highlighted a significantquantity of their respective effort on researching the ways. The ways are based on steganography as well as encryption that is combined. Following their combination, these two approaches constitute a strong alliance that can effectively address the issues that are associated with the transfer of data in a safe manner. After conducting a thorough review of the relevant literature, it has been discovered that researchers have used a wide variety of approaches to improve the reliability and secrecy of concealed signals in digital media forms.

2.1 Historical Perspectives

Steganography is mostly likely to be traced back to the usage of wax tablets used by ancient civilizations. Moreover, it continues to be used in current times despite the prevalence of digital technology. Steganography's beginnings cannot be fully understood. It is important to note that the history of steganography is both broad and diverse. In the realm of digital technology, there has been a discernible increase in interest in cryptography because of the greater security of encrypted data that has been provided by recent breakthroughs in encryption technologies. It is possible that this might be attributable to the constantly growing popularity of cryptography.

It is widely acknowledged that (Mandal et al. 2022), were the first to use the phrase "Prisoner's Problem" and established a new standard for the methodology of steganographic study. Using the scenario in which two hostages were attempting to have a conversation in a discrete manner while being continually observed, Simmons demonstrated the concept of secure clandestine communication.

2.2 Early Digital Steganography

The digital comparison to more conventional means of covert transmission in the digital realm, steganography marked a substantial level of development. When digital communication was in its early phases, it made it easier to send information in a discrete manner. Around this critical juncture, digital steganography came into being, laying the groundwork for further developments in encrypted communication.

The digital revolution has increased the need for encrypted electronic communications. New techniques for storing large amounts of digital data in new datasets led to the rise of digital steganography in the second half of the 20th century (Rustad et al. 2022) This was developed by students and professionals. Changes in the physical characteristics of the medium or incorporation of messages into tangible objects were previously the two most common methods of concealing information The transition from analog to digital camouflage is a major break from traditional methods on. The rise of electronic data in bits and bytes has created new opportunities for storing information due to the widespread use of digital technologies.

Digital steganography is utilized to hide certain information by using "least significant bits" or (LSBs) of the data. When it comes to binary representations, the modifications that are made to the least significant bit (LSB), which is the lowest numerical value, are often indiscernible to that of the human eye. The LSB algorithm evolved as a viablealternative for encrypting digital image data because of this property. A few innovative methods for

modifying or replacing the first bits of pixel values in digital images have been developed because of the inquiry into picture steganography. The visual quality of the photographs was preserved while the basic procedure secretly encoded information. As a result of their straightforwardness and ease of use, rudimentary steganography tools have the potential to identify these first, fundamental approaches with relative ease.

LSB-based techniques were crucial to the development of digital steganography, yet they were subject to a number of major restrictions that made them difficult to implement. Compression techniques and the level of complexity of the image are two elements that may have an impact on the detectability of LSB variants. Due to the potential degradation of high-frequency features, which are important for preserving visual acuity, the use of a low-pass filtering (LSB) technique was shown to be infeasible (Kaur et al. 2022). Due to the potential degradation of high-frequency features, which are important for preserving visual acuity, the use of a low-pass filtering (LSB) technique was shown. Therefore, it is infeasible due to the potential degradation of high-frequency features, which are important for preserving visual acuity, the use of a low-pass filtering (LSB) technique was shown to be infeasible (Kaur et al. 2022).

“Early digital steganography” devices were vulnerable to certain statistical analysis which is based on decryption due to the very basic construction. This construction is making them unreliable. Cryptanalysts fought with scientists over how to develop them. In accordance, cryptanalysts worked to provide them with encryption techniques is effective, as scientists introduce new methods of detection. In 2022, the field of digital steganography took a huge leap forward. Johnson developed adaptive steganography as an alternative to static encryption techniques to mask information. An embedding method that dynamically adapts itself to the newly collected data is used in this method. Steganographic systems are designed to change, making them difficult to interpret. This is why these systems are so strong.

Researchers (Kaur et al. In 2022), it discovered an encrypted network called "adaptive steganography", capable of changing the format depending on the type of channel it is embedded in. These discoveries will lead to further developments in developing simple steganographic systems. This forward thinking, which was a hallmark of iterative digital steganography, will forever influence subsequent developments. The researchers began looking for new techniques that could improve security when they realized the limitations of LSB-based techniques in which the various methods adopted included encryption, broadcast spectrum technology, and frequency domain conversion.

There is a very basic requirement for internet communication based on clandestine, as depicted by the developmental digital steganography from its very origin to its present technology form. Even though steganography continues to be hard to decipher, the early creators of digital steganography have amassed a wealth of knowledge that has made a significant contribution to the area of secure information transfer. The first efforts conducted had a long-lasting influence on the essential structure of the most recent breakthroughs in steganography, which in turn continually drove the progression of technology.

2.3 The Synergy of Steganography and Cryptography

During the information technology age, the connection between steganography and encryption became more apparent. Over the course of history, individuals have used cryptographic techniques to safeguard sensitive information by concealing encrypted conversations behind digital media materials. In the year 2022, Rathore and colleagues were the first to develop a revolutionary steganography method that made use of public-key cryptography. This technique used public-key pairs to maintain the anonymity of the disguised signal, which in turn assured that the communication that took place between the participants was kept confidential.

2.4 Advancements in Modern Steganography

The contemporary steganographic methods are distinguished by their potential to evade detection and their unparalleled level of intricacy. It can avoid the conventional methods of steganography analysis using transformation methods and discrete cosine transformation (DCT). This is done by overlaying the data in the frequency domains. Unlike LSB-based methods this method can increase the uncertainty without being affected by compression problems

Wavelet-based steganography was an innovation proposed by (Wei et al. 2022) and their results. This innovation completely changed the landscape of encrypted communications. The addition of data in the spatial and frequency domains is obtained by transforming wavelets, which is also a reliable foundation for storing signals in digital information.

2.5 Cryptographic Advancements

Growing algorithms have boosted steganography utilizing encryption. The "Advanced Encryption Standard" (DES) should now be used to encrypt sensitive data as it has superseded the "Data Encryption Standard" (DES). These researchers researched integrating steganography with AES. will be incorporated to secure private communication The (Zhou et al. 2022) encryption algorithm. Its quickness and resilience to cryptanalytic assaults made it popular in. Due to its high security, researchers are considering employing steganographic systems to safeguard embedded communications.

3 Research Methodology

An organised analysis of steganography and encryption technologies offers a systematic approach to navigating the complex realm of secure communication. Below is a comprehensive summary of the procedures required to analyse the suggested strategy. Data collection, trial design, and assessment parameters are integral components of the method that were previously defined.

This research methodology employs a sophisticated framework to effectively investigate the research inquiries and accomplish the primary objectives of the investigation. The main objective of this work is to use the Pixel Indicator approach with an enhanced iteration of the Camellia encryption algorithm to embed encrypted text into digital photos. The software has encryption and steganography functionalities. The study encompasses a diverse range of subjects, spanning from theoretical foundations to actual implementation and assessment of

effectiveness. The workflow of the process is shown in the below figure.

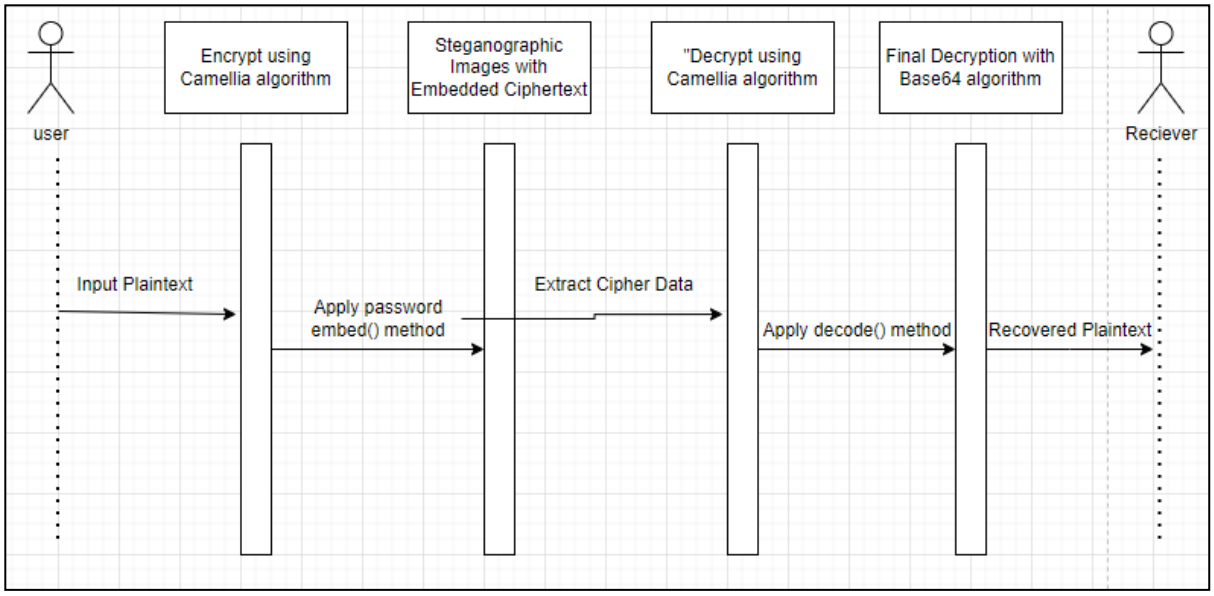

Figure 1: Sequence diagram

3.1 Data collection

The acquisition of data is an essential component of research, and covert investigations may be able to tremendously profit from the use of a diverse collection of digital photographs.The experiment is comprised of four different colour photographs, which are referred to as raw image1.jpeg, raw image2.jpeg, raw image3.jpeg, and raw image4.jpeg respectively. We can evaluate the effectiveness of the proposed technique in a variety of settings thanks to the wide range of sizes and materials that are shown in these images (Mou et al. 2023).

To conduct covert digital photo investigations, information gathering is very necessary. Raw image1.jpeg, raw image2.jpeg, raw image3.jpeg, and raw image4.jpeg were the four colour pictures that were used throughout the course of the experiment. It is necessaryto have these visualisations, which range in size and substance, to evaluate the approach that is proposed in a variety of different scenarios. The purpose of this study is to investigate the compatibility of camellia encryption with certain distinct picture formats. An extensive collection of images makes it possible to conduct a comprehensive analysis of the camellia algorithm's adaptability and effectiveness in encrypting data across a variety of picture attributes. The actual implementation of the algorithm is significantly impacted because of this realisation.

For enhancing the comprehensiveness of the analysis, various image qualityparameters are utilised. These parameters include “Mean Squared Error” or (MSE), “Structural Similarity Index Measure” or (SSIM), “Peak Signal-to-noise Ratio” or (PSNR), “Root Mean Square Error” or (RMSE), “Entropy Difference”, “Normalised Cross Correlation” or (NC), “Average Differences” or (AD), and “Maximum Difference” or (MD). While conducting an evaluation of the steganographic procedure's reliability and integrity, it is necessary to take into consideration a number of different criteria.

3.2 Encryption and Steganography

A key component of the strategy is the combination of steganographic methods and Camellia encryption. Using encryption inside the embedding function ensures the protection of the secret key, which is a crucial step in the encryption process. Users must enter the coordinates of four steganographic pictures to decode the data (Sabeti et al., 2022). The last stage in the procedure is to use the decode () function once the Camellia algorithm has decrypted the encrypted data.

It is necessary to compare decrypted data with encrypted passwords to ensure the confidentiality of the data. At this point, the encrypted data is checked to ensure that it is accurate and comprehensive. The Camellia technique is required to decode the data and convert it to Base64 so that we get the plaintext. In this intricate process, it is necessary totake into consideration the integrity of the data, efficiency, and safety. Camellia is the methodthat the system employs to encrypt and decode data, which ensures that the data is safe. In addition to ensuring the confidentiality of the content, this expedites the processing and retrieval of data. The use of this method demonstrates how advances in encryption and data management have the potential to enhance digital security.

3.3 Evaluation Metrics

To evaluate the efficacy and efficiency of the proposed methodology, it is critical to collect a variety of image quality-related metrics. Applying the Mean Squared Error (MSE) metric, which calculates the average squared discrepancy between the original cover image and the steganographic image, could prove to be quite beneficial. To conduct a thorough evaluation of image quality, the Structural Similarity Index Measure (SSIM) quantifies the alterations in structural information.

3.3.1 Mean Squared Error: The Mean Squared Error (MSE) serves as a metric for assessing the accuracy of an estimator. It is consistently non-negative, with values approaching zero indicating higher quality or accuracy.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

Where, m and n are width and height of image.

3.3.2 Structural Similarity Index Measure: The SSIM method is clearly more involved than the MSE method, but the essence is that SSIM attempts to replace the perceived alteration in the structural information of the image, whereas MSE is estimating the perceived errors.
The SSIM value can vary between -1 and 1, where 1 indicates perfect similarity.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu^2 - y + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}$$

Where μ_x, μ_y, σ_x, σ_y and σ_{xy} are the local means, standard deviations, and cross covariance for images x, y. $C_1 = (k_1L)^2$ and $C_2 = (k_2L)^2$. L is the dynamic range of the pixel-values $k_1 = 0.01$ and $k_2 = 0.03$ and by default.

3.3.3 Peak Signal to noise ratio: It is the ratio between the maximum possible power of an image and the power of corrupting noise that affects the quality of image. The larger the value of PSNR, the more efficient is a corresponding compression method.

$$PSNR = 10\ log_{10}(\frac{(L-1)^2}{MSE}) = 20\ log_{10}(\frac{L-1}{RMSE})$$

L is the number of maximum possible intensity levels (minimum intensity level supposed to be 0) in an image.

3.3.4 Root Mean Square Error: It is the error rate by the square root of MSE. The root-mean-square error (RMSE) is a frequently used measure of the differences between values (sample or population values) predicted by a model, or an estimator and the values observed.

$$RMSE = \sqrt{MSE}$$

3.3.5 Average Difference: It is simply the average difference between the raw image (x (i, j)) and stego image (y(i, j)).

$$AD = \frac{1}{MN}\sum_{i=1}^{M}\sum_{J=1}^{N}(x(i,j) = y(i,j))$$

3.3.6 Maximum difference: It is the maximum of the error signal (difference between the raw image and stego image).

$$MD = MAX|x(i,j) - y(i,j)|$$

Quantitatively assessing the efficacy of image compression, the PSNR (Peak Signal-to-Noise Ratio) is another name for the PSNR (Kunhoth et al. 2022).The measure assesses the ratio of excessive background noise to the strongest signal, serving as an indicator of compression effectiveness. For comparing predicted and actual values, the Root Mean Square Error (RMSE) proves useful, while the entropy difference quantifies the information quantity in an image. The evaluation matrix initially lacked variables like nominal cross-correlation (NC), maximum difference (MD), and average difference (AD). Through incremental enhancements, a comprehensive assessment of the proposed methodology's effectiveness in concealing and retrieving data becomes possible. Experimental methodologies consist of three distinct stages: encoding, decoding, and evaluation. Python provides the necessary infrastructure for executing algorithms in encoding and decoding processes. The stringent objective is to ensure the seamless integration of steganography and encryption methodologies. (Wang et al. 2022).

To evaluate how the size of a message influences both the security and quality of steganographic images, we conduct entropy calculations, create matrices for grading image quality, and analyze histograms. By utilizing the normalized cross-correlation method, we can determine the reliability of steganographic images in comparison to unaltered photographs.

4 Design Specification

The design specification outlines a suggested approach to enhance the security of online communication by combining steganography with encryption. It also offers a detailed strategy to accomplish this objective. The newly developed system is built upon the crucial tactics, processes, and concepts that have been covered here. Complete explanations have been provided for each component of the design to ensure that one has a thorough understanding of the system's architecture. Examples of techniques falling under this category include digital image encryption and the encapsulation of confidential keys.

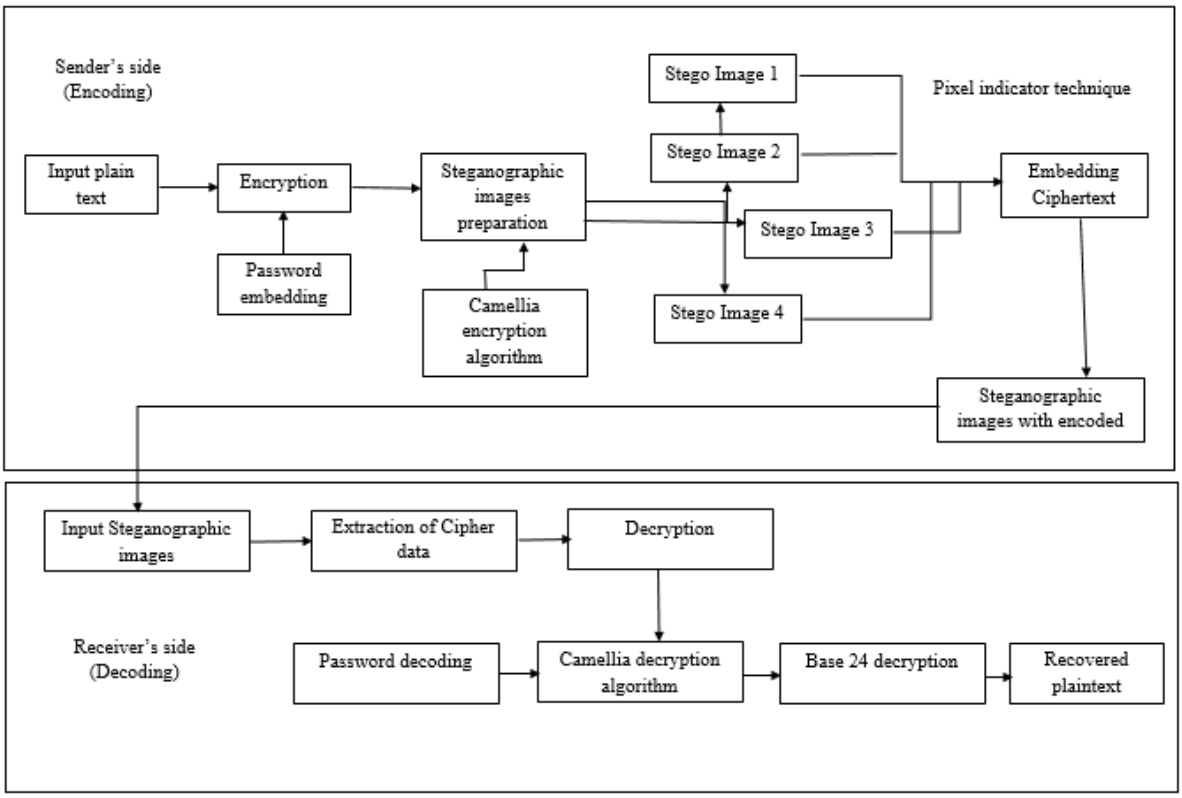

Figure 2: Design process

Integrating steganography and encryption into the system ensures a secure and dependable method of communication. The methodology relies on an enhanced version of the widely adopted and highly efficient Camellia encryption algorithm. Utilizing Pixel Indicator technology facilitates the integration of encrypted data into digital photographs. The system's well-defined components contribute to its effective operation, encompassing various operations such as key encryption, retrieval of steganographic images, Camellia decryption, and data decoding. These modules streamline the intricate process of decoding steganographic and encrypted data, providing a robust assurance of data security.

4.1 Key Components

To ensure system security, the Camellia encryption technology must be incorporated. A symmetric key block cipher with variable length keys, Camellia adds more intricacy to an already difficult encryption process. By using the password embed() method, the important

private key may be encrypted. The steganographic technique is secure because of this way of applying the secret key (Liu et al. 2022).

The relationship between steganographic and encryption techniques is shown by the Pixel Indicator technique. The gadget gathers nine RGB data by scanning three pixels at once during operation. In its 8-bit binary version, a single character is preserved by allocating the first eight RGB values.

4.2 Encoding Process

The utilization of the password embed() function plays a vital role in decrypting the secret key, an essential component across various encryption methods. The primary objective of this function is to simplify the integration of the key into the steganographic process. The encoded key holds significant importance in establishing the encryption framework for secure communications.

Users are mandated to provide four steganographic images, serving as platforms for data encryption. To conduct a thorough assessment of the system's capabilities, it is critical to employ the steganographic photo retrieval method. This approach ensures the incorporation of diverse settings and image compositions.

Before decoding the encoded text, it becomes imperative to extract the cipher data from each of the four steganographic images (Sahu and Gutub, 2022). The Camellia encryption algorithm generates ciphertext that encapsulates concealed data. Prompt initiation of the decryption procedure holds paramount importance.

4.3 Decoding Process

It is necessary to use the Camellia technique to decode the encrypted text that was received from the Stego photographs. When it comes to decoding data, it is of the highest necessity to make certain that the encryption secret key is safely stored. Utilising the decryptionprocedure is done with the intention of recovering the text that was encrypted in the first place.A specialist decode() approach is required to decrypt the encrypted data, which is the next stage in the process. Performing a detailed comparison between the decrypted data and the encoded password is one of the functions that this function does to protect the confidentiality of the encrypted data. In the subsequent step, the Base64 technique will be usedto decode the final plaintext.

5 Implementation

During implementation, the proposed secure communication system becomes a working system. This section details how the design specification's proposals will be implemented to provide a reliable and effective system. In addition to Camellia encryption and Pixel Indicator, this subject will provide the systematic encoding and decoding of data. Additionally, the presentation will focus on the integration of these two approaches. Using an all-encompassing coding system, the approach that is being discussed integrates steganography and encryption in a harmonious manner. Even under the most trying of situations, complete anonymity would be guaranteed via the use of digital communication.

5.1 Code Overview

The process of key encoding is an essential stage in the installation procedure that improves the security measures of the system. Encryption is used by the password embed() function to keep the private key safe and ensure that it accomplishes its intended purpose. It will be important to have this key to encrypt and decrypt data in the future. As a result of this property, the steganographic technique has the potential to include the key without any friction. One of the most important components of the encryption technique knownas Camellia, which is used for the purpose of ensuring the confidentiality of private communication, is the secret, which is now protected by cryptography.

The user must follow four specified steps to acquire steganographic photographs. With the enormous collection of steganographic photos, a huge number of picture combinations are examined to test the system's effectiveness in various scenarios. First, read the steganographic pictures' hidden information and then combine it with relevant information to create the encoded text. The decryption key lies within the encrypted text, so sensitive data may be recovered. Encrypting the confidential key is a prerequisite for deciphering the encrypted data. To maintain the confidentiality of the encrypted data, this function meticulously validates the decoded data with the encoded password. Following that, the Base64 algorithm will be employed to decrypt the ultimate plaintext.

5.2 Pixel Indicator Technique

The Pixel Indicator Technique is a major steganographic approach that allows the information to be encoded into digital photos in a way that is not visible to the naked eye. The purpose of this approach is to conceal information while maintaining the integrity of the visual presentation. The encoding and decoding methods for this are conducted with the pixel values serving as indicators and functions. Intelligent data decryption and encoding may be accomplished via the use of a technique known as the Pixel Indicator Technique. This technique is based on the RGB pixel values of an image. Covert activities are efficiently maintained by the approach, which employs a meticulous methodology that places a focus on precision and subtlety within its operations. The following is a list of the major components that make up this approach:

Before beginning the process of encryption, the algorithm must first convert each character into the ASCII value that corresponds to that character. To go on with the process of secret encoding, the next step comprises turning this ASCII data into a binary format that is 8 bits in length.

It is necessary to concurrently scan three pixels to get all nine RGB values. It is possible to represent a single character in binary by utilising just the first eight values of the RGB values. To ensure that every binary digit is given an exact numerical value, the RGB colour space makes use of a complex algorithm. The transformation of every binary digit that is not a '1' into an even integer is a key step in the process of obtaining an evenRGB value. Through the intentional manipulation of binary data with RGB values, it is possibleto accomplish a change that is not only subtle but also apparent. Two distinct functions are served by the numerical number 19, which is included inside the RGB colour space. To decide whether pixels are accepted for further encoding or decoding procedures, the signal is taken into consideration. Even when the value of the ninth bit is even, it is essential to do an

additional pixel reading to process more data. If the value is anomalous, there is no need to verify more pixels. This is an indication that the process of encoding or decoding has been finished.

This procedure is used methodically to each letter until the image is encoded in the fourth phase of sequential comprehensive encoding. The sequential procedure ensures a deliberate and logical approach, protecting data integrity and enabling exact recovery during decoding. The Pixel Indicator Technique ensures great decoding accuracy by extracting plenty of visual data. For extracting binary data from the RGB values that correspond to three pixels, it is feasible to do a careful examination of all three pixels concurrently.

Because of the Pixel Indicator Technique's high level of sophistication and precision, it is very difficult for unauthorised individuals to access confidential information. This technique is consistent with the basic goal of steganography, which is to conceal data while maintaining the integrity of the media the data is being concealed on.

5.3 Systematic Encoding and Decoding Processes

These activities are conducted via the embed() and decode() methods, which are responsible for their execution overall. Encoding and decoding data carefully and precisely is the most crucial component of implementation. Password embed() encodes the private key, a crucial part of secure encryption. The decode() function compares the encrypted password and decoded data during the decoding procedure. In conclusion, Base64 decoding proves our method successfully detects text.

5.4 Tools and Libraries used

Programming language: Python is used in this project due to its readability, extensive libraries like PyCrypto and cryptography, cross-platform compatibility, rapid prototyping abilities, and strong community support. Its simplicity aids in implementing complex algorithms, while its portability ensures consistent functionality across diverse environments.

Crypto: This library refers to various cryptographic libraries available in Python, such as PyCrypto or cryptography. These libraries offer implementations of various cryptographic algorithms like encryption, decryption, hashing, digital signatures, etc., which are fundamental in cryptographic projects for securing data.

PIL (Python Imaging Library): It is used for image processing tasks in Python. In this project, it is used along with steganography (hiding messages within images), watermarking, or visual cryptography, where cryptographic techniques are applied to images.

Cryptography.fernet: This module is part of the cryptography library in Python, providing a high-level symmetric encryption using the Fernet symmetric authenticated cryptography mechanism.

Hashlib: This module in Python provides functions for hashing data using various hash algorithms, such as MD5, SHA-1, SHA-256, etc. Hash functions take an input and produce a fixed-size string of bytes, which is unique to that input.

6 Evaluation

A comprehensive series of experiments and case studies were used to evaluate the efficiency and dependability of the Pixel Indicator Technique; its use in picture steganography was suggested. The purpose of these studies was to investigate Histogram analysis, picture quality, and the efficiency with which encryption and decryption systems functioned. Through these experiments, the Camellia algorithm, which is a fundamental component of encryption, was the primary emphasis. With the purpose of highlighting the possible applications of the Pixel Indicator method in secure image-based communication and data security, this research investigates the method, findings, and consequences of the system.

6.1 Case Study 1: Image Quality Metrics Analysis

The aim of this project is to check numerous picture quality characteristics to evaluate whether the Pixel Indicator Technique (PIT) can conceal data in photographs. The criteria provide a comprehensive evaluation of the steganographic image's source image fidelity (Dahlhauser *et al*. 2022). As shown in table 1, the study incorporates many measures, including Mean Squared Error (MSE), Root Mean Square Error (RMSE), Peak Signal-to-Noise Ratio (PSNR), Entropy Difference, Normalised Cross Correlation (NC), Average Differences (AD), and Maximum Difference (MD).

Table 1: Evaluation of PIT

Message Size	MSE	SSIM	PSNR	RMSE	Entropy Difference	NC	AD	MD
1000	0.0142	0.9999	66.597	0.119	0.0065	1	0.004	1
5000	0.0781	0.999	59.2	0.279	0.0312	1	0.026	1
10000	0.163	0.999	56	0.403	0.0545	1	0.054	1

The consistent and minimal MSE findings for all message sizes suggest that raw and steganographic photos are comparable. Lower MSEs indicate accuracy. SSIM indicates that unprocessed and steganographic images are structurally comparable, with a constant value of 1.0.

- PSNR assesses visual quality. A PSNR above 50 dB indicates high picture quality. PSNR improves visual accuracy.
- RMSE investigations show that steganographic and raw pictures have equal error rates, demonstrating the approach works.
- Steganographic photographs maintained the original images' information entropy with regular entropy maintenance.
- Normalised Cross-connection (NC) scores around 1.0 substantially link steganographic and raw image pixel values. Both forms seem similar.
- Steganography's sensitivity reduces average differences (AD).
- Maximum difference (MD) between steganographic and raw photos is 1.00, proving the approach can conceal information without compromising vision.
- Using precise modifications and highly correlated metrics, the Pixel Indicator Technique efficiently and seamlessly assimilates data while maintaining image integrity. The findings are relevant to real situations where communication secrecy and visual aesthetics are important.

6.2 Case Study: Visual Inspection

Visual examination of steganographic systems is necessary to understand how they hide visual information and affect perception. Researchers do a visual audit using the Pixel Indicator Technique before certifying picture data embedding. This research evaluates the technology's ability to preserve picture quality (Setiadi, 2022).

Understanding perceptual effect and visual information concealing requires studying steganographic methods like the Pixel Indicator Technique. Before trusting picture data, visual assessments are essential. The Camellia algorithm improves picture quality. This evaluates how effectively the method conceals data without compromising image quality.

Visual analysis involves comparing genuine pictures to Pixel Indicator Technique-generated steganographic images. Experts examine photographs to find any hidden changes, anomalies, or artefacts. The Pixel Indicator Technique provides steganographic visual analysis of images. Comparisons are made between baseline and steganographic pictures. Each level of encryption, especially Camellia, is checked for concealed changes, inconsistencies, and artefacts. This method obstructs image data without visible signs to preserve data while keeping image quality.

6.2.1 Observations

Photos that are almost identical to their originals Pixel Indicator Technique steganographic images show commonalities upon initial investigation. Examining steganographic photographs separately makes it difficult to see changes. This article shows how the method hides features while keeping shot quality, its main selling point.

Colour consistency and brightness differentiation Steganographic images have the same contrast and colour space as raw ones. This consistency is essential to prevent suspicious changes throughout the steganographic process. Steganographic photos have exceptional expertise in preserving textures, patterns, and subtleties. When visual material is compromised, data preservation is essential.

Pixel-Indicator Technology Steganographic pictures have no pixelation, distortions, or anomalies even being magnified several times. Every steganographic snapshot is flawless. The main goal of steganography is to mask information, and simple integration supports this. Camellia encrypts the data before uploading it, adding security to this process. This provides greater assurance that the process will not deviate significantly. This improves image quality and smooths out colors and gradients. This service is necessary to protect sensitive data from unauthorized changes.

Even with different magnifications, steganographic images do not have pixelation, distortion, or inconsistencies that can indicate hidden information. There is nothing extra in this situation. Steganography hides data by making it incomprehensible. The original is the one that retains steganography that changes the color or gradient all have amazing image quality. Unexpected changes or inconsistencies can corrupt the implanted data.

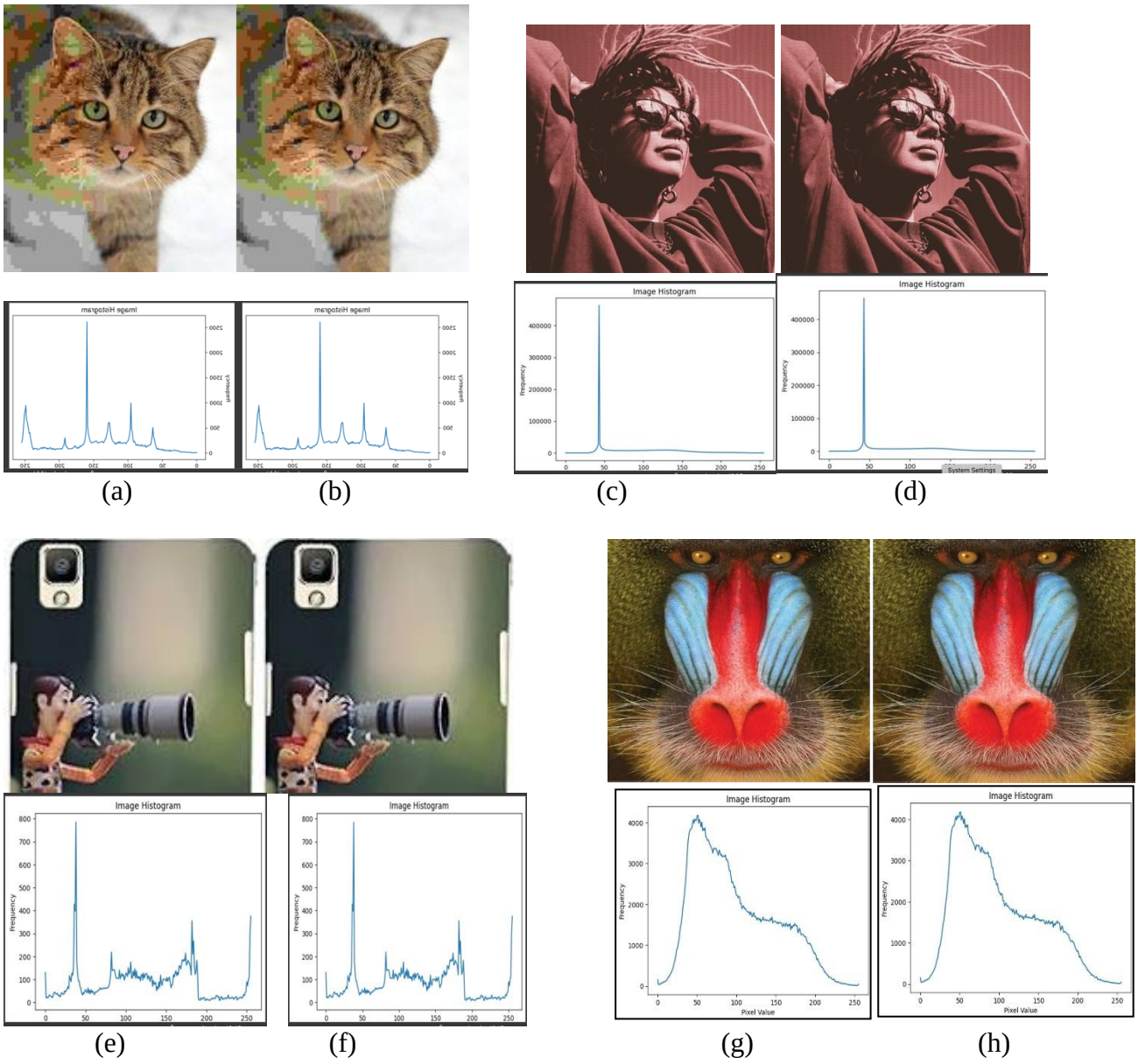

Figure 3: Visual inspection

Even at varying magnifications, steganographic photographs do not include pixelation, distortions, or inconsistencies that may suggest concealed information. This situation has no exceptions. Steganography conceals data by making it unintelligible. Both the original and the one keeping the steganography while changing colours or gradients have amazing image quality. Unexpected modifications or inconsistencies may compromise implanted data.

Examining Pixel Indicator Technique steganographic photos is a great way to evaluate photo hidden information. This method merges hidden data with visible sections without altering them. The Pixel Indicator Technique may modify visual material via steganography, according to the eye test case study. This method prioritizes visual integrity and artefact prevention, making it ideal for securely hiding visual data. Both traits are crucial. The Pixel Indicator Technique's potential may be further assessed via statistical analysis and actual implementations.

6.3 Case Study: Histogram Analysis

Steganographic methods must be tested using histogram analysis, which shows pixel intensities in photographs. This study examines how the Pixel Indicator Technique embedding method affects image statistics and the process by which the Pixel Indicator Technique generates histograms for both the original and steganographic pictures. Histograms are used to visually represent the distribution of pixel intensity to provide a thorough examination of the changes made by the steganographic method.

6.3.1 Observations

A surprising link occurs between the raw and steganographic pixel intensity distributions. The histograms are consistent at extreme levels. The overlapping peaks of the colour channels show that the steganographic process did not affect picture intensity.

The RGB histograms of steganographic images show that data may be included while keeping colour patterns (Peter et al. 2022). These photos need continual care to look good. Steganographic image histograms show no outliers or abnormalities that suggest concealed information. This eliminated oddities. Seamless, unbroken curves that match the intended criteria reveal an undiscovered steganographic method.

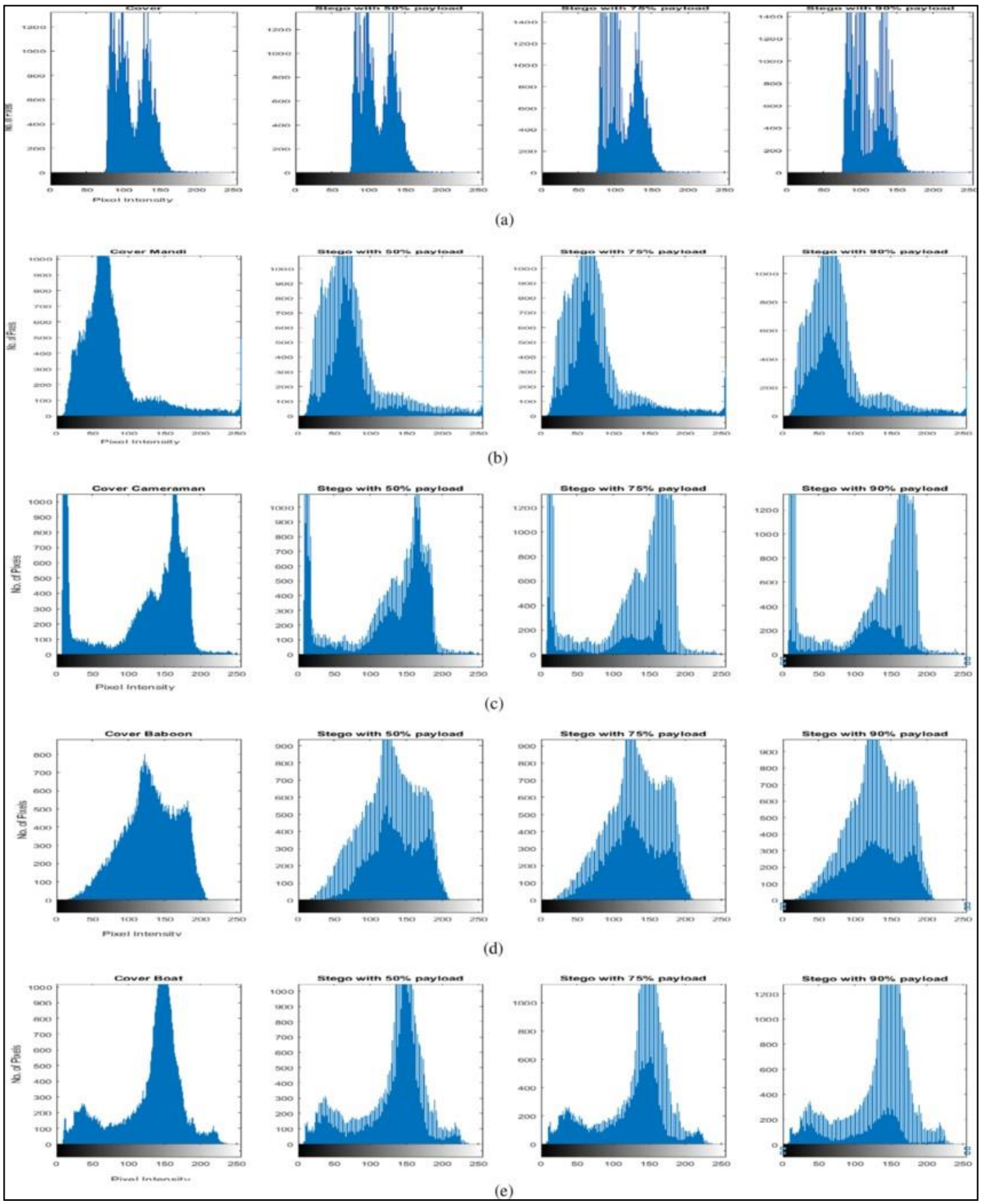

Figure 4: Histogram analysis (Hossain *et al*. 2022)

The case study shows that the Pixel Indicator Technique retains picture statistical properties, concealing sensitive data owing to its clandestine and invisible nature. The technique's efficacy can be better assessed by adding variables.

6.4 Discussion

From the extensive experiments and case studies conducted on the Pixel Indicator Technique (PIT) for steganography, several key findings emerge, shedding light on its effectiveness in concealing data within images while maintaining their integrity.

The first set of experiments involved evaluating various picture quality characteristics such as MSE, SSIM, PSNR, RMSE, Entropy Difference, NC, AD, and MD across different message sizes. The consistent and minimal MSE values suggest a remarkable similarity between raw and steganographic photos, signifying a high level of accuracy in the PIT method. Additionally, SSIM values consistently at 1.0 indicate structural similarity between the original and steganographic images, reinforcing the notion that the hidden data does not significantly alter the visual structure.

PSNR values above 50 dB across different message sizes indicate high picture quality, affirming that the PIT effectively maintains visual accuracy. Similarly, the RMSE results showing equal error rates between steganographic, and raw images reinforce the method's efficiency. Entropy maintenance and NC scores around 1.0 further support the similarity between steganographic and original pixel values.

The visual inspection case study delves deeper into the perceptual impact of PIT-generated steganographic images. Notably, experts found it challenging to discern changes between the baseline and steganographic images, emphasizing the method's ability to conceal alterations effectively. Consistency in color, contrast, and texture preservation between steganographic and raw images indicates the PIT's proficiency in maintaining visual quality while hiding data.

However, despite these positive outcomes, certain limitations and areas for improvement exist. One critical aspect is the need for a more diverse dataset to evaluate the PIT across various image types, sizes, and complexities. This would enhance the generalizability of the findings and provide a more comprehensive understanding of its performance. The experiments and case studies yield promising results regarding PIT's ability to conceal data without compromising image quality, incorporating a more diverse dataset, subjective evaluations, and robustness testing against potential attacks would strengthen its applicability and reliability in practical settings.

7 Conclusion and Future Work

The Pixel Indicator Technique, which combines pixel value hiding with encryption, conceals visual data robustly. This research examined every aspect of this technology to protect data and enable secure communication. This analysis examines the study's results and suggests further research and development.

Imperceptible conventional and Pixel Indicator Technique steganographic pictures are hard to distinguish. This basic trait keeps hidden information from view. picture quality indicators like PSNR, SSIM, and MSE are used in the Pixel Indicator Technique to preserve picture statistical integrity. Steganography works with little picture changes and stable pixel.

Images of histograms show that the Pixel Indicator Technique is undetectable. This is because the original and steganographic photos have similar pixel intensities. The histograms show no abnormalities, indicating that the technique integrates the data. Considering computing speed, the suggested steganographic approach seems efficient. When properly implemented, encryption and embedding protocols allow sensitive data to be seamlessly integrated into a system.

Future Work

Additional study is needed to explore the Pixel Indicator Technique's non-visual applications. To understand its effectiveness and flexibility, this technology must be examined in audio, video, and network protocols. Modern encryption techniques may strengthen steganography and secure secret data. An exhaustive analysis of a large collection of various images would reveal the strategy's usefulness in different circumstances. Using advanced steganalysis to determine its efficacy is crucial. Test the Pixel Indicator Technique in real-world applications like secure photo sharing and private data storage to determine its applicability. For this, trials in real-world situations must account for noise, compression, and other factors.

Visual steganography using the Pixel Indicator Technique appears promising. The efficacy, statistical reliability, and concealed nature of data suppression should be assessed. Technology is always changing, therefore, to ensure communication and data security, methods must be reviewed and adjusted.

References

Adee, R. and Mouratidis, H., 2022. A dynamic four-step data security model for data in cloud computing based on cryptography and steganography. Sensors, 22(3), p.1109.

Dahlhauser, S.D., Wight, C.D., Moor, S.R., Scanga, R.A., Ngo, P., York, J.T., Vera, M.S., Blake, K.J., Riddington, I.M., Reuther, J.F. and Anslyn, E.V., 2022. Molecular Encryption and Steganography Using Mixtures of
Simultaneously Sequenced, Sequence-Defined Oligourethanes. ACS Central Science, 8(8), pp.1125-1133.

Hossain, S., Mukhopadhyay, S., Ray, B., Ghosal, S.K. and Sarkar, R., 2022. A secured image steganography method based on ballot transform and genetic algorithm. Multimedia Tools and Applications, 81(27), pp.38429-38458.

Kaur, S., Singh, S., Kaur, M., and Lee, H.N., 2022. A systematic review of computational imagesteganography approaches. Archives of Computational Methods in Engineering, 29(7), pp.4775-4797.

Kunhoth, J., Subramanian, N., Al-Maadeed, S. and Bouridane, A., 2023. Video steganography: recent advances and challenges. Multimedia Tools and Applications, pp.1-43.

Liu, X., Ma, Z., Ma, J., Zhang, J., Schaefer, G. and Fang, H., 2022. Image disentanglement autoencoder for steganography without embedding. In Proceedings of the IEEE/CVF conference on computer vision and pattern recognition (pp. 2303-2312).

Mandal, P.C., Mukherjee, I., Paul, G., and Chatterji, B.N., 2022. Digital image steganography:A literature survey. Information sciences.

Mou, C., Xu, Y., Song, J., Zhao, C., Ghanem, B. and Zhang, J., 2023. Large-capacity and flexible video steganography via invertible neural network. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 22606-22615).

Muralidharan, T., Cohen, A., Cohen, A. and Nissim, N., 2022. The infinite race between steganography and steganalysis in images. Signal Processing, p.108711.

Peter, G., Sherine, A., Teekaraman, Y., Kuppusamy, R. and Radhakrishnan, A., 2022. Histogram shifting-based quick response steganography method for secure communication. Wireless Communications and Mobile Computing, 2022.

Rathore, M.S., Poongodi, M., Saurabh, P., Lilhore, U.K., Bourouis, S., Alhakami, W., Osamor, J. and Hamdi, M., 2022. A novel trust-based security and privacy model for internet of vehicles using encryption and steganography. Computers and Electrical Engineering, 102, p.108205.

Rustad, S., Andono, P.N. and Shidik, G.F., 2022. Digital image steganography survey and investigation (goal, assessment, method, development, and dataset). Signal Processing, p.108908.

Sabeti, V., Sobhani, M. and Hasheminejad, S.M.H., 2022. An adaptive image steganography method based on integer wavelet transform using genetic algorithm. Computers and Electrical Engineering, 99, p.107809.

Sahu, A.K. and Gutub, A., 2022. Improving grayscale steganography to protect personal information disclosure within hotel services. Multimedia Tools and Applications, 81(21), pp.30663-30683.

Setiadi, D.R.I.M., 2022. Improved payload capacity in LSB image steganography uses dilated hybrid edge detection.

Valandar, M.Y., Ayubi, P., Barani, M.J. and Irani, B.Y., 2022. A chaotic video steganography technique for carrying different types of secret messages. Journal of Information Security and Applications, 66, p.103160.

Wang, Z., Feng, G., Qian, Z. and Zhang, X., 2022. JPEG steganography with content similarity evaluation. IEEE Transactions on Cybernetics.

Wei, P., Li, S., Zhang, X., Luo, G., Qian, Z. and Zhou, Q., 2022, October. Generative steganography network. In Proceedings of the 30th ACM International Conference on Multimedia (pp. 1621-1629).

Xu, Y., Mou, C., Hu, Y., Xie, J. and Zhang, J., 2022. Robust invertible image steganography. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 7875-7884).

Zhou, Z., Su, Y., Li, J., Yu, K., Wu, Q.J., Fu, Z. and Shi, Y., 2022. Secret-to-image reversible transformation for generative steganography. IEEE Transactions on Dependable and Secure Computing.