B. TECH. PROJECT ON

Data Hiding using Efficient Steganography Techniques

Submitted By:

Khushi Sahay - 2020UEC2510

Aryan Gupta - 2020UEC2513

Sonu Sharma - 2020UEC2541

Ansh Makkar - 2020UEC2545

Under the Guidance of

(Prof. D.K. Upadhyay)

Project-I in partial fulfillment of requirement for the award of

B.Tech. in

Electronics & Communication Engineering

Department of Electronics & Communication Engineering

NETAJI SUBHAS UNIVERSITY OF TECHNOLOGY

NEW DELHI-110078

CERTIFICATE OF DECLARATION

Division of Electronics and Communication
Netaji Subhas University of Technology
New Delhi-110078, India

Certified that Khushi Sahay(2020UEC2510), Aryan Gupta(2020UEC2513), Sonu Sharma(2020UEC2541), Ansh Makkar(2020UEC2545) has carried out their project work presented in this project entitled "Data Hiding using Efficient Steganography Techniques" for the award of Bachelor of Technology, Department of Electronics and Communication, Netaji Subhas University of Technology, New Delhi, under my supervision. The project embodies results of original work, and studies are carried out by the students themselves and the contents of the project do not form the basis for the award of any other degree to the candidate or to anybody else from this or any other University/Institution.

Place: New Delhi — Prof. D. K. Upadhyay

Date:09/12/2023 — SUPERVISOR

ACKNOWLEDGMENT

We would like to express my sincere gratitude and appreciation to all those who have contributed to the successful completion of this project.

We extend my heartfelt thanks to our project supervisor, Prof. D. K. Upadhyay, for his invaluable guidance, encouragement, and expertise throughout the project. His constructive feedback and insightful suggestions were instrumental in shaping the direction of our work.

We also sincerely thank our colleagues for the time spent proofreading and correcting our mistakes, without their collective effort and support this project would not have been possible.

Khushi Sahay - 2020UEC2510

Aryan Gupta - 2020UEC2513

Sonu Sharma - 2020UEC2541

Ansh Makkar - 2020UEC2545

PLAGIARISM REPORT

Plagiarism_Report

ORIGINALITY REPORT

15%	8%	10%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	pdfs.semanticscholar.org Internet Source	2%
2	Shahid Rahman, Jamal Uddin, Habib Ullah Khan, Hameed Hussain, Ayaz Ali Khan, Muhammad Zakarya. "A Novel Steganography Technique for Digital Images using the Least Significant Bit Substitution Method", IEEE Access, 2022 Publication	2%
3	Shahid Rahman, Jamal Uddin, Habib Ullah Khan, Hameed Hussain, Ayaz Ali Khan, Muhammad Zakarya. "A Novel Steganography Technique for Digital Images Using the Least Significant Bit Substitution Method", IEEE Access, 2022 Publication	1%
4	Submitted to University of East Anglia Student Paper	1%
5	www.researchgate.net Internet Source	1%

ABSTRACT

Ensuring data security is paramount in today's interconnected world where sensitive information is constantly transmitted. As cyber threats evolve, the significance of safeguarding data against unauthorized access and interception becomes increasingly crucial.

Image steganography, a method of concealing information within digital images, serves as a vital tool for data security. Widely used methods involve embedding data in the least significant bits of pixel values or exploiting the frequency domain. Despite advancements, challenges persist, including the need for enhanced detection techniques and resistance to sophisticated attacks.

Looking ahead, the fusion of cryptography and steganography holds promise for creating a more resilient approach to data transmission. The integration of cryptographic principles with steganographic methods can fortify the security landscape, offering a sophisticated defense against potential threats in the realm of data communication.

LIST OF CONTENTS

LIST OF FIGURES

CHAPTER 1 - INTRODUCTION

In the contemporary landscape, technological advancements have led to a predominant reliance on the internet for global data transfer. While the internet offers various means such as emails and chats for swift and accurate data transmission, the looming security threat remains a significant concern. The vulnerability of personal or confidential data to theft or hacking necessitates a paramount focus on data security during the transfer process.

Data security involves safeguarding information from unauthorized access or manipulation, a critical consideration given the escalating rate of data transfer over the internet. To enhance security in online data transfers, several techniques have been developed, including Cryptography, Steganography, and digital watermarking. Cryptography encrypts information into ciphertexts and transmits it to the intended recipient using an undisclosed key. Steganography goes further by concealing ciphertext within seemingly inconspicuous images or other formats.

Cryptography and steganography are widely recognized techniques employed to manipulate information, offering applications in computer science and related fields. Steganography involves communicating in a manner that conceals the existence of communication, embedding hidden content in ordinary cover media to avoid detection. For instance, text can be concealed within an image or audio file. Cryptography, on the other hand, entails mathematical techniques for information security, ensuring confidentiality, data integrity, entity authentication, and data origin authentication. By transforming information into an unreadable format, cryptography achieves confidential transmission over a public network.

Cryptography systems can be categorized into two main types: symmetric-key systems, where a common key is shared between the sender and receiver, and public-key systems, which involve a public key accessible to everyone and a private key exclusive to the recipient of the message. Both techniques play crucial roles in protecting sensitive information in various contexts, such as safeguarding email messages, credit card data, and corporate information.

1.1 DATA SECURITY

In the contemporary digital era, the increasing reliance on electronic communication and data transmission has accentuated the critical need for robust data security measures. As the volume and significance of digital information grow exponentially, so do the threats posed by unauthorized access, manipulation, and interception. In response to these challenges, data security has emerged as a pivotal domain of study and innovation.

Figure - 1 Data Security

The protection of sensitive information from unauthorized access, disclosure, alteration, or destruction involves a diverse range of techniques and practices within the realm of data security. This imperative becomes even more pronounced in sectors where the confidentiality, integrity, and availability of data are paramount, such as finance, healthcare, defense, and personal communications.

Two of the most sophisticated and impactful branches within the realm of data security are steganography and cryptography. These disciplines address distinct aspects of secure communication but often complement each other to create a comprehensive defense against potential threats.

1.1.1 CRYPTOGRAPHY

Cryptography functions as a means to guarantee the security of information and communication through the utilization of codes, ensuring that only authorized recipients can understand and process the information, thus thwarting unauthorized access. The term "crypt" indicating "hidden" and "graphy" denoting "writing." In the domain of Cryptography, protective methods are derived from mathematical principles, employing algorithms, or rule-based calculations, to transform messages in a manner that adds complexity to the decoding process. These algorithms play roles in cryptographic key generation, digital signing, and verification procedures, securing data privacy, internet browsing, and confidential transactions such as credit card payments.

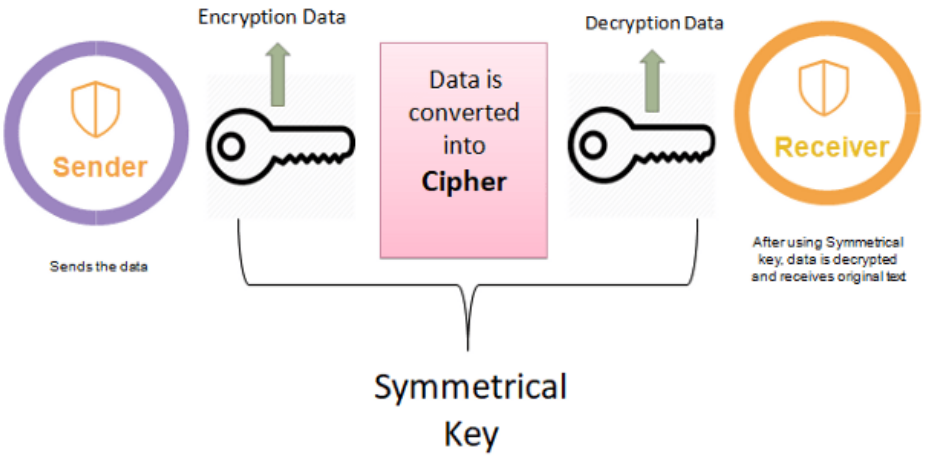

Figure - 2 Cryptography

In the contemporary computer era, cryptography is commonly linked with the conversion of ordinary plaintext into ciphertext through encryption, allowing only the designated recipient to decode it. The reversal of this process, turning ciphertext back into plaintext, is known as decryption.

Key Features of Cryptography include:

1. Confidentiality: Ensuring that information is exclusively accessible to its intended recipient, preventing unauthorized access.
2. Integrity: Guaranteeing that information remains unaltered during storage or transmission, with any modifications detected.

3. Non-repudiation: The originator/sender cannot later deny their intention to transmit information.
4. Authentication: Confirming the identities of both the sender and receiver, along with verifying the source or destination of the information.

Cryptography plays a pivotal role in maintaining the security and privacy of data, particularly in online transactions and communication.

1.1.2 CHALLENGES TO CRYPTOGRAPHY

Cryptography, the art of securing information through codes and algorithms, faces several challenges in the contemporary digital environment.

1. Quantum Computing Threat: The emergence of quantum computers poses a serious threat to traditional cryptographic systems. The computational capabilities they possess have the potential to compromise commonly employed encryption techniques, prompting the need for the creation of cryptography methods resistant to quantum.
2. Complex Key Management: Effectively managing cryptographic keys is a complex task. As systems grow in scale, ensuring the secure generation, distribution, storage, and revocation of keys becomes increasingly intricate.
3. Escalating Computational Power: With advancements in computing capabilities, attackers have more resources for brute-force attacks. Cryptographic algorithms must constantly evolve to withstand the increasing computational power available to malicious actors.
4. Side-Channel Attacks: Cryptographic systems are susceptible to side-channel attacks where attackers exploit information leaked during encryption or decryption. Protecting against these subtle channels requires additional measures to secure the entire process.
5. Post-Quantum Transition: The anticipation of quantum computers necessitates a transition to post-quantum cryptographic standards. Updating existing systems to withstand the quantum threat poses a considerable challenge.

1.1.3 STEGANOGRAPHY

Steganography is a technique that involves hiding information within other seemingly unrelated data or media to keep it confidential. Unlike encryption, which focuses on securing the content of a message, steganography is all about concealing the existence of the message itself.

The fundamental concept of steganography is to embed secret data in a way that remains undetectable to both human senses and standard analysis tools. This hidden information could be anything from text to images, and the goal is to make the presence of the concealed data inconspicuous. Steganography relies on the fact that humans typically overlook small changes in data, allowing for the covert inclusion of additional information without noticeable alterations.

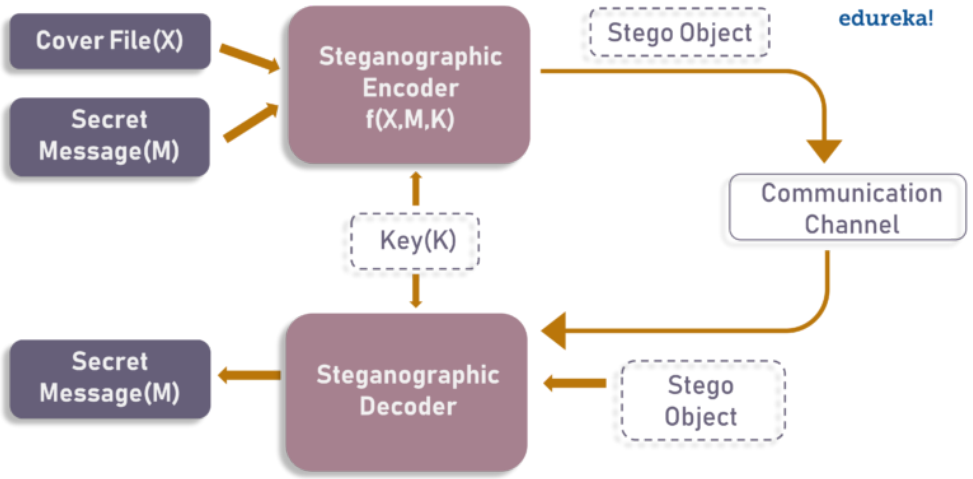

Figure - 3 Steganography

There are different techniques for steganography, each tailored to specific types of cover media. For instance, in image steganography, data may be hidden by subtly tweaking the least significant bits of pixel values. In audio steganography, information can be concealed within the frequency spectrum, while text steganography may involve embedding hidden messages through changes in formatting, spacing, or other non-essential elements.

Steganography finds applications in various areas, such as secure communication, copyright protection, and digital forensics to uncover hidden information. However, it also raises ethical concerns as it can be used for malicious purposes, including hiding malware or facilitating covert communication in cyber threats.

In essence, steganography is the art of discreet communication, enabling individuals to share information covertly by incorporating it into ordinary-looking content, thus introducing an extra layer of secrecy to the communication process.

1.1.4 ADVANTAGES OF STEGANOGRAPHY

Steganography offers several advantages in secure communication and information protection:

1. Discreet Communication: Steganography enables covert communication by concealing information within seemingly ordinary data. This discretion is valuable for confidential conversations or activities where maintaining secrecy is essential.
2. Enhanced Security: By hiding the existence of a message, steganography provides an extra layer of security beyond traditional encryption. This makes it more challenging for unauthorized parties to detect or intercept the concealed information.
3. Resistance to Detection: Steganographic techniques aim to make the embedded information difficult to detect by human senses or standard analysis tools. This resistance adds to the effectiveness of steganography in keeping hidden data confidential.
4. Versatility Across Media: Steganography can be applied to various types of media, including images, audio files, and text. This versatility allows for the integration of hidden information into different forms of communication, expanding its practical applications.
5. Copyright Protection: In digital media, steganography can be used to embed information that verifies ownership or copyright details. This aids in protecting intellectual property and serves as a form of digital watermarking.

6. Digital Forensics Applications: In a positive context, steganography is used in digital forensics to embed information for tracking and tracing purposes. This assists in identifying the source or origin of digital content.

1.2 TYPES OF STEGANOGRAPHY

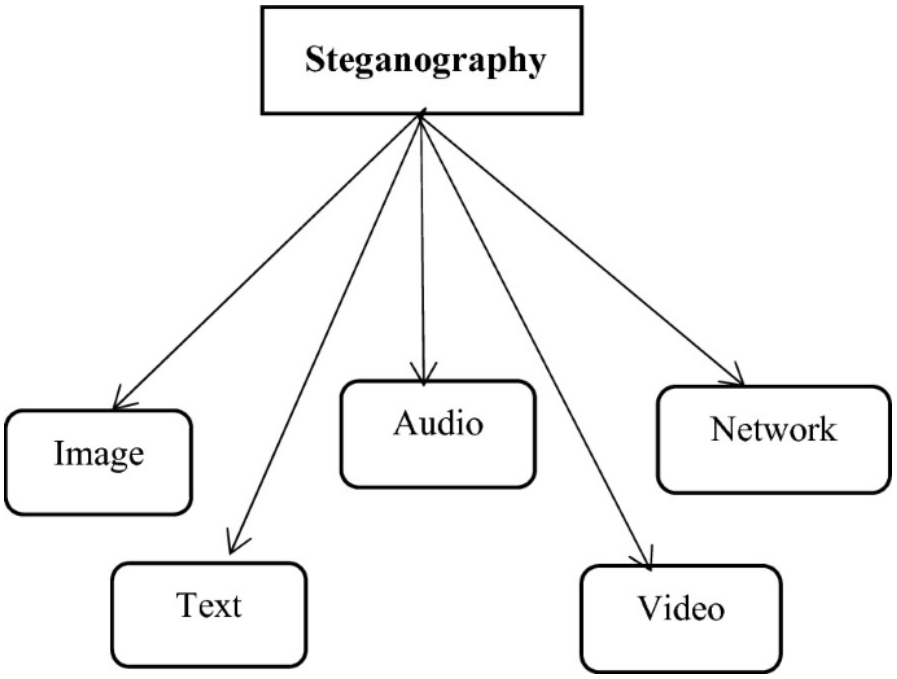

Figure - 4 Types of Steganography

Steganography encompasses various methods tailored for concealing information in different ways. In text steganography, data is hidden within written content through subtle modifications like altered spacing or invisible characters. Image steganography involves concealing information within digital images, achieved by manipulating pixel values or color patterns. Audio steganography discreetly embeds data within audio files, making imperceptible changes to the audio signal. Video steganography, akin to image steganography, conceals information within video files by subtly modifying frames or other elements. Network steganography focuses on hiding information within network protocols or traffic, employing techniques like altering packet headers or manipulating transmission timing. File steganography hides data within various file formats, utilizing methods such as embedding information in binary structures or modifying file metadata. These diverse types of steganography

provide covert communication options, each suited to different forms of content and communication channels.

1.2.1 TEXT STEGANOGRAPHY

Text steganography is a fascinating technique that involves hiding information within ordinary written text without altering the apparent meaning of the text itself. Unlike encrypting a message, where the focus is on transforming the content into a coded format, text steganography operates more subtly by making discreet modifications to the structure of the text. This can include adjusting the spacing between words, subtly changing the font size or style, or even incorporating invisible characters.

The essence of text steganography lies in embedding a secret message in a way that appears inconspicuous to someone who is casually reading the text. It's akin to a hidden conversation within the visible words. Those aware of the specific alterations or patterns can decipher the concealed information, while others, unaware of the hidden message, perceive only the apparent content.

This technique is often employed for covert communication, where the need for secrecy is paramount. By seamlessly integrating the hidden message into ordinary text, text steganography adds an extra layer of subtlety and complexity to written communication, making it a valuable tool in scenarios where discreet information exchange is essential.

1.2.2 IMAGE STEGANOGRAPHY

Image steganography is a fascinating method that involves concealing information within digital images without altering the visible aspects of the image itself. Unlike traditional encryption, which transforms the content into a coded format, image steganography focuses on subtly modifying the pixels of an image to embed hidden data. This can be done by manipulating the least significant bits of the pixel values, altering color patterns, or embedding data in specific regions of the image that are less likely to be noticed.

The core idea is to make the changes so subtle that they are imperceptible to the human eye. The resulting image appears visually identical to the original, yet it carries

an additional layer of information. This hidden data could be text, another image, or any form of information that the sender wishes to keep confidential.
Image steganography finds applications in scenarios where maintaining the secrecy of data is crucial. It allows for the covert transmission of information within the seemingly innocent guise of an image file. Those aware of the specific steganographic technique used can extract the hidden data, while others, without knowledge of the concealed information, perceive only the visible image.
This technique underscores the creative ways in which information can be safeguarded and transmitted, leveraging the visual medium of images to serve as carriers for concealed messages. Image steganography represents a sophisticated approach to secure communication, where the hidden message remains virtually undetectable to those who are not actively looking for it.

1.2.3 AUDIO STEGANOGRAPHY

Audio steganography is a captivating technique that involves hiding information within audio files without perceptibly altering the audible characteristics of the sound. Unlike encryption, which transforms the content into a coded format, audio steganography discreetly embeds data within the audio signal itself. This can be achieved by making subtle modifications to the audio waveform, typically in frequencies that are challenging for the human ear to discern.

The primary objective is to seamlessly integrate the hidden information into the audio file, making it virtually undetectable to casual listeners. These modifications might involve slight changes in the amplitude or frequency of the audio signal, ensuring that the overall sound remains natural and unchanged.

Audio steganography finds applications in scenarios where secure communication through sound is essential. The concealed information could be text, another audio file, or any data that the sender wishes to keep confidential. Those with knowledge of the specific steganographic technique used can extract the hidden data, while others, unaware of the concealed information, simply hear the regular audio.

1.2.4 VIDEO STEGANOGRAPHY

Video steganography is a captivating method that involves concealing information within video files without visibly altering the apparent content. Unlike traditional encryption, which encodes the content into a form of secret language, video steganography operates more subtly by making discreet modifications to the video data. This can include changes to specific frames, adjustments in the frames per second rate, or alterations to other elements that don't overtly impact the visual quality.

The primary goal of video steganography is to embed a hidden message within the video file in such a way that it remains imperceptible to viewers. These modifications are carefully integrated, ensuring that the overall visual and auditory experience of the video appears unchanged to an ordinary observer.

Video steganography finds applications in scenarios where maintaining the confidentiality of information is paramount. The concealed data might be text, another video file, or any form of information that the sender wants to keep private. Those with knowledge of the specific steganographic technique employed can extract the hidden data, while others, without awareness of the concealed information, perceive only the standard video content.

1.2.5 NETWORK STEGANOGRAPHY

Network steganography is a sophisticated method of hiding information within the normal flow of network communications without attracting attention. Unlike traditional encryption, which focuses on securing the content of a message, network steganography is more subtle, involving the covert embedding of data within the structure of network protocols and traffic.

In this technique, hidden information might be concealed within the headers of network packets or subtly modifying the timing of packet transmissions. Unused or less critical fields within the network protocols can be utilized to carry additional information without affecting the primary purpose of the communication.

The main objective of network steganography is to enable secret communication within the existing network infrastructure. This hidden data might include text

messages, files, or any information that needs to be transmitted discreetly. Those familiar with the specific steganographic method can extract the concealed data, while network administrators and security systems, unaware of the covert information, see only regular network traffic.

Network steganography finds relevance in scenarios where discreet communication is crucial, such as in secure military communications or covert intelligence operations. By subtly embedding information within the vast flow of network data, this technique provides a clandestine channel for transmitting sensitive information without raising suspicions. It exemplifies a strategic use of network protocols for covert communication, showcasing the ingenuity involved in securing information within the intricacies of digital communication networks.

CHAPTER 2 - LITERARY REVIEW

The term "Steganography" originated in the 1500s with the publication of Trithemius' book titled "Steganographia."

2.1 PAST

Steganography, scientifically defined as concealed or covered writing, has ancient roots dating back to around 440 BC. The term itself became prominently recognized only at the end of a fifteen-hundred-year period. The practice of steganography has been in use for thousands of years, with examples such as ancient Chinese messages written on fine silk, compressed into small balls, and covered in wax before being swallowed by messengers. Even during the Second World War, special "inks" served as crucial steganographic tools. In this era, a technique was developed to photographically reduce a page of text into a dot less than one millimeter in diameter, concealing this microdot within an ostensibly innocent letter.

2.2 PRESENT

In contemporary steganographic systems, various forms of transmission objects such as images, audio, and videos are employed as cover media, given the prevalent practice of sharing digital photos through email and other online communication channels. Modern Steganography explores the capability of concealing information within digital transmission files and extends this concealment to the network packet level.

In a study [1], a novel approach to information concealment using multi stego-images was proposed, aiming for high capacity with minimal distortion. The method involves Creating four extra pixels for every pixel in the original image involves using a modified Least Significant Bit (LSB) in a coordinated manner. The restricted data are concealed within all transmitted pixels, and subsequent adjustments are made to minimize the effects of defacement. The initial image is partitioned into four unique secret images, implementing Exchange Carrier Object (EC) modifications for each stego-image. This process combines LSB coordination with Pixel Value Differencing (PVD) to accomplish a form of steganography that allows for reversibility.

Another spatial adaptive domain color image steganography technique [2], [3] is presented, utilizing LSB replacement and adjoining pixel value differencing. Employing a block layout of 3 by 3 pixels, the method incorporates three stages: XOR of data encoding, embedding encoded bits using PVD and LSB substitution, and extraction. Experimental results show a high embedding capacity of approximately 3.498 per pixel bits (ppb) with PSNR values of 38.23 dB. The study highlights the significance of cover image selection for optimal results and suggests the incorporation of an efficient cover image selection strategy.

The Pixel Value Differencing (PVD) method in image steganography, known for its high capacity, faces challenges such as histogram-based steganalysis attacks [4], [5]. The proposed solution combines PVD with One Time Pad (OTP) encryption for enhanced security. OTP encryption, utilizing a randomly generated key of equal size, adds a layer of protection to the PVD method. The study also introduces a scheme that avoids using a range table, presenting results suggesting improved image quality compared to other techniques.

In [6] and [7], the authors emphasize high embedding capacity and adequate visual image quality in image steganography. A new algorithm is proposed based on Least Significant Bit (LSB) replacement and Enhanced Modified Signed Digit (EMSD) procedures, offering a substantial increase in embedding capacity compared to similar algorithms. The combination of EMSD and LSB replacement aims to provide enhanced security for sensitive information, high payload, and optimal stego-image quality.

A novel image steganography strategy [8] converts primary characters of a covert message into binary bits, identifying edge regions in the image. The proposed algorithm introduces randomization as a key feature, offering robustness against visual attacks and histogram-based assaults. The study focuses on exploring image quality enhancements to improve the perceptibility of the cover image.

The LSB-based bit flipping approach, not extensively used for image hiding, is explored in [9], demonstrating its efficacy in concealing messages with maximum capacity. The bit flipping technique, applied to both grayscale and color images using the RGB model, proves to be effective in achieving high imperceptibility. The study concludes that the bit flipping approach performs well across various image types.

In [10], a color image steganography method utilizing multi-level encryption (MLE) and gray-level modification (GLM) is introduced. The study encodes the secret key

and confidential information using MLE before embedding it into the gray levels of the cover image. The proposed approach emphasizes improved stego image quality, high imperceptibility, cost-effectiveness, and advanced security. The study suggests further exploration of security layers and cover steganography directions.

The Development of LSB Steganography (DLSB) method [11] utilizes LSB-based cover steganography for embedding secret messages and compares cover and secret bits. The proposed approach aims to cover the maximum number of pixels in the image, equivalent to the maximum number of bits that can be concealed. The dynamic key is a key feature, contributing to better security and making the small changes between original and proposed values imperceptible to the human visual system.

Among spatial domain methods, the LSB replacement strategy is considered the least complex, involving the use of LSB for data insertion [12].In this approach, encoding the covert message involves actions such as reversing, swapping, and circular right shifting, with the option of using an arbitrary key [13]. The benefits of Least Significant Bit (LSB) in pixel intensities are altered with the message bits, and the quantity of pixels utilized for embedding corresponds to the number of bits present in the message file. An in-depth analysis of pertinent LSB-based techniques and diverse spatial domain image steganography methodologies is conducted, considering fundamental evaluation criteria, as illustrated.

CHAPTER 3 - IMAGE STEGANOGRAPHY

Image steganography is a fascinating method of concealing information within digital images without altering their visual appearance. This technique finds application in several domains where secure communication and data protection are vital. In the realm of secure communication, image steganography enables the transmission of hidden messages within the pixels of images, providing a discreet channel for confidential information exchange. Moreover, it plays a role in copyright protection, allowing for the embedding of ownership details within images, serving as a form of digital watermarking. In covert operations, particularly in fields like intelligence or military, image steganography offers a subtle means to convey information without drawing attention. Additionally, in digital forensics, it aids in tracking and tracing by embedding information for identifying the source or origin of digital content.

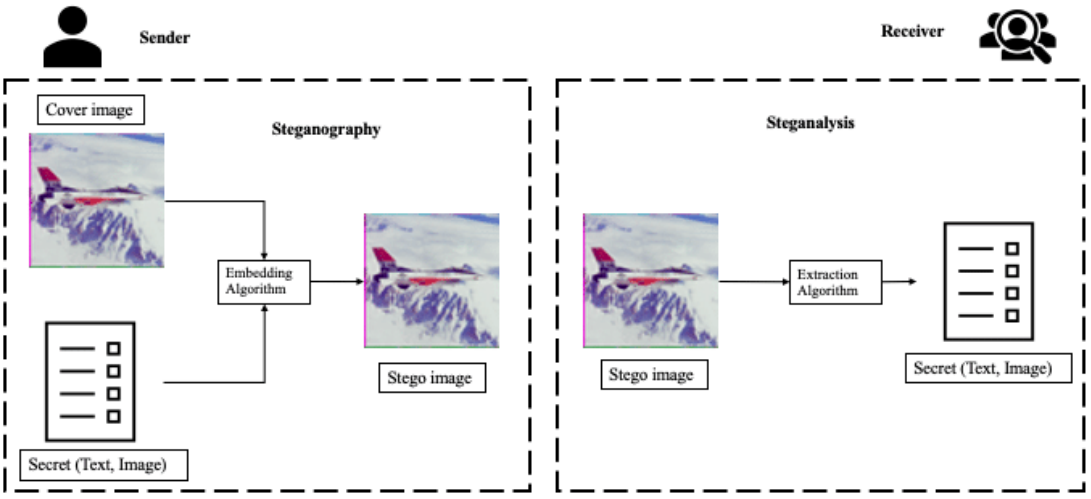

Figure - 5 Image Steganography

Various techniques are employed in image steganography, each with its unique approach. LSB (Least Significant Bit) substitution is a common method, involving the replacement of the least significant bits of pixel values with hidden data, which is often imperceptible to the human eye. Frequency domain techniques, such as using discrete cosine transform (DCT) for JPEG images, manipulate image data in a way that hides information effectively. Spatial domain techniques involve altering the

spatial arrangement of pixels or color values in an image for steganographic purposes. Spread spectrum techniques distribute hidden information across the entire image, making it challenging to detect. Transform domain techniques, such as Fourier or wavelet transforms, are applied to embed information in the frequency or spatial domains. The choice of technique depends on factors like the type of image, the desired level of security, and potential methods of detection. Image steganography stands out as a versatile and creative approach to secure information exchange within the visual medium.

3.1 STEGANOGRAPHIC APPROACHES

Image steganography employs various approaches, with spatial and frequency domain techniques being prominent methods. In the spatial domain, alterations are made directly to the pixel values or the spatial arrangement of pixels in an image. This could involve manipulating color values, adjusting pixel intensities, or modifying the structure of the image to embed hidden information. Spatial domain techniques are known for their simplicity and effectiveness in concealing data within the visible components of an image. On the other hand, frequency domain techniques involve transforming the image data into the frequency domain using mathematical transformations like Fourier or wavelet transforms. By manipulating the frequency components of the image, these techniques embed information in a way that might be less perceptible to the human eye. Frequency domain approaches are often used in formats like JPEG, where alterations are made in the transformed domain to achieve effective steganographic results. Both spatial and frequency domain techniques offer distinct advantages and trade-offs, and the choice between them depends on factors such as the image type, the desired level of security, and the potential for detection.

3.1.1 SPATIAL DOMAIN STEGANOGRAPHY

Spatial domain image steganography is a method of hiding information within the visible components of an image by directly manipulating the pixel values and spatial arrangement. This technique exploits the human eye's limitations in perceiving subtle changes, allowing for discreet communication within the apparent content of the image.

Spatial domain steganography directly operates on the pixel values and arrangement, making it relatively simple and effective. LSB substitution is like a hidden language within the binary structure of pixel values, ensuring the alterations are inconspicuous. Pixel-Value Differencing cleverly tweaks the relationships between neighboring pixels, adding a layer of complexity. Random Pixel Adjustments introduce an element of unpredictability, making detection more challenging. Grayscale Modification expands spatial steganography to grayscale images, where intensity adjustments become a subtle means of embedding hidden data. Overall, spatial domain steganography offers versatile and practical ways to ensure secure communication by subtly altering what is visible to the human eye within the image itself.

Types of Spatial Domain Steganography:

1. LSB Substitution: This is a common and straightforward spatial domain technique. It involves replacing the least significant bits of pixel values with the bits of the hidden data. As the changes are minimal, they are often imperceptible to the naked eye.

   Example: If the original pixel value is 11010110, LSB substitution might change it to 11010111.
2. Pixel-Value Differencing (PVD): PVD focuses on the differences between neighboring pixel values. By subtly altering these differences, information can be embedded without significantly changing the overall appearance of the image.

   Example: Adjusting the difference between adjacent pixel values by a small amount to encode hidden data.
3. Random Pixel Adjustments: This technique involves making random adjustments to selected pixels in the image to embed information. The randomness helps in making the alterations less noticeable.

   Example: Randomly changing the brightness or color of specific pixels.
4. Grayscale Modification: In grayscale images, modifying the intensity values of pixels provides an avenue for steganography. By adjusting pixel intensities, hidden information can be encoded.

   Example: Slightly altering the grayscale intensity of pixels to represent hidden bits.

3.1.2 FREQUENCY DOMAIN STEGANOGRAPHY

Frequency domain image steganography involves concealing information within the transformed frequency components of an image. Unlike spatial domain techniques that directly modify pixel values, frequency domain methods manipulate the mathematical representation of the image. This technique exploits the fact that changes made in the frequency domain might be less perceptible to the human eye, offering a covert means of embedding data.

Types of Frequency Domain Steganography:

1. Discrete Fourier Transform (DFT): DFT transforms the image from the spatial domain to the frequency domain. By modifying certain frequency components, hidden data can be embedded. Example: Adjusting the amplitude or phase of specific frequencies in the transformed image.
2. Discrete Cosine Transform (DCT): DCT, commonly used in JPEG compression, transforms the image into a set of cosine functions. Alterations in the coefficients of these functions allow for the hiding of information.Example: Modifying the coefficients to encode hidden data without affecting the visual quality drastically.
3. Wavelet Transform: Wavelet transform decomposes the image into different frequency components. Changes in the coefficients of these components provide a medium for steganography. Example: Adjusting the wavelet coefficients in the high-frequency bands to embed information.

Frequency domain steganography operates on the principle that alterations in transformed representations might be less noticeable. Discrete Fourier Transform allows for manipulating the frequency components, playing with the essence of the image. Discrete Cosine Transform, common in image compression, enables subtle changes without compromising the image quality significantly. Wavelet Transform, with its multi-resolution analysis, offers another layer of complexity, allowing for covert information embedding. Frequency domain steganography is particularly effective in formats like JPEG, where alterations in the transformed domain can go unnoticed due to the inherent lossy compression.

3.2 LEAST BIT SUBSTITUTION METHOD

Least Significant Bit (LSB) substitution is a widely used method in image steganography that involves altering the least significant bits of pixel values to embed hidden information.

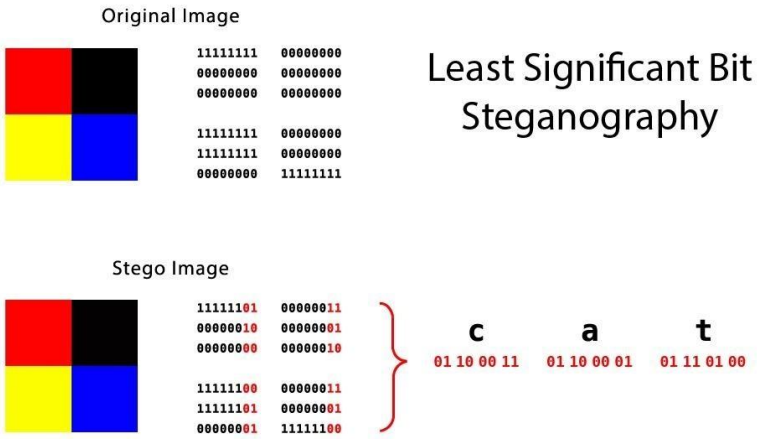

Figure - 6 LSB Method

Here's a detailed explanation in my own words:

In digital images, each pixel is represented by binary values that determine its color or intensity. In an 8-bit grayscale image, for example, each pixel has a binary representation of 8 bits. LSB substitution takes advantage of the fact that the least significant bits contribute the least to the overall intensity or color perception of an image.

The Process:

1. Original Pixel Value: Let's take an 8-bit grayscale pixel as an example, represented as 00101101.
2. Hidden Data: Suppose we want to hide the binary sequence 11001010.
3. LSB Substitution: The least significant bits of the original pixel are replaced with the bits of the hidden data. In our example, the new pixel value becomes 00101100.
4. Visual Impact: Since the change occurs in the least significant bits, the alteration is usually imperceptible to the human eye. The visual impact on the image is minimal.

Decoding:

To retrieve the hidden information, the recipient needs to extract the least significant bits of each pixel in the image. The extracted bits can then be reconstructed to reveal the concealed data.

Advantages:

1. Simplicity: LSB substitution is straightforward and easy to implement.
2. Minimal Visual Impact: Since it modifies the least significant bits, the changes are typically visually subtle.

Challenges:

1. Vulnerability to Compression: LSB substitution is susceptible to image compression, which may eliminate or alter the least significant bits.
2. Limited Capacity: The amount of information that can be hidden is constrained by the number of least significant bits available.

Applications:

1. Covert Communication: LSB substitution is often used for discreetly transmitting messages within images.
2. Digital Watermarking: It can be employed to embed copyright or ownership information within images.

In essence, LSB substitution provides a simple yet effective way to embed hidden information within the binary structure of digital images, making it a popular choice in the field of image steganography.

3.3 STEGANALYSIS

Steganalysis is the process of detecting the presence of hidden information, or steganographic content, within digital media such as images. In the context of image steganography, steganalysis aims to identify alterations made to the image in order to conceal information. Here's an in-depth explanation in my own words:

Techniques Used in Steganalysis:

1. Statistical Analysis: Statistical methods analyze the distribution of pixel values or other image features to detect deviations caused by hidden data. Anomalies in statistical patterns may indicate the presence of steganographic content.

Example: Examining the frequency distribution of pixel values to identify unexpected variations.

2. Visual Artifacts Analysis: Steganographic techniques may introduce subtle visual artifacts or distortions that are not typically present in natural images. Steganalysis algorithms can detect these anomalies.

   Example: Identifying unusual patterns in image textures or checking for inconsistencies in color gradients.

3. File Format Analysis: Steganalysis examines the file structure or format of images to detect irregularities introduced by steganographic methods. Changes to specific elements, like header information, may indicate hidden content.

   Example: Analyzing the metadata or header information for unexpected modifications.

4. Machine Learning Approaches: Machine learning techniques, such as neural networks, can be trained on a dataset of known images (with and without hidden data) to learn patterns associated with steganography. The trained model is then used to classify unknown images.

   Example: Training a neural network to recognize statistical patterns indicative of steganographic alterations.

Applications of Steganalysis:

1. Security and Forensics: Identifying steganographic content is crucial in cybersecurity and digital forensics to uncover hidden messages, malware, or illicit activities.
2. Content Authentication: Steganalysis helps ensure the integrity of digital content by detecting unauthorized or malicious alterations.
3. Media Verification: In scenarios such as media authentication or content verification, steganalysis helps ensure that images have not been tampered with.

CHAPTER 4 - REVIEW OF IMAGE IN IMAGE STEGANOGRAPHY

The combination of cryptography and steganography offers an elevated level of security for confidential information. Steganalysis involves the identification of concealed data within images [14]. With the rising prevalence of image steganography, various steganalysis techniques, including a frequently employed statistical interpretation method, have been developed.

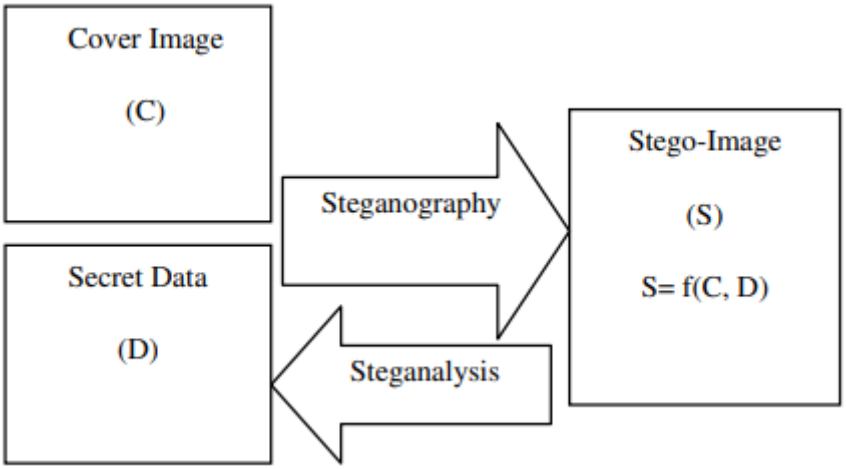

Figure - 7 Steganography and Steganalysis

In their work, **Reena M. Patel** and colleagues [15] detailed a range of embedding techniques, including the LSB insertion method. The researchers introduced novel approaches involving Multiple LSB methods. The experimentation involved taking various 8-bit grayscale images sized at 512x512 pixels, on which the Multiple LSB insertion technique was applied. Prior to embedding, the message underwent conversion into ASCII bits. The data intended for embedding had a length of 15 KB or approximately 17,143 characters. Evaluation of the results was conducted using parameters such as PSNR and MSE.

Amitava Nag et al. introduced an innovative approach to image steganography in their work [16]. Their method employed LSB insertion through X-box mapping, featuring multiple X-boxes with distinctive data. The embedding process utilized this algorithm, employing four specific X-boxes with sixteen unique values. Each obtained value was mapped to the four LSBs of the original image. The primary

objective was to enhance both the security and quality of the image. This mapping strategy elevated the security level, making it challenging to extract the data without adequate knowledge of the mapping rules.

In their study, **Weiqi Luo** and colleagues [17] conducted a thorough examination of the LSB Matching Technique for data embedding in images. They introduced an edge-adaptive approach for data concealment using a reevaluated version of LSB Matching. This approach facilitated the selection of embedding areas based on the confidential data size and the contrast between consecutive pixels in the original image. Regions characterized by sharp edges were reserved for low embedding rates. The effectiveness of their proposed method was assessed across 6000 diverse images, leading to the conclusion that their work significantly elevated the security level compared to alternative LSB-based techniques.

Miao Ma et al. [18] introduced a swift segmentation approach for Synthetic Aperture Radar (SAR) images, employing the Artificial Bee Colony (ABC) algorithm. Initially, the image underwent segmentation through the Discrete Wavelet Transform (DWT), generating low and high frequency coefficients. Subsequently, an effective fitness function was formulated for the ABC algorithm by defining the grey number within the framework of Grey Theory. The reconstructed filtered image and gradient image were utilized, with grey entropy serving as the fitness function for the ABC algorithm. Through the utilization of this algorithm, incorporating onlookers, employed bees, and scouts, the optimal threshold value was computed. The outcomes of this proposed technique indicated its superiority over Genetic Algorithm and other segmentation methods associated with Artificial Fish Swarm.

In their work, **Manoj Kumar Ramaiya** and colleagues [19] detailed a unique approach to Image Steganography employing the Data Encryption Standard, incorporating S-Box Mapping along with a secret key for encryption. The encryption process was implemented to uphold the security and authenticity of the embedded data. Preprocessing of the secret image involved utilizing an embedding function with two distinct S-Boxes. This methodology led to an improvement in both the security and image quality.

CHAPTER 5 - REVIEW OF TEXT IN IMAGE STEGANOGRAPHY

The fundamental method for hiding private information in an image is the Least Significant Bit (LSB) technique. In this method, the least significant bits of the pixels in the host image are replaced with the bits containing the confidential data. Using multiple LSBs for message embedding can increase the payload capacity of the LSB method, but this comes with the drawback of introducing noticeable changes to the host image. Although the implementation of the LSB method is simple, it is vulnerable to statistical attacks, including RS, image processing operations, and Chi-Square analysis, as documented in references [20-27].

In [20], Adnan Abdul-Aziz Gutub presented an enhanced steganographic method that improves robustness. This technique employs one channel for signaling, while the other two channels cyclically embed secret data in a predefined manner, thereby bolstering the overall resilience of the proposed approach. Experimental outcomes show a significant enhancement in payload capacity and imperceptibility when compared to current algorithms. Moreover, this method alleviates the requirement for key exchange overhead.

In their published work [21], the authors introduce a resilient method for integrating diverse bits into image pixels, taking into account pixel attributes like value, mean, and standard deviation (SD). The approach includes the insertion of two bits into a pixel when its value falls below (mean – SD/2), storing three bits if the pixel value is less than (mean + SD/2), and allocating four bits for other pixel values. To introduce an unpredictable element as a defense against potential attacks, the proposed technique incorporates a chaotic effect via a path that traverses randomly. However, the specific details regarding the generation of this random path are not disclosed.

In the study described in [22], Grover et al. present a dynamic edge-centric LSB substitution method. This approach hides three bits of confidential information in pixels with edges and two bits in pixels without edges within the blue channel of an RGB image. In contrast to the conventional LSB substitution method, this technique showcases heightened payload capacity and resilience. The confidential data is partitioned into two sets and incorporated into the original image, starting from the

central pixel and spanning across the entire image, thereby improving its overall robustness.

In [23], a new approach is presented to embed confidential data within either the GREEN or BLUE channel of an image carrier. This is accomplished by utilizing secret key bits and the least significant bit (LSB) of the RED channel. The innovation of this method lies in its reinforcement of the conventional LSB technique with an added layer of security through the integration of a secret key. The LSB of the RED channel undergoes XOR operation with the secret key bit, and the decision on whether to substitute the LSB of the GREEN or BLUE channel is based on the resultant value. Despite maintaining the same payload, this proposed technique offers heightened resilience and increased security in comparison to the standard LSB method. Nonetheless, the secure exchange of the secret key poses an ongoing challenge and introduces an additional overhead for the method.

Ibrahim and Kuan have devised a Steganography Imaging System (SIS) in [24], incorporating a secret key for heightened security. The authors utilize a zipping mechanism to compress both the secret key and secret data, thereby increasing the payload capacity. The resulting zip file is then converted into a bitstream and concealed within a cover image. Although the proposed algorithm exhibits a substantial payload capacity and produces stego images of superior quality, it is important to note that this technique is specifically designed for BMP format images.

Thanikaiselvan and Arulmozhivarman have introduced a more robust approach for color images in the transform domain by utilizing the Reversible Integer Haar Wavelet Transform (RIHWT) and Graph Theory (GT) [25]. In this technique, the RIHWT is independently applied to the RED, GREEN, and BLUE channels. Subsequently, the wavelet coefficients are chosen based on the Graceful Graph (GG) to disperse the secret data randomly among these coefficients. This method employs three distinct keys for encoding and decoding: Key1 serves as the subband selection key, determining one of the subbands (LL, LH, HL, or HH); Key2 randomly selects coefficients within the chosen subband based on GG; Key3 determines the number of bits to be stored in the selected coefficients. The proposed approach exhibits promising results in terms of imperceptibility, robustness, and payload capacity.

5.1 EMBEDDING ALGORITHM

Input: Original Color Image, Confidential Information

Output: Encoded Image

Procedure:

1. Utilize the original RGB image and confidential information.
2. Transform the RGB image into the HSI color model using the formulas outlined in section 3.1.2.
3. Convert the confidential data into a 1-D array of bits.
4. Select a pixel from the I-Plane and substitute its least significant bit (LSB) with a corresponding confidential bit.
5. Repeat Step 4 until all confidential bits are integrated into the I-Plane pixels.
6. Revert the HSI image back to the RGB color space using the provided formulas in section 3.1.3.
7. Save the resulting stego image.

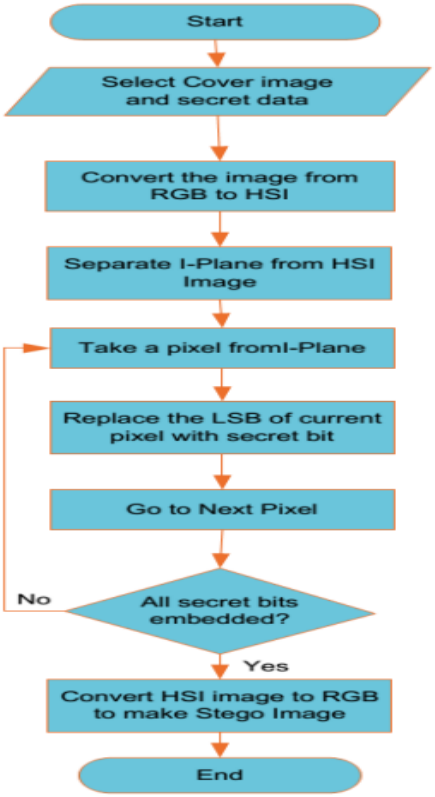

Figure 8 - Embedding Algorithm Flowchart

5.2 EXTRACTION ALGORITHM

Input: Stego Image

Output: Secret data

1. Begin by transforming the stego image into the HSI color space.
2. Focus solely on the I-Plane for the retrieval of secret data.
3. Retrieve the least significant bit (LSB) of the current pixel from the I-Plane of the HSI image.
4. Iterate through Step 3 until all secret bits are successfully decoded.
5. Transform the decoded secret bits into the corresponding secret data, such as text or images.

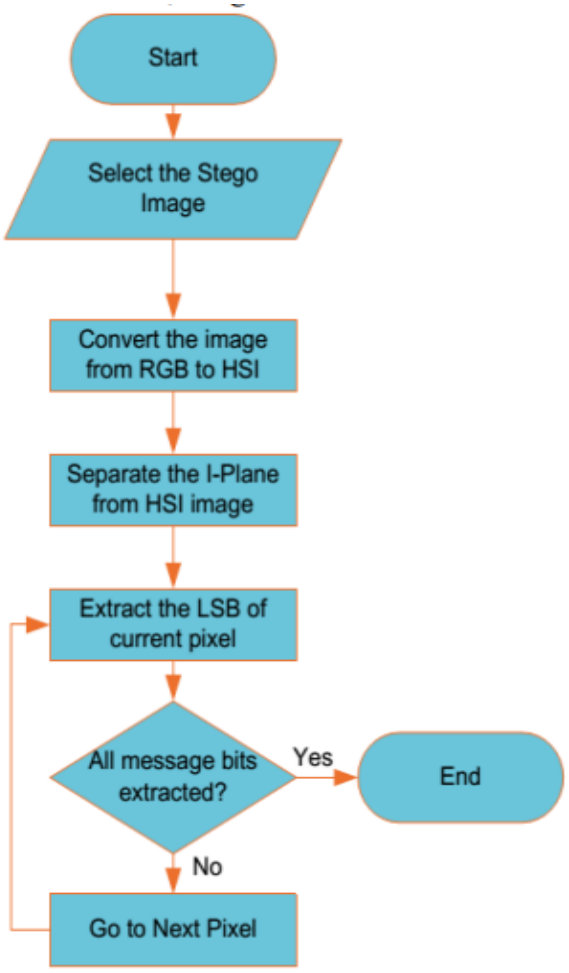

Figure 9 - Extraction Algorithm Flowchart

CHAPTER 6 - FUTURE WORK

6.1 DUAL LAYER OF SECURITY

The concept of a dual-layer security approach combining cryptography and steganography involves a sophisticated method to protect sensitive information. In this process, the first layer employs cryptography, where the secret data is transformed into an encrypted message using advanced algorithms. Cryptography ensures that even if unauthorized parties intercept the message, it remains indecipherable without the corresponding decryption key.

The second layer introduces steganography, a technique focused on concealing the encrypted message within seemingly innocuous cover media, such as an image. By embedding the encrypted data within the pixels of an image, steganography adds an extra layer of obscurity. This dual-layered approach enhances security by not only encrypting the information but also making its presence inconspicuous within another file, thus reducing the likelihood of detection by potential adversaries.

The advantages of this dual-layer security model are noteworthy. Firstly, it provides a higher level of confidentiality as the sensitive data is not only encrypted but also hidden within a nonchalant carrier, adding an additional barrier against unauthorized access. Secondly, The amalgamation of cryptography and steganography poses a formidable challenge for attackers to decipher the concealed information, thereby strengthening the overall security posture.

However, this approach is not without its challenges. Effectively implementing and managing dual-layer security requires careful consideration of the algorithms used, as well as the potential impact on the performance and usability of the system. Additionally, maintaining the secrecy of the steganographic key becomes crucial, as its compromise could lead to the exposure of the concealed data. Striking the right balance between complexity and usability is essential in navigating the challenges associated with this intricate dual-layer security strategy.

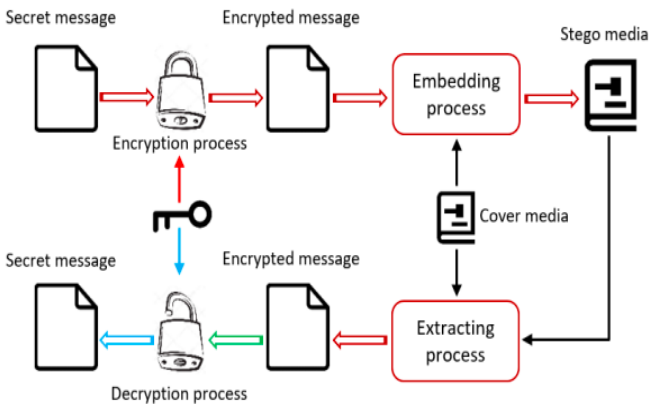

Figure - 10 Dual layer of security

6.2 Literature Review

Combination of cryptographic and steganographic techniques for enhancing information security. Cryptography's objective is data protection through encryption, focusing on confidentiality, authentication, identification, data integrity, and nonrepudiation.

Steganography aims at secret communication, hiding information within carriers like text, messages, audio, video, and DNA. While cryptography produces ciphertext as output and requires a key, steganography generates stego files and optional keys.

Cryptography provides visibility, as the ciphertext can be analyzed (cryptanalysis). Steganography remains invisible, but its security is compromised when detected (steganalysis).

Numerous studies propose combining cryptographic and steganographic techniques to address increasing threats to data security. Dhamija and Dhaka proposed a combination of SCMACS for encryption and the LSB method for steganography. A highly-secured steganography technique using DNA sequences and Hyperelliptic Curve Cryptography was suggested . Integrated visual cryptography and LSB-based steganography were combined for multi-level secret data embedding. A method incorporating AES-128 encryption, QR code encoding, and LSB-based steganography was presented for secure message transmission. DES algorithm was used for text message encryption along with K-means pixel clustering for image segmentation.

Two Fish algorithm and Adaptive B45 steganography were combined for enhanced security. Adaptive Pixel Value Differencing with AES encryption was proposed for increased embedding capacity and stego image quality. Performance analysis of Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest-Shamir-Adleman (RSA) in conjunction with Least Significant Bit (LSB) substitution indicated AES as more efficient. Huffman encoding was used along with LSB for data hiding in gray level images . Gray level modification for color images was achieved through a combination of image transposition,Blowfish encryption,and other techniques. Blowfish cryptography and LSB embedding were utilized for image and text combinations. RSA with a 128-byte key and F5 steganographic algorithm were combined for secure information embedding. Visual cryptographic technique based on Residual Number System theory was proposed for secure image sharing .

Almuhammadi et al. conducted a comparative study, classifying methods and comparing them based on the algorithms used, steganographic techniques, and cover file types. Methods starting with cryptography were found to be more common and provided improved security with minimum exposure of user's encrypted data.

6.3 EXPERIMENTAL RESULTS

We have successfully implemented a dual-layer security methodology, combining cryptographic and steganographic techniques. The integrated approach involves the utilization of both cryptographic measures and steganographic methods to bolster the overall security of the system.The results obtained from this implementation are presented as follows:

Secret Message : I Love Electronics

Figure - 11 Carrier image

Figure - 12 Stego image or Output Image

```
aryan@DESKTOP-2IRSQGI MINGW64 /c/Users/aryan/OneDrive/Desktop/cpp/__pycache__
$ python -u "c:\Users\aryan\OneDrive\Desktop\cpp\__pycache__\test.py"
Enter the secret message to encrypt and hide: I Love Electronics
Key for decryption: b'\xf4b\xe4\x1e\xc1Oqq\xe7\x99%^\xdfv\xfb\xb88\xea\xe3\x96\xaf+(\x90\x82w\xe3\xc1\xe4C\xaa\xdb'
Encrypted message: b'\xc5\xcd\x17\xb2#\xce\x1a\x8b\xefv\xe0\xf7\xc9\rW\xfcG\x0e6\xba\x81\x9f7Q]\xd3\xb6\xef\xa4\x1e\xc2\x93'
length of key is: 32
length of message is: 32
Integers hidden successfully.
received length of key is: 32
received length of message is: 32
Retrieved encrypted message: b'\xc5\xcd\x17\xb2#\xce\x1a\x8b\xefv\xe0\xf7\xc9\rW\xfcG\x0e6\xba\x81\x9f7Q]\xd3\xb6\xef\xa4\x1e\xc2\x93'
Retrieved key: b'\xf4b\xe4\x1e\xc1Oqq\xe7\x99%^\xdfv\xfb\xb88\xea\xe3\x96\xaf+(\x90\x82w\xe3\xc1\xe4C\xaa\xdb'
Decrypted message: I Love Electronics
```

Figure - 13 Decrypted Message

CONCLUSION

In conclusion, our college project on image steganography has delved into the extensive body of previous works in this field, exploring various techniques and methodologies employed for concealing information within images. Through a comprehensive review of the existing literature, we gained valuable insights into the strengths and limitations of different spatial domain steganographic methods, contributing to the understanding of this evolving domain.

Building upon the foundations laid by previous researchers, our project took a novel approach by proposing a method that combines the principles of both cryptography and steganography. This integration provides a dual layer of security, enhancing the robustness of data transmission and confidentiality. By incorporating cryptographic techniques alongside spatial domain steganography, our method aims to address the growing concerns related to data security in digital communication.

In the ever-evolving landscape of information security, our project contributes to the ongoing efforts to develop more advanced and integrated approaches. As we move forward, the dual-layered security model we have introduced opens avenues for further research and exploration, potentially influencing the future development of secure communication systems.

REFERENCES

[1] U. A. M. E. Ali, E. Ali, M. Sohrawordi and M. N. Sultan, "A LSB based image steganography using random pixel and bit selection for high payload", Int. J. Math. Sci. Comput., vol. 7, no. 3, pp. 24-31, 2021, [online] Available: https://www.mecs-press.net/ijmsc/ijmsc-v7-n3/IJMSC-V7-N3-3.pdf.

[2] M. Bachrach and F. Y. Shih, ‘‘Survey of image steganography and steganalysis,’’ in Multimedia Security, 1st ed., F. Y. Shih, Ed. CRC Press, 2017, pp. 201–214, doi: 10.1201/b12697-11.

[3] M. M. Bartere and H. R. Deshmukh, ‘‘Study of data hiding mechanism using virtual key replacement method,’’ in Proc. Int. Conf. Inventive Comput. Informat. (ICICI), Nov. 2017, pp. 1006–1010.

[4] R. Chandramouli and N. Memon, ‘‘Analysis of LSB based image steganography techniques,’’ in Proc. Int. Conf. Image Process., vol. 3, 2001, pp. 1019–1022.

[5] K. Chen, H. Che, M.-F. Leung, and Y. Wang, ‘‘An improved superpixelbased fuzzy C-means method for complex picture segmentation tasks,’’ in Proc. 14th Int. Conf. Adv. Comput. Intell. (ICACI), Jul. 2022, pp. 231–238.

[6] C. Dai, H. Che, and M.-F. Leung, ‘‘A neurodynamic optimization approach for L1 minimization with application to compressed image reconstruction,’’ Int. J. Artif. Intell. Tools, vol. 30, no. 1, Feb. 2021, Art. no. 2140007.

[7] I. Diop, S. M. Farss, K. Tall, P. A. Fall, M. L. Diouf, and A. K. Diop, ‘‘Adaptive steganography scheme based on LDPC codes,’’ in Proc. 16th Int. Conf. Adv. Commun. Technol., Feb. 2014, pp. 162–166.

[8] M. M. Emam, A. A. Aly, and F. A. Omara, ‘‘An improved image steganography method based on LSB technique with random pixel selection,’’ Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 3, p. 361, 2016.

[9] N. F. Johnson and S. Jajodia, ‘‘Exploring steganography: Seeing the unseen,’’ Computer, vol. 31, no. 2, pp. 26–34, Feb. 1998.

[10] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Hallorana, ‘‘Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research,’’ Neurocomputing, vol. 335, pp. 299–326, Mar. 2019.

[11] M. Kalita, T. Tuithung, and S. Majumder, ‘‘An adaptive color image steganography method using adjacent pixel value differencing and LSB substitution technique,’’ Cryptologia, vol. 43, no. 5, pp. 414–437, Sep. 2019.

[12] S. Kaur, S. Bansal, and R. K. Bansal, ‘‘Image steganography for securing secret data using hybrid hiding model,’’ Multimedia Tools Appl., vol. 80, no. 5, pp. 7749–7769, Feb. 2021.

[13] J. Kour and D. Verma, ‘‘Steganography techniques—A review paper,’’ Int. J. Emerg. Res. Manag. Technol., vol. 3, no. 5, pp. 132–135, 2014.

[14] Y.-K. Lee and L.-H. Chen, ‘‘High capacity image steganographic model,’’ IEE Proc., Vis., Image Signal Process., vol. 147, no. 3, pp. 288–294, 2000.

[15] Reena M. Patel & D J Shah, “Multiple LSB data hiding based on Pixel value and MSB value”, IEEE Nirma University International Conference on Engineering, pp. 1-5, 2013.

[16] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Partha Pratim Sarkar, “An Image Steganography Technique using X-Box Mapping” IEEE International Conference On Advances in Engineering, Science and Management (ICAESM), pp. 709-713, 2012.

[17] Weiji Luo, Fangjun Huang & Jiwu Huang, “Edge Adaptive Image Steganography Based on LSB Matching Revisited” IEEE, Vol.5, No. 2, pp.201-208, 2010.

[18] Miao Maa, Jianhui Lianga, “SAR image segmentation based on Artificial Bee Colony algorithm”, Applied Soft Computing 5205–5214, Elsevier, 2011.

[19] El-Sayed M. El-Alfy, “Detecting pixel-value differencing steganography using Levenberg-Marquardt neural network”, IEEE Symposium in Computational Intelligence and Data Mining (CIDM), pp. 160-165, 2013.

[20] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, “Security improvisation in image steganography using DES”, IEEE 3rd International Conference in Advance Computing (IACC), pp. 1094- 1099, 2013.

[21] Zahra Zahedi Kermani and Mansour Jamzad, “A robust steganography algorithm based on texture similarity using gabor filter”, IEEE International Symposium on Signal Processing and Information Technology, pp. 578- 582, 2005.

[22] A. Rahman, H. Ali, N. Badshah, L. Rada, A. A. Khan, H. Hussain, M. Zakarya, A. Ahmed, I. U. Rahman, M. Raza, and M. Haleem, ‘‘A selective segmentation model using dual-level set functions and local spatial distance,’’ IEEE Access, vol. 10, pp. 22344–22358, 2022.

[23] S. Rustad, D. R. I. M. Setiadi, A. Syukur, and P. N. Andono, ‘‘Inverted LSB image steganography using adaptive pattern to improve imperceptibility,’’ J. King Saud Univ., Comput. Inf. Sci., vol. 34, no. 6, pp. 3559–3568, Jun. 2022.

[24] G. Swain and A. Sahu, ‘‘A novel multi stego-image based data hiding method for gray scale image,’’ Pertanika J. Sci. Technol., vol. 27, no. 2, pp. 753–768, May 2019.

[25] K. U. Singh, ‘‘A survey on image steganography techniques,’’ Int. J. Comput. Appl., vol. 97, no. 18, pp. 10–20, Jul. 2014.

[26] N. Singh, ‘‘High PSNR based image steganography,’’ Int. J. Adv. Eng. Res. Sci., vol. 6, no. 1, pp. 109–115, 2019.

[27] G. L. Smitha and E. Baburaj, ‘‘A survey on image steganography based on block-based edge adaptive based on least significant bit matched revisited (LSBMR) algorithm,’’ in Proc. Int. Conf. Control, Instrum., Commun. Comput. Technol. (ICCICCT), Dec. 2016, pp. 132–139.

[28] S. Solak, ‘‘High embedding capacity data hiding technique based on EMSD and LSB substitution algorithms,’’ IEEE Access, vol. 8, pp. 166513–166524, 2020.