Organization Management Using Image Steganography

***Nethravathi J, **Prasanna G**
**PG Student, USN – 4MH22SCS02*
***Assistant Professor,*
Dept Of CSE, MITM, Mysore

[1]*Received: 09 April 2024; Accepted: 28 June 2024; Published: 12 July 2024*

ABSTRACT

Steganography is the practice of embedding confidential information within a carrier medium, which could include elements like a TCP/IP header, image, audio file, or video. The primary objective of steganography is to obfuscate the very existence of the hidden information, thereby minimizing the likelihood of detection by an adversary. A variety of steganographic techniques are available for embedding clandestine data within digital images. These techniques vary in complexity, each offering distinct advantages and limitations. The selection of a particular steganographic method is largely contingent upon, and the choice of technique should align with the functional needs of the deployment context. Applications may necessitate varying degrees of secrecy, the imperceptibility of the concealed data, or enhanced robustness of the carrier medium, among other factors. This study aims to deliver a thorough overview of the development and implementation of contemporary digital image steganography algorithms employed for data concealment across domains such as transformation, compression, and spatial representation. The discourse will maintain a balance between technical detail and accessibility, incorporating recent advancements in steganalysis—the field dedicated to the detection and analysis of steganographic techniques—while refraining from excessive specificity.

Keywords- *dataset; least significant bit(lsb); Most significant bit(Msb); steganography*

INTRODUCTION

In contemporary digital era, the safeguarding of organizational data is of paramount importance. Traditional methodologies, such as encryption and access controls, serve as fundamental mechanisms for protecting sensitive information. However, with the increasing sophistication Given the increasing prevalence of cyber threats, there is an urgent need to investigate novel techniques to augment data security. Image steganography, which encompasses both the art and science of embedding information within images, presents a compelling approach to this challenge. information within digital images, offers a promising augmentation to conventional security strategies.

Image steganography refers to the practice of embedding concealed information within digital images in such a manner that the presence of the hidden data is imperceptible to the casual observer. This technique diverges from traditional cryptographic methods, which primarily focus on obfuscating the content of the message. Instead, steganography aims to obscure the very existence of message. Various techniques, such as alterations to pixel values, utilization of specific image formats, and advanced algorithms, are employed to achieve this concealment. Relevance to Organizational Management In the domain of organizational management, image steganography can address several critical challenges: Enhanced Data Security: By embedding confidential organizational data within ostensibly benign images, steganography provides an additional layer of security. This method facilitates the covert transmission of sensitive information, reducing the likelihood of interception and unauthorized access. Access Control Mechanisms: Steganography can be utilized to encode access credentials or authorization tokens within images, thus implementing

[1] *How to cite the article:* Nethravathi J., Prasanna G (July, 2024); Organization Management Using Image Steganography; *International Journal of Advances in Engineering Research*, July 2024, Vol 28, Issue 1, 23-34

an extra layer of access control. Only authorized personnel equipped with the requisite decryption tools or steganographic keys can retrieve the embedded information.

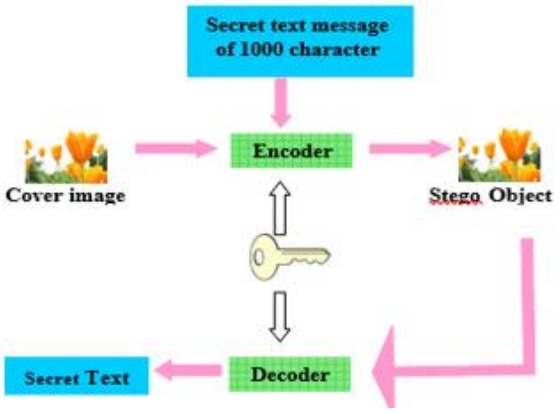

Figure 1: Steganography Model

Data Integrity Assurance: Steganography enables the incorporation of integrity checks or digital signatures within images, thereby facilitating the verification of data authenticity and integrity. This approach ensures that information remains unaltered and reliable. Secure Communication Channels: The use of steganography allows for the establishment of secure communication channels within organizational frameworks. For instance, confidential internal communications or strategic documents can be embedded within image files and disseminated through standard communication channels, minimizing the risk of detection by unauthorized parties. Compliance and Auditing: Image steganography can be leveraged to embed regulatory information or audit trails within images, thus supporting secure record-keeping and adherence to industry standards. Discreet Communication: Steganography provides a subtle method for the transmission of confidential messages between organizational entities without attracting undue attention. Protection of Intellectual Property: Embedding proprietary information or trade secrets within images can serve as a safeguard against unauthorized dissemination and intellectual property theft. Augmented Security for Digital Assets: Hidden data within images can be utilized to protect critical digital assets, such as legal documents, contracts, or research data, from unauthorized access or theft. Seamless Integration with Existing Systems: The integration of steganographic techniques into existing digital management systems can enhance their security capabilities without necessitating substantial modifications to established workflows.

Despite its advantages, the implementation of image steganography presents several challenges Detection and Countermeasures: Sophisticated methods may be required to detect and counteract steganographic attacks. Organizations must be vigilant and implement appropriate measures to mitigate unauthorized use of steganography. Data Capacity Constraints: The extent to which data can be embedded within an image is contingent upon the image's size and resolution. Large volumes of data may necessitate advanced techniques or larger image files.

Legal and Ethical Implications: The application of steganography must conform to legal and ethical standards. Organizations should ensure that their use of steganographic methods aligns with regulatory requirements and industry best practices.

Image steganography represents an innovative approach to enhancing organizational management by providing supplementary layers of security, access control, and data integrity. By embedding concealed information within digital images, organizations can achieve secure communication, safeguard sensitive data, and maintain regulatory compliance. However, effective implementation requires careful consideration of potential challenges and adherence to legal and ethical standards.

Steganography, a technique employed to conceal messages, facilitates the secure exchange of confidential information between users. One of the most prevalent methods for embedding hidden messages image pixels, specifically the least

significant two bits. However, the LSB technique adversely affects image resolution, leading to a degradation in image quality and increased susceptibility to manipulation. Consequently, there is a pressing need to address these issues by enhancing the security of the concealed information and improving image quality. The proposed method for concealing the secret message involves identifying values that are precisely aligned between the secret message and the image pixels. This approach ensures that the encoding of the secret message into the image does not alter the visible characteristics of the image. Consequently, the resolution of the image remains unaffected, preserving the integrity of the image quality. The principal objective of this paper is to investigate and analyze the various deep learning techniques employed in the domain of image steganography. The adoption of deep neural network-based automatic cost learning in steganography has gained considerable traction. Within this paradigm, steganographic methods utilizing learned costs have demonstrated superior security performance compared to those employing manually designed costs. Despite their capacity to embed substantial amounts of data, these techniques exhibit a high decoding error rate, approximately 20%. In this research, we introduce a novel steganographic algorithm that capitalizes on the sensitivity of neural networks to minor perturbations.

LITERATURE SURVEY

1. Image Steganography(Authors: Nandhini Subramanian; Omar Elharrouss; Somaya Al Maadeed; Ahmed Bouridane 2021)

Image steganography is a technique involving the concealment of data—such as textual information, photographs, or videos—within a cover image, rendering the embedded information imperceptible to the unaided observer. Recently, there has been an increasing emphasis on leveraging deep learning technologies, which have demonstrated considerable potential as effective tools in diverse domains, including image steganography. This paper aims to systematically investigate and elucidate the various deep learning methodologies employed in the domain of image steganography. These methodologies can be broadly categorized into three principal categories: traditional approaches, convolutional neural network-based techniques, and generative adversarial network-based strategies.

This work outlines the common assessment measures that were applied, the experimental setups that were taken into account, and offers a detailed explanation of the datasets that were used. A summary table that condenses these components is provided for clarity. The objective of this study is to promote future scholarly research in the domain by consolidating previous developments, recognising current obstacles, and suggesting possible paths for additional exploration.

2. Multi-Image Steganography Using Deep Neural Networks" based on the work of Abhishek Das, Japsimar Singh Wahi, Mansi Anand, and Yugant Rana (2021)

Steganography is the scientific discipline concerned with embedding concealed messages within ostensibly innocuous public communications. Traditionally, techniques such as Least Significant Bit (LSB) modification have been employed to encode lower-resolution images within higher-resolution images. The objective of this study is to utilize deep neural networks to encode and decode multiple hidden images within a single high-resolution cover image.

3. An Automatic Cost Learning Framework for Image Steganography Using Deep Reinforcement Learning" by Weixuan Tang, Bin Li, Mauro Barni, Jin Li, and Jiwu Huang (2020)

The use of deep neural network-based automatic cost learning in steganography is increasingly gaining prominence. It has been shown that steganographic techniques employing such a framework exhibit superior security performance compared to those utilizing manually crafted cost functions. However, these methods are not without limitations, such as the reliance on coarse-grained optimization targets that do not explicitly incorporate pixel-wise information and the use of function-approximated neural-network-based embedding simulators. This paper introduces a novel method for embedding cost learning, addressing these limitations and aiming to enhance the efficacy of steganographic systems. The limitations previously identified are addressed through a framework designated as agent employs a policy network to decompose the embedding process overall rewards within a simulated steganalytic environment. Concurrently, the environment network assigns rewards on a pixel-wise basis. The process of simulating message embedding in an ideal embedding simulator is achieved through a sampling procedure.

The policy network crafts a secure embedding strategy by engaging in iterative interactions between the agent and its environment. This strategy is translated into pixel-wise embedding costs, which enhances the effectiveness of message embedding. Experimental findings reveal that the proposed framework outperforms existing cost-learning approaches in both learning efficiency and stability. Furthermore, it achieves cutting-edge security performance against a range of contemporary steganalysis methods.

4. Fixed Neural Network Steganography" by Varsha Kishore, Xiangyu Chen, Yan Wang, Boyi Li, and Kilian Q Weinberger (2022)

Recent progress in image steganography has focused on utilizing encoder-decoder network pairs to embed and retrieve hidden messages within images through deep learning methods. Although these techniques can conceal significant amounts of data, they are often associated with a decoding error rate of around 20%. In response, we propose a novel steganographic approach called Fixed Neural Network Steganography (FNNS). This algorithm leverages the sensitivity of neural networks to minor perturbations, resulting in markedly lower error rates compared to existing methods that conceal more than 3 bits per pixel (bpp). FNNS consistently achieves 0% error when embedding up to 3 bits per pixel of secret data. Additionally, FNNS is designed to effectively bypass both neural and traditional statistical steganalysis techniques. Its ability to securely hide up to three bits per pixel opens up new possibilities for applications requiring robust encryption. This paper also includes a specific example of using FNNS for secure and anonymous image sharing.

5. Deep Adaptive Hiding Network for Image Hiding Using Attentive Frequency Extraction and Gradual Depth Extraction" by Le Zhang, Yao Lu, Jinxing Li, Fanglin Chen, Guangming Lu, and David Zhang (2023)

In multimedia communication, information security is bolstered through the technique of image concealing. Contemporary deep image hiding methodologies typically process the cover and secret data in isolation before merging the processed data. This rudimentary fusion approach impairs the enhancement of both the stego and revealed secret images significantly. To address these limitations, we propose the Deep Adaptive Hiding Network (DAH-Net), a novel deep image hiding architecture that incrementally extracts and integrates the necessary cover and secret information across various frequency and depth layers.

Specifically, DAH-Net employs the Attentive Frequency Extraction strategy to adaptively isolate and amalgamate the relevant cover and hidden information at the frequency domain, thereby facilitating superior quality of the stego and revealed images. To facilitate the incremental extraction and integration of attentive frequency-based secret and cover information at varying depths (or layers) within the deep image hiding network, we introduce the Gradual Depth Extraction methodology within the framework of DAH-Net. Empirical evaluations demonstrate that the proposed DAH-Net exhibits enhanced versatility and delivers state-of-the-art performance in the domains of photographic steganography, image concealing, and watermarking.

6. Learning Iterative Neural Optimizers for Image Steganography" by Xiangyu Chen, Varsha Kishore, and Kilian Q Weinberge (2023)

Image steganography involves embedding information into images through subtle modifications. Recent methods have approached this task as a traditional constrained optimization problem. In this study, we propose a different perspective, suggesting that the intrinsic manifold of natural images is the ideal framework for image steganography. To address this, we introduce an iterative neural network architecture tailored for the optimization process. Unlike conventional optimization methods such as projected gradient descent or L-BFGS, our method trains the neural network to stay aligned with the natural image manifold during optimization. We show that our learned neural optimization approach significantly improves efficiency and reliability compared to traditional techniques. Our method achieves zero error for up to 3 bits per pixel (bpp) without needing error-correcting codes and drastically reduces recovery error rates compared to existing encoder-decoder-based steganography methods.

7. Payload-Independent Direct Cost Learning for Image Steganography" by Weixiang Li, Shiang Wu, Bin Li, Weixuan Tang, and XinPeng Zhang (2023)

Recent studies have demonstrated the effectiveness of reinforcement learning (RL)-based frameworks for cost-sensitive image steganography. However, these frameworks are typically optimized for specific embedding payloads, concentrating exclusively on learning embedding probabilities rather than the associated costs. This limitation poses challenges in adapting the trained model to accommodate varying payloads. In this paper, we propose PICO-RL, a payload-independent RL-based cost learning framework. This system is capable of applying universal cost functions to any payload by directly learning them, thereby enhancing its flexibility and applicability across diverse embedding scenarios. The Optimal Probability Approximation (OPA) module in PICO-RL eliminates the need for exhaustive searches to determine a reliable probability scaling parameter. It directly computes the requisite probability map for embedding simulation based on a learned cost map for each payload.

The PICO-RL framework leverages an advanced steganalysis environment network to enhance the efficacy of reward feedback during reinforcement learning (RL) training This environmental network facilitates the development of cost maps tailored to different payload sizes, which, under the Optimal Payload Adjustment (OPA) constraint, converge to a uniform state, ensuring payload independence. Experimental results show that the PICO-RL model, after training, functions effectively as a universal cost function. It provides cost metrics that offer superior security against steganalysis attacks and shows enhanced compatibility with practical steganographic encoding techniques.

8. Joint Adjustment Image Steganography Networks" by Le Zhang, Yao Lu, Tong Li, and Guangming Lu, published in 2023.

The objective of image steganography is to generate stego images—secret images embedded within cover images—that enable covert communication between two parties. Although significant progress has been made in the field of deep image steganography, existing techniques often lack sufficient refinement, as they generally employ single-process networks for both the generation of stego images and the extraction of secret images. Consequently, there remains substantial potential for enhancing the security and quality of both stego images and extracted secret images, particularly in the context of large-capacity image steganography. To advance this field, this research introduces Joint Adjustment Image Steganography Networks (JAIS-Nets), which consist of multiple coarse-to-fine iterative adjustment methodologies.

The JAIS-Nets model we propose introduces an innovative approach to enhancing image security through advanced techniques. Our method employs Cross-Process Contrastive Refinement (CPCR) to iteratively improve both the generated stego images and the revealed secret images. This technique utilizes contrastive data from pairs of cover-stego and secret-revealed images to refine the image generation process. Additionally, JAIS-Nets incorporate the Cross-Process Multi-Scale (CPMS) adjustment method, which enhances the quality of intermediate representations by leveraging multi-scale information from various stages, including both cover-stego and secret-revealed image pairs. By integrating CPCR and CPMS, our model facilitates the concurrent optimization of stego images and their hidden secrets across multiple learning levels and image scales.

9. PRIS: Practical Robust Invertible Network for Image Steganography" by Hang Yang, Yitian Xu, Xuhua Liu, and Xiaodong Ma, published in 2023

Image steganography involves the concealment of confidential information within another image in a manner that renders it imperceptible to the public, while allowing for retrieval when necessary. Existing image steganography techniques often exhibit inadequate robustness against distortions applied to the cover images, such as those introduced by lossy compression or Gaussian noise. To address these limitations, this research introduces PRIS, an approach based on invertible neural networks. PRIS incorporates two enhancement modules—one preceding and one following the extraction process—and employs a three-step training methodology to bolster the robustness of image steganography. Furthermore, the issue of rounding error, which is an inherent aspect of practical implementations often overlooked by existing methods, is explicitly addressed. Additionally, we propose a Gradient Approximation Function (GAF) as a remedy for the challenge posed by undifferentiable rounding distortions. Empirical results

demonstrate that our proposed PRIS exhibits superior resilience and practicality compared to the most advanced robust image steganography techniques currently available.

10. DKiS: Decay Weight Invertible Image Steganography with Private Key" by Hang Yang, Yitian Xu, and Xuhua Liu, published in 2023

Image steganography, which embeds information within digital images, has historically encountered security challenges, particularly when techniques are exposed or targeted. To address these issues, a novel approach utilizing a private key for image steganography has been introduced. This method significantly enhances the security of the hidden data by requiring a private key for access, even if the underlying steganographic method is not widely disseminated. Experimental evidence supports the effectiveness and practical utility of this approach. Additionally, a significant challenge in invertible image steganography is the transmission of extraneous data, often referred to as "garbage," from the secret information to the host image. To counteract this, a decay weight mechanism has been implemented to regulate information flow, thereby eliminating redundant data and boosting the efficiency of the steganographic process.

METHODS

The Least Significant Bit (LSB) technique is a widely-used method for image steganography, where data is embedded into the least significant bits of pixel values. This technique is particularly useful for hiding information within digital images in a manner that is imperceptible to the human eye. In the context of organization management, LSB-based steganography can enhance secure communication, data integrity, and access control.

The methodology for implementing image steganography using the LSB technique for organizational management involves several key steps:

Image and Data Preparation Select Carrier Image: Choose a digital image (carrier image) that will conceal the hidden data. The image should be of adequate resolution and color depth to ensure effective embedding of data without significant visual distortion. Prepare Data to be hidden: Convert the data (e.g., text, access credentials, or confidential documents) into a binary format. This data will be embedded into the carrier image. Data Encoding: If necessary, compress or encrypt the data before embedding to reduce size and enhance security.

Data Embedding Extract LSBs from Carrier Image: Load the carrier image and extract the least significant bits from each pixel. In a typical RGB image, each pixel consists of three color channels (Red, Green, and Blue), and each channel has an 8-bit value. Embed Data into LSBs . Replace the LSBs of the pixel values with the bits of the prepared data. The embedding process should be carried out sequentially across the image pixels. Ensure that the data is distributed across multiple pixels to avoid noticeable changes in the image. Handle Data Overflow -If the size of the data exceeds the available LSBs in the image, either select a larger image or use a combination of images. Ensure that the embedding does not exceed the image's capacity.

Image Reconstruction Reconstruct the Image after embedding the data, reconstruct the image by combining the modified pixel values with the original color channels. Save the new image file, which now contains the hidden data. Verify Data Integrity: Check the integrity of the hidden data by extracting it from the reconstructed image. Ensure that the data can be accurately recovered without corruption.

Load the Stego Image: Load the image containing the hidden data (stego image).

Extract LSBs: Extract the LSBs from the stego image's pixels to retrieve the embedded data. Decode Data: Convert the extracted binary data back to its original format (e.g., text or document).Verify Data Accuracy: Compare the extracted data with the original data to ensure that it has been accurately recovered without loss or distortion.

Integration with Organizational Systems Secure Communication Channels: Implement the steganographic technique within organizational communication systems. For instance, integrate the embedding and extraction

processes into secure messaging platforms or document sharing systems. Access Control and Authentication: Use the LSB technique to encode access credentials or authorization tokens within images. Ensure that only authorized personnel with the appropriate tools can decode and retrieve these credentials. Compliance and Auditing: Maintain logs of embedded and extracted data for auditing purposes. Ensure that the use of steganography aligns with organizational policies and regulatory requirements.

DATAFLOW DIAGRAM

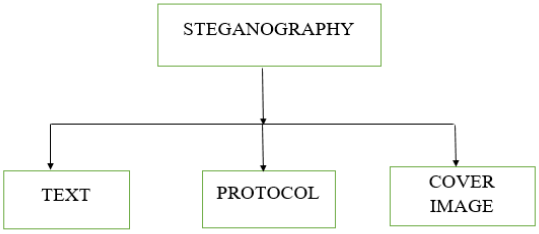

Figure 4: Hiding text with cover image

Steganography is a technique employed to conceal secret information within a seemingly innocuous, non-secret medium, thereby minimizing the likelihood of detection. One of the most fundamental and extensively utilized methods in image steganography is the Least Significant Bit (LSB) technique. This approach involves embedding concealed data into the least significant bits of pixel values in a cover image. The LSB method is favored for its simplicity and effectiveness, providing a means to integrate hidden text with minimal perceptual impact on the visual quality of the cover image.

Image Representation: A digital image consists of pixels, and each pixel contains color information. In a color image, each pixel typically has three components: Red, Green, and Blue (RGB).
Each color component of a pixel is usually represented by an 8-bit binary number, giving a range of 0 to 255.
Least Significant Bit (LSB): The LSB is the lowest bit in a binary number. Changing this bit has a minimal effect on the overall value of the byte, making it ideal for hiding data.
Embedding Data: The process of hiding data involves replacing the LSB of each pixel's color component with bits of the secret message.
For example, if the binary representation of a pixel's red component is 11001010, and the bit to be hidden is 1, the modified binary value would be 11001011.
Extraction of Data: To extract the hidden data, the LSB of each pixel's color component is read in the same sequence as they were modified.

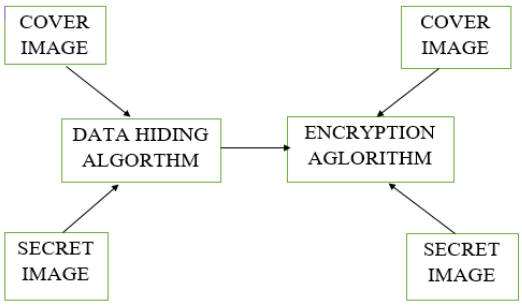

Figure 4.1: Hiding Secret Image with cover image

Least Significant Bit (LSB) steganography can also be used to hide an entire image within another image (cover image). The fundamental concept remains the same: modify the least significant bits of the pixels of the cover image to embed the hidden image.

Image Representation: Both the cover image and the secret image are composed of pixels, and each pixel contains color information represented by Red, Green, and Blue (RGB) values.
Each RGB value is an 8-bit binary number.

Least Significant Bit (LSB): The LSB is the lowest bit in an 8-bit binary number. Modifying this bit has a minimal effect on the overall color value of the pixel, making it an ideal candidate for hiding data.
Embedding Image: The process of hiding a secret image involves replacing the LSBs of the cover image's pixels with the bits of the secret image's pixels. Extraction of Image: To retrieve the hidden image, the LSBs of the cover image's pixels are read and reconstructed into the hidden image.

BLOCK DIAGRAM

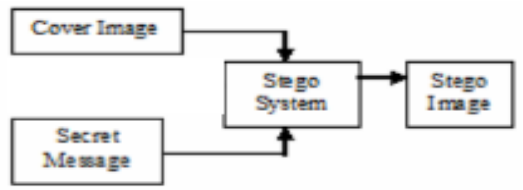

Figure 5.1: Block Diagram

Data embedding technique using MSB (Most Significant Bit).In MSB steganography, the most significant bits of the pixel data in the cover image are modified to embed the secret information. The rationale behind MSB steganography is that the most significant bits typically contribute more to the overall color intensity and are less likely to be noticed by the human eye when altered.

Here's a simplified overview of the MSB steganography technique:

Image Selection: Choose a cover image (canvas) and a secret image to hide within it. Pixel Extraction: Extract the pixel values (RGB or grayscale values) from both the cover image and the secret image.

Data Embedding: Modify the most significant bits of the cover image pixels to encode the secret information. The most significant bits are altered to match the corresponding bits from the secret image. Output Generation: Generate a new image containing the modified pixel values, which embed the secret information. This image appears similar to the original cover image but contains hidden data. Decoding: To retrieve the hidden information, extract the most significant bits from the modified image and reconstruct the secret image.

MSB steganography has its advantages and disadvantages compared to LSB steganography. While it may offer better resistance to certain types of detection algorithms, it typically allows for a lower payload capacity due to the fewer bits available for encoding data. If you're interested in implementing MSB steganography, you would need to adapt the algorithm in the servlet to manipulate the most significant bits of the pixel data instead of the least significant bits. This would involve modifying the hide () method to perform the encoding and decoding operations using MSB manipulation techniques.

Data hiding using image Watermarking and cryptography are distinct from steganography. Image steganography is a technique that conceals highly sensitive information within a cover image, enabling the resultant stego image to be transmitted securely over an insecure channel. Unlike cryptography, where unauthorized individuals are unable to decrypt the sensitive information, steganography ensures that the concealed information remains imperceptible to

unauthorized parties. Consequently, while encrypted data may sometimes draw attention due to its visible encrypted nature, data concealed through steganography remains unobtrusive and less likely to attract suspicion.

In the context of image concealment, a digital image comprises a finite array of discrete values known as pixels. Pixels represent the smallest unit of an image, with each pixel containing values that denote the intensity of a specific color at any given point. Consequently, an image can be conceptualized as a matrix, or a two-dimensional array, organized into a defined number of rows and columns. The term "digital image" in this context refers to "raster graphics," which are essentially grid-based data structures that depict a matrix of pixels and can be stored in various file formats as image files.

As previously established, the fundamental unit of an image is referred to as a pixel. Each pixel functions as an individual sample of the original image; hence, an increased number of samples contributes to a more precise representation of the original information. The uniqueness of each pixel is determined by its intensity level, which contributes to the image's chromatic vibrancy. imaging systems, colors are typically represented by three or four component intensities. For example, RGB color model utilizes red, green, and blue to define color attributes, whereas the CMYK color model employs cyan, magenta, yellow, and black. The RGB color model is an additive color system that produces a broad spectrum of colors through the combination of red, green, and blue light in varying intensities. The model's designation derives from the initials of these three primary additive colors. Although it has applications in traditional photography, the RGB color model is predominantly employed for the acquisition, representation, and display of images in electronic devices such as computer monitors and televisions.

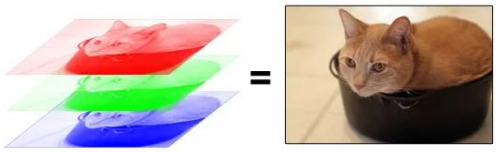

Figure 5.2: Data Embedding and Extraction Using LSB Steganography

These color channels are quantified using 8-bit values, where each channel can take on any integer value within the range of 0 to 255. Consequently, each pixel's color can be expressed as a triplet of 8-bit binary values, each corresponding to one of the color channels. This representation allows for the encoding of color information in a format that is interpretable by digital systems, leveraging binary code to define the pixel's color attributes within a specified color space.

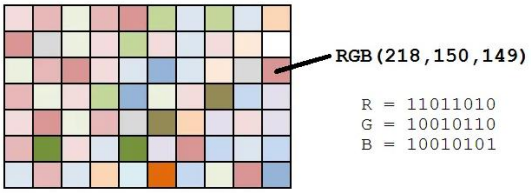

Figure 5.3: LSB Steganography: Pixel Value and Binary Representation

CONCLUSION

Steganography seeks to conceal the presence of a secret by embedding it within ostensibly innocuous covers. The application of digital image steganography, along with its various derivatives, is on the rise. Individuals are increasingly employing steganography as a means to circumvent regulations restricting robust encryption and cryptography, thereby facilitating covert communication. Analogous to other pivotal advancements in the digital era—such as the ongoing interplay between cryptographers and cryptanalysts, security professionals and hackers, or record

labels and piracy—steganography and steganalysis will perpetually evolve in a dynamic adversarial relationship, continuously developing novel techniques to counteract each other.

Data Concealment in Network Environments: Safeguarding sensitive data transmitted over networks by concealing it to mitigate the risks associated with potential data breaches. Secure Peer-to-Peer Communication: Facilitating private exchanges between individuals by embedding confidential messages within seemingly innocuous data to ensure privacy. Protection of Private Messages in Digital Publishing: Embedding private messages within public content to prevent unauthorized access and ensure secure communication during online transmission.

Inclusion of Redundant Audio or Visual Data: Integrating replacement audio or visual content to address potential degradation or corruption caused by poor connection quality or transmission errors.

FUTURE ENCHANCEMENT

This project holds the potential for further development, enabling its application to various image formats, such as GIF, TIFF, and others. Additionally, it could be extended to encompass other media forms, including audio and video, in future implementations.

The primary objective of this application is to facilitate the discreet concealment of proprietary and sensitive information. The application employs images as the medium for hidden texts, which serve as less conspicuous carriers of textual information compared to other information security methods. This approach confers a strategic advantage over traditional systems by enhancing the covert nature of data concealment.

The application is primarily intended to be used to inconspicuously hide confidential and proprietary information by anyone seeking to hide information. This software has an advantage over other information security systems because the hidden texts are in the form of image, which are not obvious text information carriers.

Because of its user-friendly interface, the application can also be used by anyone who wants to securely transmit private information. The main advantage of this program for individuals is that they do not have to have any knowledge about steganography or encryption. The visual way to encode the text, plus the visual key makes it easy for average users to navigate within the program.

Digital Image Steganography system allows an average user to securely transfer text messages by hiding them in a digital image file. A combination of Steganography and encryption algorithms provides a strong backbone for its security. Digital Image Steganography system features innovative techniques for hiding text in a digital image file or even using it as a key to the encryption.

Digital Image Steganography system allows a user to securely transfer a text message by hiding it in a digital image file. 128 bit AES encryption is used to protect the content of the text message even if its presence were to be detected. Currently, no methods are known for breaking this kind of encryption within a reasonable period of time (i.e., a couple of years).

Additionally, compression is used to maximize the space available in an image. The application is primarily intended to be used to inconspicuously hide confidential and proprietary information by anyone seeking to hide information. This software has an advantage over other information security systems because the hidden texts are in the form of image, which are not obvious text information carriers.

Because of its user-friendly interface, the application can also be used by anyone who wants to securely transmit private information. The main advantage of this program for individuals is that they do not have to have any knowledge about steganography or encryption. The visual way to encode the text, plus the visual key makes it easy for average users to navigate within the program.

Digital Image Steganography system allows an average user to securely transfer text messages by hiding them in a digital image file. A combination of Steganography and encryption algorithms provides a strong backbone for its security. Digital Image Steganography system features innovative techniques for hiding text in a digital image file or even using it as a key to the encryption.

Digital Image Steganography system allows a user to securely transfer a text message by hiding it in a digital image file. 128 bit AES encryption is used to protect the content of the text message even if its presence were to be detected. Currently, no methods are known for breaking this kind of encryption within a reasonable period of time (i.e., a couple of years).

Additionally, compression is used to maximize the space available in an image. The application is primarily intended to be used to inconspicuously hide confidential and proprietary information by anyone seeking to hide information.

This software has an advantage over other information security systems because the hidden texts are in the form of image, which are not obvious text information carriers. Because of its user-friendly interface, the application can also be used by anyone who wants to securely transmit private information. The main advantage of this program for individuals is that they do not have to have any knowledge about steganography or encryption. The visual way to encode the text, plus the visual key makes it easy for average users to navigate within the program.

Digital Image Steganography system allows an average user to securely transfer text messages by hiding them in a digital image file. A combination of Steganography and encryption algorithms provides a strong backbone for its security. Digital Image Steganography system features innovative techniques for hiding text in a digital image file or even using it as a key to the encryption.

Because of its user-friendly interface, the application can also be used by anyone who wants to securely transmit private information. The main advantage of this program for individuals is that they do not have to have any knowledge about steganography or encryption. The visual way to encode the text, plus the visual key makes it easy for average users to navigate within the program.

Digital Image Steganography system allows an average user to securely transfer text messages by hiding them in a digital image file. A combination of Steganography and encryption algorithms provides a strong backbone for its security. Digital Image Steganography system features innovative techniques for hiding text in a digital image file or even using it as a key to the encryption. Because of its user-friendly interface, the application can also be used by anyone who wants to securely transmit private information. The main advantage of this program for individuals is that they do not have to have any knowledge about steganography or encryption. The visual way to encode the text, plus the visual key makes it easy for average users to navigate within the program. Digital Image Steganography system allows an average user to securely transfer text messages by hiding them in a digital image file. A combination of Steganography and encryption algorithms provides a strong backbone for its security. Digital Image Steganography system features innovative techniques for hiding text in a digital image file or even using it as a key to the encryption.

REFERENCE

1. Multi-Image Steganography Using Deep Neural Networks (Abhishek Das, Japsimar Singh Wahi, Mansi Anand, Yugant Rana 2021) found online ahttps://paperswithcode.com/paper/multi-image-steganography-using-deep-neural

2. Image Steganography(Authors: Nandhini Subramanian; Omar Elharrouss; Somaya Al Maadeed; Ahmed Bouridane 2021)found online athttps://link.springer.com/chapter/10.1007/978-3-642-27183-0_21

3. An Automatic Cost Learning Framework for Image Steganography Using Deep Reinforcement Learning (Weixuan Tang, Bin Li, Mauro Barni, Jin Li, Jiwu Huang 2020) found online at https://paperswithcode.com/paper/an-automatic-cost-learning-framework-for

4. Fixed Neural Network Steganography (Varsha Kishore, Xiangyu Chen, Yan Wang, Boyi Li, Kilian Q Weinberger 2022) https://paperswithcode.com/paper/fixed-neural-network-steganography-train-the
5. https://paperswithcode.com/task/image-steganography

6. http://umpir.ump.edu.my/id/eprint/4978/1/CD6559.pdf

7. https://www.ijcsit.com/docs/Volume%206/vol6issue01/ijcsit20150601152.pdf

8. https://www.irjmets.com/uploadedfiles/paper/issue_3_march_2023/34156/final/fin_irjmets1678290311.pdf

9. https://www.ijsr.net/archive/v11i5/SR22511125940.pdf

10. https://www.researchgate.net/publication/216052617_DIGITAL_IMAGE_STEGANOGRAPHY

11. https://www.researchgate.net/publication/220803240_An_overview_of_image_steganography