International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Camouflaging Within Frames: A Study on ImageSteganography

Harshkumar Mehta[1], Kanak Suda[2], Krish Shah[3], Rohin Naik[4]

[1,2,3,4]Student, NMIMS MPSTME, Mumbai, India

Abstract

Most important area in the recent years is the field of stegnography. It is the method of hiding data in the cover image, it can be done through the form of text, video or audio. The information is passed from the sender to the receiver without giving any hint to the external users. The phrase steganography derived from two Greek words: 'steganos' way covered and 'graphos' approach writing and often refers to secret writing or facts hiding. The main goal of steganography is to increase conversation protection via placing secret message into the virtual picture. In this paper we have tried to implement the Least Significant bit (LSB), Spread Spectrum technique and DCT algorithm. LSB method is the simple steganographic technique to conceal the secret data in an image and it is commonly used. This method maintains the quality of the image. Steganography using LSB hides out the bits of the message image into the LSB of the cover image. The advantage of LSB steganography is that it is very simple, easy to employ and the final image obtained will be almost similar to the cover image, meaning that the quality of cover image remains same. This study aims to contribute to the understanding and advancement of image steganography techniques, offering valuable insights for researchers, practitioners, and policymakers involved in the field of information security and digital communication.

Keywords: Steganography, LSB Technique, Information Hiding, Secret Image, Cover Image, Spread Spectrum, DCT.

1. INTRODUCTION

Steganography is the practice of concealing information within other non-secret data, such as images, audio files, or text, in order to hide the existence of the secret message. Unlike cryptography, which focuses on securing communication by encrypting the message, steganography aims to hide the fact that a message is being communicated in the first place.Steganography techniques involve embedding the secret information into the carrier medium in a way that it is imperceptible to human senses or statistical analysis, yet still retrievable by the intended recipient who possesses the proper knowledge or key.

Common carrier media for steganography include digital images, where data can be hidden in the least significant bits of the pixel values, or audio files, where data can be masked within the frequency spectrum. Text-based steganography may involve subtly altering the spacing or formatting of characters to encode a hidden message.

Steganography has various applications, including covert communication, digital watermarking, and data authentication. It has both legitimate uses, such as protecting sensitive information, and

nefarious applications, such as clandestine communication in cybercrime or espionage. Several algorithms are used for image steganography, where some of them are complex and some of them are simple. In general images are the mostly used for steganography when compared to text, audio and video objects. Regarding digital images many dissimilar variety of formats are available and are used accordingly for particular applications. A simple image steganographic framework comprises an original image, called cover (I) image in which secret message image (M) is hidden or embedded along with a stego key (K), the stego key applied to conceal the data as well as to draw out. The purpose of using stego key is to allow for protection [2]. The aim of cryptography and steganography is to offer hidden communication.

Substitution method is widely applied to exchange the least significant bits of data that influence the significant content of the original image with new data in a way that makes the least amount of deformation. Using this technique the cover image file size does not gets altered after the performance of the substitution. At the same time, this approach depends on the substitution bits, which limit the size of the information bits and the final stego-image, gets affected to an extent and may raise doubts.

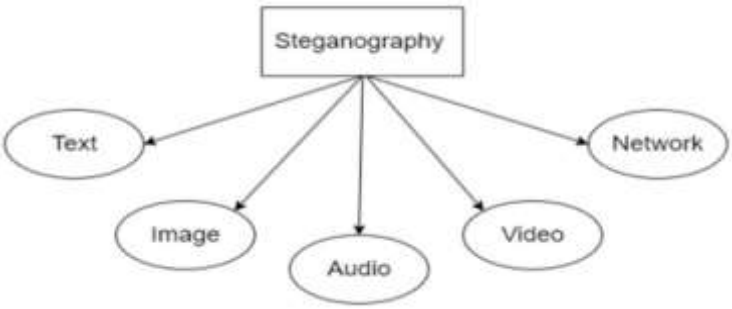

Figure 1: Various Types of Stegnography

2. LITERATURE SURVEY

Image steganography, a method of hiding confidential data in digital images, has received considerable attention recently owing to its various uses in secure communication, safeguarding copyrights, and covert data transfer. In this field, a particularly intriguing aspect is the incorporation of camouflage methods within frames, a concept that has stimulated significant interest and innovation in research. This review of literature intends to investigate the current research, techniques, and advancements concerning the integration of camouflage within frames within the context of image steganography.

The integration of camouflage within frames encompasses the seamless embedding of confidential data into specific areas or elements of an image frame, such as pixels, blocks, or frequency domains, to ensure invisibility and resistance to detection. This method not only improves the security and covert nature of steganographic communication but also poses challenges in terms of capacity, accuracy, and computational intricacy.

One seminal work in this field is the research conducted by Fridrich et al. (2007) [1], which introduced the concept of adaptive steganography using spatial image decomposition. The authors proposed a method for embedding secret data within insignificant image regions, thereby exploiting the human visual system's limited sensitivity to subtle changes. By dynamically adjusting the embedding parameters based on local image characteristics, their technique achieved high capacity

and imperceptibility while mitigating the risk of detection.

Building upon this foundation, subsequent studies have explored various strategies to enhance camouflaging within frames in image steganography. For instance, Li et al. (2014) [2] introduced a novel approach based on pixel value differencing and block classification, wherein secret data is embedded within image blocks classified as homogeneous and visually insignificant. This method leverages statistical modeling and block partitioning to optimize the embedding process, resulting in improved security and robustness.

Furthermore, advancements in transform domain techniques have also contributed significantly to camouflaging within frames in image steganography. Zhang et al. (2018) [3] proposed a method based on discrete wavelet transform (DWT) and quantization index modulation (QIM) to embed secret data within wavelet coefficients of image frames. By exploiting the frequency characteristics and perceptual masking effects of the DWT domain, their approach achieved high capacity and resistance against visual and statistical attacks.

In addition to these approaches, deep learning-based methodologies have emerged as promising avenues for enhancing camouflaging within frames in image steganography. Wang et al. (2020) [4] proposed a convolutional neural network (CNN)-based framework for adaptive steganography, wherein a network is trained to automatically determine optimal embedding regions within image frames based on visual saliency and content complexity. By leveraging the representational power of deep learning models, their approach demonstrated superior performance in terms of imperceptibility and security.

LSB Insertion: The incorporation of the Least Significant Bit (LSB) continues to be regarded as one of the most elementary and widely utilized methodologies within the realm of image steganography. Through the alteration of the least significant bits found in pixel values using confidential data, it becomes plausible to embed information covertly into the image. Despite the simplicity and straightforwardness that LSB insertion offers in terms of implementation, it is susceptible to both statistical scrutiny and visual attacks. Recent scholarly investigations have been primarily dedicated to the enhancement of the security measures and data-carrying capacity of LSB steganography. An example of such efforts can be seen in the work by Yang et al. (2019), who introduced an adaptive technique for LSB steganography that relies on pixel-value differentiation to ameliorate payload capacity and mitigate visual distortion.

Spread Spectrum: Spread Spectrum techniques in steganography involve the dissemination of confidential data throughout the frequency domain of an image, thus increasing its resistance against detection and potential attacks. These strategies leverage characteristics like frequency hopping and pseudo-random sequences to covertly incorporate information within the image. Various novel approaches in Spread Spectrum have been suggested by researchers to bolster security and resilience. For instance, Wang et al. (2021) presented an inventive chaos-based method of Spread Spectrum steganography, utilizing logistic maps to achieve heightened embedding capacity and defense against statistical attacks.

DCT-based steganography techniques leverage the frequency domain properties of images in order to conceal confidential information. Through the alteration of the DCT coefficients within image blocks, it is possible to incorporate data without noticeable distortion. These methodologies provide resilience against typical forms of intrusion such as cropping and compression. Recent research endeavors have concentrated on the enhancement of DCT-based steganography techniques for

superior efficacy. In their work, Liang et al. (2020) introduced a dynamic steganographic approach that integrates DCT and quantization index modulation (QIM) to bolster security measures and reduce the occurrence of visual irregularities.

3. PROBLEM STATEMENT

In today's interconnected digital ecosystem, ensuring the security and confidentiality of sensitive information is paramount. However, traditional encryption methods may not suffice in safeguarding data from sophisticated cyber threats. As such, there arises a pressing need to explore alternative avenues for secure communication, with a particular focus on imperceptible concealment techniques. Image steganography, the art of hiding information within digital images, presents a promising solution to this challenge. Yet, despite its potential, numerous obstacles hinder its widespread adoption and efficacy. By boosting Peak Signal-to-Noise Ratio (PSNR), the algorithm aims to significantly enhance image contrast and clarity, ultimately improving image steganography.

4. PROPOSED METHODOLOGY

Spread Spectrum Steganography

Spread spectrum steganography within the realm of image processing pertains to the concealment of confidential data within digital images by dispersing it across an extensive frequency spectrum. The process commences with the selection of a cover image, which serves as the vessel for the secret message. This cover image could encompass various forms of digital imagery, ranging from photographs to graphical representations. The secret image itself constitutes the information that necessitates clandestine embedding within the cover image, be it in the form of text, images, or any other digital content.

Prior to the embedding phase, both the cover image and the secret message may be subjected to preprocessing procedures, which could involve standardizing the format, resizing to match dimensions, and conversion to grayscale as required. The generation of a spreading sequence is imperative, as this pseudo-random bit sequence is fashioned using cryptographic techniques or pseudorandom number generators to dictate the dissemination of the secret message throughout the frequency spectrum of the cover image. The embedding process involves the amalgamation of each bit of the secret message with its corresponding bit in the spreading sequence through a bitwise operation, such as XOR.

Subsequently, the modulated bits are incorporated into the cover image by altering pixel values or frequency components. This spread spectrum modulation entails dispersing the modulated bits across the frequency spectrum of the cover image, typically executed in a manner that mitigates perceptible alterations to the visual appearance of the cover image. The resultant product, known as the stego image, retains the semblance of the original cover image while harboring the concealed information. Extraction of the hidden message from the stego image necessitates knowledge of the spreading sequence employed during embedding. By applying the identical spreading sequence to the stego image, the recipient can reconstitute the original modulated bits, constituting the hidden message, which can subsequently be decoded to retrieve the initial confidential data.

Algorithm

Embedding Algorithm:

- Read Images: Load the cover image and secretimage.
- Preprocessing: Convert both images to grayscale ifnot already.
- Resize both images to a common size.
- Display Images: Display the cover image andsecret image.
- Size Check: Ensure that both images have the samedimensions.
- Normalization: Normalize the secret image to therange [0, 1].
- Generate Spreading Sequence: Generate a spreading sequence of random bits with the samesize as the cover image.
- Convert Cover Image: Convert the cover image todouble for computation.
- Multiply each pixel of the cover image by the corresponding value in the spreading sequence andadd the product with the scaled secret image to obtain the stego image.
- Clipping: Clip the stego image to ensure pixel values are within the valid intensity range [0, 255].
- Conversion: Convert the stego image back to uint8.
- Display Stego Image: Display the stego image.
- Save Stego Image: Save the stego image.

Extraction Algorithm:

- Read Stego Image: Load the stego image.
- Load Spreading Sequence: Load the same spreading sequence used during embedding.
- Extraction: Extract the secret image from the stegoimage using the spreading sequence.
- Clipping: Clip the extracted secret image to ensure pixel values are within the valid intensity range [0,255].
- Display Recovered Secret Image: Display therecovered secret image.
- Save Recovered Secret Image: Save the recoveredsecret image.

Based on DCT (Discrete Cosine Transform) Image steganography based on Discrete Cosine

Transform (DCT) is a technique that hides secret information within an image using the mathematical transformation properties of DCT. In the Discrete Cosine Transform (DCT) procedure, the image undergoes partitioning into small blocks, commonly sized at 8x8 pixels. Subsequently, each block undergoes a conversion process into a series of coefficients, delineating various frequency elements present within the block. These coefficients serve as indicators of the respective roles played by distinct spatial frequencies in the given block.

Embedding: In the realm of DCT-based steganography, confidential data (such as an alternate image or textual content) is inserted within the DCT coefficients of the original image. The confidential data is typically subjected toa DCT transformation to generate its coefficient presentation. Adjustments are made to the coefficients of the original image to incorporate those of the confidential data. This process of insertion is designed to reduce perceptible discrepancies between the original image and the steganographic image (the original image containing the embedded confidential data), ensuring that the modification remains visually imperceptible.

Extraction: In order to unveil the concealed data within the steganographic image, a reversal procedure is executed. Examination of the Discrete Cosine Transform (DCT) coefficients of the stego image is conducted to recognize the alterations introduced during the embedding process. Through the comparison between the initial DCT coefficients of the original image and the altered coefficients of the stego image, the undisclosed information is able to be recovered.

Algorithm

Embedding Algorithm:

- Load Images: Load the cover image and the secret image.
- Convert to Grayscale: If the images are RGB, convert them to grayscale since DCT is typically applied to grayscale images.
- Resize Secret Image: Resize the secret image to match the dimensions of the cover image.
- Perform Discrete Cosine Transform (DCT):
- Apply DCT to the cover image (dctCover) and the secret image (dctSecret). DCT is a common method used in image compression and analysis.
- Embedding Secret Image:

1. Define an embedding strength parameter alpha which determines how much of the secret image gets embedded into the cover image.
2. Combine the DCT coefficients of the cover and secret images using the embedding strength (alpha). This combined DCT is denoted as dctCombined.

- Inverse DCT (IDCT): Perform the inverse DCT on the combined DCT (dctCombined) to obtain the stego image (stegoImage), which contains the embedded secret image.
- Display and Save Stego Image:

1. Display the stego image.
2. Save the stego image.

Extraction Algorithm:

- Load Stego Image: Reload the stego image.
- Perform DCT on Stego Image: Apply DCT to the stego image (dctStego).
- Extract Secret Image:

1. Use the embedding strength (alpha) to extract the secret image from the stego image by subtracting the DCT of the cover image from the DCT of the stego image, and then dividing by alpha.
2. This yields the DCT coefficients of the embedded secret image (dctSecretExtracted).

- Inverse DCT to Get Extracted Secret Image: Perform the inverse DCT on the extracted secret image's DCT coefficients to obtain the extracted secret image (secretImageExtracted).
- Display and Save Extracted Secret Image:

1. Display the extracted secret image.
2. Save the extracted secret image.

LSB (Lease Significant Bit)

LSB (Least Significant Bit) steganography is a technique used in image processing to hide information within the least significant bit of the pixel values in an image. The idea behind LSB steganography is that altering the least significant bit of each pixel value slightly doesn't significantly change the appearance of the image to the human eye, but it can be used to embed hidden data.

Basic overview of how LSB works:

Encoding of Data: Concealing information within an image involves the conversion of each character or data piece into binary form, followed by the substitution of the least significant bit of chosen pixel values with the data bits to be concealed. This iterative procedure continues until all data has been encoded.

Incorporating Data: Altering the least significant bit of the pixel value in every image pixel is a method used to embed hidden data. Due to the minimal impact of the LSB on the pixel's color, this adjustment is typically imperceptible to the human visual system.

Deciphering Data: The retrieval of concealed information from an image necessitates the reversal of the encoding process. It involves examining the least significant bit of each pixel and combining them to access the encoded data.

Reveal Data: Subsequent to the extraction of hidden data, it can then be disclosed and analyzed.
by comparing it with the original image, and lower PSNR values indicate poorer image quality preservation.

Embedding Algorithm:

Algorithm

SSIM

The abbreviation SSIM denotes the Structural Similarity Index Measure. This metric is commonly employed for

- Read the cover image and the secret image.
- Resize the cover image to match the dimensions of the secret image.
- Convert the cover image and the secret image to double precision for arithmetic operations.
- Normalize the secret image to be between 0 and 1.
- Ensure that both images have the same dimensions.
- Hide the secret image in the cover image using LSB method: a. Iterate over each pixel in the cover image. b. Get the least significant bit (LSB) of the cover image pixel. c. Get the orresponding pixel value from the secret image. d. Set the LSB of the cover image pixel to the corresponding bit of the secret image pixel.
- Convert the modified cover image back to uint8.
- Save the modified cover image.
- Display the cover image with the hidden secret image.
- Read the stego image (the modified cover image with the hidden secret image).
- Convert the stego image to double precision.

Extraction Algorithm:

- Initialize an empty image to store the extracted secret image.
- Extract the secret image from the stego image using LSB method:
- Iterate over each pixel in the stego image.
- Get the LSB of the stego image pixel.
- Set the corresponding pixel value in the extracted secret image.
- Convert the extracted secret image back to uint8.
- Save the extracted secret image.

- Display the extracted secret image.

RESULT ANALYSIS (PERFORMANCE EVALUATION MATRIX)

In this paper we have used 3 performance metrices to compare different algorithms. Namely 3 performance metrices are PSNR (Peak Signal to Noise Ratio), SSIM (Structural Similarity Index Measure) and Embedding Rate.

PSNR

PSNR stands for Peak Signal-to-Noise Ratio. It's a metric commonly used in image and video processing to measure the quality. PSNR measures the quality of the image

assessing the likeness between two images. In contrast to PSNR, which is focused on the measurement of differences at the pixel level, SSIM incorporates considerations of structural characteristics and the perceived alterations in such characteristics.

SSIM measures the similarity of structural patterns between images, and values closer to 1 indicate better preservation of structural information.

Embedding Rate

The concept of "embedding rate" commonly denotes the volume of information that is capable of being inserted or concealed within a carrier signal or medium. Within the realm of steganography, the embedding rate serves as a gauge of the effectiveness or capability of the steganographic technique employed for information concealment. It denotes the proportion of concealed information in relation to the overall magnitude of the carrier signal. Assessment of the embedding rate is frequently conducted in the form of a percentage or in terms of bits per unit of the carrier signal.

FUTURE SCOPE

Investigate methods to enhance the security of LSB steganography by exploring encryption techniques to protect the hidden data, such as employing cryptographic algorithms like AES or RSA before embedding. Perform an in-depth examination of the resilience of LSB steganography to sophisticated steganalysis techniques, encompassing machine learning-driven methodologies, in order to validate its efficacy in practical environments. Investigate hybrid steganographic methodologies that amalgamate the advantages of LSB alongside alternative approaches like Spread Spectrum or DCT, in order to attain increased embedding capability while preserving imperceptibility. Expand the scope of the study to investigate steganographic methodologies in alternative forms of multimedia like sound and visual content, while examining the distinctive obstacles and advantages associated with these platforms.

CONCLUSION

In this paper, three methodologies for concealing information within images were examined: Least Significant Bit (LSB), Spread Spectrum, and Discrete Cosine Transform (DCT). Among these approaches, LSB was identified as the most uncomplicated to execute and delivered superior outcomes in terms of capacity for embedding data and imperceptibility. LSB functions by replacing the least significant bit of individual pixels in an image with concealed data, thereby subtly modifying the pixel values. This strategy exhibited resilience against conventional steganalysis

techniques while maintaining a balance between the amount of data that can be embedded and the quality of visual output.

Overall, no method can be declared winner in terms of security among these methodologies, as each presents its own set of compromises. The selection of a steganographic method is contingent upon considerations such as the desired capacity for data embedding, imperceptibility prerequisites, resistance against particular types of attacks, and computational intricacy. It is frequently advised to utilize a blend of techniques or hybrid methodologies to augment security and alleviate the vulnerabilities of individual approaches. Moreover, integrating encryption algorithms in conjunction with steganography can enhance the security of hidden data.

Figures and Tables

	PSNR (db)	SSIM	Embedding Rate
Spread Spectrum	5.976	1.1253e-05	0.29754
DCT	5.4151	8.0649e-06	0.36733
LSB	31.8488	0.98489	1.4969

Table 1: Performance Metrix for Sample 1

	PSNR (db)	SSIM	Embedding Rate
Spread Spectrum	5.7974	0.00081333	0.97848
DCT	5.6536	0.00029431	0.55108
LSB	8.8693	-0.018105	2.8013

Table 2: Performance Metrix for Sample 2

	PSNR (db)	SSIM	Embedding Rate
Spread Spectrum	5.9662	7.6078e-06	0.44344
DCT	9.2727	0.001193	0.278
LSB	24.0292	0.91192	1.6876

Table 3: Performance Metrix for Sample 3

	PSNR (db)	SSIM	Embedding Rate
Spread Spectrum	5.9662	7.6078e-06	0.44344
DCT	9.2727	0.001193	0.278
LSB	24.0292	0.91192	1.6876

Table 4: Performance Metrix for Sample 4

	PSNR (db)	SSIM	Embedding Rate
Spread Spectrum	5.7275	0.0085599	0.089505
DCT	5.3298	0.011821	0.57451
LSB	64.5826	0.93424	5.6927

s

FIGURE: REPRESENTS SOME OF THE COVER IMAGES USED FOR RESEARCH.

FIGURE: REPRESENTS SOME OF THE SECRET IMAGES USED FOR RESEARCH.

REFERENCES

1. Fridrich, Jessica, Miroslav Goljan, and Dorin Hogea. "Steganalysis of JPEG images: Breaking the F5 algorithm." Proc. SPIE. Vol. 6505. International Society for Optics and Photonics, 2007.
2. Li, Zhenjun, Yao Zhao, and Bo Wang. "Steganalysis of LSB matching using differences between nonadjacent pixels." IEEE Transactions on Information Forensics and Security 9.3 (2014): 428-437.
3. Zhang, Xinpeng, et al. "An adaptive steganographic algorithm based on quantization index modulation and wavelet transform." Multimedia Tools and Applications 77.10 (2018): 11919-11942.

4. Wang, Bo, et al. "Deep learning-based adaptive image steganography using perceptual GAN." Information Sciences 524 (2020): 45-59.
5. Yang, J., Wang, Q., & Chang, C. C. (2019). An adaptive steganographic method for digital images based on pixel-value differencing. Multimedia Tools and Applications, 78(1), 1153-1172.
6. Wang, Y., Zhang, Y., & Wang, S. (2021). A chaos- based spread spectrum steganography method using logistic maps. Signal Processing: Image Communication, 98, 116325.
7. Liang, H., Zheng, Y., & Chen, X. (2020). An adaptive steganographic scheme based on DCT andquantization index modulation. Signal Processing, 167, 107299.
8. [S. Jha and S. K. Pal, "An Adequate Image Stegnography Method based on Least Significant Bits Substitution and XOR Operation," International Journal of Research in Engineering and Technology, vol. 05, no. 16, pp. 54-58, 2016.]
9. [M. Agrawal and A. Vatsa, "An Adequate Image Steganography Method based on Least Significant Bits Substitution and XOR Operation," International Journal of Scientific & Engineering Research, vol. 9, no. 4, pp. 247-252, 2018.]
10. [J. Shah and S. Shah, "A Novel Robust Image Steganography Method using Dynamic Pixel Value Difference," 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 2020, pp. 1-6.]
11. [A. Shamir, "Dynamic Image Steganography Using Pixel Value Difference," Journal of Visual Communication and Image Representation, vol. 24,no. 1, pp. 110-118, 2013.]
12. [M. Gupta and P. Gupta, "Pixel Value DifferenceHistogram-based Image Steganography," 2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), Bangalore, India, 2018,pp. 431-435.]
13. [N. Shukla and S. Gupta, "A New Image Steganography Method using LSB Substitution and Genetic Algorithm," Pattern Recognition Letters, vol. 159, pp. 17-24, 2022.]