International Journal of Engineering Trends and Technology
ISSN: 2231–5381 / https://doi.org/10.14445/22315381/IJETT-V71I11P229

Volume 71 Issue 11, 276-285, November 2023

Review Article

Digital Image Steganography and Steganalysis: A Comprehensive Review of Evolution of Advanced Techniques

[1]Sunil Kumar, [2]Sudeshna Chakraborty

[1,2]Shri Venkateshwara University, Gajraula, Uttar Pradesh, India.

[1]Corresponding Author : dsksaini05@gmail.com

Received: 20 July 2023 Revised: 22 September 2023 Accepted: 2 October 2023 Published: 04 November 2023

Abstract *- Steganalysis is the process of detecting the presence of hidden information, such as a message or data, within another message or data. The goal of steganalysis is to identify the presence and type of steganography technique used to hide the information, which can be important for various applications, including law enforcement, intelligence gathering, and cyber security. Therefore, steganography techniques can thought of as hiding information in various types of media, such as images, videos, audio files, and even text data. While steganography techniques for media-based data, such as images and videos, have gained more attention in recent years, steganography for text data has been used for much longer. In fact, the concept of text steganography can be traced back to ancient Greece, where messages were hidden within wax tablets by writing them in between the lines of text. Text steganalysis techniques typically involve analyzing the statistical properties of the text, such as word frequency or character frequency distributions. Other techniques include analyzing the structure and syntax of the text, as well as performing linguistic analysis to identify patterns that may indicate the presence of hidden information. In this study, we shall perform a systematic study of the evolvement of traditional as well as contemporary techniques. The study will also reflect how generative artificial intelligence has impacted the quality of digital image steganography.*

Keywords *- Digital Image Steganalysis, Steganography, Encryption.*

1. Introduction

In the early days of steganography, it was relatively easy to detect hidden messages because the techniques were fairly basic and often relied on simple manipulation of an image's Least Significant Bits (LSBs). As a result, steganalysis techniques were initially focused on detecting these basic LSB-based steganography methods. However, as steganography techniques became more advanced and started using higher-order bits or other more complex methods, steganalysis methods had to evolve as well. The field of steganalysis started to incorporate more advanced statistical analysis techniques, such as chi-square analysis, histogram analysis, and wavelet analysis.

These techniques allowed steganalysis to detect more sophisticated steganography methods that manipulated image data more complexly. As the digital age progressed and the amount of data being transmitted online exploded, steganography became increasingly important as a means of hiding sensitive information within seemingly innocuous files, including images. As a result, steganalysis methods continued to evolve to keep pace with new steganography techniques. One key development was the increased use of machine learning algorithms in steganalysis, which allowed analysts to detect hidden messages more accurately and efficiently.

In addition to advances in the underlying techniques used in steganalysis, the field has also seen increased collaboration between researchers and practitioners in law enforcement, intelligence gathering, and cyber security. This collaboration has helped drive innovation and development in the field and increase the impact and effectiveness of steganalysis methods in real-world applications. Today, steganalysis continues to be an important area of research as the use of steganography for hiding information continues to evolve and become more sophisticated. As a result, steganalysis researchers must continue to innovate and develop new techniques to keep up with the changing landscape of digital communication and data transmission. In the early days of steganography, the techniques used to hide information were often quite simple and could be easily detected by basic steganalysis techniques. Some of the most common techniques included changing the order of letters in a message, using invisible ink, or writing messages in code. While these techniques may have been effective in some cases, they were also quite limited in

reliability and security. For example, messages written in invisible ink could be revealed by a number of methods, such as heating the paper or using special chemicals. Similarly, an attacker could decipher code-based techniques with access to the key or algorithm used to encrypt the message.

As technology advances, steganography techniques have become more sophisticated, making them more difficult to detect and more reliable in concealing information. Modern steganography techniques can hide messages within digital media, such as images or audio files, using complex mathematical algorithms that make the hidden information virtually undetectable to even advanced steganalysis techniques. However, it is important to note that steganography techniques are not foolproof, and there are still limitations and potential vulnerabilities that skilled attackers can exploit. For example, some steganography techniques may be vulnerable to attacks that exploit weaknesses in the underlying encryption or data transmission protocols. Additionally, the use of steganography itself can be a red flag that prompts further investigation, which may lead to the discovery of hidden information.

2. Literature Review

Pan et al. (2000) [1] proposed a secure data-hiding scheme for two-color images. The scheme embeds data into the least significant bits of the image using a secret key. The authors suggested that the scheme is robust against cropping, rotation, and JPEG compression attacks. They also claimed that the proposed scheme maintains good visual quality. Grover (2001) [2] provided an overview of digital data watermarking and discussed the difference between steganography and watermarking. The author highlighted the legal implications of data watermarking, including the need for copyright protection. Grover pointed out that watermarking techniques are imperfect and can be removed by attackers. He emphasized the importance of developing more robust watermarking techniques that can withstand different attacks. Johnson et al. (2001) [3] presented an overview of steganography and its various techniques. The authors discussed the applications of steganography in different domains, such as military, espionage, and entertainment. They highlighted the challenges of steganography, including the need for large amounts of data to hide a small amount of information and the difficulty of detecting steganographic messages. The authors also suggested future research directions to improve the security and robustness of steganographic techniques.

Lee and Chen (2002) [4] proposed an object-based image steganography technique using affine transformations. The authors suggested that their method is more robust against different attacks, such as cropping and scaling, compared to other existing methods. They also claimed that their method achieves higher embedding capacity and lower distortion. Pal and Madhavan (2002) [5] investigated steganographic communication techniques and their potential applications.

The authors presented a survey of different steganographic techniques and discussed the challenges of detecting steganographic messages. They suggested steganography can be used for covert communication, espionage, and digital watermarking. Fridrich and Goljan (2002) [6] presented a practical steganalysis technique for digital images. The authors suggested that their method is more robust and reliable than other existing methods. They highlighted the importance of steganalysis in detecting hidden messages and suggested future research directions to improve the accuracy and efficiency of steganalysis.

Bailey et al. (2003) [7] provided an overview of steganography in images. The authors discussed the different techniques for hiding data in images and highlighted the importance of detecting steganographic messages. They also discussed the challenges of steganography, including the trade-off between embedding capacity and distortion, and suggested future research directions to improve the security and robustness of steganography. Adnan et al. (2003) [8] reviewed image watermarking techniques and their applications. The authors presented a survey of different image watermarking techniques and discussed the challenges of embedding and detecting watermarks in images. They suggested that watermarking can be used for copyright protection, authentication, and tamper detection.

Chandramouli et al. (2004) [9] an overview of image steganography and steganalysis. The authors discussed the different techniques for hiding data in images and detecting hidden messages. They also discussed the challenges of steganography, including the need for large amounts of data to hide a small amount of information and the difficulty of detecting steganographic messages. The authors suggested future research directions to improve the security and robustness of steganography. Wu et al. (2004) [10] proposed an iterative method of palette-based image steganography. The authors suggested that their method achieves high embedding capacity and low distortion compared to other existing methods. They also claimed that their method is more robust against different attacks, such as cropping and scaling. The authors suggested future research directions to improve the security and robustness of the palette.

Duric et al. (2005) [11], in a chapter in the "Handbook of Statistics", provides an overview of steganography and steganalysis. It explains the concept of information hiding, the goals of steganography, and the methods used to hide information. The chapter also discusses steganalysis techniques, which are used to detect hidden information, and the challenges associated with it. Martin et al. (2005) [12] examine whether the process of steganography can produce natural-looking images. The study compares the results of different image steganography techniques and evaluates the resulting images using perceptual quality measures. The

authors conclude that some steganography methods can produce natural-looking images while others cannot. Hashad et al. (2005) [13] present a new steganography technique that uses Discrete Cosine Transform (DCT) to hide information in an image. The proposed technique inserts the secret data into the image's frequency domain using DCT, making it difficult for steganalysis tools to detect the hidden information. The authors evaluate the proposed technique and show it can achieve high capacity and robustness.

Kharrazi et al. (2006) [14] propose a new steganalysis approach that combines multiple techniques to improve detection accuracy. The study uses fusion techniques to combine the results of several steganalysis tools and evaluates the performance using image steganography as a case study. The authors show that the proposed approach can significantly improve the detection accuracy compared to individual steganalysis tools. Torres-Maya et al. (2006) [15] present a new image steganography system based on Bit Plane Complexity Segmentation (BPCS) and Integer Wavelet Transform (IWT). The proposed system uses BPCS to segment the image into different bit-planes and IWT to embed the secret data into the low-frequency sub-bands. The authors evaluate the proposed system and how it can achieve high capacity and robustness. Wang and Chen (2006) [16] propose a new image steganography method that uses two-way block matching to embed the secret data. The proposed method divides the cover image into blocks and searches for a matching block in a pre-defined database to embed the secret data. The authors evaluate the proposed method and show it can achieve high payload and good visual quality.

Parvez et al. (2019) [17] provide a comprehensive survey of image steganography in their review article. The article covers different image steganography techniques, evaluation metrics, and recent trends in steganography research. The authors also highlight the challenges associated with image steganography and provide directions for future research. A (2008) [18] proposes a new image steganography method that uses the intensity values of the RGB color channels to embed the secret data. The proposed method adjusts the number of embedded bits based on the intensity values to achieve high capacity and good visual quality. The author evaluates the proposed method and shows that it can achieve high capacity and good robustness.

Kharrazi et al. (2007) [19] provided a comprehensive overview of image steganography and steganalysis. The paper presents different concepts of steganography, including various techniques and challenges in the field of image steganography, and covers different steganalysis approaches. The authors discussed steganalysis techniques such as histogram-based, model-based, and feature-based, and they provided a survey of the state-of-the-art in steganography and steganalysis.

Chang et al. (2008) [20] present a new method for sharing secrets in stego images with authentication. The paper proposes a scheme that enables the sender to embed a secret message into a cover image and creates a stego image with an embedded secret message. The receiver can extract the secret message from the stego image using the authentication code. The proposed scheme also ensures the integrity and authenticity of the secret message. The authors demonstrate that the proposed scheme is more secure and robust than existing methods for sharing secrets in stego images.

Jalil et al. (2009) [21] discussed various techniques for digital watermarking, including visible and invisible watermarking, spread spectrum-based watermarking, and fragile watermarking. They concluded that the watermarking technique choice depends on the application, data type, and security requirements. Wu et al. (2009) [22] proposed a new approach to secret image sharing with steganography and authentication. The authors used steganography to embed secret images into cover images and authentication to verify the integrity of the secret images. The proposed approach was evaluated through experiments, and the results showed that the method could effectively share secret images with high security.

Cheddad et al. (2010) [23] classified steganography methods into four categories: spatial domain, frequency domain, transformation domain, and hybrid domain. They also discussed various steganalysis techniques used to detect the presence of hidden information in digital images. The authors concluded that combining different steganography techniques could enhance the security and robustness of the steganographic system. Mishra et al. (2015) [24] reviewed various steganography techniques, including image, audio, and video steganography. They also provided a comparison between steganography and cryptography techniques and highlighted the limitations of each technique. The authors concluded that combining steganography and cryptography could enhance the security of data communication—Sharma et al. (2017) [25] reviewed spatial domain techniques based on image steganography. The authors discussed various spatial domain techniques, including LSB substitution, PVD, and Pixel Value Differencing (PVD) techniques. They also provided a comparison between different spatial domain techniques and highlighted the limitations of each technique. The authors concluded that the choice of steganography technique depends on the application, security requirements, and computational complexity.

Kadhim et al. (2019) [26] classified steganography techniques into five categories: LSB-based techniques, spatial do-main techniques, transform domain techniques, compression-based techniques, and hybrid techniques. They also discussed various evaluation metrics used to evaluate the performance of steganographic systems. The authors

concluded that the future research direction in image steganography should focus on enhancing the security and robustness of steganographic systems. Liu et al. (2020) [27] reviewed recent advances in image steganography using Generative Adversarial Networks (GANs). The authors discussed various GAN-based steganography techniques, including GAN-based image steganography and GAN-based text steganography. They also provided a comparison between different GAN-based steganography techniques and highlighted the limitations of each technique. The authors concluded that GAN-based steganography is a promising direction for future research in steganography. Georges et al. (2020) [28] discussed various artificial intelligence approaches, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and generative models. They also provided a comparison between different artificial intelligence approaches and highlighted the limitations of each technique. The authors concluded that combining artificial intelligence and steganography could enhance the security and robustness of steganographic systems. Gabriel et al. (2020) [29] presented a two-layer image-steganography system for covert communication over enterprise networks. The proposed system consists of a secret message encryption layer and a steganography layer for hiding the encrypted message in the cover image. The encryption layer uses the Advanced Encryption Standard (AES) algorithm to encrypt the secret message, while the steganography layer uses the Least Significant Bit (LSB) method to embed the encrypted message in the cover image. The authors evaluate the proposed system using metrics such as Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index Measure (SSIM), and Bit Error Rate (BER) and demonstrate the effectiveness of their system in terms of message-hiding capacity and imperceptibility of the stego-image. The authors conclude with a discussion of future work, including exploring the use of deep learning techniques for improving the security and robustness of the proposed system.

3. Digital Image Steganography Techniques

The field of image steganography has evolved over time, and various techniques have been developed for hiding information in digital images. Here are some of the commonly used techniques for image steganography in chronological order:

3.1. Least Significant Bit (LSB) Substitution

This is one of the earliest and most straightforward techniques for image steganography. In this technique, the least significant bits of the pixel values in an image are replaced with the bits of the secret message to be hidden. As the LSBs of the pixel values have a negligible effect on the overall quality of the image, this technique is often used for embedding messages without affecting the image's visual appearance. The LSB technique can be implemented in different ways. One common approach is to use the LSBs of each pixel's color channels (red, green, and blue) to store the bits of the secret message. For instance, if a message bit is 0, the LSB of the corresponding color channel is set to 0; if it is 1, the LSB is set to 1. The message bits are then retrieved by extracting the LSBs of the color channels.

Another variation of the LSB technique is the LSB matching method, which aims to minimize the distortion caused by the embedding process. In this method, the LSBs of the cover image pixels are slightly modified to match the message bits. By doing so, the changes in the image are made less detectable, making it harder for a steganalysis algorithm to detect the presence of hidden information. Despite its simplicity, the LSB technique has some limitations. Firstly, it is vulnerable to attacks that can detect the changes in the LSBs of the pixels. Secondly, the amount of data that can be embedded using this technique is limited by the number of LSBs available for embedding. Finally, suppose the message is embedded in a small portion of the image. In that case, it may be vulnerable to cropping attacks, where an attacker can remove the hidden message by cropping the image.

Overall, the LSB technique is a widely used and effective method for hiding secret messages in images. However, to ensure the security of the embedded information, it is important to use additional techniques such as encryption, steganography keys, secret sharing, and the LSB technique. Here is a high-level step-by-step description of the LSB technique:

3.2. Masking and Filtering Techniques

These techniques are used to embed information by altering the color values of pixels in an image, making it difficult to detect the embedded data. In masking techniques, the secret data is embedded by replacing the Least Significant Bits (LSBs) of the cover image pixels with the bits of the secret data. This process is usually done systematically so as not to significantly affect the cover image's visual quality significantly. The most commonly used masking technique is the Least Significant Bit (LSB) method, which replaces the LSBs of the cover image pixels with the bits of the secret data. However, the LSB method is vulnerable to attacks since the changes in the LSBs can be detected using statistical analysis. In filtering techniques, the secret data is embedded by modifying the high-frequency components of the cover image. High-frequency components are those parts of the image that contain rapid changes in pixel values, such as edges, textures, and patterns. These high-frequency components are modified to embed the secret data in filtering techniques. One of the major filtering techniques used for image steganography is LBP. Local Binary Pattern (LBP) is a texture descriptor that characterizes the local structure of an image. It is a simple and computationally efficient technique that extracts a histogram of patterns from the image. The LBP technique was first introduced by Ojala et al. in 1996 for facial recognition and

texture classification. The LBP operator works by comparing the gray value of a center pixel to its surrounding pixels. For a given center pixel, the LBP operator assigns a binary code to each surrounding pixel based on whether its gray value is greater than or less than the gray value of the center pixel. This binary code is then converted into a decimal value and stored in a histogram bin. The LBP operator can be applied to images in different ways, such as using a circular neighborhood or a rectangular neighborhood. The choice of neighborhood size and shape can affect the performance of the LBP operator.

LBP has been applied in various fields, including face recognition, texture classification, and image retrieval. One of the advantages of LBP is its robustness to illumination changes, which makes it suitable for use in low-light environments. In steganography, LBP has also been used as a feature extractor for detecting hidden image messages. The algorithm of the LBP method for image steganography is as follows:

- Divide the cover image into non-overlapping blocks of a fixed size.
- Convert each block from the cover image into a grayscale image.
- For each pixel in the grayscale image, compare its intensity value with the intensity values of its 8 surrounding pixels in a 3x3 neighborhood.
- If the intensity value of the center pixel is greater than or equal to the intensity value of the surrounding pixel, assign a value of 1 to that pixel's position in a binary code. Otherwise, assign a value of 0.
- Concatenate the binary codes for all the pixels in the block to form a binary string.
- Divide the binary string into sub-strings of a fixed length, where the length is the number of bits required to represent the maximum value of a secret message symbol.
- Convert each sub-string into an integer value and map it to a corresponding secret message symbol using a pre-defined mapping table.
- Embed the secret message symbol into the cover image block by adding or subtracting the value of the mapped symbol from the intensity value of a selected pixel in the block.
- Repeat steps 3 to 8 for all the blocks in the cover image.
- Output the stego image obtained by combining the stego blocks.

3.3. Transform Domain Techniques

These techniques involve transforming the image into another domain, such as the frequency domain or wavelet domain, and then embedding the message in the transformed coefficients. Transform domain techniques are a type of image steganography technique that operates in the frequency domain of an image, as opposed to the spatial domain. These techniques are based on various mathematical transforms such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT), which convert an image from the spatial domain to the frequency domain.

These techniques divide the image into non-overlapping blocks of fixed size, and the transform is applied to each block. The transformed coefficients are then modified to embed secret information, and the inverse transform is applied to obtain the stego-image. The secret information can be embedded by modifying the transformed coefficients' magnitude, phase, or both.

One of the advantages of transform domain techniques is that they offer better security than spatial domain techniques, as the secret information is hidden in the frequency domain, which is less perceptually significant to the human eye. Furthermore, transform domain techniques are more robust to common image processing operations such as compression and filtering, which makes them suitable for applications where images may undergo such operations.

DCT (Discrete Cosine Transform) is a widely used transform domain technique in image steganography. It transforms the image data from the spatial domain to the frequency domain using a set of cosine functions. The DCT coefficients represent the image content and are commonly used for data hiding. The basic algorithm for DCT-based image steganography involves the following steps:

- Break the image into non-overlapping blocks of a fixed size.
- Compute the DCT of each block using a pre-defined matrix.
- Select a set of DCT coefficients for embedding the secret data. These coefficients should have minimal impact on the visual quality of the image.
- Modify the selected DCT coefficients by a small amount to embed the secret data.
- Reconstruct the image by computing the inverse DCT.

DWT (Discrete Wavelet Transform) is another widely used transform domain technique in image steganography. It transforms the image data from the spatial domain to the frequency domain using a set of wavelet functions. The DWT coefficients represent the image content and are commonly used for data hiding. The basic algorithm for DWT-based image steganography involves the following steps:

- Break the image into non-overlapping blocks of a fixed size.
- Compute the DWT of each block using a pre-defined wavelet function.
- Select a set of DWT coefficients for embedding the secret data. These coefficients should have minimal impact on the visual quality of the image.
- Modify the selected DWT coefficients by a small

amount to embed the secret data.
- Reconstruct the image by computing the inverse DWT

DFT (Discrete Fourier Transform) is a transform domain. The technique transforms the image data from the spatial domain to the frequency domain using a set of complex exponential functions. The DFT coefficients represent the image content and are commonly used for data hiding. The basic algorithm for DFT-based image steganography involves the following steps:
- Break the image into non-overlapping blocks of a fixed size.
- Compute the DFT of each block using a pre-defined matrix.
- Select a set of DFT coefficients for embedding the secret data. These coefficients should have minimal impact on the visual quality of the image.
- Modify the selected DFT coefficients by a small amount to embed the secret data.
- Reconstruct the image by computing the inverse DFT.

All three transform domain techniques have advantages and disadvantages. DCT is computationally efficient and widely used in image and video compression but is sensitive to image rotation and scaling. DWT has good localization properties and is robust to rotation and scaling but computationally intensive. DFT has good frequency resolution but is computationally intensive and has poor localization properties.

3.4. Spread Spectrum Techniques

This technique involves spreading the secret message across multiple pixels in an image, making it harder to detect the embedded data. Spread spectrum techniques refer to the family of techniques that are used to hide or embed data in a signal by spreading it over a wide frequency range. The basic idea behind these techniques is to modify a carrier signal's amplitude, phase or frequency so that the embedded data becomes indistinguishable from the noise. Spread spectrum techniques have found widespread applications in various fields, such as wireless communication, digital watermarking, and steganography.

In the context of steganography, spread spectrum techniques are used to embed secret data in a cover image by spreading it over a wide frequency range. The basic steps involved in spread spectrum steganography are as follows:
- Selection of the cover image: The first step in spread spectrum steganography is to select a cover image that willbe used to hide the secret data.
- Generation of the pseudorandom noise sequence: A Pseudorandom Noise (PN) sequence is generated that will be used to spread the secret data over a wide frequency range. The PN sequence should be statistically random and should have a large period to prevent detection.
- Embedding of the secret data: The secret data is embedded in the cover image by modifying the amplitude, phase, or frequency of the cover image so that the embedded data becomes indistinguishable from the noise.
- Extraction of the secret data: The secret data is extracted from the stego image by using the same PN sequence that was used for embedding.

Spread spectrum techniques can be broadly classified into two categories: direct sequence and frequency hopping.
- Direct sequence spread spectrum: In this technique, the secret data is directly embedded in the cover image by spreading it over a wide frequency range. The PN sequence is added to the cover image by using either additive or multiplicative methods.
- Frequency hopping spread spectrum: In this technique, the secret data is embedded in the cover image by hopping the frequency of the carrier signal. The PN sequence determines the hopping sequence, which is then used to embed the secret data.

One of the advantages of spread spectrum techniques is their robustness to noise and other signal distortions. Since the embedded data is spread over a wide frequency range, it is less susceptible to noise and other signal distortions. However, spread spectrum techniques are computationally expensive and require a large bandwidth for embedding a small amount of data.

3.5. Steganography using Digital Watermarking

In this technique, a watermark is embedded in an image to authenticate and protect the ownership of the image. The watermark can also carry a hidden message.

The aim of watermarking [9] is to make the embedded data imperceptible to human senses while being resilient to various attacks such as compression, cropping, and filtering.

There are two main types of watermarking techniques:
- Spatial Domain Watermarking: This technique embeds the watermark in the spatial domain of the media, where the embedding process is done directly on the pixels of the media. This technique usually adds the watermark by modifying the least significant bits of the pixel values. However, since this method involves direct modification of the original media, it is more susceptible to attacks and may result in visible media degradation.
- Transform Domain Watermarking: This technique is based on transforming the media into a different domain, where the watermark can be added by modifying the transform coefficients instead of the original pixel values. This method is more robust against attacks since it does not involve direct modification of the original media.

The most commonly used transform domain techniques for watermarking are:

- Discrete Cosine Transform (DCT) Watermarking: This technique involves transforming the media into the frequency domain using the DCT, where the watermark is added by modifying the frequency coefficients. The added watermark can be extracted by applying the inverse DCT on the modified coefficients.
- Discrete Wavelet Transform (DWT) Watermarking: This technique involves transforming the media into the frequency domain using the DWT, where the watermark is added by modifying the wavelet coefficients. The added watermark can be extracted by applying the inverse DWT on the modified coefficients.
- Singular Value Decomposition (SVD) Watermarking: This technique involves transforming the media into the frequency domain using SVD, where the watermark is added by modifying the singular values. The added watermark can be extracted by applying the inverse SVD to modified singular values.
- Spread Spectrum Watermarking: This technique involves adding the watermark by embedding it as a small signal in the frequency domain of the media. The added watermark can be extracted by correlating the media with a known pseudorandom sequence.

Watermarking techniques have a wide range of applications in protecting intellectual property rights, content authentication, and data security.

4. State of Digital Image Steganography in Recent Times

In recent years, the field of steganography has been greatly influenced by advancements in Artificial Intelligence (AI) and Machine Learning (ML). Using AI and ML techniques has opened up new possibilities in steganography and allowed for the development of more sophisticated and secure methods for information hiding. One major development in AI-based steganography has been the use of deep learning techniques for image steganography. Deep learning models such as Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs) have been used to develop novel steganographic algorithms that can hide information more efficiently and securely than traditional methods.

For example, GAN-based steganography can generate images with embedded messages virtually indistinguishable from the original image. Another area where AI has made an impact is in the development of steganalysis techniques. Steganalysis is the process of detecting the presence of hidden information in digital media. AI and ML techniques have been used to develop more accurate and efficient steganalysis methods that can detect hidden information even in the presence of sophisticated steganographic algorithms.

Moreover, AI-based steganography has been extended to new areas, such as text steganography and audio steganography. Researchers have used deep learning models to develop text steganography techniques to hide information in natural language text while maintaining its linguistic properties. AI-based audio steganography methods have also been developed to embed information in audio signals while preserving their perceptual quality. Some of the major AI techniques are:

4.1. GAN-Based Steganography

This technique uses Generative Adversarial Networks (GANs) to generate steganographic images. GAN-based steganography involves training a Generative Adversarial Network (GAN) [30] on a dataset of cover images and secret messages. The GAN consists of a generator network and a discriminator network. The generator network takes in a secret message and outputs a stego image, a cover image with the secret message embedded in it. The discriminator network takes in an image and outputs a probability score indicating whether it is a stego image or a cover image.

During training, the generator network learns to create stego images that fool the discriminator network into thinking they are cover images. In contrast, the discriminator network learns to distinguish between stego and cover images. After training, the generator network can be used to create stego images from new secret messages, while the discriminator network can be used to detect stego images created by the generator network.

To embed a secret message using GAN-based steganography, the sender first encodes the message into a numerical form that can be input into the generator network. The generator network then takes in the encoded message and a cover image and outputs a stego image that embeds the secret message. The stego image is then sent to the receiver, who can use the discriminator network to detect whether the image contains a hidden message. If the discriminator network detects a hidden message, the receiver can use the generator network to extract the message from the stego image.

4.2. CNN-Based Steganography

Convolutional Neural Networks (CNNs) have also been used for image steganography. In this technique, a CNN is trained to embed secret data into the image by modifying the pixel values in a way that is imperceptible to the human eye. CNN-based steganography is a technique that uses Convolutional Neural Networks (CNNs) to hide secret messages in images. CNNs are a type of neural network widely used in image processing and computer vision tasks. The basic idea behind CNN-based steganography is to use CNN's ability to learn and extract high-level features from images to embed secret messages in them.

The CNN-based steganography [30] technique involves two phases: the embedding phase and the extraction phase. In the embedding phase, the secret message is first transformed into a bit sequence and then divided into blocks. Each block is then encoded into a sequence of image patches fed into the CNN. The CNN then modifies the patches by adjusting their pixel values to encode the secret message. The modified patches are then recombined to form the stego image. In the extraction phase, the stego image is fed into the CNN, which extracts the patches and decodes the secret message from the modified pixel values.

The extracted message is then reassembled into the original message by concatenating the decoded bit sequences. CNN-based steganography has several advantages over traditional steganography techniques. First, it is highly resistant to attacks, as CNN's ability to learn and extract features makes it difficult for attackers to detect the hidden message. Second, it is highly efficient, as the CNN can process large amounts of data in parallel, making it suitable for real-time applications.

Recent advancements in CNN-based steganography have led to novel techniques that use deep learning models such as Generative Adversarial Networks (GANs) and Autoencoders for steganography. These techniques have shown promising results in terms of embedding capacity and security.

4.3. Autoencoder-Based Steganography

Autoencoders are neural networks that can be used for image compression and reconstruction. They have also been adapted for image steganography, where the encoder network hides secret information in the image, and the decoder network extracts the hidden information. Autoencoder-based steganography [31] is a type of image steganography that uses autoencoders to hide secret information in images. Autoencoders are neural networks that learn to encode input data into a compressed representation and decode the compressed representation back to the original input data.

In autoencoder-based steganography, the encoder part of the autoencoder is trained to embed secret information into the image. In contrast, the decoder part is trained to recover the original image from the embedded image. The secret information is usually added to the image by modifying the compressed representation of the image before it is decoded back to the original image. There are different ways to modify the compressed representation of the image to embed the secret information. One common approach is to add the secret information to the bottleneck layer of the autoencoder, which is the layer that has the lowest dimensionality. Another approach is to modify the weights of the autoencoder to embed the secret information. Autoencoder-based steganography has several advantages over traditional steganography techniques. First, it provides a high capacity for hiding secret information because the compressed representation of the image can be very large. Second, it is more robust to attacks because the secret information is distributed throughout the compressed image representation rather than in specific locations. Finally, it can be easily integrated with other deep learning techniques, such as Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs) for improved performance. However, autoencoder-based steganography also has some limitations.

Table 1. Comparative analysis of different techniques

Technique	Advantages	Disadvantages
LSB	Easy to implement, hiding capacity is high	Low robustness, sensitive to image processing
Masking/filtering	High robustness, hiding capacity is high	Requires more computational resources
Transform domain techniques	High hiding capacity, high robustness, resistant to image processing	Difficult to implement, some techniques require more computational resources, may have issues with quality loss of image after embedding
Spread spectrum	High robustness, imperceptibility, can be used for audio and video steganography	Lower hiding capacity compared to some other techniques, may have issues with synchronization of sender and receiver
Watermarking	High robustness, can be used for copyright protection and authentication	Hiding capacity is low, may have issues with quality loss of image after embedding
GAN-based	High hiding capacity, high robustness, can be used for different types of steganography (image, audio, and video)	Requires large amounts of training data, may be susceptible to adversarial attacks
CNN-based	High hiding capacity, high robustness, resistant to image processing, can be used for different types of steganog- raphy (image, audio, and video)	Requires large amounts of training data, may have issues with quality loss of image after embedding
Autoencoder-based	High hiding capacity, high robustness, resistant to image processing, can be used for different types of steganog- raphy (image, audio, and video)	Requires large amounts of training data, may have issues with quality loss of image after embedding, may have issues with over fitting during training

It requires a large amount of data to train the autoencoder effectively, which can be time-consuming and computationally expensive. It is also vulnerable to attacks that specifically target the autoencoder, such as attacks that aim to detect the modification of the compressed representation. Therefore, it is important to carefully design the autoencoder to ensure it is robust to attacks while providing a high capacity for hiding secret information. Table 1 depicts the comparative analysis of all the above-stated techniques.

5. Conclusion

Image steganography has come a long way since its inception, and new techniques are being developed constantly. With the advancements in machine learning and deep learning, we can expect more sophisticated steganography techniques to emerge in the future. Based on the advantages and disadvantages of the various techniques discussed earlier, it is clear that no single technique is perfect for all applications. The choice of technique depends on the specific requirements of the application, such as the size of the cover image, the amount of data to be hidden, the level of security needed, and so on. In the future, we can expect a hybrid approach that combines multiple techniques to achieve better performance.

For example, we can use a combination of transform-based techniques and machine learning techniques to achieve higher security and better hiding capacity. Another possibility is the development of steganography techniques that can adapt to the cover image's characteristics, such as texture, color, and structure. Overall, the future of image steganography is bright, with new and more powerful techniques emerging as the field advances. With the increasing need for secure data transmission and storage, image steganography will continue to play an important role in the field of information security.

References

[1] Hsiang-Kuang Pan, Yu-Yuan Chen, and Yu-Chee Tseng, "A Secure Data Hiding Scheme for Two-Color Images," *Proceedings ISCC 2000. Fifth IEEE Symposium on Computers and Communications*, pp. 750-755, 2000. [CrossRef] [Google Scholar] [Publisher Link]

[2] Derrick Grover, "Data Watermarking: Steganography and Water-Marking of Digital Data," *Computer Law and Security Review*, vol. 17, no. 2, pp. 101-104, 2001. [CrossRef] [Google Scholar] [Publisher Link]

[3] Johnson, N.F., Duric, Z., Jajodia, S. (2001). Exploring Steganography. In: Information Hiding: Steganography and Watermarking-Attacks and Countermeasures. Advances in Information Security, vol 1. Springer, Boston, MA. https://doi.org/10.1007/978-1-4615-4375-6_2

[4] Yeuan-Kuen Lee, and Ling-Hwei Chen, "Object-Based Image Steganography Using Affine Transformation," *International Journal of Pattern Recognition and Artificial Intelligence*, vol. 16, no. 6, pp. 681-696, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[5] S.K. Pal, and CE Veni Madhavan, "Investigating Steganographic Communications," *IETE Technical Review*, vol. 19, no. 4, pp. 207-212, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[6] Jessica Fridrich, and Miroslav Goljan, "Practical Steganalysis of Digital Images: State of the Art," *Proceedings Volume 4675, Security and Watermarking of Multimedia Contents IV*, 2002. [CrossRef] [Google Scholar] [Publisher Link]

[7] K. Bailey, Joan Condell, and K. Curran, "Steganography in Images: An Overview," *Irish Machine Vision and Image Processing Conference (IMVIP2003)*, 2003. [Google Scholar] [Publisher Link]

[8] W.A. Wan Adnan et al., "A Review of Image Watermarking," *Proceedings. Student Conference on Research and Development, SCORED 2003*, pp. 381–384, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[9] Rajarathnam Chandramouli, Mehdi Kharrazi, and Nasir Memon, "Image Steganography and Steganalysis: Concepts and Practice," *Second International Workshop on Digital Watermarking, IWDW 2003*, pp. 35-49, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[10] Mei-Yi Wu, Yu-Kun Ho, and Jia-Hong Lee, "An Iterative Method of Palette-Based Image Steganography," *Pattern Recognition Letters*, vol. 25, no. 3, pp. 301-309, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[11] Zoran Duric, Michael Jacobs, and Sushil Jajodia, "6 - Information Hiding: Steganography and Steganalysis," *Handbook of Statistics*, vol. 24, pp. 171-187, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[12] A. Martin, G. Sapiro, and G. Seroussi, "Is Image Steganography Natural?," *IEEE Transactions on Image processing*, vol. 14, no. 12, pp. 2040-2050, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[13] A.I. Hashad, A.S. Madani, and AEMA Wahdan, "A Robust Steganography Technique Using Discrete Cosine Transform Insertion," *2005 International Conference on Information and Communication Technology*, pp. 255-264, 2005. [CrossRef] [Google Scholar] [Publisher Link]

[14] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, "Improving Steganalysis by Fusion Techniques: A Case Study with Image Steganography," *Transactions on Data Hiding and Multimedia Security*, pp. 123-137, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[15] S. Torres-Maya, M. Nakano-Miyatake, and H. Perez-Meana, "An Image Steganography Systems Based on BPCS and IWT," *16th International Conference on Electronics, Communications and Computers (CONIELECOMP'06)*, pp. 51-51, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ran-Zan Wang, and Yeh-Shun Chen, "High-Payload Image Steganography Using Two-Way Block Matching," *IEEE Signal Processing Letters*, vol. 13, no. 3, pp. 161-164, 2006. [CrossRef] [Google Scholar] [Publisher Link]

[17] Inas Jawad Kadhim et al., "Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research," *Neurocomputing*, vol. 335, pp. 299–326, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] Mohammad Tanvir Parvez, and Adnan Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography," *IEEE Asia-Pacific Services Computing Conference*, pp. 1322-1327, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[19] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, "Image Steganography and Steganalysis: Concepts and Practice," *Mathematics and Computation in Imaging Science and Information Processing*, pp. 177-207, 2007. [CrossRef] [Google Scholar] [Publisher Link]

[20] Chin-Chen Chang, Yi-Pei Hsieh, and Chia-Hsuan Lin, "Sharing Secrets in Stego Images with Authentication," *Pattern Recognition*, vol. 41, no. 10, pp. 3130–3137, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[21] Zunera Jalil, and Anwar M. Mirza, "A Review of Digital Watermarking Techniques for Text Documents," *2009 International Conference on Information and Multimedia Technology*, pp. 230-234, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[22] C.C. Wu, M.S. Hwang, and S.J. Kao, "A New Approach to the Secret Image Sharing with Steganography and Authentication," *The Imaging Science Journal*, vol. 57, no. 3, pp. 140–151, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[23] Abbas Cheddad et al., "Digital Image Steganography: Survey and Analysis of Current Methods," *Signal Processing*, vol. 90, no. 3, pp. 727-752, 2010. [CrossRef] [Google Scholar] [Publisher Link]

[24] Rina Mishra, and Praveen Bhanodiya, "A Review on Steganography and Cryptography," *2015 International Conference on Advances in Computer Engineering and Applications*, pp. 119-122, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[25] Neha Sharma, and Usha Batra, "A Review on Spatial Domain Technique Based on Image Steganography," *2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN)*, pp. 24-27, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[26] N. Revathy, and G. Vijitha, "A Secure Image Steganography Technique to Hide Multimedia Files in RGB Images," *SSRG International Journal of Electronics and Communication Engineering*, vol. 5, no. 6, pp. 14-18, 2018. [CrossRef] [Publisher Link]

[27] Jia Liu et al., "Recent Advances of Image Steganography with Generative Adversarial Networks," *IEEE Access*, vol. 8, pp. 60575-60597, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[28] Jeanne Georges, and Dalia A. Magdi, "Using Artificial Intelligence Approaches for Image Steganography: A Review," *Internet of Things-Applications and Future*, pp. 239–247, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[29] Arome Junior Gabriel, Adebayo Olusola Adetunmbi, and Preye Obaila, "A Two-Layer Image-Steganography System for Covert Communication Over Enterprise Network," *International Conference on Computational Science and Its Applications - ICCSA 2020*, pp. 459-470, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[30] Weixuan Tang et al., "CNN- Based Adversarial Embedding for Image Steganography," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2074–2087, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[31] KV Sriram, and R.H. Havaldar, "Convolutional Neural Network Based Data Security in Image Steganography," *SSRG International Journal of Electrical and Electronics Engineering*, vol. 10, no. 7, pp. 102-109, 2023. [CrossRef] [Publisher Link].