Interdisciplinary Journal of Information, Knowledge, and Management

An Official Publication of the Informing Science Institute

SCOPUS INDEXED

Vol.: 20, Issue 1 March 2025

ISSN: (E) 1555-1237

Advancements and Challenges in Image Steganographer: A Comprehensive Review

Laxmi[1], Dr. Rajkumar[2]

[1]Research Scholar, CSE, UIET, MDU (ROHTAK

laxmi.bhardwaj2015@gmail.com

[2]Associate Professor, CSE, UIET, MDU (Rohtak

raj.kumar.uiet@mdurohtak.ac.in

Abstract

Image steganography, a combination of computer vision and encryption, is a classic challenge for hiding information in cover images for covert communication. This review paper examines conventional and modern image steganography approaches, including key issues and advancements. Explore the classical tension between concealing maximum information and avoiding discovery, stressing payload capacity in steganographic algorithms. Dissecting traditional methods like embedding RAR archives in JPEG files reveals weaknesses to third-party changes that risk hidden data. Image domain, transform domain, and file-format-based steganography approaches are described, along with their pros and cons. Image domain methods, such as the Least Significant Bit (LSB) method, are widely used for covert information transfer via pixel-level statistical changes. Modern advances include deep learning in image steganography. End-to-end auto encoder-based models show promising embedding capacity and durability against passive attacks. The study emphasizes the complex relationship between deep steganography and security issues by highlighting adversarial situations and their possible susceptibility to assaults. A visual representation of a common encoder-decoder network for deep steganography models shows attack channels for deleting or changing secret images and the usual path for correct image recovery. The article indicates that steganography algorithms must balance payload capacity, detection robustness, and adaptability to cover image patterns. This paper covers the progression from classical to deep learning-based image steganography and the associated issues that pave the way for future research..

Keywords*- steganographic, Deep Learning, Machine Learning, Image steganography*

I INTRODUCTION

The combination of computer vision and security is well-known in image steganography. Image steganography uses a shifting cover image to communicate secret information without the receiver knowing. Conventional picture steganography algorithms hide information well in cover images. Due to this, payload capacity—the ratio of hidden information to delivered information—receives little attention. A key consideration in steganography is payload size. Because additional information contained under the cover will look different, it will be more likely to be found. A RAR archive (The Roshal Archive file format) usually hides a JPEG file. Image steganography hides huge files during transmission. It may store unlimited data in this instance. However, changing the carrier file will lose all secret information, therefore it must be sent as is. Example: reading the image aloud and storing it again. Secrecy would be compromised. Pixel-level steganography is often used to enhance package capacity while preventing easy alterations. The most famous methods in this subject are LSB [1], BPCS [2], and their extensions. LSB techniques can increase payload capacity by 50%. Failure would reveal merely a fuzzy hidden image structure (Figure 1).

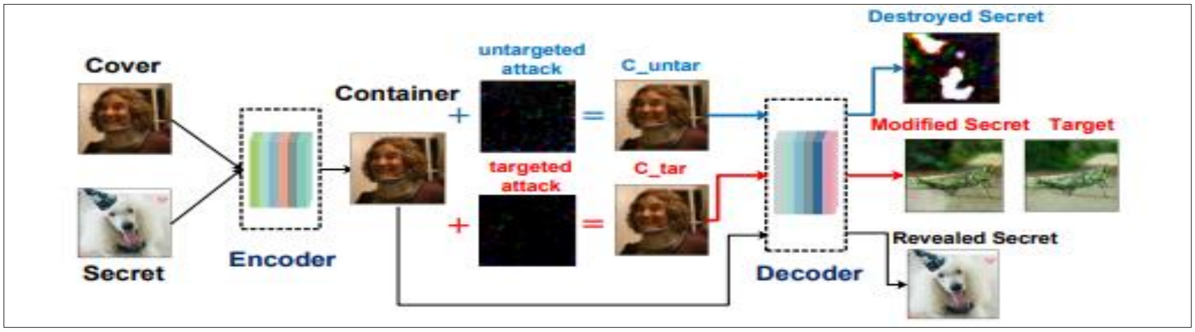

Figure 1. Typical encoder-decoder network for deep stenography model. Line 1 attack path: delete the secret image. Line—2 attack path: modify the secret image. Line 3 normal path: the receiver can recover the correct secret image.

However, most of these procedures can be statistically analyzed, making confirmation of their utilization easy. Several traditional steganography methods can hide information in JPEG DCT components. Balanced traits come from these tactics. Despite knowing that A. Almohammad [3]'s work yields 20% of the payload capacity (based on patterns), a statistical investigation has not found this. The most secure traditional picture steganography systems have created many functions that analyze image embedding localizations in recent years. This makes content-adaptive steganography possible. A distortion function domain must be built by assigning a changing cost or embedding impact to each pixel based on its effect [4]. A weighted norm is utilized to accurately describe the feature space. WOW (Wavelet Obtained Weights) [5] embeds information into an image based on its textural complexity. Several generic content-adaptive steganography algorithms have been described to avoid statistical analysis [6-7]. According to [8], the work focuses on content-adaptive batched steganography. Calculating the average payload capacity may be difficult because these methods depend on cover picture patterns. Recently, deep learning has showed promise in computer vision. Most deep learning-based photo steganography tools use deep neural networks. These apps have improved embedding capacity over earlier methods [9]. Deep neural networks can decipher buried binary information in images [10], and light fields can [11]. Deep neural networks may also hide many photos in one image [12]. The backbone network for image-to-image deep learning models is commonly an autoencoder. This autoencoder is end-to-end trained. After training the network, the sender can use the encoder to convert a hidden picture into a container image of the same size. This is possible with properly trained networks. The receiver can extract the secret picture from the container image using the sender's decoder. Since the sender provided the decoder, this is possible. Hayes et al.[13] found that passive attack approaches make deep learning-based steganography harder to recognize. Despite using deep learning, deep steganography (DS) may be vulnerable to adversarial assaults. Because it includes hostile instances, adversaries can abuse it. Adversarial attacks and distributed systems are linked [14], adding insult to injury. We tried adversarial attack strategies to gain attack capabilities that standard steganography cannot deliver.

The cover image patterns are so important in these systems that it may be difficult to determine the normal payload capacity. Patterns are significant, so yes. Recent computer vision advances have proven that deep learning can be effective in this field. The capacity of deep learning-based image steganography to embed information appears promising compared to older methods. Using deep neural networks may be a major factor. So cuz. Deep neural networks may express binary information in light fields [15] and hide binary information inside a picture [16], but they can also hide one or more images within an equivalent-sized image [17]. They can perform many new tasks due to this talent. Most image-to-image deep learning models teach a core network autoencoder from start to finish [18]. The encoder can convert a secret image into a container image of the same size if the sender has completed network training. This is feasible provided they complete the training [19]. The receiver can extract the secret image from the container image using the sender's decoder. In their prior work, [20] showed that passive attack strategies make deep learning-based steganography hard to distinguish. Deep steganography (DS) uses deep learning and is useful. However, it also shows confrontational conditions that enemies could assault. Asymmetrical attacks and distributed systems are intrinsically intertwined [21]. We tried to use adversarial attack technologies to gain attack capabilities that standard steganography cannot.

II STEGANOGRAPHY METHODS

Standard steganography using balance features can hide data in JPEG DCT components. That's feasible. For trends, his study [26] suggests that more than 20% of payload capacity is available, even though statistical research hasn't revealed this. Many functions that check image embedding localizations have been added to most safe standard image steganography systems. This created a content-adaptive steganography system. He [27] can create a distortion function domain by assigning each pixel a matching effect or dispersing a variable cost. Spreading warping function costs does this. This figure displays feature space using a weighted norm. Awesome Wavelet Obtained Weights lets you insert data [28]. This is why image regions' textural complexity is considered. The study found that numerous content-adaptive steganography methods can bypass statistical analysis [29]. Our main aim is developing batch steganography that works with several information formats [30]. The average cargo capacity of the vehicle under discussion may be difficult to establish because these methodologies depend on cover image patterns. Thus, designs matter most. Recent advances suggest deep learning may work for computer vision. Deep learning-based image steganography appears to embed information better than conventional methods [31]. This is partly due to deep neural networks. Deep neural networks may hide binary information in light fields [32] and one or more images inside a similar image [33]. They can also do other things with their talent. The autoencoder, the main network of most image-to-image deep learning models, is trained from start to finish. After network training, the sender can use the encoder to convert a secret image into a container image of the same size. A decoder provided by the sender allows the recipient to independently extract the secret image from the container image. He [34] previously showed that passive attack tactics make it impossible to distinguish deep learning steganography. It may be difficult to do.

JPEG RAR Steganography

One type of steganography that uses a feature built into file formats like JPEG and RAR is called "steganography theorized on file formats." RAR [35] and JPEG [9] are two file types. After the JPEG file has scanned the EOI (End of Image) segment, which is shown by the hex number 0xd9, the rest of the segments are skipped over. Because of this, any information added afterward is fine. A RAR file's magic file header is written in hexadecimal as "0x52 0x61 0x72 0x21 0x1a 0x07 0x00." The parser doesn't care about the rest of the data that comes before the file title. Although it is actually a RAR folder, the binary of the RAR file can be dumped after the JPEG file and make it look like a JPEG image file [36]. This is something that can be carried out. But the method is very open to any changes that might be made to the file. When third parties are used for tracking, information that isn't needed may be cut off to save transmission resources, or images may be changed to get around possible security measures. Any changes to the steganography will make it useless, and all the information that was hidden will be lost. It's going to be the internet in 2018, xx, 1 4 of 15.

LSB Method

When it comes to image domain steganography, the most common way is LSB-based, which is also written as LSB-based [37]. For privacy at the pixel level, these methods hide data. Most LSB methods are meant to change certain parts of the cover image so little that a person's eyes can't even tell the difference. Most images are made up of the highest bits of each pixel, and the LSB bits (the part of a pixel that is highlighted in Figure 2) are statistically similar to data that is made up at random[38]. This is what led to these methods. Now it looks like changing the LSB to hide information won't change the way it looks.

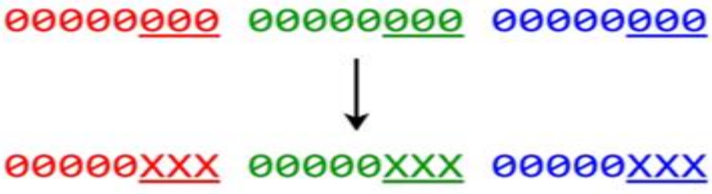

Figure.2: LSB operation

There are two main ways to get the secret story out there. This is done so that the least important parts of the image data will look like random data. Adding the secret message one at a time after encrypting or compressing it is the first type of method for making the message random. The second type of method builds the hidden sequence from a random seed that everyone agrees on. The information that is being hidden has to be spread out for this method to work.

JPEG Steganography

The research conducted by [39] and [40] is included in the field of transformation domain steganography. The work that Chang and Almohammad have done is an example of steganography using JPEG. The first step in the process of creating a JPEG file is breaking an image down into 8x8 pixel blocks. Following that, the color space of these blocks is changed from RGB to YCrCb, which is an abbreviation that stands for luminance and chrominance. Following this, a Discrete Cosine Transformation (DCT) is carried out, the result is quantized, and the information that is still there is encoded. The sensitive information will be buried inside the quantized DCT components in the event that you do lossy compression after quantization has been performed. In the altered domain, this results in the creation of an LSB embedding. As a consequence of the fact that we are unable to quickly determine this using statistics, the LSB technique has a carrying capacity that is much lower.

Convolutional Neural Network

Convolutional neural networks [41] have been used by individuals since the 1990s nonetheless, they have gained a great deal of notoriety in recent times, particularly when AlexNet [42] gained victory in the ImageNet competition. Additionally, it has been used to establish new benchmarks in a variety of domains, including object segmentation [43], sorting [44], and others. The massive amount of training data, the advent of modern GPU technology, and the Rectified Linear Unit's (ReLU) [45] efforts and expansions [46] all contributed to the advancements that were achieved a few years ago. In addition, these characteristics are of great assistance to the task that we conduct. Additionally, the convolution process is used rather often in conventional computer vision algorithms, indicating that it is not only a technique that is utilized in neural networks. As an example, the Gaussian smoothing kernel is often used in order to reduce the amount of noise in photos and to soften them. By using a convolution between the initial image and a gaussian function, which is the same as the implementation stage, it is feasible to do this. Many additional contributions were produced by using the conventional procedures. Some examples of patterns, kernels, or filter pairs that are created manually include the Sobel-Feldman filter [47] for edge detection, the Log-Gabol filter [48] for texture recognition, the HOG filter [49] for object identification, and a great deal of other examples (Future Internet 2018, xx, 1 5 of 15). On the other hand, things like designing and adjusting designs that are done by hand are very sophisticated jobs that could only be beneficial for particular kinds of employment. On the other hand, convolutional neural networks are able to autonomously generate patterns for specific tasks by using a technique known as back-propagation [49]. Another advantage is that combinations of convolution processes [50] may assist in the rapid acquisition of high-level characteristics, which is another advantage.

Autoencoder Neural Network

The traditional auto encoder neural networks [51] were the source of inspiration for our technique throughout the development of this technology. Initially, these networks were trained to generate an output image that was similar to the representation of the input image. This first training was carried out. Generally speaking, it is made up of two neural networks: one encoding network, which is a decoding network d = g(h), and one decoding network, which is a decoding network h = f(x). Under the assumption that d equals x, both of these networks are affected by the constraint. As a consequence of this, they are able to acquire knowledge on the conditional probability distribution of p(h|x) and p(x|h) respectively. It has been proved that the auto encoder design is capable of extracting significant characteristics from images by decreasing the dimension of the hidden layer (h). A wide range of applications have made use of this capacity, such as denoising [52], dimension reduction [53], image synthesis [54], and a number of other applications.

Neural Network for Steganography

We used classic autoencoder neural networks as a jumping off point for our method. At first, these networks were taught to simulate the input picture as closely as possible in their output images. This was the first setup for the networks. In most cases, it is made up of two neural networks: one network for encoding, which was decoded as d = g(h), and one network for decoding, which was decoded as h = f(x). The requirement that d = x ensures that both of these networks are limited. They are able to acquire the knowledge necessary to acquire the conditional probability distribution of p(h|x) and p(x|h) correspondingly as a finish product. Through the process of reducing the dimension of the hidden layer (h), the autoencoder architecture has proved its capacity to take out significant characteristics from images.

Traditional Steganography Methods

The frequency domain and the spatial domain are the two primary domains in which steganography techniques are effective. Whenever the spatial region is used, the private data is included by directly altering the values of the pixels. It is essential to keep in mind that they are susceptible to statistical hacking or having their images altered [55], despite the fact that they are recognized for their capacity to manage a large amount of data well. One sort of approach that falls within the category of “spatial domain is the LSB Replacement and its successors. Pixel Value Differencing (PVD), Pixel Indicator Approach (PIT), and Exploiting Modification Direction (EMD) are some of the approaches that are also available” [55].On the first step, the pixels of the image are transformed into the frequency domain system. This may be accomplished by a technique that is referred to as transform or frequency domain. In order to conceal the confidential information, the coefficient numbers are altered in such a way that they are not visible to the naked eye. The use of the inverse transform is the last step in the process of obtaining the steno image. Statistical assaults are not able to quickly break these approaches, despite the fact that they are not particularly good at what they do. In the realm of transform domain techniques, the most well-known ones are the “Discrete Fourier Transform (DFT), the Discrete Edge Transform (EDT), the Discrete Contourlet Transform (CT), and the Discrete Wavelet Transform (DWT)”. (12) and (13).

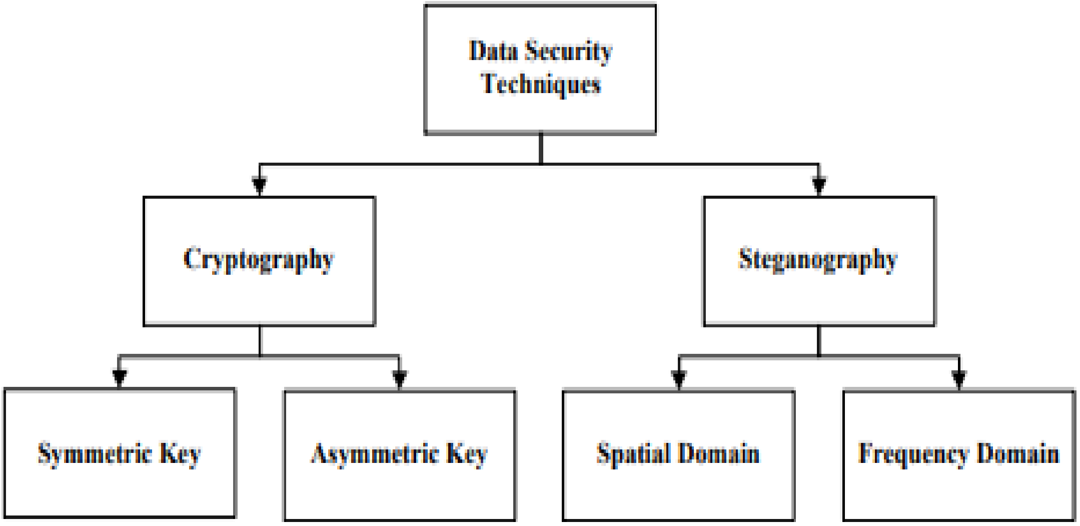

Figure 3. Data security classes [7].

One of the most well-known strategies in the space domain is LSB Replacement, which more often goes by the acronym LSB. Because of its ease of use and the possibility of achieving a large volume, this technique is used by a significant number of individuals. When using this strategy, the cover image pixel that is considered to be the least significant is where the confidential information is put. We behave in this manner in order to reduce the amount of misunderstanding that occurs. It is impossible to tell the difference between the original image and the stego image that was created. In addition, it is possible to conceal data by making use of more than one LSB of a pixel. This serves the purpose of increasing the payload capacity. Nevertheless, this can make the stego image seem even more unfavorable [56]. You need to be aware that the initial LSB has already undergone a lot of enhancements in a variety of ways. A piece of software known as LSB Matching (LSBM) has been responsible for the improvement of the LSB technique [57]. In this particular instance, the inserted bit and the LSB of the cover pixel need to be identical. In the event that it does not, random values of either +1 or -1 are used to add to that pixel. It is done in this manner in order to prevent the asymmetrical artifacts that are produced by the standard LSB approach and may be discovered by steganography tools [58]. LSB Matching Revisited, often known as LSBMR, was presented by [59] as a means of improving the functional capabilities of the approaches that had been used in the past. In addition to making relatively minor adjustments to the carrier image, it conceals information in the LSB. It does this by simultaneously hiding two bits in two frames. Pixels themselves contain the first secret bit, and the relationships between the first two bits determine the value of the second secret bit. [60] The goal is to increase the difficulty level of finding the concealed information compared to utilizing traditional methods.

Bit concealment is feasible close to the cover image's edge, when pixel intensity values change fast. Private and sensitive information may be further concealed in this way. These types of steganography techniques are referred to as Edges Based Embedding (EBE) Steganography. This is due to the fact that they are able to conceal very big messages inside certain edge pixels. There are a number of research articles that have been published on this problem, including [61][62].When using the PVD approach, it is believed that the cover image is composed of many blocks of two pixels that do not overlap with one another. This demonstrates yet more method for concealing binary data. In order to determine the number of bits that are included inside the payload, it is necessary to determine and quantify the difference that exists between the two images [63].The difference is broken down into its component elements in order to do this. In the Cyclic Steganographic Technique, often known as CST, the act of concealing something is repeated by using color bands of pixels that are next to one another [64]. There is a distinction between the color channel of this pixel and the channels that were used for the pixels that came before it and the pixels that will come after it. The pixel that is now being considered will have the LSB of the red channel selected for it. The pixel that comes after this one will have the blue channel selected, and the pixel that comes after that will have the green channel selected before it. Consequently, the layout remains unchanged for three pixels that are located in close proximity to one another. The concept of randomization is described and discussed in conjunction with CST in [65]. Within the LSB of the pixels, the secret data is concealed in a manner that is completely random in this version.

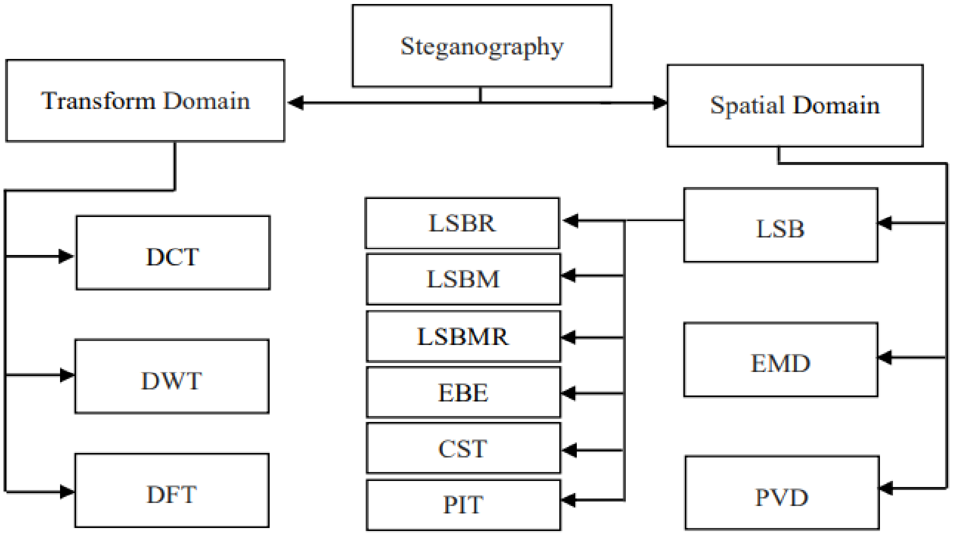

Figure 4. Traditional steganographic techniques.

The adoption of PIT, which is a variant of LSB methods, may make traditional systems more safe and resilient. This is by using the PIT. The embedding procedure is carried out by picking one of the color channels of the pixel to act as an indication for the other two channels 67]. This chooses is made in order to carry out the embedding process. For the purpose of embedding the pixel, this approach is applied. In [68], which is an enhancement that is applied, careful consideration is given to the length of the secret message. At the same time, the existence of data in other channels is indicated by the use of two LSBs (LSBs) of a particular channel. [69] Presents an additional form that uses three of the LSBs (LSBs) of one of the channels of the pixel as an indicator. This form is offered in another form. One other way that is used to enhance security is the utilization of electronic mail communication (EMD). This approach is used to split the cover image into sections that each consist of n pixels. A notational method that is 2n+1-directional is used to express the top-secret numbers that are included inside these n pixels of the cover image. An individual pixel is subjected to a measurement of ±1 at a particular instant in time. As a result of the fact that there are two hundred and one different ways in which the pixels may be altered, there are two hundred and one different numbers that can be hidden in secret for a quantity of n [70]. A plan that is offered in article [71] is called Improved EMD (IEMD), and it is an effort to improve the EMD method. The plan is presented as an attempt to improve the EMD approach. This system makes use of a notation method that is referred to as 8-ary. Pair of pixels that are clustered together are used to include the secret digit into the image.

Summary of traditional method

Steganographer, the art of hiding information within other data, employs various techniques across different domains to conceal messages effectively. In the realm of digital images, traditional steganographic methods leverage both spatial and frequency domains for embedding information. In the frequency domain, transformations like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT) are utilized. These techniques alter the representation of the image, making it suitable for embedding hidden data. DCT, popular in JPEG compression, transforms blocks of pixels into frequency components, enabling the hiding of information in less noticeable areas. Similarly, DWT decomposes the image into different frequency bands, allowing subtle data embedding in the wavelet coefficients. DFT, though less common in image steganography, can be employed similarly by transforming the image into its frequency representation.

On the other hand, in the spatial domain, techniques like Least Significant Bit (LSB) substitution are widely employed. LSB-based methods replace the least significant bit of pixel values with the secret data, causing minimal perceptual change. Techniques such as LSB replacement (LSBR), LSB matching (LSBM), and LSB matching revisited (LSBMR) modify the LSBs of pixels to encode information. Enhanced Bit Encoding (EBE) goes beyond LSB, utilizing multiple bits for embedding, thereby increasing the payload capacity. Cover Selection Technique (CST) strategically selects pixels for embedding based on their similarity to the secret data, minimizing visual distortion. Pixel Indicator Technique (PIT) embeds data by altering pixel values to encode a message, often employing a predefined indicator pattern to mark embedded locations.

Each technique comes with its strengths and weaknesses, influencing factors such as payload capacity, robustness against attacks, and perceptual quality. Understanding these methods allows steganographer to choose the most suitable approach based on their specific requirements and constraints.

.

Table 1. Comparison among different information security techniques.

Technique	Description	Methodology	Key Advantage	Key Disadvantage
Steganography	Conceals data within other data or media.	Covert data embedding	Covert communication Data presence is hidden	Limited data capacity Vulnerable to detection
Encryption	Converts data into an unreadable format.	Mathematical algorithms	Strong data protection Requires decryption key	Encryption can attract attention Data not hidden
Watermarking	Embeds a watermark to verify data integrity.	Embedded data integrity	Data integrity verification Various applications	May be altered or removed without detection
Access Control	Restricts access to authorized users only.	User authentication	Effective access restriction User-specific	Vulnerable to password breaches Requires setup
Firewalls	Monitors and controls network traffic.	Packet inspection	Network security Filters unauthorized traffic	Can create network bottlenecks False positives
Intrusion Detection	Monitors for suspicious activities.	Anomaly detection	Detects network intrusions Real-time alerts	False alarms May miss sophisticated attacks
Antivirus Software	Scans for and removes malware.	Signature-based detection	Protects against known threats Regular updates	Limited against zero-day threats System resource
Biometric Authentication	Uses unique biological traits for access control.	Fingerprint, iris, etc.	Highly secure Difficult to impersonate	Costly Requires specialized hardware

Natural language processing (NLP) has become more popular in recent years, prompting scientists to investigate ways to automatically generate steganographic text for the purpose of transmitting secret information. Under this steganographic technique, which is called "natural modification of the cover media," information is hidden in a text even while it is being written. Here we look at how steganography has changed over the years and how it stacks up against other taxonomies. Experts will be able to better understand how the present methods work thanks to this.

III MATERIALS AND METHODS

This study looked at the techniques and methods for hiding image that have been released from 2015 to 2023. Studies that didn't have anything to do with image steganography were left out. We only used the original, full versions of the report. This part has the subsections Data Sources, Search Process, Data Selection, and Data Extraction.

Data Sources

Search using Keywords: Use relevant keywords related to study, such as "steganography," "information security," "data encryption," Combine these keywords with Boolean operators (AND, OR) to refine search.

Advanced Search: Utilize the advanced search features provided by these databases to narrow down your results based on publication date, authors, journals, and other criteria.

Review Citations: Look at the citations of papers that are closely related to topic. This helps find more recent research that builds upon the earlier work.

Google Scholar: Since you have access to Google Scholar, use it to search for papers and articles. Google Scholar often provides a broader search scope and may include papers not available in other databases.

Search Process

The first query focuses on text steganography techniques and includes variations of the term " image steganography" along with keywords related to different approaches, such as "format based," "linguistic," "random," and "statistical." This query aims to capture papers discussing various methods and a technique in image steganography. The second query delves into the intersection of image steganography and neural networks or deep learning. It includes variations of "text data steganography" and "image steganography method," combined with keywords related to neural networks, deep learning, natural language processing (NLP), and natural language understanding. This query seeks to identify research that explores the application of machine learning and NLP techniques in text steganography.

Data Selection

Research assessments must give serious consideration to the selection of data in order to carry out their processes. Following the acquisition of search results derived from our specified keywords, we used three separate filtering strategies to include the search criteria. We chose and agreed upon the criteria early on in the filtering process. We collected all of the findings into separate study papers when the inquiry was over and organized them according to these chosen keywords. Following that, a second filter was executed to determine whether the papers were relevant to the study subject by analyzing their titles and abstracts. In the third and last filter, we read the contents of a research article that was chosen from among the possible studies.

Data Extraction

We examined each of the preliminary studies to evaluate whether or not there were any text steganography-related subjects. In a spreadsheet, we included all of the research we discovered, along with their titles, abstracts, and justifications. The search procedure was finished in March of 2021, and a total of 203 publications were found. Following the selection and refusal criteria, the pertinent research papers were painstakingly pulled from the database making use of the search strategy depicted in Figure 5. In the end, fifty different preliminary investigations were discovered.

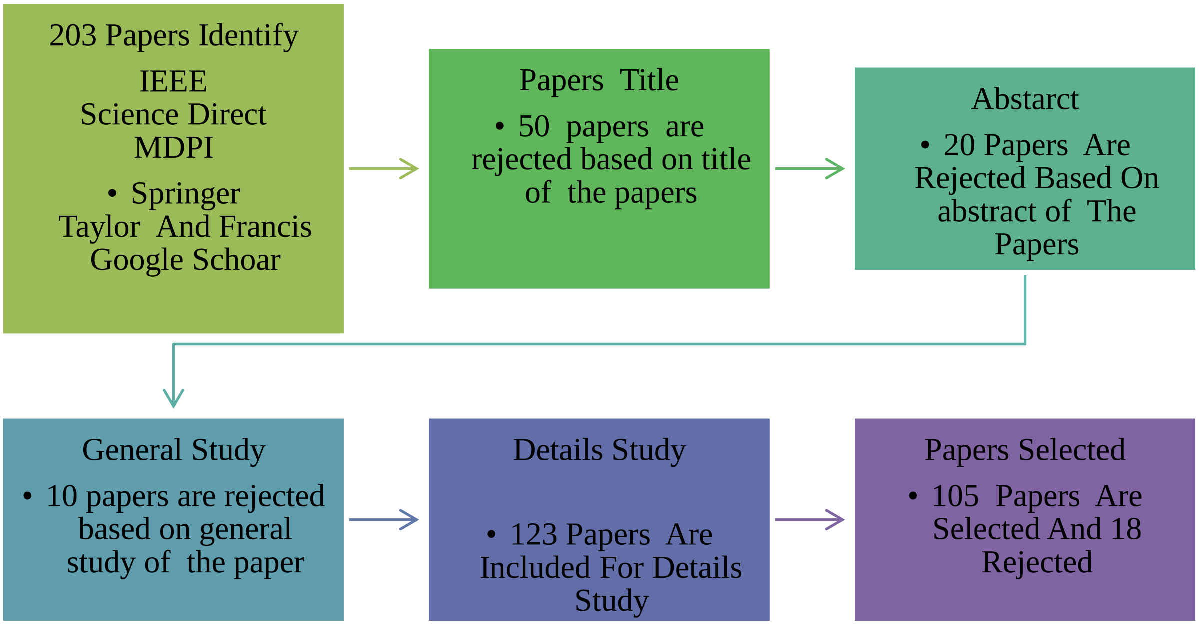
203 Papers Identify
IEEE
Science Direct
MDPI
• Springer
Taylor And Francis
Google Schoar
Papers Title
• 50 papers are rejected based on title of the papers
Abstarct
• 20 Papers Are Rejected Based On abstract of The Papers
General Study
• 10 papers are rejected based on general study of the paper
Details Study
• 123 Papers Are Included For Details Study
Papers Selected
• 105 Papers Are Selected And 18 Rejected

Figure 5. Search process

IVLITERATURE SURVEY

Security Techniques In Image Steganography

When it comes to steganography, the security characteristic is one of the components that poses the largest degree of difficulties. What we mean when we speak about security in this context is the process of making the concealed secret information undetectable or the embedded size and locations unguessable. This is what we mean when we say that security is a process. A substantial amount of research has been conducted in this area, which makes use of a wide range of techniques to improve the steganographic security of information. Figure 4 provides a summary of the results that correspond to the protection of images via the use of steganography, and Figure 5 provides a classification of the research articles in line with the findings.

The concept of encryption, which encodes the secret information before embedding it, is one that is often used in order to achieve security. A further possibility is that the whole image might be encrypted as a step in the operation of an algorithm. The Rivest, Shamir, and Adleman (RSA) method, the Advanced Encryption Standard (AES), and the Triple Data Encryption Standard (3DES) algorithm are all examples of classical encryption algorithms that are used in order to achieve this purpose. In addition, user-defined techniques are applied during the course of this procedure. A second way for ensuring security is known as randomization, which includes the dissemination of secret information across the initial image in a manner that is random. Randomization is a strategy that may provide security. It is possible to make use of a number of approaches within the framework of this concept. Some of these methods include chaotic functions, user-defined keys, and pseudorandom sequence generators. When it comes to providing an extra layer of security, randomization may be used on its own or in combination with encryption schemes. Both of these methodologies are viable options.

Chaotic functions are well-known for their unpredictable outputs, which are a result of their random nature. The outputs of chaotic functions are unpredictable for specific input parameter values. When it comes to the process of selecting the placement of pixels, the result is subsequently utilized appropriately. The cover image can be transformed into another bit plane, embedded, and then re-transformed back into its original form. This is yet another method that can be utilized to conceal confidential information and improve security. Because it eliminates the correlations between adjacent pixels, the region-based idea also plays a role in enhancing the overall security.

Randomization based Techniques

In situations when these approaches are used, the only way to ensure security is via randomization. Utilizing the Linear Congruential Generator (LCG) in [72] allows for the selection of pixel values in a random manner. Using the LSB approach and a sequence similar to 3-3-3-2, eight bits from the secret message are concealed. For this reason, the red channel has three hidden bits, the green channel three as well, and the blue channels two apiece. The authors of [73] propose hiding three binary pictures within a grayscale paper. At every stage, Ultra Unique Numbers (UUNs) are used to mask the rearranged binary pixel values that are meant to be invisible in a grayscale picture. In order to choose pixels in [74], a large number of unique series are generated using random numbers. A PRNG is also used in [33] to choose an embedding pixel. Just like that, this is executed. To streamline the creation of three PRNGs, the Skew Tent Map (SKTM) is used in the paper [75]. In addition to encoding secret messages before inserting them, they also embed color channels, match pixel points to specified RGB channels, and more.To choose an embedding pixel location, one may use the improved chaotic system model for a one-dimensional system that was put out in [76]. A chaotic LM and a sine map function are tools that the chaotic system uses. Anywhere a message can be hidden using the Beta Chaotic Map (CM) described in [77], it will remain undetected. Selecting PRNG-enabled random bits for embedding is accomplished according to the steps outlined in [78]. Users have the opportunity to specify both the key seed value and the quantity of bits to insert. Using the user-selected key's random chain codes, the pixels in [79] are made to appear randomly. Bytes in the key block are encoded in hexadecimal, hence the sequence of bytes in these chains is completely at random. This pattern ensures that the sub cover image's pixels have the secret message bits placed into their left-side bits (LSB).

Encryption

Steganographic techniques that are based solely on cryptography or that combine cryptography with randomization will be presented in the sections that follow. In addition, a number of image encryption strategies will be discussed, which can be applied to encrypt the secret image and can also be utilized throughout the process of steganography.

Encryption based steganography: The method described in [80] suggests that the secret message should be encrypted by utilizing an XOR operation with a key that is defined by the user. In order to create the top secret message that is going to be concealed, the encrypted text message is then subjected to a shifting operation that involves four bits. After some time has passed, the cover image is modified to incorporate the secret data by employing the standard LSB approach. In accordance with the method proposed in [81],

Randomization and encryption based steganographic techniques:

An approach that may be used to improve the security of LSB steganography is presented in the research article [82]. When using this method, the sensitive communication is encrypted using a method known as One-Time Pad (OTP), which is an encryption technique. After that, randomization is achieved by the employment of the columnar transposition and RGB color plane scattering approach using the technique. In addition, the approach described in [83] uses OTP to encrypt the secret message, but it also uses PRNG to choose a pixel position for LSB embedding and encrypt the secret message. Overall, this method is rather effective. For the purpose of encrypting the secret message, employs the Advanced Encryption Standard (AES) algorithm. After that, the LSB approach is used to insert the message at a location that is chosen at random by the LCG mechanism. In addition, the AES method is applied in [58] in order to encrypt the secret message before the process of splitting it into blocks. This serves as a precautionary measure. In order to segment the cover image, a technique that is referred to as a Non-Uniform Block Adaptive Segmentation on image (NUBASI) algorithm is brought into play. Last but not least, a proof-of-work random number generator (PRNG) is used to choose a message block at random for the purpose of embedding it into an image segment. Ultimately, there are 32 distinct pattern orders of segments that are preset and may be selected at random. These pattern orders are predefined. According to [84], the secret message is encrypted using the Vigenère Cipher, and it is compressed using the Huffman Coding. Both of these ciphers are applied. Next, the image is segmented into blocks so that the KT algorithm may be used to generate groups of blocks. This phase is followed by the next stage. The use of an arbitrary function is used in order to ascertain whether blocks and groups are capable of being applied in order to hide a specific pixel inside the group in a manner that is inconsistent with the other pixels. By executing bitwise XOR operations between pixels that are next to one another, the authors of [60] come up with the idea that the secret message may be encoded. Using a local user selection is the next stage, which requires locating a particular location among the four LSBs in order to hide a secret bit. This is done in order to conceal the secret bit. Using a technique called as Modified LSB (MDLSB), which is described in [85], it is possible to embed data in the cover image. This is performed by using the approach. In order to achieve randomness, there are two levels that are employed, namely segment selection and pixel selection, which are determined by the user's input. In addition, the use of the DEFLATE approach, which is an algorithm for lossless compression, is applied in order to get around the issue of embedding size in the layer that comes after it. The Advanced Encryption Standard (AES) encryption method is used at the succeeding layer in order to further encrypt the communication that is considered confidential. A technique that is referred to as the Artificial Bee Colony (ABC) is applied in order to reduce the quantity of noise that is brought about by information that is incorporated.

Region based Steganography

Steganography is hidden in convinced areas of the cover image in order to increase the level of security shown. Within the next few paragraphs, we will discuss a few different solutions. While there are ways that simply utilize the edges of the image, there are other methods that use both the edges and the smooth areas of the image. The term "smooth areas" refers to regions of the image that do not undergo significant changes in intensity, while the term "image" refers to regions of the image that undergo changes in intensity that are significant over a short distance. Through the use of the Canny edge detection, edge pixels are located and selected for the purpose of being embedded in [86]. Right at the beginning of the process of data compression, the Huffman code is assigned to the hidden bits. The number of pixels that will be inserted is then determined by the coherent bit length L, and the edge pixels are selected at random after that. This is the next phase, which involves making a 2k adjustment in order to make it easier to not notice anything. Edge recognition and morphological dilatation are going to be used in the steganographic procedure, as claimed by [87]. The sharp borders of the images are where the secret message is concealed when using this approach. The morphological compression operator improves the sharp regions that are being examined by the Canny edge operator, which also examines these areas. To create a modified version of the original image channels, the four most significant bits (MSBs) of the RGB channels are simply combined together. The Canny operator is then used in this process. In order to determine which of the images the reference is, a 3x3 dilation operator is then used. When the hybrid XOR technique is used, the bits are inserted into the LSB bits that are left over from the process. This ensures that the pixels around the edge are altered as little as physically feasible. This is in accordance with the stringent security regulations.

Bit-Plane System

A virtual bit-plane is exploited in the LSB steganography methods that are discussed below. These approaches are described in more detail below. For the purpose of concealing secret information, higher plane systems are employed as an alternative to the utilization of an 8-bit plane. For these devices to be able to meet the Zeckendorf criteria, it is important for them to be able to implant the sensitive information that can be withdrawn at a later time. According to the reference number 99, it is feasible to describe any positive integer in a form that is one of a kind by adding together one or more Fibonacci numbers that are not sequential. Consequently, the representation of the number is considered to be genuine if there are no consecutive ones that take place in the sequence since this indicates that the sequence is complete. As opposed to making use of the conventional binary bit planes, The core of this system is the Lucas Number system, which is characterized by the use of eleven-digit representations. As a consequence, the Lucas sequence is employed for the purpose of image bit plane representations. This results in the usage of 11 bits rather than 8 bits for the purpose of describing the intensity of the pixel. Image bit plane representations are utilized. While the embedding process takes place in the second bit-plane, the stego image undergoes a deterioration of ±1 as a consequence. The blue and green channels of the RGB color image are employed for the goal of data embedding, while the red channel is utilized for the purpose of providing an indication. As was indicated before, embedding should be done in line with the enlarged Zeckendorf theorem in order to manage duplicate representation in an appropriate manner.

Pixel Indicator Techniques

Channels are divided into two distinct kinds in data embedding techniques that are based on indicators. These channels are referred to as indicator channels and data channels. The indicator channel is in charge of identifying the data channel that will be used to hide data. This is done with the intention of ensuring a greater degree of safety is achieved. uses the two bits of one channel that are the least important as an indication to identify whether or not the other two data channels include any potentially secret information. This is done by analyzing this information. There is a selection made for the indicator channel based on a sequence that is generated from R, G, and B. Specifically, RGB, RBG, GBR, GRB, BRG, and BGR are the components that make up this sequence. For the goal of strengthening security, the length of the secret message is employed as selection criteria for indicative purposes. This is done in order to avoid any potential vulnerability. At the same time that data is being concealed in channels, the intensity of the pixel is also taken into account.

The seventh bit of a pixel and the seventh bit of the pixel value +1 are both discussed in [88], **Pranab K. Muhuri and colleagues (2022):** Limited investigation of integrating integer wavelet transformation and particle swarm optimization for image steganography, specifically in terms of capacity, imperceptibility, and robustness.[88]

Ayushi Chaudhary et al. (2022): Lack of comprehensive analysis of pros and cons of different steganographic methods, including combination of sequence and asymmetric encryption. Need to evaluate effectiveness of methods against steganalysis.[89]

Wafa M. Eid et al. (2022): Lack of comprehensive overview and analysis of steganalysis methodologies for spatial and transform domains in 2D and 3D images. Need to consider conventional machine learning and deep learning techniques.[90]

Jiahao Liu et al. (2022): Need for comprehensive overview and analysis of steganalysis methodologies for spatial and transform domains in 2D and 3D images. Need to consider conventional machine learning and deep learning techniques.[91]

Bibek Ranjan Ghosh et al. (2022): Need for comprehensive overview of diverse steganographic methods utilized for concealment of information in 2D and 3D images. Focus on dataset used and evaluation of methods.[92]

Ismail Taha Ahmed et al. (2022): Limited exploration of deep learning application, particularly utilization of pre-existing CNNs like AlexNet, in image steganalysis for binary classification.[93]

Bhatia,A. et al. (2021): Limited investigation of GANs in image steganography, including steganographic capacity, visual quality, and robustness against steganalysis.[94]

Hu, Y. et al. (2021): Need to enhance steganographic capacity and robustness through application of multi-scale feature fusion techniques in CNN-based image steganography.[95]

M. Esaiselvam et al. (2021): Limited exploration of using steganography techniques (Contour reframing, Deep Image prior, PEM method) to detect and quantify image tilt angles for piracy detection.[96]

Nandhini Subramanian et al. (2021): Limited exploration of deep learning methods (standard, CNNs, GANs) in image steganography. Need for more comprehensive evaluation measures.[97]

Pei Li et al. (2021) Limited exploration of deep learning integration in steganography and steganalysis. Need for analysis of challenges and future developments.[98]

Ismail Kich et al. (2021): Limited exploration of CNN-inspired approach using Auto-Encoder networks and U-net design for color image steganography. Need for performance evaluation on popular datasets.[99]

Luo et al. (2020): Opportunity to improve robustness and imperceptibility of image steganography using deep learning models and exploring pixel-value differencing Proposed Algorithm for Steganography Limited discussion on the specific techniques or mechanisms employed in the proposed algorithm for embedding and extracting data. Lack of detailed exploration of potential vulnerabilities, robustness, and security considerations of the proposed algorithm.[100]

Srushti S Yadahalli et al. (2020): Absence of comparison with more recent and advanced steganography techniques beyond LSB and Discrete Wavelet Transform. Insufficient exploration of the trade-offs between different steganographic methods in terms of capacity, security, and visual quality.[101]

B. Vishnu Leena Vishnu Namboothiri et al. (2020): Limited discussion on the specific mathematical or computational details of the Pixel Value Differentiating (PVD) technique. Need for a comprehensive analysis of the impact of Edge Detection in enhancing security and embedding capacity.[102]

T. Kalaichelvi P. Apuroop et al. (2020): Lack of in-depth explanation of the CAPTCHA-based authentication mechanism and its integration with image steganography. Need for a more detailed comparison of the proposed approach's security benefits and challenges compared to traditional methods.[103]

J. H. Lee D. Y. Kang et al. (2020): Inadequate discussion on the specific architecture and training process of the deep neural network model used for recovering hidden image information. Limited exploration of the potential limitations or cases where the proposed approach may not work effectively.[104]

Omar Elharrouss Noor Almaadeed et al. (2020): Lack of detailed explanation of the k-LSB-based method and its potential impact on capacity and security compared to other steganography techniques. Insufficient analysis of the trade-offs between image resolution enhancement and potential loss of steganographic content during decoding.[105]

Table 2.Summary of the Most of the Mentioned Randomization-Based Techniques

Ref	Features and Pros	Cons	PSN R (dB)
[30]	The cover image has been rotated 90 degrees. Security is achieved by randomizing pixels with a linear congruential generator and putting them in a 3R-3G-2B pattern.	Do not take many tests When compared to other ways that do the same thing, embedding doesn't look at what appears inside the image. Nothing was tested for steganography. Statistically and geometrically not resistant to hits	512 x 512 PSNR: R: 64.0484 G: 64.5621 B: 67.362
[31]	Two binary images may be concealed by the cover image. Using three different random number series, shuffling-based security may be achieved with the use of mathematical processes known as UUN Simple techniques.	A image's content stays the same when you add it. Nothing was tested for steganography. Cannot withstand strikes on geometry and structure PSNR is not very strong	PSNR: 37.71: 40.46
[32]	It is possible for a grayscale image to hold a binary image. Using a series of random numbers to do randomization embedding. Many series and numbers that show up often have been taken out.	Every part of the image is taken into account. There won't be any steganography tests. Not strong enough to protect against strikes based on geometry and organization	PSNR: 83.97: 63.45
[33]	Contains integrated A 3R-3G-2B with 8 BPP Five MSBs make up a bit that is subject to an XOR operation, and a secret bit is hidden in the LSB.There are five possible MSBs and a pixel that are chosen at random using a PRNG.Encryption uses the XOR technique, which is extremely easy to use and very effective. Implementations that are simple to understand	That the information can't be retrieved is what security is all about. The change affects every part of the image. Steganography tests will not be done. Shape and organization-based strikes are not strong enough to stop them	512x512 RGB bmp images Payloads 100: 262144 bits. PSNR: 39.263: 73.798

[34]	Three types of PRNGs will be made by SKTM: scramble secret messages, pick an embedding color channel, and pick a pixel spot.The LSBs come in versions 1 and 4.Good statistical features can be seen in the chaotic image.So that statistical threats can't hurt the algorithm while it's running	The hidden bits' positions are the focus of StegExpose's detection, which reveals around half of the information that is embedded.	PSNR=65.97 :55.49 4-LSB, C= 809:36,167 Bytes
			PSNR= 52.621:36.101

[35]	Improved 1D chaotic behaviour (an improved LM and sine map) Improved robustness against statistical attacks.	A modest PSNR level Within the histogram, there are many jumps.Insufficient tests have been carried out for the chi square test. It’s not taken into account by embedding that exchanging image content settings can be time-consuming.	Avg PSNR= 38.209
[36]	Using Beta chaotic map Good Visual quality	Clear Histogram deformity Complexity of the Beta map Embedding does not take into account the image content Key exchange overhead	USC-SIP Image Database. PSNR: 57.5 – 56.79
[37]	PRN generator to define embedding locations. User-defined Key seed value & number of embedded bits. Not complex Variable embedding capacity	Embedding does not take into account the image content Key exchange overhead Few tests .Non-standard image No steganalysis experiments	Message length: 343: 8866 characters Avg PSNR= 68.49
[38]	Uses chains of a random sequence of indices (codes) of the bytes in the carrier image. Use of the full capacity of the cover image. Robustness, and undetectability have been improved through extracting chains of randomly selected pixels from the cover image based on a user key	Not compared to rival techniques. Uses non-standard images. Uses relatively large Stego secret key No steganalysis experiments	Image size= 147456 Payload=18432 Bytes Image size=111156 Payload= 13894 Bytes PSNR avg = 51.31
[40]	Randomizing and encrypting the secret message with the help of the KT method, which was created by the person using it, made it safe. When KT is used instead of Chi-square, output is better.	Not compared to rival techniques Image content not considered No numerical results Stego-key value exchange overhead	Greyscale 512x512 from USC-SIPI
[41]	Finds matching cover photos and words that need the fewest changes. For randomizing the data, using a quadratic embedding sequence that	Security is related to the embedding locations Image content not considered Stego-key value exchange overhead	Color image: 256x384 Payload= 23KB. Avg PSNR =52.739

	isn't patterned and has endless i/p parameters. A specially made assignment problem that has been improved is solved by the Hungarian algorithm.	No steganalysis experiments Complexity high	

[43]	As a way to get the highest possible PSNR, randomizing the embedding position and making improvements with Chaotic LM were used to change the LM parameters using the Genetic and Bat algorithms.	High complexity
		No steganalysis tests
		Key exchange overhead
		Image structure not considered
			PSNR
			Org= 47.52
			Optimized=48.44
			SM2LSBPSNR,
			Org= 44.53
			Optimized=45.22

[45]	Randomization key generated using Brownian motion Nonlinear Brownian motion adds more security High capacity	Image contents not considered Complex Payload size not mentioned in the steganalysis Key exchange overhead	128 × 128, 256 × 256, 512 × 512 Avg. PSNR= 48.467 without Brownian
[47]	Randomization is achieved by combining two chaotic LMs to generate PRNG. LM is utilized to generate a DNA sequence The sequence is added to the secret message's DNA sequence using the ASCII format. The result is LSB embedded.”	No tabulated experiments Image regions not considered Key exchange overhead	Payload: 37-character (296 bits) PSNR 99 dB

Table 3 table form for each paper, including author names, advantages, and disadvantages:

Paper Title & Authors (Year)	Advantages	Disadvantages
Pranab K. Muhuri et al. (2022)	Novel steganography method using integer wavelet transformation and PSO.Potential for increased image quality and robustness	Complexity in optimizing PSO parameters Computational intensity for large images
Ayushi Chaudhary et al. (2022)	New perspective on steganography methods, Consideration of pros and cons, Utilization of sequence and asymmetric encryption	Method description is brief Limited evaluation details
Wafa M. Eid et al. (2022)	Comprehensive overview of steganalysis methodologies, Exploration of spatial and transform domains, Analysis of diverse	Limited information on specific datasets Lack of in-depth evaluation metrics

	steganographic methods	
Jiahao Liu et al. (2022)	Comprehensive analysis of steganalysis methodologies Exploration of spatial and transform domains Consideration of conventional and deep learning techniques	Repetition of content with similar paper Lack of unique contribution
Bibek Ranjan Ghosh et al. (2022)	Comprehensive overview of steganographic methods, Highlighting commonly used datasets, Exploration of information concealment	Minimal innovation beyond existing studies Limited focus on unique contributions
Ismail Taha Ahmed et al. (2022)	Utilization of deep learning in steganalysis, Expedited training using pre-existing CNNs High classification precision	Limited focus on the proposed method's uniqueness Lack of comparison with other deep learning models
Bhatia, A. et al. (2021)	Application of GANs in image steganography Exploration of steganographic capacity and visual quality	Limited depth in analyzing GAN-based steganography Lack of comprehensive evaluation metrics
Hu, Y. et al. (2021)	Enhancing steganographic capacity and robustness,Multi-scale feature fusion using CNNs	Methodology and approach could be further detailed Lack of quantitative performance improvement assessment
M. Esaiselvam et al. (2021)	Unique application of steganography for image tilt angle detection, Exploration of multiple steganography methods	Limited depth in analyzing the method Focus on a specific aspect of steganography
Nandhini Subramanian et al. (2021)	Exploration of deep learning methods in steganography Overview of datasets and evaluation measures, Contribution to understanding deep learning's role	Lack of in-depth analysis and comparison Potential overlap with other papers' content
Pei Li et al. (2021)	Integration of deep learning in steganography and steganalysis, Focus on challenges and future developments	Lack of detailed analysis of proposed method, Limited demonstration of superior performance
Ismail Kich et al. (2021)	CNN-inspired approach for color image steganography, Utilization of Auto-Encoder networks and U-net design	Lack of detailed performance evaluation, Limited exploration beyond specific approach
Luo et al. (2020)	Application of deep learning for improved steganograph,Exploration of pixel-value differencing, Focus on enhancing robustness and imperceptibility	Limited explanation of deep learning model architecture, Emphasis on a specific steganography technique
J. H. Lee D. Y. Kang et al. (2020)	Automatic recovery of hidden image information, Use of deep neural network model and entropy features	Limited clarity on the proposed approach, Lack of detailed experimental results
Omar Elharrous Noor Almaadeed et	K-LSB-based steganography method, Resolution enhancement of stego image	Lack of detailed explanation of K-LSB approach. Unclear impact of resolution enhancement

al. (2020)		
Srushti S Yadahalli et al. (2020)	Comparison of two image steganography techniques, Analysis of resulting image parameters	Limited focus on broader context of steganography, Lack of exploration beyond specific methods
B. Vishnu Leena Vishnu Namboothiri et al. (2020)	Use of PVD for improved image steganography, Incorporation of Edge Detection technique	Limited comparison with other steganography methods, Limited depth in discussing advantages and disadvantages
T. Kalaichelvi P. Apuroop et al. (2020)	Combination of CAPTCHA and Image Steganography, Improved security and confidentiality	Lack of detailed implementation description, Limited exploration beyond proposed combination
J. H. Lee D. Y. Kang et al. (2020)	Automated recovery from image steganography, Use of deep neural network and entropy features	Unclear methodology and approach detail, Lack of comprehensive experimental results
S. Kavitha et al. (2020)	Exploration of image steganography with different techniques, Evaluation of image quality and security	Limited depth in discussing proposed technique, Lack of detailed advantages and disadvantages
Jawwad A R. et al. (2020)	Comparative analysis of steganography algorithms, Evaluation based on accuracy, precision, recall, and f1-score	Limited exploration of unique steganography approach. Lack of broader context discussion
Ahmed A. et al. (2022)	Development of new image steganography using quantum substitution boxes. Potential to improve robustness, security, and imperceptibility. Exploration of quantum computing benefits	Complex implementation due to quantum principle Limited real-world quantum computing resources

Table .4 Steganography method

Steganography method	Improved	Needs to be improved
Traditional LSB based	Easy implementation	Security, payload capacity, visual quality of stego image and recovered image
Transform domain based	Better security and payload capacity than traditional LSB	Visual quality of stego and reconstructed images
Machine learning based	Better visual quality of stego and reconstructed images	High complexity, payload capacity can be improved
Support vector machine based	Better security	Not suitable for large dataset
CNN based	High payload capacity, reconstruction quality	Computational cost, security from deep learning based steganalysis
GAN based	High visual quality stego and reconstructed images, low computation cost	Security from deep learning based steganalysis

Table 4 outlines various steganography methods along with their improved aspects and areas that require further enhancement. Traditional LSB-based techniques offer easy implementation but suffer from shortcomings in security, payload capacity, and the visual quality of both the stego and recovered images. Transform domain-based methods provide better security and payload capacity compared to LSB, though they may still fall short in terms of visual quality. Machine learning-based approaches excel in enhancing the visual quality of stego and reconstructed images but are burdened by high complexity, and there's room for improvement in payload capacity. Support vector machine-based techniques offer better security but may not be suitable for handling large datasets effectively. CNN-based methods boast high payload capacity and reconstruction quality but come with increased computational costs and are vulnerable to security threats from deep learning-based steganalysis. GAN-based approaches offer high visual quality in stego and reconstructed images, coupled with low computational costs, but may face challenges in security against deep learning-based steganalysis. In summary, while each method has its strengths, there's ongoing research to address their respective limitations and enhance their overall effectiveness in steganographic applications.

Dataset description

This dataset contains 44,000 512x512 pixels images containing different malicious payloads, i.e., JavaScript, HTML, PowerShell, URLs, and ethereum addresses, embedded via the Least Significant Bit (LSB) technique. The payloads are selected to fit in the first bit of each color channel, i.e., max 512x512x3 bits

https://www.kaggle.com/datasets/marcozuppelli/stegoimagesdataset

Performance evolution

The quality of the steganographer image by minimizing the distortion caused by embedding the secret information and aim to increase the amount of secret information that can be embedded within an image while maintaining a good level of quality image as well as aim to be efficient and fast in both the embedding and extraction processes, Here are some commonly will be used metrics

Peak Signal to Noise Ratio (PSNR) is a commonly used metric to measure the quality of an image in the context of image steganography. The formula to calculate PSNR is:

$$\mathbf{PSNR = 10 * \log10((M^{\wedge}2) / MSE)} \quad \textbf{Eq.5.1}$$

Where M is the maximum pixel value of the image (usually 255 for 8-bit images), and MSE is the mean squared error between the original and steganographer images.

Structural Similarity Index (SSIM): The Structural Similarity Index (SSIM) is a widely used metric for evaluating the quality of steganographic images. It measures the similarity between two images in terms of luminance, contrast, and structure. The formula for SSIM is as follows:

$$\mathbf{SSIM(x,y) = [l(x,y)^{\wedge}alpha] * [c(x,y)^{\wedge}beta] * [s(x,y)^{\wedge}gamma]} \quad \textbf{Eq. 5.2}$$

Where:

x and y are the original and steganographic images, respectively.

- l(x,y) is the luminance similarity measure, which represents the similarity of the mean brightness between x and y.
- c(x,y) is the contrast similarity measure, which represents the similarity of the standard deviation of brightness between x and y.

- s(x,y) is the structural similarity measure, which represents the similarity of the structural information between x and y.

Mean Absolute Error (MAE): MAE measures the average absolute difference between the pixels in the original and steganographic images. A lower MAE value indicates better image quality. In the context of image steganography, the Mean Absolute Error (MAE) is a metric that measures the average absolute difference between the pixel values of the original image and the steganographic image. The formula for calculating the MAE is:

$$MAE = (1/N) * \sum i=1 \text{ to } N \mid I(i) - S(i) \mid \quad \text{Eq. 5.3}$$

Where N is the total number of pixels in the images, I(i) and S(i) are the pixel values of the original and steganographic images, respectively, at the ith pixel location.

Mean Square Error (MSE): MSE is a common metric for evaluating image quality. It measures the average of the squared differences between the pixels in the original and the steganographic images. A lower MSE value indicates better image quality. In image steganography, the Mean Square Error (MSE) is a commonly used evaluation metric to measure the quality of the steganographic image compared to the original image. It is calculated using the following formula:

$$MSE = (1/N) * \sum(i=1 \text{ to } N) [I(i) - S(i)]^2 \quad \text{Eq. 5.4}$$

Where:

- N is the total number of pixels in the image
- I(i) is the intensity value of the ith pixel in the original image
- S(i) is the intensity value of the ith pixel in the steganographic image

Visual Information Fidelity (VIF): VIF is a metric that measures the similarity between the original and steganographic images in terms of the amount of visual information preserved. A higher VIF value indicates better image quality. The formula for VIF can be expressed as:

$$VIF=(2*sigma\_xy+C1)*(2*sigma\_xy+C2)/(sigma\_x\_sq+sigma\_y\_sq+C1)/(sigma\_x\_sq+ sigma\_y\_sq + C2) \quad \text{Eq. 5.5}$$

Where:

- sigma_xy is the covariance between the original and steganographic images.
- sigma_x_sq and sigma_y_sq are the variances of the original and steganographic images, respectively.

C1 and C2 are constants that stabilize the division in the formula and prevent the denominator from being too small. VIF values range from 0 to 1, with a higher value indicating better visual information fidelity between the original and steganographic images. A VIF value of 1 indicates perfect visual information fidelity between the two images.

Normalized correlation coefficient (NCC) : The normalized correlation coefficient (NCC) is a metric commonly used to measure the correlation between the original and steganographic images in image steganography. The formula for NCC can be expressed as:

$$NCC = (1/n) * \sum(x - \mu\_x) *(y - \mu\_y) / \sigma\_x*\sigma\_y \quad \text{Eq. 5.6}$$

Where:

n is the total number of pixels in the images

x and y are the original and steganographic images, respectively

- μ_x and μ_y are the mean pixel values of the original and steganographic images, respectively σ_x and σ_y are the standard deviations of the pixel values of the original and steganographic images, respectively.

The NCC value ranges from -1 to 1, where a value of 1 indicates a perfect positive correlation between the original and steganographic images, a value of -1 indicates a perfect negative correlation, and a value of 0 indicates no correlation. A higher NCC value indicates better image quality, as it implies a stronger correlation between the original and steganographic images.

IV CONCLUSION

In conclusion, image steganography, as a convergence of computer vision and cryptography, has undergone significant developments, presenting both traditional challenges and innovative solutions. This review paper navigates through the landscape of image steganography, examining classical and contemporary methods while addressing critical issues within the field. The classical struggle between concealing maximal information and avoiding detection is explored, with a focus on the significance of payload capacity in steganographic algorithms. Traditional methods, such as embedding RAR archives within JPEG files, are dissected, revealing vulnerabilities to third-party alterations that pose threats to the integrity of concealed data. The review outlines three fundamental categories of steganography methods: image domain, transform domain, and file-format-based. Image domain techniques, notably the LSB method, take center stage as commonly employed strategies, leveraging statistical characteristics for covert information transfer. Delving into contemporary advancements, the paper discusses the integration of deep learning into image steganography. Autoencoder-based models exhibit promising results in terms of embedding capacity and resilience against traditional passive attack methods. However, the emergence of adversarial examples and susceptibility to adversarial attacks underscore the intricate relationship between deep steganography and security challenges. A visual representation of a typical encoder-decoder network for deep steganography models is presented, illustrating attack paths and the conventional path for correct image recovery.The paper concludes by emphasizing the need for a balanced approach in steganography methods, considering factors such as payload capacity, detection resilience, and adaptability to varying cover image patterns. Further research needs to explore how well the CNN and unet based encode and decoder architecture helps develop steganalysis algorithms for images.

References

1. Mielikainen, J. Lsb matching revisited. IEEE Signal Process. Lett. 2006, 13, 285–287.
2. Kawaguchi, E. Eason, R. Principle and applications of BPCS-Steganography. In Proceedings of the SPIE 3528, Multimedia Systems and Applications, Boston, MA, USA, 22 January 1999.
3. Almohammad, A. Hierons, R.M. Ghinea, G. High Capacity Steganographic Method Based Upon JPEG. In Proceedings of the Third International Conference on Availability, Reliability and Security, Barcelona, Spain, 4–7 March 2008.
4. Pevný, T. Filler, T. Bas, P., Using High-Dimensional Image Models to Perform Highly Undetectable Steganography. In Information Hiding Lecture Notes in Computer Science Springer: Berlin/Heidelberg, Germany, 2010 pp. 161–177.
5. Holub, V. Fridrich, J., Designing steganographic distortion using directional filters. In Proceedings of the 2012 IEEE International Workshop on Information Forensics and Security (WIFS), Tenerife, Spain, 2–5 December 2012 pp. 234–239.
6. Holub, V. Fridrich, J. Denemark, T. Universal distortion function for steganography in an arbitrary domain. EURASIP J. Inf. Secur. 2014, 2014. doi:10.1186/1687-417X-2014-1.
7. Sedighi, V. Cogranne, R. Fridrich, J. Content-Adaptive Steganography by

Minimizing Statistical Detectability. IEEE Trans. Inf. Forensics Secur. 2016, 11, 221–234. doi:10.1109/TIFS.2015.2486744. Future Internet 2018, xx, 1 14 of 15

8. Cogranne, R. Sedighi, V. Fridrich, J., Practical strategies for content-adaptive batch steganography and pooled steganalysis. In Proceedings of the 2017 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), New Orleans, LA, USA, 5–9 March 2017 pp. 2122–2126.
9. Digital Compression and Coding of Continuous-Tone Still Images: Requirements and Guidelines Technical Report ISO/IEC 10918-1:1994 Joint Photographic Experts Group Committee: La Jolla, CA, USA, 1994.
10. Roshal, A. RAR 5.0 Archive Format. 2017. Available online: https://www.rarlab.com/technote.htm (accessed on 5 October 2017).
11. Juneja, M. Sandhu, P. Designing of robust image steganography technique based on LSB insertion and encryption. In Proceedings of the IEEE International Conference on Advances in Recent Technologies in Communication and Computing, Kerala, India, 27–28 October 2009 pp. 302–305.
12. Chang, C.C. Chen, T.S. Chung, L.Z. A steganographic method based upon JPEG and quantization table modification. Inf. Sci. 2002, 141, 123–138.
13. Lecun, Y. Boser, B. Denker, J.S. Henderson, D. Howard, R.E. Hubbard, W. Jackel, L.D. Backpropagation applied to hand-written zip code recognition. Neural Comput. 1989, 1, 541–551.
14. Krizhevsky, A. Sutskever, I. Hinton, G.E. Imagenet classification with deep convolutional neural networks. In Proceedings of the 25th International Conference on Neural Information Processing Systems, Lake Tahoe, NV, USA, 3–6 December 2012, pp. 1097–1105.
15. Hu, J. Shen, L. Sun, G. Squeeze-and-Excitation Networks. arXiv 2017, arXiv:1709.01507. 16. Li, Y. Qi, H. Dai, J. Ji, X. Wei, Y. Fully Convolutional Instance-aware Semantic Segmentation. arXiv 2017, arXiv:1611.07709
16. Nair, V. Hinton, G.E. Rectified linear units improve restricted Bolzmann machines. In Proceedings of the 27th International Conference on Machine Learning, Haifa, Israel, 21–24 June 2010 Volume 27, pp. 807–814.
17. Deng, J. Dong, W. Socher, R. Li, L.J. Li, K. Fei-Fei, L. ImageNet: A Large-Scale Hierarchical Image Database. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Miami, FL, USA, 20–25 June 2009.
18. Sobel, I. Feldman, G. An Isotropic 3 × 3 Image Gradient Operators. In Pattern Classification and Scene Analysis Wiley: Hoboken, NJ, USA, 1973 pp. 271–272.
19. Fischer, S. Sroubek, F. Perrinet, L.U. Redondo, R. Cristóbal, G. Self-invertible 2D log-Gabor wavelets. Int. J. Comput. Vis. 2007, 75, 231–246.
20. Dalal, N. Triggs, B. Histograms of oriented gradients for human detection. In Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, San Diego, CA, USA, 20–25 June 2005 Volume 1, pp. 886–893.
21. Rumelhart, D.E. Hinton, G.E. Williams, R.J. Learning representations by back-propagating errors. Nature 1986, 323, 533.
22. Zeiler, M.D. Fergus, R. Visualizing and Understanding Convolutional Networks. In Proceedings of the Computer Vision—ECCV 2014, Zurich, Switzerland, 6–12 September 2014 Volume 8689, pp. 818–

833, doi:10.1007/978-3-319-10590-1_53.

23. Olah, C. Mordvintsev, A. Schubert, L. Feature Visualization. Distill 2017, doi:10.23915/distill.00007.
24. Mahendran, A. Vedaldi, A. Understanding Deep Image Representations by Inverting Them. arXiv 2015, arXiv:1412.0035
25. Hinton, G.E. Zemel, R.S. Autoencoders, minimum description length and Helmholtz free energy. In Proceedings of the Advances in Neural Information Processing Systems, Denver, Colorado, 28 November–1 December 1994 pp. 3–10.
26. Vincent, P. Larochelle, H. Bengio, Y. Manzagol, P.A. Extracting and composing robust features with denoising autoencoders. In Proceedings of the 25th international conference on Machine learning, Helsinki, Finland, 5–9 July 2008 pp. 1096–1103.
27. Wang, W. Huang, Y. Wang, Y. Wang, L. Generalized autoencoder: A neural network framework for dimensionality reduction. In Proceedings of the IEEE conference on computer vision and pattern recognition workshops, Columbus, OH, USA, 23–28 June 2014 pp. 490–497. 29.
28. Kingma, D.P. Welling, M. Auto-Encoding Variational Bayes. arXiv 2013, arXiv:1312.6114. 30. El-emam, N.N. Embedding a large amount of information using high secure neural based steganography algorithm. Int. J. Inf. Commun. Eng. 2008, 4, pp. 223–232. Future Internet 2018, xx, 1 15 of 15
29. Saleema, A. Amarunnishad, T. A New Steganography Algorithm Using Hybrid Fuzzy Neural Networks. Procedia Technol. 2016, 24, 1566–1574. doi:10.1016/j.protcy.2016.05.139.
30. Volkhonskiy, D. Nazarov, I. Borisenko, B. Burnaev, E. Steganographic Generative Adversarial Networks. arXiv 2017, arXiv:1703.05502.
31. Shi, H. Dong, J. Wang, W. Qian, Y. Zhang, X. SSGAN: Secure Steganography Based on Generative Adversarial Networks. arXiv 2017, arXiv:1707.01613.
32. Baluja, S. Hiding Images in Plain Sight: Deep Steganograph. In Advances in Neural Information Processing Systems 30 Guyon, I. Luxburg, U.V. Bengio, S. Wallach, H. Fergus, R. Vishwanathan, S. Garnett, R., Eds. Curran Associates, Inc.: Red Hook, NY, USA, 2017 pp. 2069–2079.
33. Morkel, T. Eloff, J.H. Olivier, M.S. An overview of image steganography. In Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, 29 June–1 July 2005 pp. 1–11.
34. Kadhim, I.J. Premaratne, P. Vial, P.J. Halloran, B. Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing 2019, 335, 299–326.
35. Li, B. He, J. Huang, J. Shi, Y.Q. A survey on image steganography and steganalysis. J. Inf. Hiding Multim. Signal Process. 2011,2, 142–172.
36. Abraham, A. Paprzycki, M. Significance of steganography on data security. In Proceedings of the International Conference on Information Technology: Coding and Computing, Las Vegas, NV, USA, 5–7 April 2004 Volume 2, pp. 347–351.
37. Fridrich, J. Goljan, M. Du, R. Detecting LSB steganography in color, and gray-scale images. IEEE Multimed. 2001, 8, 22–28.
38. Johnson, N.F. Jajodia, S. Steganalysis of images created using current steganography software. In Proceedings of the Information Hiding: Second International Workshop, IH'98, Portland, OR, USA, 14–17 April 1998 pp. 273–289.
39. Amritha, P. Sethumadhavan, M. Krishnan,

R. On the Removal of Steganographic Content from Images. Def. Sci. J. 2016, 66, 574.

40. Hosam, O. attacking image watermarking and steganography-a survey. Int. J. Inf. Technol. Comput. Sci. 2019, 11, 23–37.

41. Zhang, C. Lin, C. Benz, P. Chen, K. Zhang, W. Kweon, I.S. A brief survey on deep learning based data hiding, steganography and watermarking. arXiv 2021, arXiv:2103.01607v2.

42. Baluja, S. Hiding images in plain sight: Deep steganography. Adv. Neural Inf. Process. Syst. 2017, 30, 2069–2079.

43. Baluja, S. Hiding images within images. IEEE Trans. Pattern Anal. Mach. Intell. 2019, 42, 1685–1697.

44. Wang, Z. Zhou, M. Liu, B. Li, T. Deep Image Steganography Using Transformer and Recursive Permutation. Entropy 2022,24, 878. [CrossRef]

45. Chen, F. Xing, Q. Fan, C. Multilevel Strong Auxiliary Network for Enhancing Feature Representation to Protect Secret Images.IEEE Trans. Ind. Inform. 2021, 18, 4577–4586. [CrossRef]

46. Zhu, J. Kaplan, R. Johnson, J. Fei-Fei, L. Hidden: Hiding data with deep networks. In Proceedings of the European Conference on Computer Vision (ECCV), Munich, Germany, 8–14 September 2018 pp. 657–672.

47. Luo, X. Zhan, R. Chang, H. Yang, F. Milanfar, P. Distortion agnostic deep watermarking. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 14–19 June 2020 pp. 13548–13557.

48. 51. Tancik, M. Mildenhall, B. Ng, R. Stegastamp: Invisible hyperlinks in physical photographs. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 14–19 June 2020 pp. 2117–2126.

49. Wengrowski, E. Dana, K. Light field messaging with deep photographic steganography. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Long Beach, CA, USA, 15–20 June 2019 pp. 1515–1524.

50. Zhang, C. Benz, P. Karjauv, A. Sun, G. Kweon, I.S. Udh: Universal deep hiding for steganography, watermarking, and light field messaging. Adv. Neural Inf. Process. Syst. 2020, 33, 10223–10234.

51. Hayes, J. Danezis, G. Generating steganographic images via adversarial training. Adv. Neural Inf. Process. Syst. 2017,30, 1954–1963.

52. Zhang, C. Benz, P. Karjauv, A. Kweon, I.S. Universal adversarial perturbations through the lens of deep steganography: Towards a Fourier perspective. In Proceedings of AAAI Conference on Artificial Intelligence, Virtual, 2–9 February 2021 pp. 3296–3304.

53. Jung, D. Bae, H. Choi, H.S. Yoon, S. Pixel steganalysis: Pixel-wise hidden information removal with low visual degradation.IEEE Trans. Dependable Secure. Comput. 2023, 20, 331–342.

54. Xiang, T. Liu, H. Guo, S. Zhang, T. PEEL: A Provable Removal Attack on Deep Hiding. arXiv 2021, arXiv:2106.02779.

55. 58. Zhong, S. Weng, W. Chen, K. Lai, J. Deep-learning steganalysis for removing document images on the basis of geometric median pruning. Symmetry 2020, 12, 1426.

56. 5. Szegedy, C. Zaremba, W. Sutskever, I. Bruna, J. Erhan, D. Good fellow, I. Fergus, R. Intriguing properties of neural networks.arXiv 2013, arXiv:1312.6199.

57. Goodfellow, I.J. Shlens, J. Szegedy, C. Explaining and harnessing adversarial examples. arXiv 2014, arXiv:1412.6572.

58. Pevny`, T. Filler, T. Bas, P. Using high-dimensional image models to perform

highly undetectable steganography. In Proceedings of the Information Hiding: 12th International Conference, IH 2010, Calgary, AB, Canada, 28–30 June 2010 pp. 161–177.

59. Qin, J. Wang, J. Tan, Y. Huang, H. Xiang, X. He, Z. Coverless image steganography based on generative adversarial network. Mathematics 2020, 8, 1394.
60. Shang, Y. Jiang, S. Ye, D. Huang, J. Enhancing the security of deep learning steganography via adversarial examples. Mathematics2020, 8, 1446.
61. Zhu, X. Lai, Z. Zhou, N. Wu, J. Steganography with High Reconstruction Robustness: Hiding of Encrypted Secret Images. Mathematics 2022, 10, 2934.
62. Moosavi-Dezfooli, S.M. Fawzi, A. Fawzi, O. Frossard, P. Universal adversarial perturbations. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Honolulu, HI, USA, 21–26 July 2017 pp. 1765–1773.
63. Chen, H. Zhu, T. Zhao, Y. Liu, B. Yu, X. Zhou, W. Low-frequency Image Deep Steganography: Manipulate the Frequency Distribution to Hide Secrets with Tenacious Robustness. arXiv 2023, arXiv:2303.13713.
64. Yin, X. Wu, S. Wang, K. Lu, W. Zhou, Y. Huang, J. Anti-rounding Image Steganography with Separable Fine-tuned Network.IEEE Trans. Circuits Syst. Video Technol. 2023.
65. . Pan, W. Yin, Y. Wang, X. Jing, Y. Song, M. Seek-and-hide: adversarial steganography via deep reinforcement learning. IEEE Trans. Pattern Anal. Mach. Intell. 2021, 44, 7871–7884.
66. Wang, Z. Feng, G. Wu, H. Zhang, X. Data hiding during image processing using capsule networks. Neurocomputing 2023,537, 49–60.
67. Zhang, K. Zuo, W. Chen, Y. Meng, D. Zhang, L. Beyond a gaussian denoiser: Residual learning of deep cnn for image denoising.IEEE Trans. Image Process. 2017, 26, 3142–3155.
68. Liao, F. Liang, M. Dong, Y. Pang, T. Hu, X. Zhu, J. Defense against adversarial attacks using high-level representation guided denoiser. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–22 June 2018 pp. 1778–1787.
69. Ilyas, A. Santurkar, S. Tsipras, D. Engstrom, L. Tran, B. Madry, A. Adversarial examples are not bugs, they are features. Adv. Neural Inf. Process. Syst. 2019, 32, 125–136.
70. Yuan, X. He, P. Zhu, Q. Li, X. Adversarial examples: Attacks and defenses for deep learning. IEEE Trans. Neural Netw. Learn. Syst. 2019, 30, 2805–2824.
71. Ma˛dry, A. Makelov, A. Schmidt, L. Tsipras, D. Vladu, A. Towards deep learning models resistant to adversarial attacks. arXiv2017, arXiv:1706.06083.
72. Carlini, N. Wagner, D. towards evaluating the robustness of neural networks. In Proceedings of the 2017 IEEE Symposium on Security and Privacy (sp), San Jose, CA, USA, 22–24 May 2017 pp. 39–57.
73. Thys, S. Van Ranst, W. Goedemé, T. Fooling automated surveillance cameras: adversarial patches to attack person detection. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, Long Beach, CA, USA, 16–17 June 2019.
74. Xu, K. Zhang, G. Liu, S. Fan, Q. Sun, M. Chen, H. Chen, P.Y. Wang, Y. Lin, X. Adversarial t-shirt! evading person detectors in a physical world. In Proceedings of the Computer Vision–ECCV 2020: 16th European Conference, Glasgow, UK, 23–28 August 2020 pp. 665–681.
75. Komkov, S. Petiushko, A. Advhat: Real-world adversarial attack on arcface face id

system. In Proceedings of the 2020 25th International Conference on Pattern Recognition (ICPR), Milan, Italy, 10–15 January 2021 pp. 819–826.

76. Ilyas, A. Engstrom, L. Athalye, A. Lin, J. Black-box adversarial attacks with limited queries and information. In Proceedings of the International Conference on Machine Learning, PMLR, Stockholm, Sweden, 10–15 July 2018 pp. 2137–2146.

77. Brendel, W. Rauber, J. Bethge, M. Decision-based adversarial attacks: Reliable attacks against black-box machine learning models. arXiv 2017, arXiv:1712.04248.

78. Chen, P.Y. Zhang, H. Sharma, Y. Yi, J. Hsieh, C.J. Zoo: Zeroth order optimization based black-box attacks to deep neural networks without training substitute models. In Proceedings of the 10th ACM Workshop on Artificial Intelligence and Security, Dallas, TX, USA, 3 November 2017 pp. 15–26.

79. Cheng, M. Singh, S. Chen, P. Chen, P.Y. Liu, S. Hsieh, C.J. Sign-opt: A query-efficient hard-label adversarial attack. arXiv 2019,arXiv:1909.10773.

80. Byun, J. Cho, S. Kwon, M.J. Kim, H.S. Kim, C. Improving the transferability of targeted adversarial examples through object- based diverse input. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, New Orleans, LA, USA, 18–24 June 2022 pp. 15244–15253.

81. Li, M. Deng, C. Li, T. Yan, J. Gao, X. Huang, H. Towards transferable targeted attack. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition, Seattle, WA, USA, 13–19 June 2020 pp. 641–649.

82. Dong, Y. Liao, F. Pang, T. Su, H. Zhu, J. Hu, X. Li, J. Boosting adversarial attacks with momentum. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, Salt Lake City, UT, USA, 18–22 June 2018 pp. 9185–9193.

83. Liu, Y. Chen, X. Liu, C. Song, D. Delving into transferable adversarial examples and black-box attacks. arXiv 2016,arXiv:1611.02770.

84. Li, Y. Bai, S. Zhou, Y. Xie, C. Zhang, Z. Yuille, A. Learning transferable adversarial examples via ghost networks. In Proceedings of the AAAI Conference on Artificial Intelligence, New York, NY, USA, 7–12 February 2020 Volume 34, pp. 11458–11465.

85. Xu, X., Pan, J. S., Wang, J., & Zhu, W. (2018). A survey on image steganography and steganalysis techniques. Journal of Information Hiding and Multimedia Signal Processing, 9(6), 1361-1376.

86. Malik, A. Sikka, G. Verma, H.K. A high capacity text steganography scheme based on LZW compression and color coding. Eng. Sci. Technol. Int. J. **2017**, 20, 72–79

87. Sadié, J.K. Metcheka, L.M. Ndoundam, R. A high capacity text steganography scheme based on permutation and color coding. arXiv **2020**, arXiv:2004.00948.

88. Pranab K. Muhuri, Zubair Ashraf, Swati Goel (2022), A Novel Image Steganographic Method based on Integer Wavelet Transformation and Particle Swarm Optimization, Applied Soft Computing, Volume 92, 106257, ISSN 1568-4946, https://doi.org/10.1016/j.asoc.2020.106257.

89. Ayushi Chaudhary Ashish Sharma Neeraj Gupta Digital Data Protection using Barcode & Steganographic Approach 2022 International Conference on Automation, Computing and Renewable Systems (ICACRS)Year: 2022

90. Wafa M. EidSarah S. AlotaibiHasna M. AlqahtaniSahar Q. Saleh Digital Image Steganalysis: Current Methodologies and

Future Challenges IEEE Access Year: 2022

91. Jiahao Liu Ge Jiao Xiyu SunFeature Passing Learning for Image Steganalysis IEEE Signal Processing Letters Year: 2022
92. Bibek Ranjan Ghosh Siddhartha Banerjee Ayush Chakraborty Swapnajoy Saha Jyotsna Kumar Mandal A Deep Learning Based Image Steganalysis Using Gray Level Co-Occurrence Matrix 2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT) Year: 2022
93. Ismail Taha Ahmed Baraa Tareq Hammad Norziana Jamil Image Steganalysis based on Pretrained Convolutional Neural Networks 2022 IEEE 18th International Colloquium on Signal Processing & Applications (CSPA) Year: 2022
94. Bhatia, A., & Bedi, P. (2021). Image steganography using generative adversarial networks. Journal of Information Security and Applications, 60, 102805.
95. Hu, Y., & Guo, S. (2021). Image steganography based on convolutional neural networks with multi-scale feature fusion. Soft Computing, 25(4), 2943-2954.
96. M. Esaiselvam R. SambathKumar K. Yuvaraj D. Sriram Technique for Estimating Position of the Pirate identification using Machine Learning Algorithms from an image 2021 International Conference on System, Computation, Automation and Networking (ICSCAN) Year: 2021
97. 97. Nandhini Subramanian Omar Elharrouss Somaya Al-Maadeed Ahmed Bouridane Image Steganography: A Review of the Recent Advances IEEE Access Year: 2021
98. Pei Li Yeli Li Hongjuan Wang Chang Liu Research on Steganalysis of Digital Image Based on Deep Learning2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE) Year: 2021
99. Ismail Kich El Bachir Ameur Youssef Taouil Amine Benhfid Image Steganography Scheme Using Dilated Convolutional Network 2021 12th International Conference on Information and Communication Systems (ICICS) Year: 2021
100. Luo, C., Zhang, W., & Huang, J. (2020). Deep learning based image steganography using pixel-value differencing. Journal of Ambient Intelligence and Humanized Computing, 11(6), 2325-2335.
101. Srushti S Yadahalli Shambhavi Rege Reena Sonkusare (2020) Implementation and analysis of image steganography using LSB and Discrete Wavelet Transform techniques 2020 5th International Conference on Communication and Electronics Systems (ICCES) IEEE
102. B. VishnuLeena Vishnu NamboothiriSandeep R. SajeeshLeena Vishnu Namboothiri (2020) Enhanced Image Steganography with PVD and Edge Detection 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC) IEEE
103. T. KalaichelviP. Apuroop (2020) Image Steganography Method to Achieve Confidentiality Using CAPTCHA for Authentication 2020 5th International Conference on Communication and Electronics Systems (ICCES) IEEE
104. . J. H. LeeD. Y. KangJ. E. LeeS. H. LeeJ.-I. Park (2020) Automatic Recovery of Hidden Image from Image Steganograph y Using DNN and Local Entropy Features 2020 35th International Technical Conference on Circuits/Systems, Computers and Communications (ITC-CSCC) IEE

105. Omar ElharroussNoor Almaadeed Somaya Al-Maadeed (2020) An image steganography approach based on k-LSBs (k-LSB) 2020 IEEE International Conference on Informatics, IoT, and Enabling Technologies (ICIoT) IEEE