Ianna Journal of Interdisciplinary Studies, EISSN: 2735-9891
Volume 7, Issue 1, 2025

An In-Depth Review of Steganography: Methods, Uses, and Progress in Digital Security

Mr.Ravi Kumar Sahu
Research scholar Sage University Indore
ravi.sahu92@gmail.comDr. Hare Ram Sah
Professor
Institute of advance computing
Sage university, Indore
ramaayu@gmail.com

Abstract: Communication is the foundation of development globally, with data networks requiring advanced security measures. The security and confidentiality of transmitted information over the internet, a conglomerate of interconnected, unmanaged networks, are crucial as data volumes grow. Cryptography and steganography are key techniques in ensuring data security, with cryptography encrypting data and steganography concealing it. Cryptography, while secure, can draw attention, leading to potential attacks. Steganography, however, embeds data within multimedia content, making it undetectable. This survey covers various steganography methods, illustrating their evolution from ancient techniques to modern digital applications. Steganography's core principles cover objects, secret messages, and keys ensure secure, hidden data transmission. Evaluating steganographic systems involves metrics like invisibility, security, and robustness. Advances in digital processing and encoding techniques continue to enhance steganography's effectiveness in secure data transfer across diverse media formats, making it an essential tool in modern information security.

keywords-Steganography, Data Security, Information Hiding, Network Security, Multimedia Content, Image Steganography, Text Steganography, Digital Watermarking, Secure Data Transmission.

I INTRODUCTION

Every developing region in the globe relies on communication as its foundational requirement. Particularly in the instance of data networks, the expansion of contemporary communication technologies necessitates unique security measures. Confidentiality and security of transmitted information are universally desired. The security of data exchanged over the internet is a big worry since the internet is not just one network but a global collection of interconnected, unmanaged networks. As the amount of data being transmitted over the Internet continues to rise, network security is assuming greater significance. Cryptography and steganography are two crucial methods for ensuring security. In the field of information security, both are famous and frequently employed. Data encryption relies heavily on steganography and cryptography [1]. Only the sender and the recipient know the encryption key, which is used to change the communication into an encrypted form in cryptography. Only the recipient with the encryption key will be able to read the message. On the other hand, an attacker's suspicions could be aroused during an encrypted message's transmission, leading to violent interceptions, attacks, or decryptions. Steganography methods were created to address the drawbacks of cryptographic systems. It is possible to communicate in a way that makes it undetectable; this technique is known as steganography. Accordingly, steganography conceals data so that it cannot be detected [2]-[3]. "Embedding" describes the act of concealing information within any type of multimedia content, including images, sounds, and videos, in steganography. So can combine the two methods to make data transmissions more secure. Thus, there is a complete separation between cryptography (the art of protecting information) and steganography (the art of concealing information). It is challenging to

decipher steganographic data without a defined process because of the aspect of invisibility or hiddenness. Steganalysis is a method for detecting steganography. Every steganography method needs to have two things: a high degree of invisibility and enough data capacity (the efficiency of hidden information). The process involves embedding the cover file from the sender and the convenient approach is applied at the expected beneficiary end to reveal the hidden message. Figure 1 below shows the techniques applied in steganography.

Basic Structure of Steganography

The fundamentals of Steganography are made up of three mechanisms, which are shown in Figure 1 and explained below.

The Cover or Carrier: For encrypting the secret information, the cover item can be an image (spat, jpg, bmp, png, and so on), an mp3 (sound documents), a message record, a video record, and, surprisingly, a TCP/IP bundle too.

The Message: It can be a simple text or content, a secret image, an audio or video that is going to be transmitted securely.

The Key: Key based steganography is also play a vital role. In the time of encoding and decoding key is used and it tends to be an instance, dark light or irregular numbers, and so forth. depending upon when we encrypting secret message. Key is only to communication body and also gives more robustness, tough time to attackers etc.

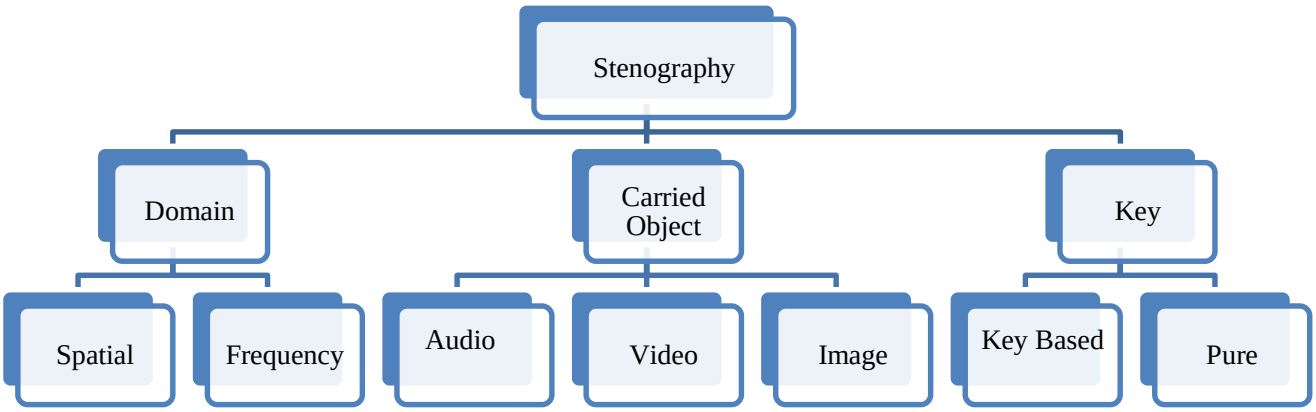

Figure 1 Image Steganography Classification

Confidential data is concealing within the image in a way that the attackers cannot detect the secret information. Embedded image can be obtained through encrypted, Figure 2 showing the Steganography block diagram

Ianna Journal of Interdisciplinary Studies, EISSN: 2735-9891
Volume 7, Issue 1, 2025

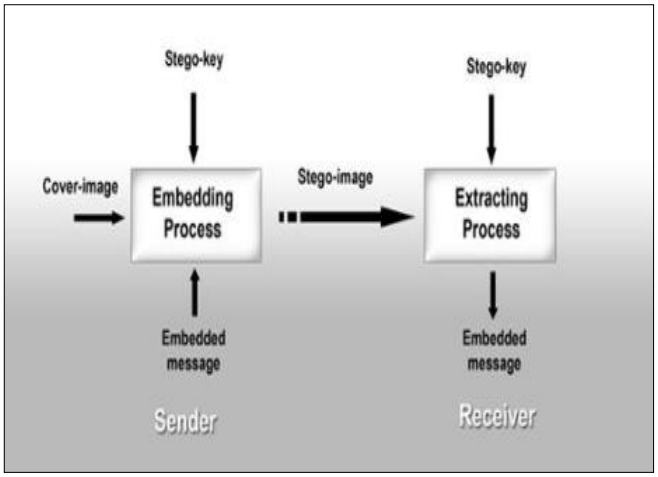

Figure 2 Steganography block diagram

This survey covers a wide range of steganography techniques, including but not limited to: LSB, LSBM, LSBMR, SSHDT, RSTEG, OPA, Genetic-X mean algorithm, VSS, SDSS, FDSS, BPCS, GLM algorithm, SDS, Transform domain techniques, distortion techniques, and many more. This document incorporates all of the articles published on steganographic methods. Every single paper that was used to compile the literature review was sourced from IEEE Explore.

Background of steganographer

The term "Steganography" is derived from the ancient Greek words "Stegano" and "Graphy." Cover writing is the combined meaning. Its versatility dates back thousands of years. In the fifth century, Histaiacus tattooed a phrase on the head of his slave and then had the slave move his hair to convey the message. The art of code-breaking was well-known among the ancient Greeks. A wax-layered tablet was used by one of the ancient Greeks, Demeratus, to write messages. This method involves scratching the message onto a wooden writing tablet. The message was scratched when the wax was scraped off. Following this, the wooden tablet was covered once more with wax, giving the impression that it was blank. The transmission of messages is secure and does not raise suspicion [4]. A method for writing secret messages that the ancient Chinese utilized has been rediscovered by one of Italy's mathematicians, Jerome Carden, nearly fifty years ago. One way was for the sender and the recipient to each use a sheet of paper with grid holes to create a mask. Then, they would write a secret message on the blank paper and then share the mask. Once the grid mask is removed, the empty space on the paper is filled in, giving the impression of harmless writing. Utilizing magazine byproducts, the Germans developed microdot technology based on numerous phases during World War I [5]. During World War II, a variety of methods were employed to encrypt messages, such as invisible ink, the Enigma machine, various null ciphers, and opencoded texts [6]. Additionally, a Saudi ruler initiated a secret writing project at Abdulaziz City of Science and Technology. It was discovered in a text that was almost a thousand years old. They gathered these manuscripts from Turkey and Germany [7]. To learn more about the background of steganography and the methods utilized globally, one can peruse a wide variety of publications [8]. The advent of wireless systems, interconnected multimedia systems, and electronic digital cameras has greatly increased the possibilities for information regeneration and dissemination, thanks to digitization of data. Due to the increase in computer processing power and internet speeds over the past twenty years, steganography techniques have been shifted to digital processing. More secure and reliable steganography methods are being developed thanks to recent advances in signal processing [9], encoding techniques, and information theory. There is little doubt that steganography will continue to advance in the digital realm as a secure data transfer method that is gaining interest from a wide range of industrial applications. Modern steganography methods make it possible to embed data in a variety of media, including but not limited to text codes ,audio ,video and even DNA [11]. Various formats, including Extensible Markup Language (XML),

executable (EXE), and Hyper Text Markup Language (HTML) [12], are also woven within it. Many of the most recent and popular digital steganography techniques were also discussed and shown in the aforementioned publications [13].

Basic Concepts and Terminologies A. Digital Mediums of Steganography

Depending upon a cover object steganography techniques used generally five types for embedding secret messages. Which are explained one by one respectively?

1) Image Steganography

For inserting the encoded data, a picture is utilized. In this sort of steganography, image pixels are utilized for encrypting secret message bits. Due to its generous measure of respective bits, the image is a widely used object and thought to be the best cover [12].

2)Network Steganography

The type of Network Steganography is the kinds of steganography, which are used network protocols as cover object such as IP, TCP, ICMP and UDP and so on. Information is concealed in a couple of fields of the header of TCP/IP bundles that is open or never used [13].

3) Audio Steganography

This kind of audio steganography is tied in with concealing a mystery message in the Audio. It is a method used to get the transmission of privileged conceals its presence. It additionally may give privacy to secret messages assuming that the message is encoded. It used some digital plans like as WAVE, AVI, MPED, MIDI or etc. [14].

4) Video Steganography

Video steganography is a part of information stowing away, which is a strategy that embeds messages into cover contents and is utilized in many fields like clinical frameworks, policing security, access control, and so forth. DCT changes ordinarily alter values 8.667 - 9. Shroud the information in every one of the images in the video and utilized which isn't recognizable by the HVS. Mp4, MPEG, H.264, and AVI etc. are the formats utilized by video steganography [15], [16].

5)Text Steganography

In this kind of the text steganography, it is a component of concealing mystery text messages inside one more message as a covering message or creating a cover message connected with the first mystery message. [17]

II GENERAL PROCEDURE IN STEGANOGRAPHY

An essential principle of digital steganography is the undetectable concealment of secret or private information within a cover medium. Binary bits, text, images, and videos are all possible secret data types. Images, videos, or text, or any other widely used digital format, can likewise serve as the cover media. What is called "Stego-media" is actually the embedded cover media that contains "secret data" that is hidden inside a "cover" or "host" media. The idea of stegomedia is to transmit data over an unsecured or open route. The generic stegano system is shown in Fig. 1 as a block diagram. It is common practice for systems that aim to improve security to employ an encryption scheme and/or security key while embedding. In addition to the embedding map and encryption password, the key may also store the threshold value used to pick the embedding coefficients. Typically, the equation can be used to depict an embedding system.

$$C = Em(C, En(S, k1), k2) \quad (1)$$

Where, C is the cover media, S is the secret data,

The stegomedia is denoted by C, while the secret keys k1 and k2 are utilized by the encryption function En(.) and the embedding function Em(.) accordingly. The secret data, denoted as

$$Sr = D(Ex(C^*, k2), k1) \quad (2)$$

is retrieved after passing the stego-data through a channel. The decryption function, denoted as D(.), and the extraction function, Ex(.), are both inverse embedding functions. The distorted stego media received at the receiver's end, caused by channel noise or intruder attacks, is denoted as C*.

Properties of steganography

To be effective, steganographic systems must possess the following three qualities: invisibility, security, and the ability to conceal information [18]. In contrast, the study by [19] identified four characteristics, including robustness and the aforementioned previous features. When evaluating a steganographic system, these metrics are the most reliable. Different steganographic systems have different handling requirements depending on their intended use. All the characteristics of data embedding are present in watermarking and steganography. Some qualities are more important than others; for example, artifacts have a greater impact and stego-file modification immunity is reduced as the amount of secret data in the stego-image grows [20]. Optimal conditions should be maintained for all properties. When the great capacity, imperceptibility, and security of secret information are paramount, a sufficiently strong steganographic system may not be necessary in all applications. Neither imperceptibility nor high capacity is prerequisites for digital watermarking. It is vitally necessary to have robustness in response to unwanted and harmful attacks, according to. [21]. Figure 3 shows the essential components of any steganography system. More detailed explanations of the attributes are provided in the following section.

Imperceptibility

The most important thing about data embedding is that it can't be seen, even with advanced statistical methods. This is because the secret data is being hidden in the digital image, which is the main strength of any steganographic methodology [22]. Additionally, attackers can utilize statistical approaches to identify the presence or absence of secret data transfer. Accordingly, steganographic methods shouldn't change how people perceive or quantify cover media because of hidden data. Statistical similarity between the original data file and the stego-file indicates improved data transfer security. While it's true that adding secret data to a cover image would make it noisier, that shouldn't stop it from being sent securely [23].

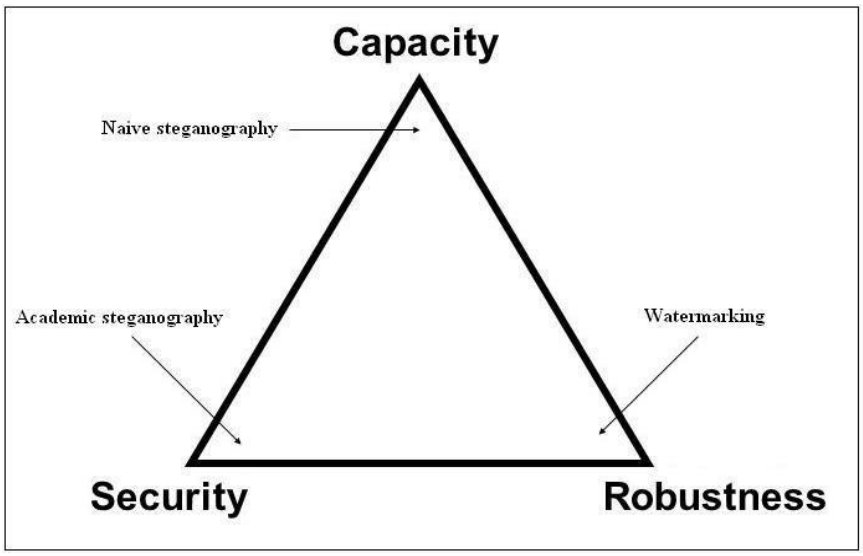

Figure 3. Trade-off between the properties of the data hiding

Security

"Security" in a steganographic context means "un-notice ability" or "undetectability" loosely. This means that any steganography method is considered safe as long as the hidden information can't be recovered or identified statistically. Encrypted transmission of hidden information is a must for steganography. Ensuring the security of data transmissions via open channels is of utmost importance to prevent unauthorized access by individuals or computers.

Payload capacity

The goal of any good steganographic system should be to transmit as much information as possible while utilizing as little cover media as possible. This often necessitates a large embedding capacity since it helps to lessen the likelihood of interception while transmitting over an unsecured network. The embedding rate was described by [24] as the ratio of the amount of concealed information (in bits) to the size of the cover image. Steganography has a significant difficulty in maintaining a higher payload capacity while simultaneously ensuring security and imperceptibility.

Robustness

This is a representation of the embedding and decoding scheme's capability to deal with stego-image corruption caused by image processing operations such as scaling, resizing, rotation, etc. [25]. The notion of transmitting stego-files via the internet makes active attack scenarios irrelevant when dealing with steganography. The result is that the receiver gets a stego-file that is free of distortion. Changes made to stego-files, such as compressing them, changing their format, or transferring them from digital to analog, weaken the steganographic systems. For a fingerprint system, however, resilience is essential in the face of intentional file manipulation.

Table 1 Comparison of characteristics of Information Security techniques.

Characteristics	**Steganography**	**Watermarking**	**Cryptography**
Goal	Preserve the confidential data from the detection	Preserve the authenticity of the cover media	Obfuscate the form or content of data
Cover Selection	Free cover selection	Restriction	N/A
Challenges	Imperceptibility, Security and Capacity	Robustness	Robustness
Key	Optional	Optional	Compulsory
Output	Stego-file	Watermarked-file	Cipher-text
Visibility	Certainly not	Sometimes	Always
The system is invalid if	Detected	Removed or replaced	De-ciphered
Attacks	Steganalysis	Any image processing	Cryptanalysis

Application of Steganography

Steganography is a simple and ever-present method for anyone wishing to conceal sensitive information within an object. The desire to prevent unauthorized individuals from gaining access to the information or from being aware of its existence is one of the reasons why people want to keep certain information private. Useful applications include the pre-recorded listening to music or radio announcements, among others [26]. Several programs may keep their secret message substitutions secret by using steganography .These programs include:

- Protection of Data Alteration
- Modern computer and networking technology
- Media
- Data Base System
- Intelligence services or Intellectual Properties.
- groups and companies
- Medical imaging systems
- Securing multimodal biometric data.
- Digital Watermarking
- E-Commerce
- Corporations with trade secrets to protect.
- Military and defense communication.
- Steganography may become limited under laws because

The most common kind of cover communication for steganography images is a single file type, according to careful analyses of the many uses of this technique. As a result, end-to-end user communication always makes use of images for security purposes. Therefore, it is important to study images to determine which ones are appropriate for certain areas. It is important to keep in mind a few things regarding the image. The use of steganography does not reveal secret correspondence, which means that investigations into the source side, message, and beneficiary are incomplete.

LITERATUTE REVIEW

Ambika et al. (2024) Proposed an attention-guided GAN for coverless image steganography that hides information while preserving critical areas of medical images. This method maintains diagnostic accuracy and resists steganalysis but avoids the typical distortion caused by GANs.[27]

Mikołaj Płachta et al. (2022) Evaluated JPEG steganography detection using deep and shallow learning methods on the BOSS dataset. Algorithms like nsF5 were easily detectable, while J-Uniward at low embedding densities was much harder to detect. Ensemble classifiers showed promising results.[28]

Muhammad Rafly Yanuar et al. (2024) introduced a steganography method combining the LSB 3-3-2 technique with Josephus permutation to improve security and randomness. Tested on RGB images, this method achieved higher payload capacity and better image quality than traditional LSB methods.[29]

Li Li, Xinpeng Zhang et al. (2024) developed a steganography approach using neural networks within AIGC art-style image creation. The method hides secret messages during the image styling process, achieving high capacity and resisting modern steganalysis without needing the original cover image. [30]

Fan Zhang et al. (2024) presented the VRIS model, which protects hidden data from both human vision and machine learning detection. It uses feature fusion, Gaussian noise, and adversarial training to confuse detection models while allowing accurate image reconstruction. [31]

Lin Huo et al. (2024) Proposed CHASE, a GAN-based steganography model that hides color images in greyscale covers using chaotic mapping and image permutation. It achieves high image fidelity and strong steganography resistance, even at high embedding capacities. [32]

Xinran Li et al. (2023) Introduced a cover selection strategy that chooses the most steganography-suitable images based on their undetectability against steganalysis tools. The approach significantly improves the security of hidden communication. [33]

May Alanzy et al. (2023) Proposed a multi-level steganography (MLS) system combining AES and Blowfish encryption with pixel randomization. The method ensures high security, low MSE, and high PSNR, providing reliable data protection with strong encryption. [34]

Mariusz Boryczka et al. (2023) Used ant colony optimization (ACO) to improve steganography by selecting complex regions in images for data hiding. The method balances high data capacity with minimal quality loss, achieving secure and efficient embedding. [35]

Lu Zeng et al. (2023) Proposed an image-to-image steganography method using a U-Net with multi-scale fusion to embed one image into another's Y channel. It achieves high hiding capacity, invisibility, and strong generalization across datasets. [36]

Table 2 Literature Review on Previous Study

S.No.	Author(s)	Year	Method/Technique	Key Features	Dataset/Results
1	Ambika et al.	2024	Attention-guided GAN for Coverless Steganography	Preserves critical image areas; immune to steganalysis	Improves disease classification; high image fidelity
2	Mikołaj Płachta et al.	2022	DL & Ensemble Classifiers for JPEG Steganalysis	Evaluates nsF5, UERD, J-Uniward using BOSS dataset	nsF5: 97.9% detection; J-Uniward: 56.3% accuracy
3	Muhammad Rafly Yanuar et al.	2024	LSB 3-3-2 with Josephus Permutation	Improved security and randomness with RGB images	Outperforms traditional LSB in quality and payload
4	Li Li, Xinpeng Zhang et al.	2024	Neural Network-based AIGC Art Steganography	Uses encoder-decoder; 3 bpp embedding capacity	Robust against modern steganalysis
5	Fan Zhang et al.	2024	Visually Robust Image Steganography (VRIS)	Dual deception: human & ML; noise injection; adversarial setup	High PSNR & SSIM; 96.24% ML misclassification rate
6	Lin Huo et al.	2024	CHASE: Chaotic Mapping with GANs	Hides color images in greyscale; improved fidelity	Outperforms SOTA in fidelity & stego resistance
7	Xinran Li et al.	2023	Steganographic Cover Selection	Symmetric selection to maximize undetectability	Superior cover selection using steganalytic tools
8	May Alanzy et al.	2023	Multi-Level Steganography with AES & Blowfish	Dual encryption; pixel randomization for enhanced security	Low MSE, high PSNR, robust encryption
9	Mariusz Boryczka et al.	2023	Ant Colony Optimization (ACO)-based Steganography	Combines spatial & frequency domains; high capacity, low distortion	Competitive results with minimal quality loss
10	Lu Zeng et al.	2023	Image-to-Image Steganography with U-Net	Multi-scale fusion; high hiding capacity (8 bpp); Y channel embedding	High PSNR & SSIM; strong generalization

III SOME CHALLENGES OF IMAGE STEGANOGRAPHY

For steganography strategies, it is vital the assessments of the encoded picture to be utilized to implant the message into the cover picture without fluctuating its different characteristics .After that, the output image is termed as stego or encrypted image. It is necessary that the encrypted image should be dissident from perceptible alteration and any obscure cannot have the choice to track down these movements and need to control that is implanted image as an ordinary picture, however the favored data sent through this image stay secure. All cover steganography structure faces the significant difficulties based on the given three major criteria of steganography.

Size of payload: Maximum hiding size of secret information into cover objects. Is the most extreme concealing limit conceivable relying upon the cover object for stowing away? Steganography points adequate implanting limit. High payload and robustness is regularly inconsistent because it is very complicated to achieve both of them simultaneously which is needed.

Perception of the image: it is necessary that an encrypted image should produce a high perception and that how an original and encrypted image is remain same.

Toughness for attackers: it is strongly necessary to give a tough time against different type of attacks from assailants, which recognize steganography methods. The stego picture ought to give power against picture handling strategies like pressure, editing, resizing, etc; the point at to restricted data ought not to be much annihilated on the off chance that any of these Steganalysis strategies are performed on stego picture.

In this manner, the ideal steganographic strategy should satisfy the above all the targets as high limit, great visual picture quality, and imperceptibility. Nonetheless, most frequently, cover steganographic methods are defenceless against assailants due the contortion artefacts in the image and better steganographic methods have a great perception of the image due to embedding message up to some limits. Subsequently, how to accomplish all the basics needs of steganography as large embedding capacity, great perception of the image, and imperceptibility is a genuinely moving examination issue because of the inconsistencies of the both secret message bits and image pixels.A table comparing information security techniques such as watermarking, steganography, and cryptography Table 1 Showing The comparing information security techniques such as watermarking, steganography, and cryptography[37].

Table 3 comparing information security techniques such as watermarking, steganography, and cryptography

Criteria	Watermarking	Steganography	Cryptography
Cover Selection	Digital images, audio, video	Digital images, audio, video, text	Plaintext, data
Origin	Insertion into media for authentication	Concealment within media	Encryption of data
Output	Watermarked media	Steganographic media	Encrypted data
Authentication	Provides proof of ownership or authenticity	Provides covert communication	Ensures data integrity and authenticity

Objectives	Protect intellectual property, authentication	Covert communication, data hiding	Secure communication, data integrity
Interpretability	Perceptible under certain conditions	Perceptible only with extraction	Interpretable only with decryption
Robustness	Varies with algorithm; can be robust to attacks	Varies with algorithm; generally less robust	Generally robust if strong algorithms are used
Visibility	Generally visible upon inspection under certain conditions	Invisible without extraction	Completely invisible to unauthorized users
High Payload	Medium to high payload capacity	Medium to high payload capacity	High payload capacity
Attack Resistance	Varies; can be attacked by signal processing techniques	Susceptible to detection and extraction attacks	Resistant to brute force, cryptanalysis attacks
Merits	Easy to implement, effective for copyright protection	Effective for covert communication	Strong security, widely used
Demerits	Can degrade media quality, detectable	Limited robustness, can be detected	Requires key management, computationally intensive
Purpose	Lost with significant degradation or attacks	Lost if the carrier is altered or compromised	Lost if decryption key is lost

Table 2 presents a comprehensive comparison of steganographic techniques categorized into spatial, frequency, and adaptive domains. In the spatial domain, methods such as LSB Replacement, LSB Matching, and Pixel Value Differencing (PVD) manipulate pixel values directly, embedding data by altering either the least significant bits or comparing neighboring pixel values. Frequency domain techniques, like Discrete Cosine Transform (DCT) and Spread Spectrum, modify frequency components to embed information, with DCT altering frequency coefficients and Spread Spectrum techniques hiding data within the frequency spectrum. Adaptive domain approaches, such as the F5 Algorithm and WOW Algorithm, tailor embedding strategies based on noise estimation or data characteristics to enhance robustness and invisibility. This comparative analysis highlights the diversity of steganographic methods tailored to exploit different domains for efficient and covert data embedding.

Table 4 comparing the spatial, frequency, and adaptive domains

Criteria	Spatial Domain	Frequency Domain	Adaptive Domain
Numerical Detectability	High	Medium	Low
Computational Complexity	Low	Medium to High	High
Layout	Direct pixel manipulation	Transform domain manipulation (e.g., DCT, DWT)	Context-aware, varies dynamically
Format	Bitmap, raw pixel data	Compressed formats (e.g., JPEG)	Adaptive to both spatial and frequency domains
Management of Pixels	Direct modification	Modification in transformed coefficients	Adaptive modification based on content
Imperceptibility	Low to medium (depends on changes)	Medium to high (better imperceptibility)	High (optimizes based on content characteristics)
System Category	Simple systems	More complex systems	Advanced systems
Focus Capacity Payload	Medium	High	High
Geometric Attack Resistance	Low	Medium to high	High
Virtual Features	None	Various frequency coefficients	Context-aware features
Integrity	Low to medium	Medium to high	High
Non-Structure Attack Resistance	Low	Medium to high	High

Performance Evaluation Metrics

The performance evaluation metrics for steganography based on the Hiding Limit of Secret Message. Include the metrics PSNR (Peak Signal-to-Noise Ratio), MSE (Mean Squared Error), RMSE (Root Mean Squared Error), and NCC (Normalized Cross-Correlation). These metrics collectively assess the effectiveness of steganographic techniques in embedding secret messages while minimizing perceptible changes to the cover image [38]

Table 5 Performance Evaluation Metrics

Metric	Formula	Description
PSNR (Peak Signal-to-Noise Ratio)	$PSNR=10\log_{10}\frac{MAX^2}{MSE}$	Measures the peak error. Higher PSNR indicates better quality. MAX is the maximum possible pixel value (e.g., 255 for 8-bit images).
MSE (Mean Squared Error)	$MSE=\frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(I(i,k)-k(i,j)^2$	Measures the average squared difference between the original and stego images. Lower MSE indicates better quality. III is the original image, and KKK is the stego image.
RMSE (Root Mean Squared Error)	$RMSE=\sqrt{MSE}$	Measures the square root of the MSE. Lower RMSE indicates better quality.
NCC (Normalized Cross-Correlation)	$NCC=\frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(I(i,k)-k(i,j)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}(I(i,k)-I(i,j)^2\sum_{i=1}^{m}\sum_{j=1}^{n}(I(i,k)-k(i,j)^2}}$	Measures the similarity between the original and stego images. Higher NCC indicates better quality.

Data Sets Used For Image Steganography

A steganographic dataset is a collection of media objects that incorporates cover objects and compares steganographic objects. The PhysioBank Data sets consist of physiological datasets, the UCI KDD datasets [used for information mining, and FVC2002 used in biometrics are only a few examples of famous models. The method of acquiring pictures was one area where we encountered limitations. A small number of images captured during the on-location photography technique will need to be removed from the dataset. Hence, just a small fraction of the sample (16%) deals with images taken inside. At the very least, we believe that a true representation of verified applications requires coherence across indoor and outdoor photos. Date, time, implanting rate, and the path to ancient rarity were among the events recorded throughout the inquiry, and all unique artifacts were hashed (MD5) for verification reasons. Because of this, we were able to verify that, following the implanting mechanism, the Cover photographs and the Steganographic pictures did not resemble each other. Additionally, this proves that the particular payload could be recovered if the tools used could do so. they organized a final dataset with a total of 14,000 photographs towards the end of the trial. This dataset included the original cover pictures, pre-processed cover pictures, and the final Steganographic pictures. [40]

Table 6 Image Steganography Datasets

S.No.	Dataset Name	Description	Image Type	No. of Images	Size Range	Source
1	BOSSBase	Standard dataset for steganalysis and steganography	Grayscale	10,000	512×512 pixels	BOSSbase.org
2	BOWS-2	Widely used for embedding and testing steganography	Grayscale	10,000	512×512 pixels	bows2.gipsa-lab.inria.fr
3	COCO	Real-world complex image dataset	RGB	330,000+	Various sizes	cocodataset.org
4	ImageNet	Large-scale dataset for image recognition tasks	RGB	14 million+	Various sizes	image-net.org
5	ALASKA	Benchmark dataset for steganalysis competition	JPEG	50,000+	Various sizes	Kaggle (ALASKA challenge)
6	Dresden Image Database	Dataset for digital image forensics	RGB	14,000+	Various sizes	forensics.inf.tu-dresden.de
7	Stego-Image Database (Custom)	Generated by embedding secret data into cover images	RGB/Grayscale	Custom	Custom sizes	Self-generated
8	USC-SIPI Image Database	Classical test images (Lena, Baboon, Peppers, etc.)	Grayscale/RGB	1,000+	Various sizes	sipi.usc.edu

IV CONCLUSION

Digital Era of Steganography the period of digital steganography plays a significant role in the realm of the digital world with the use of signal data processing programming and data theories .The expanding technological innovation patterns of steganography used as a part of the different field like in networking, military, health, interactive media and so forth Moreover, the advancement of steganography is increasingly turning out to be where individuals are not just intrigued on concealing messages. Additionally, they are also willing to acquire the hidden data without twisting or removing the actual message in interactive media. It was examined in the University of Michigan with around three million pictures from the cloud trying to find a trace to stenographic data, but they could not find a bit of any covert message; although evidences to the failed result was stated Steganography, as a method for concealing sensitive information within digital media, has evolved significantly over time, driven by advancements in digital processing and encoding techniques. This survey has explored a wide array of steganographic methods, ranging from image and audio to video and text steganography, highlighting their applications in diverse fields such as network security, multimedia systems, and biometrics. The core principles of steganography imperceptibility, security, and robustness remain critical for evaluating the effectiveness of steganographic systems. Techniques like LSB, LSBM, and various transformation domain methods have been discussed, emphasizing their roles in secure data transmission. Looking ahead, the field of steganography faces challenges in balancing payload capacity, robustness against attacks, and maintaining perceptual quality of cover media. Researchers continue to explore new methodologies to enhance the security and reliability of steganographic systems amidst evolving threats of detection (steganalysis).

Future Directions and Challenges

Cover steganography researchers face the difficult task of finding equilibrium between payload, robustness, perception, etc. Some steganographic approaches are allowed, but these procedures are seen as being presented to at least one sort of Steganalysis. Since confidentiality in steganography relies on the consistency of these characteristics, no existing steganography method can provide all of them. Steganographers still face a clear challenge due to the properties' complete lack of relationship with one another: how to establish reliability among the key assessment models of cover steganography without compromising the secrecy of any of the parameters that are most important and vulnerable. In the future, machine learning and deep learning are poised to advance significantly across several critical fronts. Key directions include enhancing explain ability through methods like Explainable AI (XAI), continual learning to adapt to evolving data environments, and integrating multimodal learning for comprehensive data understanding. Automating model development and deployment via AutoML and addressing ethical considerations through frameworks for AI usage are also pivotal. Furthermore, AI's role in sustainability and environmental applications is set to expand, alongside efforts to bolster model robustness against adversarial attacks and ensure data privacy. However, challenges persist in maintaining fairness, scalability, and interpretability of AI systems, alongside the need for seamless deployment and real-time learning capabilities, marking crucial areas for ongoing research and development in the field.

REFERENCES

1. J. Kadhim, P. Premaratne, P. J. Vial and B. Halloran. (2019). “Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research,” *Neurocomputing*, vol. *335*, pp. 299–326.
2. Dhawan, Sachin, and Rashmi Gupta. "Analysis of various data security techniques of steganography: A survey." Information Security Journal: A Global Perspective 30.2 (2021): 63- 87.
3. Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. Neurocomputing, 335, 299-326.
4. Yang, Peng, Yingjie Lao, and Ping Li. "Robust Watermarking for Deep Neural Networks via Bi-Level Optimization." Proceedings of the IEEE/CVF International Conference on Computer Vision. 2021.
5. Pirandola, Stefano, et al. "Advances in quantum cryptography." Advances in Optics and Photonics 12.4 (2020): 1012-1236.
6. Saini, Ravi, Kamaldeep Joshi, and Rainu Nandal. "An Adapted Approach of Image Steganography Using Pixel Mutation and Bit Augmentation." Smart Computing Techniques and Applications. Springer, Singapore, 2021. 217-224.
7. 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
8. Wafa M. Eid;Sarah S. Alotaibi;Hasna M. Alqahtani;Sahar Q. Saleh Digital Image Steganalysis: Current Methodologies and Future Challenges IEEE Access Year: 2022
9. Jiahao Liu; Ge Jiao; Xiyu SunFeature Passing Learning for Image Steganalysis IEEE Signal Processing Letters Year: 2022
10. 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
11. S. P. Jakhar, A. Nandal, A. Dhaka, B. Jiang, L. Zhou, and V. N. Mishra, ‘‘Fractal feature based image resolution enhancement using wavelet– fractal transformation in gradient domain,’’ *J. Circuits, Syst. Comput.*, vol. 32, no. 2, Jan. 2023, Art. no. 2350035.
12. A. Dhaka, A. Nandal, H. G. Rosales, H. Malik, F. E. L. Monteagudo, M. I. Martinez-Acuna, and S. Singh, ‘‘Likelihood estimation and wavelet transformation based optimization for minimization of noisy pixels,’’ *IEEE Access*, vol. 9, pp. 132168–132190, 2021.
13. J.C. Ingemar, M.L. Miller, A.B. Jeffrey, J. Fridrich, T. Kalker, Digital watermark-ing and steganography, 2008. doi:10.1016/B978-0-12-372585-1.X5001-3.
14. F.Y. Shih, Digital Watermarking and steganography: Fundamentals and Tech-niques, CRC Press, 2017.
15. I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, Morgan Kaufmann, 2007.
16. J.C. Judge, Steganography: Past, Present, Future, Lawrence Livermore National Lab., CA (US), 2001.
17. D. Kahn, The history of steganography, Information Hiding, Springer, 1996, pp. 1–5.
18. H. Wang, S. Wang, Cyber warfare: steganography vs. steganalysis, Commun. ACM. 47 (2004) 76–82.

19. B. Li, J. He, J. Huang, Y.Q. Shi, A survey on image steganography and steganal-ysis, J. Inf. Hiding Multimed. Signal Process 2 (2011) 142–172.
20. L.M. Marvel, C.T. Retter, C.G. Boncelet, A methodology for data hiding us-ing images, in: Proceedings of the IEEE Military Communications Conference, IEEE, 1998, pp. 1044–1047.
21. H. Mathkour, B. Al-Sadoon, A. Touir, A new image steganography technique, in: Proceedings of the 2008 4th International Conference on Wireless Com-munications, Networking and Mobile Computing, IEEE, 2008, pp. 1–4.
22. A.A.J. Altaay, S. Bin Sahib, M. Zamani, An introduction to image steganogra-phy techniques, in: Proceedings of the 2012 International Conference on Ad-vanced Computer Science Applications and Technologies (ACSAT), IEEE, 2012, 122–126.
23. 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
24. S. Edward Jero, P. Ramu, R. Swaminathan, Imperceptibility - robustness trade-off studies for ECG steganography using continuous ant colony optimization, Expert Syst. Appl. 49 (2016) 123–135, doi:10.1016/j.eswa.2015.12.010.
25. Mushenko, Alexey, Alexander Zolkin, and Aleksandr Yatsumira. "Steganography Analysis of Chaotic Carrier Signal Transmission with Non-linear Parametric Modulation." 2021 International Russian Automation Conference (RusAutoCon). IEEE, 2021.
26. Alsaawy, Yazed, et al. "Double SteganographyNew Algorithm for More Security." 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom). IEEE, 2021.
27. Ambika,Virupakshappa,Deepak S. Uplaonkar (2023)“Deep Learning-Based Coverless Image Steganography on Medical Images Shared via Cloud “2023, 59(1), 176; https://doi.org/10.3390/engproc2023059176, 18 January 2024
28. Mikołaj Płachta,Marek Krzemień,Krzysztof Szczypiorski,rzysztof Szczypiorski,Artur Janicki (2022) “Detection of Image Steganography Using Deep Learning and Ensemble Classifiers” 2022, 11(10), 1565; https://doi.org/10.3390/electronics11101565, 13 May 2022
29. Muhammad Rafly Yanuar,Suryadi MT,Catur Apriono,Muhammad Firdaus Syawaludin (2024) “Image-to-Image Steganography with Josephus Permutation and Least Significant Bit (LSB) 3-3-2 Embedding” 024, 14(16), 7119; https://doi.org/10.3390/app14167119, 14 August 2024
30. Li Li,Xinpeng Zhang, Kejiang Chen,Guorui Feng,Deyang Wu,Weiming Zhang (2024) “Image Steganography and Style Transformation Based on Generative Adversarial Network” 2024, 12(4), 615; https://doi.org/10.3390/math12040615, 19 February 2024
31. Fan Zhang,Yanhua Dong,Hongyu Sun (2024) “Research on Key Technologies of Image Steganography Based on Simultaneous Deception of Vision and Deep Learning Models” 2024, 14(22), 10458; https://doi.org/10.3390/app142210458, 13 November 2024
32. Lin Huo,Ruipei Chen,Jie Wei,Lang Huang (2024)“A High-Capacity and High-Security Image Steganography Network Based on Chaotic Mapping and Generative Adversarial Networks” 2024, 14(3), 1225; https://doi.org/10.3390/app14031225, 1 February 2024

33. Xinran Li, Daidou Guo,Chuan Qin (2023)“Diversified Cover Selection for Image Steganography” 2023, 15(11), 2024; https://doi.org/10.3390/sym15112024, 6 November 2023
34. May Alanzy,Razan Alomrani,Bashayer Alqarni,Saad Almutairi “Image Steganography Using LSB and Hybrid Encryption Algorithms” 2023, 13(21), 11771; https://doi.org/10.3390/app132111771, 27 October 2023
35. Mariusz Boryczka,Grzegorz Kazana (2023) “Hiding Information in Digital Images Using Ant Algorithms” 2023, 25(7), 963; https://doi.org/10.3390/e25070963, 21 June 2023
36. Lu Zeng, Ning Yang,Xiang Li,Aidong Chen,Hongyuan Jing,Jiancheng Zhang (2023)“Advanced Image Steganography Using a U-Net-Based Architecture with Multi-Scale Fusion and Perceptual Loss” 2023, 12(18), 3808; https://doi.org/10.3390/electronics12183808, 8 September 2023
37. Taha, Mustafa Sabah, et al. "A Steganography Embedding Method Based on P single/P double and Huffman Coding." 2021 3rd International Cyber Resilience Conference (CRC). IEEE, 2021.
38. Hussain, Mehdi, et al. "Image steganography in spatial domain: A survey." Signal Processing: Image Communication 65 (2018): 46-66.
39. Taha, Mustafa Sabah, et al. "Information Hiding: A Tools for Securing Biometric Information." Technology Reports of Kansai University 62.04 (2023): 1383-1394.
40. Wahab, Osama Fouad Abdel, et al. "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques." IEEE Access 9 (2021): 31805- 31815.