Comprehensive Survey of Image Steganography: Techniques, Challenges, and Future Directions

[1]Sharath Babu CG, [2]Dr.Komala K

[1]Research Scholar, Assistant Professor, Department of Computer Science and Engineering, Sri Siddartha Institute of Technology Thumkur, Karnataka

[2]Associate Professor, Department of Electronics and Communication Engineering, Sri Siddartha Institute of Technology Thumkur, Karnataka

[1]sharathbabu1997@gmail.com, [2]komalak@ssit.edu.in

Abstract:

In the rapidly advancing digital world, the need for secure data transmission has become paramount, leading to the significant development of image steganography. Image steganography involves embedding secret messages within digital images, ensuring that the existence of the hidden information remains undetectable. This survey paper provides a comprehensive classification and analysis of various image steganography methods, categorized into Spatial Domain, Transform Domain, Adaptive Steganography, and Statistical Methods. By examining each method's principles, advantages, and limitations, this paper identifies critical challenges and research gaps in the field. These include enhancing robustness against image processing attacks, balancing computational efficiency, increasing embedding capacity, improving detection resistance, simplifying implementation, and enhancing key management and synchronization. Furthermore, the paper evaluates recent advancements, particularly those involving deep learning techniques such as Convolutional Neural Networks (CNNs) and Generative Adversarial Networks (GANs), and their impact on improving the effectiveness and robustness of steganographic methods. This survey aims to provide a thorough understanding of the current state of image steganography and to guide future research towards more secure and efficient data hiding techniques**.**

Keywords*: Image Steganography, Secure Data Transmission, Deep Learning Techniques, Steganographic Methods.*

1 INTRODUCTION

Steganography is the art and science of hiding information within other seemingly innocuous data to conceal the existence of the hidden information. Unlike cryptography, which merely scrambles data to make it unreadable, steganography embeds secret messages within a medium such as images, audio files, or text documents [1]. The primary objective of steganography is to prevent detection, whereas the goal of cryptography is to prevent unauthorized access.

By embedding information within a medium that appears ordinary and harmless, steganography offers an additional layer of security [2]. This technique has historical roots, dating back to ancient times when hidden messages were used for covert communication.

The process of steganography typically involves several key steps. First, the data to be hidden (the payload) is prepared, which may involve compression or encryption to reduce its size and enhance security [3]. Next, a cover medium is selected, which is the data within which the payload will be embedded. Common cover media include digital images, audio files, and video clips due to their large sizes and redundant data, which provide ample space for embedding hidden messages without noticeable degradation [4]. The payload is then embedded into the cover medium using a steganographic algorithm, which modifies specific bits of the cover data. The result is a stego-medium, which looks and functions almost identically to the original cover medium, thereby concealing the presence of the hidden information [5-6]. Figure 1 shows the steganography process.

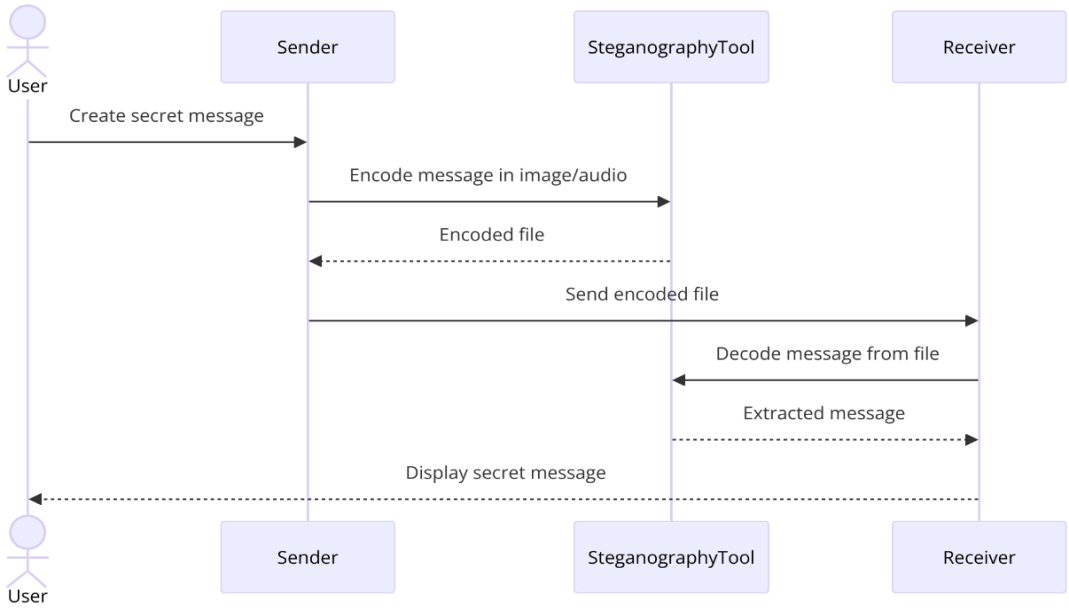

Figure 1 steganography process

Multimedia objects including photos, music, video, text, and network protocol make up the bulk of cover objects utilized in today's sophisticated digital environment to hide concealed communications [7]. "Cover media" describes the place set aside for the safekeeping of very confidential and secret data. FIGURE 2 employs six different steganography techniques for steganography based on cover media in the digital medium. Steganography includes a range of methods for hiding data on different kinds of carriers, as Figure 2 illustrates. In order to do this, a concealed message must be included into a cover object, which may be any type of file—text, images, emails, networks, videos, or audio files. A thorough description of each of the aforementioned kinds is given in the section that follows [8].

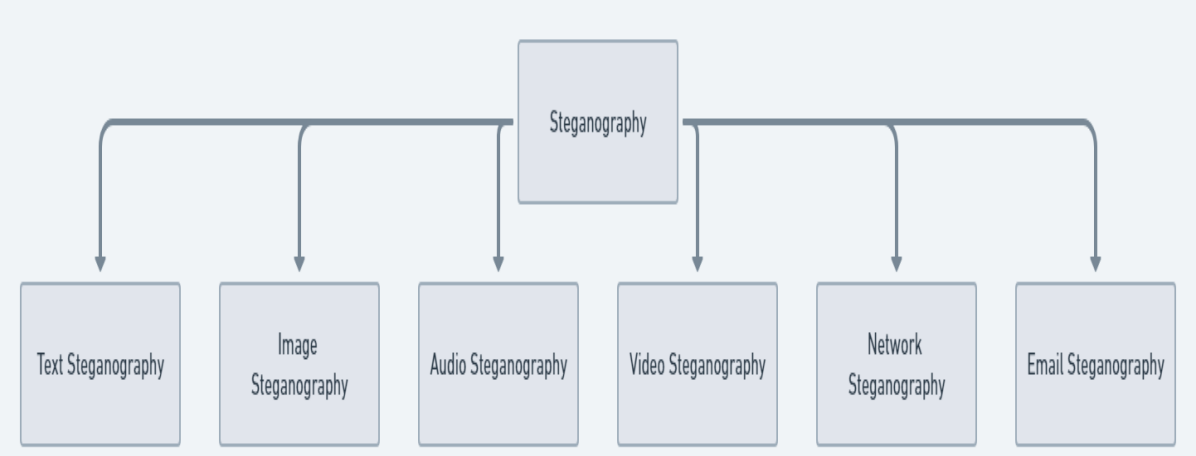

Figure 2 types of steganography

- **Text Steganography**
  Text steganography involves hiding information within text files. Techniques include using invisible characters, altering the format and structure of text, or embedding hidden messages within the text's whitespace or punctuation. Methods such as line-shift coding, word-shift coding, and feature coding are often employed to achieve this.

- **Image Steganography**
  Image steganography, as previously discussed, entails embedding secret messages within digital images. This is usually done by manipulating the least significant bits (LSBs) of pixel values to encode the hidden data. The goal is to ensure the modifications are imperceptible to human eyes, making the hidden message undetectable in the cover image.

- **Audio Steganography**
  Audio steganography hides information within audio files. Techniques include modifying audio samples or using methods like phase coding, spread spectrum, and echo hiding. The changes to the audio file are made in such a way that they are imperceptible to human hearing, ensuring the hidden message remains concealed.

- **Video Steganography**
  Video steganography involves embedding information within video files. This technique takes advantage of the redundancy in video frames and the high capacity of video files to hide data. Methods include altering the pixel values, manipulating the motion vectors, or embedding data in the audio stream of the video. The goal is to keep the hidden message undetectable while maintaining the video's visual and auditory quality.
- **Network Steganography**
  Network steganography hides information within network protocols and communications. This can be done by manipulating packet headers, inter-packet delays, or using covert channels within the network traffic. The aim is to transmit hidden data without altering the appearance or behavior of the network communication, thus avoiding detection by network monitoring tools.

- **Email Steganography**
  Email steganography embeds hidden messages within email communications. Techniques include altering the formatting of the email, embedding information in attachments, or using certain keywords and phrases to encode the message. The objective is to conceal the hidden information within the normal flow of email communication, making it undetectable to standard email security tools.

A steganographic system must possess the capability to hide information, ensure security, and remain undetectable [9]. The investigation conducted by [10] identified four attributes, which include robustness and the traits previously described. The efficacy of a steganographic system can be evaluated using the following metrics: Various steganographic systems require different handling protocols depending on the specific circumstances. There exist similarities between watermarking, steganography, and data embedding techniques. As the quantity of confidential data embedded within the stego-image increases, there is a balance to be struck between the resistance to manipulation of the stego-file and the impact on the visual quality of the image artifacts [11]. Ensuring optimal maintenance of every property is of utmost importance. For certain purposes, it may not be necessary to possess an exceptionally dependable steganographic system. However, it is essential to implement strong security protocols, a significant storage capacity, and ensure the protection of confidential information. When considering digital watermarking, it is not necessary for a watermark to possess both a large capacity and imperceptibility. The importance of resilience in defending against unauthorized and malicious attacks has been emphasized by [12].

The term "image steganography" refers to the technique of concealing one image within another. Picture steganography, in contrast to encryption, aims to decrease the detectability of the encoded data and minimize the likelihood of arousing suspicion by modifying the cover image. Steganography is a technology utilized for the purpose of extracting concealed data and discovering covert messages within an image [13]. Steganalysis is a technique used to differentiate between a conventional picture and a stego image. Furthermore, a comprehensive analysis is conducted to accurately determine the exact location and content of the concealed image within the primary image. Deep learning (DL) has become increasingly popular and is being widely applied in various domains due to the abundance of accessible data. Deep learning techniques have a wide range of applications, including recommendation systems, photo identification, automatic voice recognition, natural language processing, image classification, and medical image processing [14]. Steganography has made significant advancements due to the utilization of deep learning techniques such as convolutional neural networks (CNNs) and generative adversarial networks (GANs), despite being a relatively new subject. The application of these techniques in both steganography and steganalysis has significantly advanced these fields. Figure 3 shows the Types of image stegnography methods.

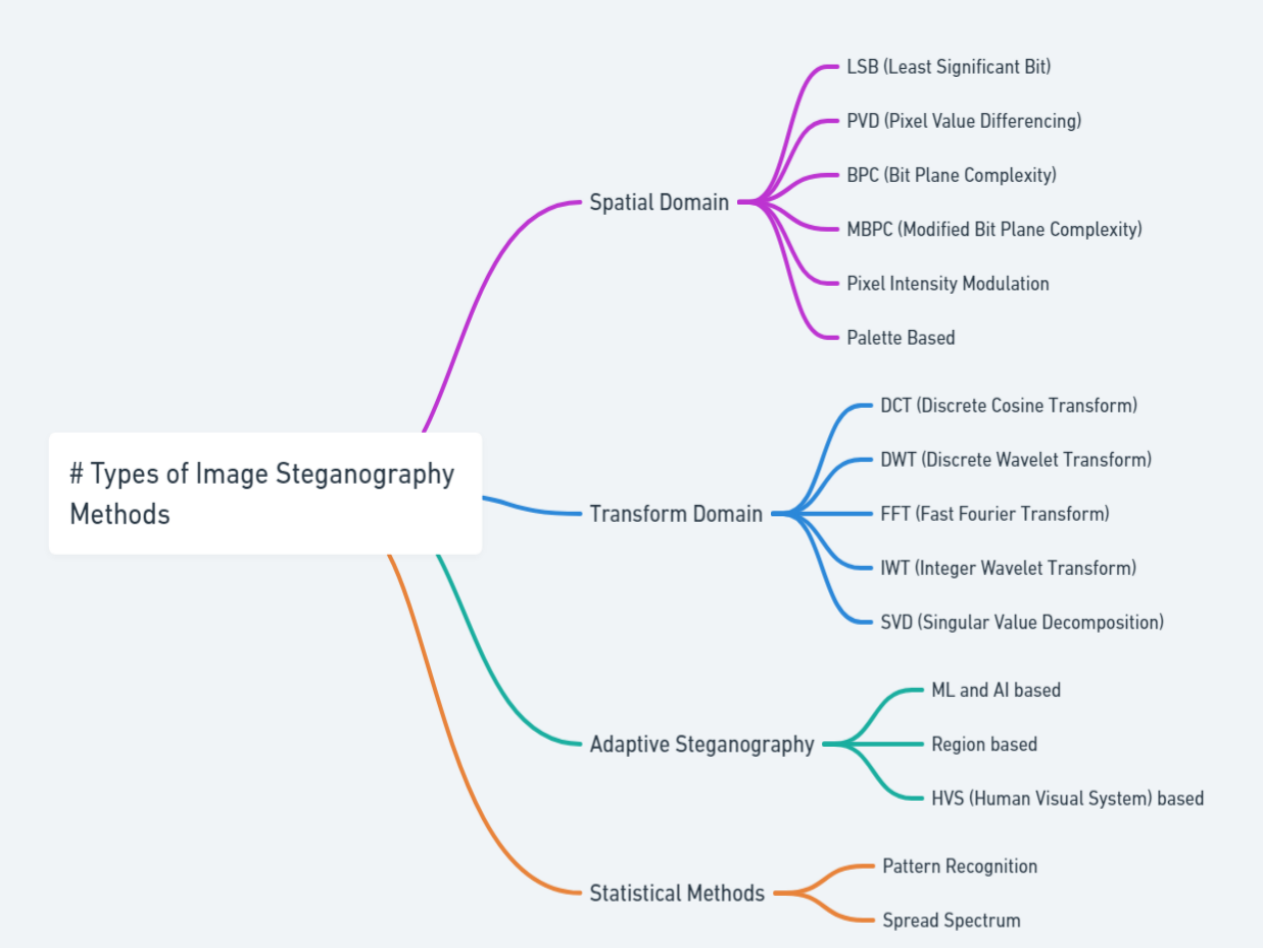

Figure 3 Types of image stegnography methods

The types of image steganography methods can be categorized into four primary domains: Spatial Domain, Transform Domain, Adaptive Steganography, and Statistical Methods. Each domain encompasses various techniques with unique approaches to embedding data within images [15]. In the **Spatial Domain**, data is embedded by directly altering the pixel values of an image. The **Least Significant Bit (LSB)** method, for example, hides information by modifying the least significant bits of the pixel values, making it a straightforward and widely used technique. **Pixel Value Differencing (PVD)**, on the other hand, hides data by changing the difference between the values of adjacent pixels, which can provide better imperceptibility. **Bit Plane Complexity (BPC)** and its advanced version, **Modified Bit Plane Complexity (MBPC)**, involve modifying the complexity of the bit planes of an image to embed data. **Pixel Intensity Modulation** embeds information by adjusting the intensity of the pixels, while **Palette Based** methods embed data by altering the palette of indexed color images, changing the color indices to hide information.

The **Transform Domain** involves embedding data in the frequency coefficients of an image, providing better resistance to common image manipulations and compression. **Discrete Cosine Transform (DCT)** embeds data in the frequency components after applying DCT, which is commonly used in JPEG compression.

Discrete Wavelet Transform (DWT) uses wavelet transforms to embed data in different frequency components, offering multi-resolution analysis. **Fast Fourier Transform (FFT)** hides data in the Fourier coefficients of the image, while **Integer Wavelet Transform (IWT)** is a lossless version of wavelet transform that embeds data without introducing distortions. **Singular Value Decomposition (SVD)** is another technique where data is embedded in the singular values of the image matrix, offering robustness against various image processing operations.

Adaptive Steganography includes techniques that adaptively select embedding locations to maximize imperceptibility and robustness. Methods based on **Machine Learning (ML) and Artificial Intelligence (AI)** leverage advanced algorithms to determine optimal embedding sites. **Region-based** techniques focus on specific regions of an image for data embedding, ensuring that the modifications are less noticeable. **Human Visual System (HVS) based** methods consider the characteristics of human vision to hide data in areas where changes are less likely to be detected by the human eye.

Statistical Methods use statistical properties of the image to embed data, offering higher security. **Pattern Recognition** techniques involve embedding data by altering patterns within the image that are recognizable by specific algorithms. **Spread Spectrum** methods spread the hidden data across the image, making it more resistant to noise and other image processing attacks. These diverse methods provide a range of options depending on the required balance between imperceptibility, robustness, and complexity.

To make image steganography, the Least Significant Bits (LSB) replacement approach is frequently employed. Higher-quality pixels are frequently present in images, but not all of them are utilized. The premise behind least significant bit (LSB) approaches is that a very small fraction of pixel values will change in a way that is not visible to the human eye. To represent the encrypted data in binary form, a conversion step is utilized. The least significant places in the noisy zone are found by scanning the cover image. The binary bits from the concealed image are included in the least significant bits (LSBs) of the cover image. When using the alternative method, it's crucial to exercise caution since if you add too much text to the cover image, it might cause significant modifications that reveal personal information.

The encoder-decoder architecture has a major influence on CNN-based picture steganography. To create the stego picture, the encoder needs two inputs: the cover image and the secret image. The encoded secret picture is output by the decoder after receiving the stego image as input. The fundamental idea hasn't changed despite several attempts to investigate different designs. The convolutional and pooling layers are in charge of the expected changes, even if the hidden image and input cover picture are related in different ways. Different approaches use different iterations of filters, filters' size, activation schemes, loss functions, and stages. Remember that in order to guarantee that every pixel in the hidden image is dispersed over the cover image, the sizes of the cover image and the secret image must coincide.

General Adversarial Networks (GANs), a kind of deep Convolutional Neural Networks (CNNs), were suggested by Goodfellow et al. (2014) [35]. A Generative Adversarial Network (GAN), which trains a generative model using an adversarial process based on concepts from game theory, may be tasked with producing images. The generator and discriminator networks of the GAN architecture compete with one another to produce the best image. The generator model uses the data to produce an output image that is very similar to the original input image.

Discriminator networks are employed in the method to discern real from false images. By training the two networks, the generator model lowers noise introduction while faithfully replicating the input data. When it comes to recognizing fake images, the discriminator model is very accurate. Other advances have been proposed to improve GAN's performance and suitability for applications that need to generate false pictures.

1.1 Challenges

Here are five key challenges in image steganography:

- **Limited Embedding Capacity**

  The amount of data that can be hidden within an image without noticeable distortion is inherently limited. Striking the right balance between embedding a significant amount of data and maintaining the visual quality of the image is a major challenge.

- **Robustness Against Image Processing Attacks**

  Images often undergo various processing operations such as compression, resizing, filtering, and cropping. Ensuring that the embedded data remains intact and recoverable after such operations is a critical challenge for steganographic techniques.

- **Detection and Steganalysis Resistance**

  Steganalysis techniques are continuously improving and becoming more sophisticated in detecting hidden data. Developing steganographic methods that can effectively evade detection by advanced steganalysis tools is a significant ongoing challenge.

- **Computational Efficiency**

  Some advanced steganographic methods, particularly those in the transform domain, can be computationally intensive. Ensuring that these methods are efficient and can be executed quickly without requiring excessive computational resources is crucial for practical applications.

- **Key Management and Synchronization**

  Many steganographic methods rely on secret keys for embedding and extracting data. Managing these keys securely, ensuring their proper distribution, and maintaining synchronization between the sender and receiver are critical for maintaining the security and integrity of the hidden data.

1.2 Motivation and contribution

In an era where digital data transmission and security are paramount, image steganography has emerged as a vital technique for covert communication. The need for secure methods to hide sensitive information within digital images has grown alongside advancements in digital technology and the proliferation of multimedia content. Image steganography not only provides an additional layer of security by concealing the existence of the hidden information but also maintains the usability and appearance of the digital content. This survey paper aims to explore the diverse methods of image steganography, analyze their effectiveness, and address the technical and perceptual challenges they face. By evaluating the current state of research and advancements in this field, this paper seeks to provide a comprehensive understanding of the strengths and limitations of various steganographic techniques, paving the way for future innovations and improvements in secure data embedding and transmission.

- **Comprehensive Classification and Analysis**: This paper systematically categorizes and analyzes various image steganography methods, highlighting their principles, advantages, and limitations.
- **Identification of Challenges and Research Gaps**: The survey outlines key challenges in image steganography, such as embedding capacity and robustness, and identifies critical research gaps for future exploration.
- **Evaluation of Recent Advances**: The paper evaluates recent innovations, especially deep learning techniques like CNNs and GANs, and their impact on improving steganographic methods' effectiveness and robustness.

2 RELATED WORK

The approach suggested by [16] may be used to combine three grayscale images into a single color image. The suggested technology reduces the size of three grayscale images by using compressive sensing in conjunction with a 2D chaotic system as the compression method. A 3D discrete cosine transform is used to integrate the compressed images with the cover image, creating an aesthetically pleasing stego-image in the process. Two color pictures are embedded into the frequency domain of a cover image using the technique described in [7]. Before embedding, the pictures are compressed using the two-dimensional compressive sensing approach. In order to build deep neural networks particularly intended for the hiding of many hidden images, [17] first introduced the use of convolutional neural networks in the field of deep learning. To efficiently carry out the responsibilities of hiding and retrieving information from these networks, specific training is required. High-capacity image steganography is a well-known technique that highlights the need of preserving quality via reversible color modification. [18] Presented the first technique for embedding hidden images with reversible color alterations. The technique demonstrated a high degree of reversibility, whereby the color transformation's reversibility was affected by a restricted set of restrictions. [19] Devised a method for the lossless retrieval of hidden images. This method's primary goals are to stop permanent alterations from occurring and to encourage more study into how to employ sophisticated matching and transformation algorithms to improve the quality of stego-images. Nevertheless, the stego-image's Peak Signal-to-Noise Ratio (PSNR) frequently dropped below 30 dB. By compressing and embedding hidden images within the concealing of images, researchers used compressive sensing to improve the overall quality of stego-images. Numerous compressive sensing methods have been created to lessen the deterioration of picture quality while the image is being recovered. Two-dimensional compressive sensing, parallel block compressive sensing, and semitensor product compressive sensing are among the techniques covered in [20]. There were several obstacles in the way of achieving lossless recovery. But deep learning advances, particularly in convolutional neural networks and deep invertible networks, substantially enhanced steganography while also restoring picture quality. Diverse methods of picture steganography have been devised to optimize the concealment of data inside images, while also guaranteeing that the concealed data may be extracted without compromising its quality. Pixel value differencing, quotient value differencing, and edge detection techniques are used in the aforementioned methodologies. As of right now, these approaches don't take into account the possibility of avoiding steganalysis methods that use

deep learning. Finding a steganography technique that can produce excellent stego-pictures and offer robust defence against steganalysis based on learning is essential. The technique should also enable the lossless recovery of encrypted images. To guarantee peak performance in the future, this is required [21].

The trend of hiding numerous images behind one cover picture has become more common as the big data era has progressed. The suggested method for creating a color composite image involves combining three grayscale images. Two color images that had previously been compressed using two-dimensional compressive sensing were embedded into the frequency domain of a cover image in order to create a stego-image with visually pleasing properties. A 2D chaotic system and compressive sensing techniques were used to compress the grayscale images. The compressed images were included into the cover image using the 3D discrete cosine transform. In the field of deep learning, convolutional neural networks (CNNs) have been utilized to build deep neural networks for the aim of multi-secret picture concealment. The extraction and concealment methods used in this procedure require specific expertise, as mentioned in reference [22].

The use of invertible neural networks to multi-image steganography was later utilized [23]. This approach has reversible extraction and concealment operations with the same set of parameters. The second strategy makes use of invertible neural networks' flexible performance to accomplish multiple picture concealment via recurrent cascade. On the other hand, the first method achieves multiple picture concealing by increasing the number of channels in the concealed image branch. One drawback of these techniques is that the stego-picture quality rapidly declines as the quantity of concealed secret pictures rises.

To improve anti-steganalysis performance, a number of low-capacity picture steganography methods have surfaced in recent years. One kind of data encryption that is often employed is content-adaptive steganography. It includes using areas of texture and noise to conceal sensitive information. The architecture used in the presented technique efficiently avoids distortion during the embedding process, boosting the method's potential to evade detection by steganography tools. Additive and non-additive distortion functions are the two categories into which the distortion functions fall. When the distortion function is written as the total of the costs that assess the influence of every embedding modification element, it is regarded as additive. The aforementioned instances are well-known instances of additive distortion function-based single-channel grayscale picture steganography [24].

Additive distortion has been used to distribute payloads uniformly across channels in order to modify color pictures. The reference work has an impact on this method's functioning [18]. Nonadditive models account for pixel interactions, which leads to a more accurate portrayal of realistic visuals. In order to improve steganalysis resistance, synchronization in pixel modification is the goal of ideas like Synchronizing Modification Direction (SMD) or Clustering Modification Direction (CMD) by [25]. Using both grayscale and color pictures improves these algorithms' ability to detect escape attempts. Furthermore, the capacity of these models is usually kept below 0.5 bits per pixel (BPP). To improve capacity, the pixel value differencing or quotient value differencing-based picture steganography technique [11] has been suggested. Generally speaking, these methods can achieve 1BPP to 4BPP. The devices are made to withstand steganalysis methods such as Random Substitution (RS) and Pixel Distribution Histogram (PDH). Additionally, some scholars have attempted to assess how

resistant stego-images produced by their proprietary algorithms are to steganalysis. Anti-steganalysis is not the main goal of deep learning-based image steganography methods. The software program StegExpose was used by the group ISN to analyze how well the stego-images resisted steganalysis. In contrast, HiNet performed an investigation to compare the stego-images' performance to that of SRNet and StegExpose in terms of anti-steganalysis. DeepMIH assessed the stego-images' anti-steganalysis efficacy against SiaStegNet and SRNet. When coupled with other steganalysis techniques, the application of these approaches shows definite benefits. In order to measure how well picture steganography technology resists steganalysis, the goal is to increase the usage of different steganalysis techniques for upcoming evaluations. Throughout this range, SPAM use will be implemented [13–17]. Table 1 shows the survey table.

Table 1 survey table

Method	Advantage	Disadvantage	Research Gap
Least Significant Bit (LSB)	Simple and widely used; high capacity	Low robustness to image processing attacks and compression	Enhancing robustness while maintaining simplicity and capacity
Pixel Value Differencing (PVD)	Provides better imperceptibility compared to LSB	Limited robustness to geometric transformations	Improving robustness to geometric and compression-based attacks
Bit Plane Complexity (BPC)	Efficient in embedding data without significant distortion	Computationally intensive	Reducing computational complexity while retaining efficiency
Discrete Cosine Transform (DCT)	Better resistance to compression (e.g., JPEG)	Moderate computational complexity	Balancing computational efficiency with robustness to various attacks
Discrete Wavelet Transform (DWT)	Multi-resolution analysis; good imperceptibility	Complexity in implementation	Simplifying implementation without compromising performance
Fast Fourier Transform (FFT)	Robust to a variety of image processing operations	High computational cost	Developing more efficient algorithms with reduced

			computational demands
Integer Wavelet Transform (IWT)	Lossless embedding; no distortion introduced	Limited embedding capacity	Increasing embedding capacity while maintaining lossless properties
Singular Value Decomposition (SVD)	High robustness to image processing attacks	High computational complexity	Optimizing for faster processing while keeping robustness high
Machine Learning (ML) and AI-based	Adaptive and intelligent embedding; high imperceptibility	Requires large datasets and training time	Reducing training time and improving efficiency of ML models
Region-based Techniques	Focuses on less noticeable regions, improving imperceptibility	Complexity in identifying optimal regions	Simplifying region identification without losing effectiveness
Human Visual System (HVS) based	Embeds data in visually less sensitive areas	Requires accurate HVS modeling	Enhancing HVS models for better accuracy and imperceptibility
Pattern Recognition	High security by altering recognizable patterns	Complexity in maintaining pattern integrity	Balancing security with simplicity in pattern management

2.1 Research gap

- **Enhancing Robustness**:
  Develop techniques that improve robustness against various image processing operations, such as compression, filtering, and geometric transformations, without compromising embedding capacity and imperceptibility.
- **Balancing Computational Efficiency**
  Optimize computationally intensive methods like DCT, DWT, and SVD to reduce processing time and resource consumption while maintaining or enhancing their robustness and data-hiding capabilities.
- **Increasing Embedding Capacity:**
  Innovate methods to increase the amount of data that can be securely embedded within an image without causing noticeable distortion or degradation of image quality.
- **Improving Detection Resistance:**
  Create advanced steganographic techniques that can effectively evade detection by modern steganalysis tools, incorporating adaptive and intelligent algorithms to stay ahead of evolving detection methods.

- **Simplifying Implementation**
  Design simplified yet effective steganographic methods that can be easily implemented without requiring extensive computational resources or complex configurations, making them more accessible for practical applications.
- **Enhancing Key Management and Synchronization**
  Develop secure and efficient key management protocols to ensure the proper distribution and synchronization of keys between the sender and receiver, thereby maintaining the security and integrity of the hidden data.

3 CONCLUSION

In conclusion, image steganography has proven to be a crucial technique for secure communication in the digital era, offering an additional layer of security by embedding hidden information within seemingly innocuous images. This survey has systematically classified and analyzed various steganography methods, highlighting their strengths, limitations, and areas for improvement. The primary challenges identified include enhancing robustness against image processing attacks, balancing computational efficiency, increasing embedding capacity, improving detection resistance, simplifying implementation, and optimizing key management and synchronization. Recent advancements, particularly in deep learning, have shown promise in addressing some of these challenges, but further research is needed to fully realize their potential. By pinpointing these research gaps, this paper aims to inspire continued innovation and development in the field, ultimately leading to more secure, efficient, and imperceptible steganographic techniques that can keep pace with evolving digital security demands.

REFERENCES

[1] Ahsan K., and Kundur D., "Practical Internet Steganography: Data Hiding in IP" found online at http://www.ece.tamu.edu/~deepa/pdf/txsecwrksh03.pdf.

[2] Chapman, M. Davida G, and Rennhard M.. "A Practical and Effective Approach to Large-Scale Automated Linguistic Steganography" found online at http://www.nicetext.com/doc/isc01.pdf

[3] Dai Y., Liu G., and WangBreaking Z., "Predictive-CodingBased Steganography and Modification for Enhanced Security", IJCSNS International Journal of Computer Science and Network Security, vol.6 no. 3b, March 2006.

[4] X. Duan, H. Song, C. Qin, M. K. Khan, Coverless steganography for digital images based on a generative model. Comput. Mater. and Continua. 55(3), 483–493 (2018).

[5] V. Holub, J. Fridrich, T. Denemark, Universal distortion function for steganography in an arbitrary domain. EURASIP J. Inf. Secur.2014(1), 1 (2014).

[6] B. Li, M. Wang, J. Huang, X. Li, in Proceedings of the 2014 IEEE International conference on Image Processing: 27-30 October 2014; Paris, ed. by B. Pesquet-Popescu, J. Fowler. A new cost function for spatial image steganography (IEEE, 2014), pp. 4206–4210.

[7] W. Tang, S. Tan, B. Li, J. Huang, Automatic steganographic distortion learning using a generative adversarial network. IEEE Signal Proc. Lett.24(10), 1547–1551 (2017).

[8] Y.-Q. Zhang, K. Zhong, and X.-Y. Wang, "High-capacity image steganography based on discrete hadamard transform," IEEE Access, vol. 10, pp. 65 141 – 65 155, Jun 2022.

[9] I.-J. Lai and W.-H. Tsai, “Secret-fragment-visible mosaic image-a new computer art and its application to information hiding,” IEEE Trans. Inf. Forensic Secur., vol. 6, no. 3, p. 936 – 945, Sep. 2011.

[10] Y.-L. Lee and W.-H. Tsai, “A new secure image transmission technique via secret-fragment-visible mosaic images by nearly reversible color transformations,” IEEE Trans. Circuits Syst. Video Technol., vol. 24, no. 4, pp. 695 – 703, Apr. 2014.

[11] W. Zhang, H. Wang, D. Hou, and N. Yu, “Reversible data hiding in encrypted images by reversible image transformation,” IEEE Trans. Multimedia, vol. 18, pp. 1469 – 1479, Aug. 2016.

[12] D. Hou, W. Zhang, and N. Yu, “Image camouflage by reversible image transformation,” J. Vis. Commun. Image Represent., vol. 40, pp. 225 – 236, Oct. 2016.

[13] D. Hou, C. Qin, N. Yu, and W. Zhang, “Reversible visual transformation via exploring the correlations within color images,” J. Vis. Commun. Image Represent., vol. 53, pp. 134 – 145, May. 2018.

[14] Z. B. Xianyi Chen, Haidong Zhong, “A GLCM-feature-based approach for reversible image transformation,” CMC-Comput. Mat. Contin., vol. 59, no. 1, p. 239 – 255, 2019.

[15] P. Ping, J. Fu, Y. Mao, F. Xu, and J. Gao, “Meaningful encryption: Generating visually meaningful encrypted images by compressive sensing and reversible color transformation,” IEEE Access, vol. 7, pp. 170 168 – 170 184, Nov. 2019.

[16] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, “A visually secure image encryption scheme based on compressive sensing,” Signal Process., vol. 134, pp. 35 – 51, May. 2017.

[17] A. D. Ker, P. Bas, R. Bohme, R. Cogranne, S. Craver, T. Filler, J. Fridrich, and T. Pevny, “Moving steganography and steganalysis from the laboratory into the real world,” in Proc. 1st ACM Workshop Inf. Hiding Multimedia Secur., Jun. 2013, pp. 45–58.

[18] B. Li, M. Wang, X. Li, S. Tan, and J. Huang, “A strategy of clustering modification directions in spatial image steganography,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 9, pp. 1905–1917, Sep. 2015.

[19] T. Denemark and J. Fridrich, “Improving steganographic security by synchronizing the selection channel,” in Proc. 3rd ACM Workshop Inf. Hiding Multimedia Secur., Jun. 2015, pp. 5–14.

[20] W. Zhang, Z. Zhang, L. Zhang, H. Li, and N. Yu, “Decomposing joint distortion for adaptive steganography,” IEEE Trans. Circuits Syst. Video Technol., vol. 27, no. 10, pp. 2274–2280, Oct. 2017.

[21] W. Tang, B. Li, W. Luo, and J. Huang, “Clustering steganographic modification directions for color components,” IEEE Signal Process. Lett., vol. 23, no. 2, pp. 197–201, Feb. 2016.

[22] X. Qin, B. Li, S. Tan, and J. Zeng, “A novel steganography for spatial color images based on pixel vector cost,” IEEE Access, vol. 7, pp. 8834–8846, 2019.

[23] D. B. Khadse and G. Swain, “Data hiding and integrity verification based on quotient value differencing and merkle tree,” Arab. J. Sci. Eng., vol. 48, no. 2, pp. 1793–1805, Feb. 2023.

[24] G. Swain, “High capacity image steganography using modified LSB substitution and pvd against pixel difference histogram analysis,” Secur. Commun. Netw., Sep. 2018.

[25] G. Swain, “A data hiding technique by mixing MFPVD and LSB substitution in a pixel,” Inf. Technol. Control, vol. 47, no. 4, pp. 714–727, Feb. 2018.