Mesopotamian Journal of Computer Science

Volume 5 | Issue 1 Article 27

1-1-2025

A Review of Image Steganography Based on Metaheuristic Optimization Algorithms

Fatima Abdulhussain Khalil
Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq,
fatima2masoudi@gmail.com

Ammar Ali Neamah
Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq

Hasanen Alyasiri
Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq

How to Cite This Article

Khalil, Fatima Abdulhussain; Neamah, Ammar Ali; and Alyasiri, Hasanen (2025) "A Review of Image Steganography Based on Metaheuristic Optimization Algorithms," *Mesopotamian Journal of Computer Science*: Vol. 5: Iss. 1, Article 27.
DOI: https://doi.org/10.58496/MJCSC/2025/027
Available at: https://map.researchcommons.org/mjcsc/vol5/iss1/27

Mesopotamian journal of Computer Science
Vol. **(2025)**, 2025, **pp**. 417–442
DOI: https://doi.org/10.58496/MJCSC/2025/027 ;ISSN: 2958-6631
https://mesopotamian.press/journals/index.php/cs

Review Article

A Review of Image Steganography Based on Metaheuristic Optimization Algorithms

Fatima Abdulhussain Khalil[1,*], Ammar Ali Neamah[1], Hasanen Alyasiri[1]

[1] *Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq*

ARTICLEINFO

Article History
Received 11 Jul 2025
Revised 15 Sep 2025
Accepted 10 Oct 2025
Published 11 Oct 2025

Keywords
Classification
Feature Extraction
Feature Selection
Frequency Domain
Metaheuristic Algorithms
Spatial Domain
Steganalysis
Steganography

ABSTRACT

Due to the widespread popularity of digital images on the Internet, image-based steganography has become a widely adopted technique for embedding secret information into everyday visual content. In parallel, steganalysis plays a vital role in digital forensics and information security by seeking to uncover hidden content within these images. Although steganographic techniques—particularly those employing adaptive embedding strategies—have made significant progress, many steganalysis approaches still struggle to generalize effectively across different image types and embedding methods. This contrast highlights the need for more intelligent, flexible, and robust analysis frameworks. This review examines steganographic techniques for digital images and the application of metaheuristic algorithms in steganalysis. These algorithms are employed in tasks such as feature selection and parameter optimization. They can also function as classifiers themselves, thereby enhancing the detection of hidden information. We conducted a structured review of over 100 research articles, categorizing steganographic approaches based on their embedding domain (spatial and frequency) and steganalysis techniques according to the metaheuristic algorithms they utilize. Metaheuristic algorithms have demonstrated significant promise in improving the effectiveness of steganalysis by optimizing both feature selection and classification processes. However, their performance is often influenced by factors such as parameter tuning, initialization strategies, and the quality of extracted features. Recent studies also show a growing trend toward hybrid and ensemble-based techniques, which further enhance detection accuracy and reliability.

1. INTRODUCTION

When it comes to concealing data, steganography involves the practice of hiding information within other data to transmit a secret message to the receiver using a method for embedding the secret message into its host medium, as shown in Figure 1. It has been used since the early days of secret communication, but its importance has grown significantly with the rise of the Internet [1], [2]. In this paper, a complete survey of image steganography techniques is reported, including fundamental issues, classification aspects, performance evaluation, detection mechanisms, and the contributions of metaheuristic methods. Literature on metaheuristic algorithms (comprehensive reviews related to steganography and steganalysis) is still limited. To the best of our knowledge, our work is one of the first systematic reviews that covers the use of metaheuristic algorithms in both steganography (spatial and frequency domains) and steganalysis, thus addressing a clear gap in the state of the art. As the reviewed studies indicate, the use of metaheuristics to enhance the efficiency of data hiding in digital images has attracted considerable attention, and interest in this topic has been steadily growing in recent years. However, despite the increasing number of primary research articles, comprehensive reviews, especially those that jointly examine both data hiding and steganalysis, remain scarce. In the context of metaheuristics applied to data hiding, one of the few recent reviews was conducted by Melman and Evsutin (2023) [3], who presented a survey of image data hiding schemes (steganography and watermarking) based on metaheuristic optimization. They summarized publications from the past six years with respect to embedding purpose, optimization purpose, and metaheuristic type. They noted the trade-off between imperceptibility, capacity, and robustness. The results were mainly reported in terms of **PSNR**, **SSIM**, **MSE**, **RMSE**, **NCC**, **QI**. Although their review provides valuable insights into the applications of metaheuristics in image data hiding, it is limited to embedding

*Corresponding author. Email: fatima2masoudi@gmail.com

Fig. 1. Steganography and steganalysis.

approaches without a detailed discussion of steganalysis methods or experiments on standard benchmark datasets. Beyond steganography and steganalysis, metaheuristic algorithms have also been successfully employed in several other domains, particularly in cybersecurity. For instance, Alyasiri et al. [4] applied Genetic Programming (GP), Grammatical Evolution (GE), and Cartesian Genetic Programming (CGP) to intrusion detection tasks and showed that evolutionary computation can evolve compact, human-readable rules that accurately identify both known and previously unseen attack types. Similar optimization approaches have been applied in fields such as malware detection, watermarking, and image processing, highlighting the versatility of metaheuristics as powerful optimization frameworks. These successes in external domains motivate further exploration of metaheuristic techniques within steganalysis, especially for improving generalization against novel or adaptive embedding schemes [5–7]. Building on these observations, our review provides several contributions:

- **Metaheuristic Role in Steganography and Steganalysis:** This review highlights the role of metaheuristic algorithms in image steganography and steganalysis, focusing on their influence on embedding quality and robustness. Furthermore, it examines steganalysis techniques with particular attention to the classifiers employed and the evaluation of their performance.
- **Standard Datasets:** We compare all methods on benchmark datasets such as BOSSbase 1.01 (grayscale), 18 datasets from the UCI repository, and classical benchmark images (Lena, Baboon, and Pepper in grayscale and color) to ensure reproducibility and comparability.
- **Feature Extraction Table**: In Table IV, we organize feature extraction methods according to the domain in which they are applied, helping researchers to identify and use relevant techniques easily.
- **Analysis of Performance Metrics:** We provide a comprehensive overview of commonly used performance measures (PSNR, SSIM, BER, AUC, etc.), discussing their advantages and limitations in the context of steganography and steganalysis.
- **Unified Presentation of Results:** Instead of fragmented reporting, our review arranges results by embedding domain (spatial vs. frequency) and purpose (steganography vs. steganalysis), facilitating systematic comparison.
- **Emerging Trends:** We highlight modern approaches such as hybrid metaheuristic frameworks, ensemble classifiers, and the integration of metaheuristics with deep learning (CNNs, GANs).
- **Novelty and Timeliness:** By combining both data hiding and steganalysis in the context of metaheuristic optimization, our survey provides a broader perspective and highlights the most relevant details, making it a timely contribution to the field.
- **Future Directions:** We include research recommendations covering quantum-resilient steganography, lightweight methods for resource-constrained devices, and cross-media steganography, pointing toward promising future research lines.

2. METHODOLOGY

References included in this review were collected and selected by following several steps. The search was initiated using the fundamental key phrases “image steganography,” “steganalysis,” and “metaheuristic algorithms” in combination. For completeness, two direct search terms were systematically used: “steganography with metaheuristics algorithms” and “steganalysis with metaheuristic algorithms.” Searches were also broadened to encompass the spatial domain as well as the frequency domain by employing the keywords: “spatial domain steganography metaheuristic,” “frequency domain steganography metaheuristic,” and more specific queries such as “DCT/DWT/DFT steganography metaheuristic.” In addition, the well-known metaheuristic algorithms’ names were employed individually, including GA, PSO, ACO,GWO, and ABC, and given the context of steganography and steganalysis. A process of systematic review was used to identify, extract and appraise the included references. It included three main phases: If a paper met both the criteria in the first step, it was not necessary to follow the subsequent steps. Likewise, if it met the condition for the second step, the third will not be applied.

1. **Topic relevance**
   Any article whose main source (journal or conference) contained any information related to image steganography, steganalysis, or watermarking in the context of metaheuristic optimization algorithm was regarded as relevant. We included this step to avoid missing out on specific obscure works on the topic, published in less highly ranked venues.
2. **Quality assessment**
   Non-subject-matter sources were evaluated using ranking systems and indexing systems.
   - **Journals:** Papers published in journals indexed in Scopus were considered, with their quality further assessed using the Scimago Journal Rank (SJR). Journals ranked in Q1–Q3 were accepted, while those in Q4 were excluded.
   - **Conferences:** For the conference ranking in contrast to the journal ranking, several systems were used. In particular, we utilized ERA, CORE, and Qualis. Second, conferences were added that scored at least B−by two of these systems or higher.
3. **Citation-based validation**
   The third step was done for the papers that did not fulfil the criteria of the first or second step, and these were assessed separately. Using Google Scholar, we calculated the mean number of citations/year. Papers that have ≥ 10 citations per year were retained as influential, and the rest were discarded.

Such a systematic three-stage approach ensured systematic identification from the literature and selection on stringent quality and impact criteria. This approach ensured the literature identified was representative of the field and academically valid, by topic-specific relevance, quality control through indexing and ranking systems, and confirmatory validation through citation impact. Accordingly, the review provided a comprehensive overview covering the research works in which image steganography and steganalysis algorithms were constructed and optimized based on metaheuristic optimization algorithms and applied in both spatial and frequency domains. The final set of references reflects the coverage and depth of the field, balancing methodological rigor and scientific relevance in the domain of secure data hiding.

3. STEGANOGRAPHY

Steganography is the art and science of hiding communication by putting secret information into a cover medium, including text, images, audio, or video. The word "steganography" comes from the Greek word for "covered writing"(στεγαν ΄ο ς, γραφ ειν) [8]. In this context, the cover object is simply a digital medium like an image, audio file, video, text, or even a network protocol that is used to carry the hidden information. After embedding, the medium takes the form of a stego object that conceals the hidden data while keeping the original content visually intact. Embedding denotes the process of hiding secret content within a cover, and extraction refers to retrieving that content from the stego object. Depending on the medium used, image, audio, video, or text steganography allows various ways to ensure the safe and imperceptible concealment of the data [9–11], as illustrated in Figure 2. The rapid evolution of steganography has driven substantial progress in steganalysis, resulting in a continuous arms race between the two [12], [13]. Even though steganography is commonly thought of as a modern security subject, it has a long history. One of the earliest known uses of this was in 440 BC, when Demeratus, the King of Sparta, concealed a warning message on a wooden block and coated it with wax to hide the writing [14]. Steganography today means hiding information in file formats with high redundancy. Most of the time, steganographic approaches are grouped by carrier media types, each of which has its own pros and cons. The embedding approach must be strong enough to protect the hidden message from possible man-in-the-middle assaults, no matter what medium is chosen. It is essential to differentiate steganography from cryptography. Cryptography protects the privacy of communication by changing the data that is sent into a form that unauthorized users can’t understand.

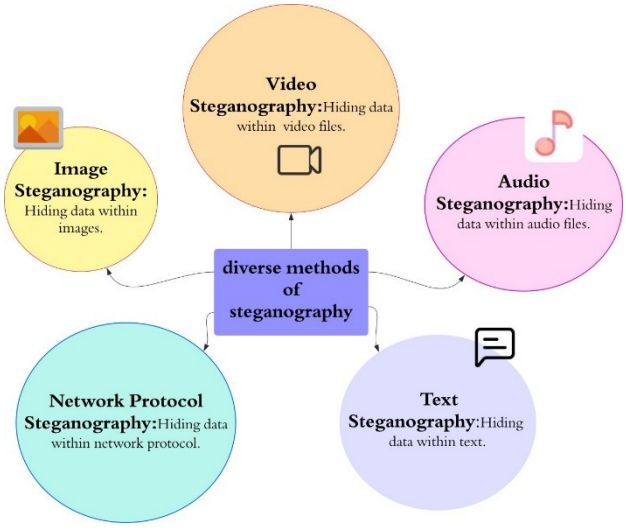

Fig. 2. Digital medium to achieve steganography

Steganography, on the other hand, hides the fact that the communication is happening at all. In some cases, both methods can be used together. Cryptography can secure the message's content, while steganography can protect its existence, providing additional security [15], [16].

3.1 Phases of Steganography

Any steganography algorithm has to work through the following stages to effectively transmit a hidden message from a sender to a receiver:

1. **Sender:** The sender's main task is to include the hidden message into the digital medium and transmit it over a communication channel.
1. **Communication Channel:** The communication channel refers to the physical or wireless medium that transmits the stego object (e.g., an image) containing the secret message. This transmission can occur over a network or through any alternative transmission medium.
2. **Receiver:** This is the final phase of the steganography process, where the stego media are received and subsequently analyzed to reveal the hidden text sent.

3.2 Important Characteristics of Steganographic Systems

To be effective and practical, a steganographic system must meet specific basic requirements. Such features not only make the secret data invisible but also ensure that the system can work with practical constraints. Below are the most commonly known requirements.

1. **Statistical Undetectability or Imperceptibility:** Imperceptibility is the system's capacity to hide information without appreciably changing the carrier file. The more secure the hidden communication, the less obvious the changes are. If the changes lead to perceptible distortions or statistical anomalies, the hidden information will be more likely to be detected.
2. **Capacity for Steganography:** The term steganographic capacity refers to the Greatest Amount of data that can be concealed within a carrier medium. Certain file formats allow greater capacity without sacrificing security by offering more flexible or redundant places for data embedding.
3. **Robustness:** Robustness determines the resistance of a steganographic system against intentional or unintentional distortions. Some steganographic methods are highly sensitive to compression or format conversion, while others

maintain the integrity of the hidden message despite modifications. Techniques that embed data in perceptually significant regions of an image or audio file tend to be more robust [17–19].

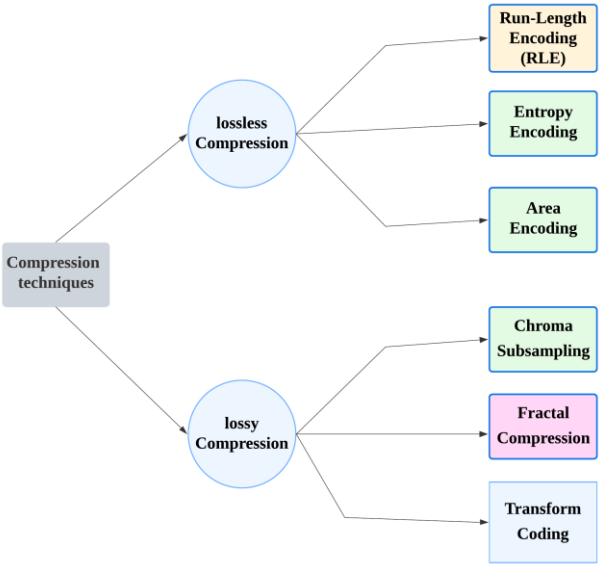

Fig. 3. Various Data Compression Techniques.

3.3 Evaluation of Steganographic System Performance

Metrics include PSNR, MSE, payload capacity, and visual fidelity.

3.4 Data Compression

Information compression is a key element of steganography, which has made it more practical and efficient to hide information in digital data. Rapid expansion of data transmission across networks has increased the need for secure and efficient information transfer. Lossless and lossy compression are the two main categories of information compression techniques (as shown in Figure 3). Compression reduces the size of files containing hidden data, facilitating storage and transmission without drawing unnecessary attention. By reducing file sizes, compression aids in preserving the natural appearance of the carrier medium, which is crucial for avoiding detection by unauthorized entities. In addition, compression techniques improve the utilization of bandwidth and storage resources, enabling faster and more cost-effective data transmission. Whether using lossless or lossy methods, compression achieves a balance between preserving data quality and maximizing efficiency. Thus, compression functions are a vital component in steganographic systems, supporting secure and seamless hidden communication in many applications [20].

4. IMAGE STEGANOGRAPHY

Images are commonly utilized in steganography because they allow for the covert embedding of data without visibly altering their appearance, making them ideal for safeguarding sensitive information [21]. Their widespread use and ease of sharing over the internet make them a practical medium for hiding information, especially in "noisy" areas with high color variations where modifications are less detectable [22]. The significant amount of bits in digital images allows ample space for embedding data, ensuring the original image remains visually unchanged [23]. Additionally, the non-causal nature of images allows random access to any pixel, enabling flexible and efficient data embedding By taking advantage of the imperfections in human visual perception, hidden data can remain undetected within digital media [18]. Images enable secure transmission of confidential data, as secret messages can only be extracted using a specific key, ensuring access is limited to the intended recipient [24]. Moreover, the versatility of image steganography in various applications contributes to its widespread adoption [25]. A deeper understanding of how data is hidden requires a closer look at the digital structure of images, including pixels, color channels, and bit depth, since these properties determine the possible locations and methods for embedding secret information. The following subsection presents these points.

4.1 Image Files

As previously mentioned, the most common cover object for steganography is an image. The digital photo world is populated with many image file extensions, most of which serve a very specific purpose. Different steganography algorithms are used for these different image formats [26]. Computers represent images as an array of binary digits (bits), These values indicate varying levels of brightness across distinct regions of the image. This digital representation is organized in the form of a grid, and each position on the grid is traditionally called a pixel. On the web, the majority of digital images are formed by a rectangular grid of pixels and store color information about each pixel. The pixels are arranged in rows, side by side. "Bit depth" refers to the amount of binary digits used in a color model, which in turn determines how many bits it takes to describe one pixel. An 8-bit value is used per pixel in greyscale or black-and-white images, enabling the display of 256 shades of grey. On the other hand, color digital images typically use 24 bits and conform to the RGB (Red, Green, Blue) color model. By color space standards, bit depth is defined to be 8 bits per channel. This means that 8 bits are assigned to represent the intensity of each primary color: red, green, and blue. This allows each pixel to be capable of displaying more than 16 million colors. Background colors on the webpages are often expressed in hexadecimal values in six digits, or three pairs of hexadecimal values, representing red, green, and blue. For example, a white background is represented by the hex value FFFFFF, where FF stands for 100% red, 100% green, and 100% blue. In decimal, this is (255, 255, 255), and in binary, it's (11111111, 11111111, 11111111). A total of three bytes that make up the white color, which is similar to how the color of a pixel is defined in an image [27]. However, keep in mind that the more colors you display, the larger your image file will be. As an example, a 1024×768 24-bit image has just over 2 million pixels; each pixel is made up of 24 bits, with 1 byte for red, 1 byte for green, and 1 byte for blue. This leads to a file size of over 2 megabytes. It is useful, if not essential, to perform file compression in order to facilitate and speed the transfer thereof [28], [29].

5. DOMAIN-BASED CATEGORIZATION OF IMAGE STEGANOGRAPHY

5.1 Spatial Domain Methods

The spatial domain approach in image steganography involves embedding confidential information directly into the pixel values of the host image. Unlike techniques that require converting the image into any other domain, eg, frequency domain, this method works directly with the unaltered image data. Several techniques fall under the spatial domain category, each with its own strategy for hiding information. Among the most commonly used methods in this domain are the Least Significant Bit (LSB) technique and Pixel Value Differencing(PVD) [30], [31].Some other methods include Exploiting Modification Direction (EMD), Quantization-based methods, Gray Level modification, Multiple Bit-planes, and Palette based steganography techniques. Because they are simple and efficient, spatial domain techniques are considered to be the simplest and least difficult embedding and extraction techniques in steganography. Furthermore, spatial domain techniques exhibit a higher degree of compatibility with the human visual system (HVS), enabling greater embedding capacity compared to transform domain methods, while maintaining a reasonable level of image quality. Nevertheless, it is crucial to acknowledge that spatial domain techniques are without limitations. One significant constraint is the restricted capacity for embedding data. The length of the secret information that can be hidden within a cover image is often limited by the available pixel space in that image. Moreover, certain spatial domain methods may be susceptible to detection through advanced analytical techniques such as statistical steganalysis. Therefore, selecting an appropriate technique that strikes an optimal balance between security and the recoverability of hidden data is essential [32–43].

5.1.1 Least Significant Bit (LSB)

The LSB method is one of the easiest, widely used, spatial domain steganography methods and has high capacity. It hides secret information in the least significant bits of a high-capacity host image. Since these bits carry minimal information, modifying them does not cause noticeable changes to the visual quality of the image, making it undetectable to the human eye. The secret data is directly embedded by replacing the least significant bits of the cover image without introducing significant distortion. However, this embedding process generates noise 50%, which is derived from the average bit embedding rate (that is, the number of embedded bits per pixel). Despite its simplicity and high capacity, the LSB technique has limitations. For example, when the stego value (the modified value) is compared to the plain value (the original value), modifications like incrementing or decrementing the value by one (e.g., a change of ±1 in the 1st LSB or ±4 in the 3rd LSB) It can leave behind traceable statistical violations. These violations make the stego-image susceptible to detection through advanced steganalysis techniques [44]. To achieve the effectiveness of the Least Significant Bit (LSB) steganography technique, several advanced versions have been developed. These versions include the following:

1. **LSB Matching Algorithms**: LSB matching is a steganographic technique in which the decision to increment or decrement a pixel of the cover image by one is made randomly, allowing embedding of message bits with minimal

detectable changes [45].

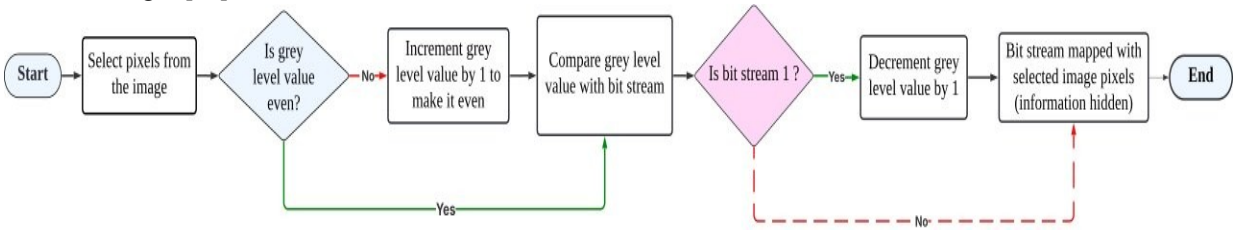

Fig. 4. Gray level modification (GLM) Algorithm.

2. **Adaptive LSB Embedding:** This technique modifies bits according to image features, including texture content or edge pixel characteristics.
3. **Optimized LSB Substitution:** Optimized LSB substitution utilizes learning methods.
4. **Expansion to Up to 4 LSB Planes**: It has been expanded to a maximum of 4 LSB planes to increase embedding capacity [46–54].

5.1.2 Gray Level Modification (GLM) Steganography

Gray Level Modification (GLM) Steganography is a technique for representing binary data (0s and 1s) by modifying the gray level values of image pixels, rather than embedding or hiding the data. Pixels are chosen according to a predefined mathematical function, and their gray levels are adjusted to ensure they are all even. Then, each bit in the binary data stream is mapped as follows: If the bit is 0, the pixel value is left unaltered If the bit is 1, the pixel's gray level is decremented by 1 to make it odd, representing the bit value. This method provides better-quality stego images compared to other digital steganography techniques [55–57]. The process is illustrated in Figure 4.

5.2 Transform Domain Methods

In this approach, the secret to be hidden is embedded in the transform or frequency domain of the cover. It is a more difficult technique for embedding a message into an image than spatial domain methods. The domain of embedding techniques in which the message is hidden in transform coefficients is called transform domain embedding. Several algorithms have been suggested for these approaches, which are more complex than spatial domain methods [23]. For frequency-domain-based schemes, the initial step involves transforming images into the frequency domain, followed by embedding messages into the transform coefficients [58]. Various algorithms and transformations are applied to the image to conceal the message. The transform domain approaches are categorized into: Discrete Fourier Transformation (DFT), Discrete Cosine Transformation (DCT), Discrete Wavelet Transformation (DWT) Techniques [59]. The embedding and extraction process are computationally complex in transform domain-based algorithms, but they
are robust to attacks and effectively maintain the stego object quality with no or minimum distortion [60].

5.2.1 Discrete Wavelet Transform (2D-DWT)

The WT transforms spatial domain information into the frequency domain. Wavelets have been used in image steganography due to their capability of separating high-frequency and low-frequency information on a pixel-by-pixel basis. Discrete
wavelet transformation (DWT) is applied instead of discrete cosine transformation (DCT) since it provides resolution by levels for images [61], [62], [18]:

- **LL (Low-Low):** This is obtained by applying low-pass filtering to both the horizontal(rows) and vertical (columns)directions.
- **LH (Low-High) and HL (High-Low)**: The HL and LH sub bands are created by applying low-pass filtering in one direction and high-pass filtering in the opposite direction.
- **HH (High-High):** The HH sub band is produced by high-pass filtering in both directions and contains high-frequency components [62].

These sub-bands allow image steganography systems to embed data in less perceptually significant areas (such as HL, LH, or HH), thereby increasing imperceptibility and potentially enhancing robustness to compression and noise. The process can be iteratively applied to the LL sub-band to achieve multi-level decomposition, enabling finer control over embedding strategies.

5.2.1.1 Advantages of 2D-DWT in Steganography.

- **High imperceptibility:** Embedding in high-frequency sub-bands minimizes visual artifacts.
- **Better robustness:** Provides resistance to common signal processing attacks and image transformations.
- **Multi-resolution capability**: Allows embedding at various scales depending on security and capacity requirements.

5.2.1.2 Commonly Used Wavelets:

Haar, Daubechies, Coiflets, and Biorthogonal wavelets are frequently employed due to their compact support and energy compaction properties. 2D-DWT-based steganography is often combined with other transforms (e.g., DCT) or optimization algorithms to further enhance performance in terms of capacity, imperceptibility, and robustness.

5.2.2 Discrete Fourier Transform (DFT)

The DFT is one of the frequency transforms widely used in steganography. The DFT of a digital image is a 2D DFT since a digital image can be described as a function of two variables, $f\ (x, y)$. In the context of information hiding, it is possible to hide secret data in certain frequency coefficients by transforming an image to a frequency field such that no visual distortion is made on the image. This way, the hidden information can no longer be visible to human eyes while keeping the entire image quality. Hence, 2D-DFT offers a firm mathematical foundation for steganography, enabling the data hiding techniques to obtain transparency and security simultaneously by utilizing the frequency domain representation of digital images [63]. Where $f\ (x, y)$ represents the image in the spatial domain (host-image), and $F(u, v)$ represents the image in the frequency domain (stego-image).
Note that M and N represent the size of the image.

$$F(u,v) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} e^{-j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} f(x,y) \quad (1)$$

$$\mathrm{u} = 0,1,\ldots,\mathrm{M}-1\ \mathrm{v} = 0,1,\ldots,\mathrm{N}-1$$

The inverse Discrete Fourier Transform (IDFT) is represented by the following equation.

$$f(x,y) = \sum_{u=0}^{M-1}\sum_{v=0}^{N-1} e^{j2\pi\left(\frac{ux}{M}+\frac{vy}{N}\right)} F(u,v) \quad (2)$$

$$x = 0,1,\ldots,M-1\ y = 0,1,\ldots,N-1$$

5.2.3 Discrete Cosine Transform (DCT)

One important transformation in image processing is the discrete cosine transform (DCT), which offers numerous advantages:

- It is able to carry energy in the very low frequency range for image data.
- It can reduce the effect of blocking artefact, which is caused when boundaries between sub images become noticeable [64]. DCT coefficients play a crucial role in JPEG compression by dividing an image into segments of varying importance. This process transforms the image from the spatial domain into the frequency domain, allowing it to be separated into high, medium, and low-frequency components.

Discrete Cosine Transform (DCT) is a mathematical operation that transforms an image from the spatial domain (pixel representation) to the frequency domain. Most of the signal information is concentrated at low frequencies, while high frequencies can often be neglected with minimal distortion [65]. Steganography algorithms that use the Discrete Cosine Transform (DCT) typically select specific frequency coefficients to hide information. The coefficients are selected based on their perceptual significance, favoring those that are less noticeable to the human eye. The most commonly used coefficients are usually the low-frequency components, as they carry most of the image's energy and are less likely to cause visible distortions [66]. The image is divided into 8 × 8 pixel blocks. The 2D-DCT is then applied to each block from top to bottom and left to right, transforming pixel data into frequency components, producing the following:

- DC (Direct Component): DC (Direct Component): This coefficient represents the block's average intensity, calculated by summing the 64 pixel intensities and dividing by 8.
- AC (Alternative Components): The remaining 63 coefficients represent intensity variations between pixels in the block. These are divided into low and high frequencies:
    1. Low frequencies: are used to create a blurred approximation of the original image, containing essential structural information.
    2. High frequencies: Contribute to fine details, such as edges and textures [67–71].

Two-Dimensional Discrete Cosine Transform (2D-DCT):

An extension of DCT for 2D image blocks.

- Forward 2D-DCT The mathematical expression for the forward 2D-DCT is defined as [72]:

$$G(f,e) = \frac{2}{L}\alpha(f)\alpha(e)\sum_{o=0}^{L-1}\sum_{w=0}^{L-1} g(o,w)\cos\left(\frac{f\pi}{2L}(2o+1)\right)\cos\left(\frac{e\pi}{2L}(2w+1)\right) \quad (3)$$

In this formula, $f,e = 0,1,2,\ldots,L-1$, and $f(o,w)$ denotes the intensity value of the pixel located at coordinates (o,w).and $C(k)$ is the scaling factor defined as:

$$\alpha(k) = \begin{cases} \frac{1}{\sqrt{2}}, & \text{if } k = 0 \\ 1, & \text{otherwise} \end{cases} \quad (4)$$

Inverse 2D-DCT (IDCT) To recover the original function, the inverse 2D-DCT is given by [70]:

$$g(o,w) = \frac{2}{L}\sum_{f=0}^{L-1}\sum_{e=0}^{L-1}\alpha(f)\alpha(e)G(f,e)\cos(\frac{f\pi}{2L}(2o+1))\cos(\frac{e\pi}{2L}(2w+1)) \quad (5)$$

Here, $f,e = 0,1,2,\ldots,L-1$.

The forward and inverse DCT techniques convert spatial pixel data to the frequency domain and transform it to that of its analog counterpart in the spatial domain. Representation results in successful image reconstruction.

TABLE I : STANDARD JPEG QUANTIZATION TABLE FOR LUMINANCE.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

TABLE II : STANDARD JPEG QUANTIZATION TABLE FOR CHROMINANCE

17	18	24	47	99	99	99	99
18	21	26	66	99	99	99	99
24	26	56	99	99	99	99	99
47	66	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99
99	99	99	99	99	99	99	99

In Table I, the value 16 represents the DC coefficient. The remaining values correspond to AC coefficients [73].

5.2.4 JPEG Compression

JPEG (Joint Photographic Experts Group) is among the most well-known standards that uses lossy image compression techniques. It significantly reduces image file size by eliminating redundant and less perceptually significant data while maintaining acceptable visual quality. JPEG compression is particularly important in steganography, as it defines the structure and behavior of transform-domain embedding techniques. The JPEG compression process involves several key steps:

1. **Color Space Conversion**: The source image is converted from the RGB color space to YCbCr. In this representation, the Y component indicates luminance, while the Cb and Cr components represent chrominance. Since the human eye is more sensitive to changes in luminance than in chrominance, we can subsample the chrominance components commonly in 4:4:4, 4:2:2, and 4:2:0 formats without noticeable loss of quality.
2. **Block Splitting:** The image is split into non-overlapping blocks (usually 8 × 8 pixels).
3. **Discrete Cosine Transform (DCT):** Each 8 × 8 block is transformed using 2D-DCT. This transforms the image's pixel values in the spatial domain to the coefficients in the frequency domain, with the top-left coefficient being the DC (low-frequency) component and the others being AC (high-frequency) components.
4. **Quantization:** DCT coefficients are quantized using a standard quantization matrix. Higher frequency coefficients are more aggressively quantized, resulting in data loss, which contributes to compression. Quantization is the primary source of loss in JPEG compression. [74], [64].
5. **Entropy Coding:** The quantized coefficients are reordered in a zig-zag pattern to group low-frequency components together, then compressed using Huffman or arithmetic coding [75], [76–78].

5.2.4.1. Advantages.

- High compression efficiency: Reduces file size significantly, making it suitable for transmission and storage.
- Suitable for frequency-domain embedding: Enables use of robust embedding methods in the DCT domain.
- Widespread format: JPEG is a universally accepted image format, increasing the covertness of steganographic methods.

5.2.4.2. Challenges.

- **Lossy nature:** Makes it difficult to embed and reliably extract hidden data without degradation.
- **Steganalysis vulnerability:** Frequency-domain artifacts can sometimes be detected by statistical analysis tools if not carefully designed. JPEG compression-based steganography often uses advanced techniques like matrix encoding, syndrome-trellis codes, or combines with wavelet and optimization-based methods to enhance imperceptibility, capacity, and robustness.

5.2.5 JPEG Steganography

In most steganographic systems, data is typically embedded within the nonzero discrete cosine transform (DCT) coefficients of JPEG images. The primary JPEG steganographic methods can be classified as follows:

- **nsF5 Algorithm:** The nsF5 algorithm is an enhanced version of the original F5 steganographic algorithm. It was specifically designed to address the issue of shrinkage. In this problem, DCT coefficients of ±1 can be reduced to zero during data embedding, resulting in the loss of hidden information. To avoid this, nsF5 utilizes wet paper codes, which prevent the modification of zero-valued coefficients, thereby maintaining embedding accuracy and improving overall efficiency. The algorithm embeds hidden data by altering the least significant bits (LSBs) of non-zero AC DCT coefficients in unaltered JPEG objects. The embedding process is guided by syndrome coding, which ensures that only valid coefficients are altered, thus minimizing both perceptual and statistical distortions. Moreover, nsF5 employs matrix encoding to further reduce the number of changes required, enhancing resistance to steganalysis. In more recent developments, syndrome-trellis codes (STCs) have been adopted in place of wet paper codes. These codes provide higher embedding efficiency, particularly at lower payload rates. By combining theoretical rigor with practical effectiveness, nsF5 remains a robust and reliable method for secure, imperceptible data hiding in JPEG images [79].

- **UERD Algorithm:** Another steganography embedding model, known as UERD, aims to minimize the detectability of the hidden data to the observer by minimizing the effect of embedding on the statistical properties of the cover data. This is achieved through a post-analysis of specific parameters of the DCT coefficient at the mode level, block level, and surrounding region level. Therefore, the analysis can indicate where “noisy" regions would be suitable for embedding while maintaining statistical invariance of features such as file histograms. In contrast, “wet" (with predictable statistics) regions carry a higher risk of detection. Notably, UERD does not rule out the possibility of embedding in DC mode or zero DCT coefficients while security is offered due to statistical profiles. It maintains uniformity in the relative changes of certain calculated statistical parameters due to embedding, and, like nsF5 and J-UNIWARD, it utilizes syndrome-trellis codes (STC) to embed message bits in the test values [80].

TABLE III : COMPARISON OF STEGANOGRAPHY TECHNIQUES BY DOMAIN

Technique	Domain	Payload	Quality	Robustness	Ease
LSB PVD	Spatial	High Medium	High -	Weak -	Simple -
DCT DWT DFT	Frequency	Medium - -	High - -	Secure - -	It’s easier than other frequency domain techniques. Complex -

6. STEGANALYSIS AND DETECTION METHODS

Steganalysis is the practice of detecting hidden information. To achieve this, researchers have developed various tools and approaches. In practice, the field has two complementary components: artistic, where features or anomalies indicating hidden information must be found, and scientific, which is the careful construction and application of analysis tools to unearth or extract the hidden information. A steganalysis algorithm is considered to be good when it accurately detects the hides and recovers it in some cases. The main purpose of steganalysis is to disclose hidden messages in the carrier and, accordingly, improve data security and integrity. In other words, steganalysis is a blend of possibly creative skills together with sound technical knowledge to reveal hidden information [81–83]. Steganographic attacks, also known as stego-attacks, are any techniques that an adversary can apply to reveal, extract, modify, or destroy hidden data in a stego object. The nature and complexity of these attacks depend on the information available to the attacker and the specific objectives they aim to achieve. There are seven primary attack strategies used to detect hidden data within steganographic objects [84–87] and are generally classified into the following types:

1. **Stego-Only Attack:** The attacker only has access to the stego file containing hidden data. They analyze the file using trial-and-error methods or statistical techniques to detect anomalies or extract hidden information.
2. **Known-Cover Attack:** The attacker has access to both the original cover object and the stego object. By comparing the two, the hidden data can be extracted through analysis of the differences.
3. **Known-Message Attack**: The attacker already knows the hidden message. By analyzing the stego object containing this known message and comparing it with similar files, the attacker can infer patterns or reconstruct the cover object. This information can later be used to detect or extract future hidden messages.
4. **Known Steganographic Algorithm Attack**: The attacker possesses complete knowledge of the embedding technique being used, but does not possess the cover object or the hidden message. This information can be exploited to simulate the embedding process or to train steganalysis tools tailored to that particular method, increasing the likelihood of successful detection.
5. **Chosen-Stego Attack:** The attacker has access to both the stego object and the steganographic algorithm. This allows for a detailed analysis of how the data was embedded and increases the chances of successful extraction.
6. **Chosen-Message Attack:** A specific message is deliberately embedded into a cover object under the attacker's control. This allows researchers or attackers to study the embedding behavior of the algorithm and develop method for detection or extraction.
7. **Known-Stego Attack:** The steganographic algorithm, as well as its purpose, is available to the attacker. This makeshe attack particularly dangerous, as the attacker can exploit the knowledge of the algorithm to directly extract the hidden message.

6.1 Two Main Types of Steganalysis Based on Analysis Objective

Steganalysis refers to the process of detecting hidden information within a stego object. Depending on the goal of the analysis, steganalysis can be broadly categorized into two main types:

6.1.1 Targeted Steganalysis

Targeted steganalysis is designed to detect steganographic content generated by a specific embedding algorithm. It operates under the assumption that the analyst knows or can guess the steganographic method used.

6.1.2 Blind (Universal) Steganalysis

The field of blind or universal steganalysis seeks to detect hidden content without any knowledge of the steganographic method or embedding schema. It is more challenging but broadly applicable.

6.2 Feature Extraction

Feature extraction is a crucial step in steganalysis, the process of detecting hidden information within stego media. It involves identifying and quantifying measurable attributes from cover or stego images that can reveal the presence of hidden data. These features serve as the input to classification models that aim to distinguish between clean (cover) and altered (stego) content.

6.2.1 Purpose and Importance: The success of steganalysis largely depends on the quality and relevance of the extracted features. Well-designed feature sets can capture subtle statistical anomalies or structural modifications introduced by data embedding, even if those changes are imperceptible to human vision.

6.2.2 Types of Features Extracted:

- Statistical Features: Include measures such as mean, variance, skewness, kurtosis, and histogram statistics of pixel values or transform coefficients.
- Frequency-Domain Features: Derived from DCT, DWT, or FFT, these features analyze the frequency components of an image to detect unusual patterns caused by embedding.
- Co-occurrence Matrix Features: Capture spatial dependencies and relationships between neighboring pixels.
- Common features include contrast, homogeneity, correlation, and energy.
- Image Noise Residuals: Many embedding operations disturb the natural noise distribution of an image. Analyzing these residuals can help detect anomalies.
- Edge and Texture Features: Extracted using operators like Sobel, Prewitt, or Gabor filters, these features help detect distortions along edges or in textured region.

6.2.3 Feature Extraction Methods:

- **Handcrafted Feature Extraction**: Based on domain knowledge and statistical analysis. Examples include the SPAM (Subtractive Pixel Adjacency Matrix) model and SRM (Spatial Rich Model).

- **Automated Feature Learning:** Deep learning methods (e.g., Convolutional Neural Networks) automatically learn relevant features during training, often outperforming handcrafted approaches in large-scale datasets.

6.2.4 Use in Classification: Once features are extracted, they are fed into classifiers such as Support Vector Machines (SVM), Random Forests, k-Nearest Neighbors (k-NN), or deep neural networks. The classifier learns to distinguish between cover and stego samples based on feature patterns.

6.2.5 The extracted features must be:

- The features need to be affected by the data hiding process. That is, the stego-image and the cover-image must have relatively distinct features.
- The features must be flexible enough to work effectively with various image formats and data hiding techniques.

TABLE IV THE FOLLOWING TABLE ILLUSTRATES SEVERAL FEATURE EXTRACTION METHODS

Name	Dim	Domain	Notes
CHEN	486	JPEG	CHEN is a feature-extraction technique for JPEG steganalysis that uses Markov processes to model both inter- and intra-block correlations among JPEG coefficients, and it can subsequently be used for detection or classification tasks [88], [89].
CC-CHEN	972	JPEG	It's an enhanced version of the CHEN model, enhanced by Cartesian calibration [90], [91].
LIU	216	JPEG	All 216 features proposed are concatenated.
CC-PEV	548	JPEG	Cartesian-calibrated PEV feature set [92]
SPAM	686	Spatial	It consists of features based on differences between adjacent pixels using first-order and second-order Markov chains. The SPAM feature vector comprises 686 features in the second-order Markov process.[93], [94], [95].
CDF	1,234	Both	has been proposed as the union of SPAM and CC-PEV[96],[97].
CC-C300	48,600	JPEG	First high-dimensional rich model for JPEG steganalysis [98] ,[90].
CF∗	7,850	JPEG	the 7850-dimensional CF∗ features are formed by co-occurrence matrices [99].
CC − JRM ∗ ∗	22,510	JPEG	The CC-JRM steganalysis feature, with 22,510 dimensions, is constructed from a sub-model system that combines the joint distribution of the frequency and spatial domains[100].
SRM	34,671	Spatial	The 34,671-D Spatial Rich Model (SRM) feature is based on a rich model in the spatial domain [101].
SRMQ1	12,753	Spatial	it's a spatial domain rich model with the fixed quantization q = 1c [102].
J+SRM	35,263	Both	Union of SRMQ1 and CC-JRM.
CSR	1,183	Spatial	Content-Selective Residuals (targeted at S-UNIWARD).
DCTR	8,000	JPEG	FAST features from DCT residuals.
maxSRM	34,671	Spatial	SRM with selection channel knowledge
SCRMQ1, CRMQ1	18,157	Spatial / Color	Spatial & Color Rich Model (Tc=3 truncation).
PHARM	12,600	JPEG	PHARM project features.
CFA-aware CRM	5,514 4,146 10,323	Spatial/Color	CFA-aware Color Rich Models.
GFR	17,000	JPEG	Gabor Filter-based JPEG Rich Model.
sigma-features	1,980	Spatial	Selection-channel aware PSRM variant.
SCA-DCTR GFR PHARM	various	JPEG	Selection-channel aware variants.
PhaseAwareNet	__	JPEG	JPEG-Phase-Aware Net (Caffe /MatConvNet).
SRNet	__	JPEG/Spatial	Tensor Flow implementation.
JIN-SRNet	__	Spatial/JPEG	Pytorch pretrained SRNet.

7.Metaheuristic Algorithms in Steganography

Metaheuristic algorithms are designed to address specific problems, whereas metaheuristic algorithms are generalized and problem-independent, This enables them to be used for a variety of real-world optimization problems. Metaheuristics represent an advanced form of heuristics in which researchers have developed generalized optimization techniques inspired by biological and natural processes. However, these algorithms do not guarantee the optimal solution, but aim to achieve near-optimal results [103], [3]. A short overview of the metaheuristics is presented to tackle various optimization challenges. Its classification is illustrated in Figure 5.

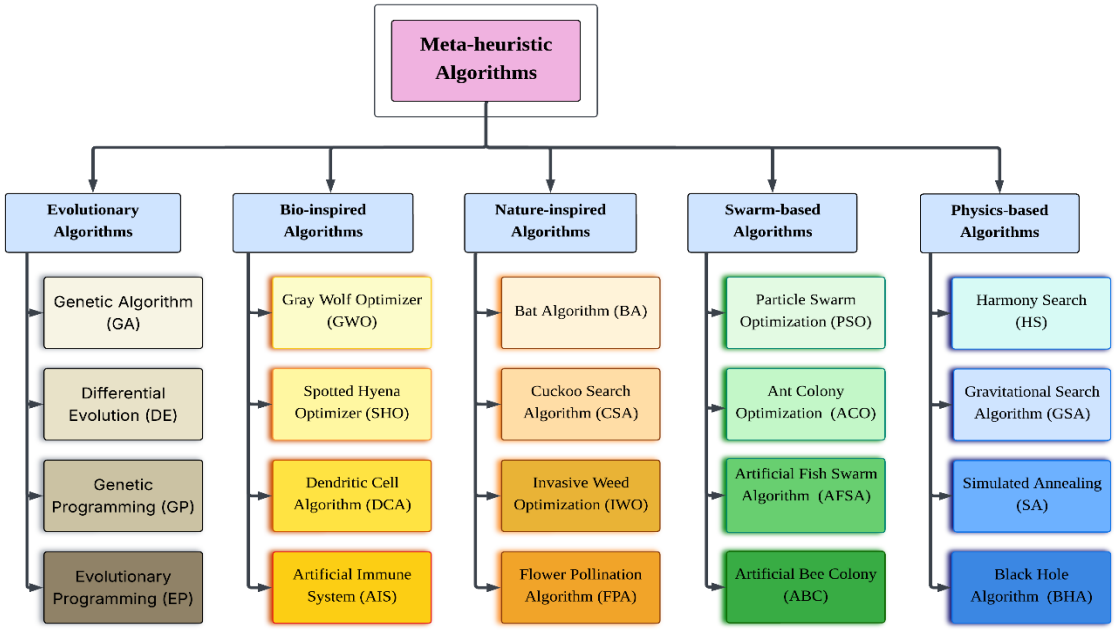

Fig. 5. Classification of Metaheuristic Algorithms.

7.1 Applications in Image Steganography

Metaheuristic algorithms are employed in various stages of steganography, including:

- Pixel or block selection: Choosing the most suitable pixels or blocks for embedding to maximize imperceptibility.
- Payload distribution: Optimizing how and where the secret bits are distributed across the image.
- Transform coefficient tuning: Adjusting DCT/DWT coefficients to minimize distortion.
- Feature selection: In steganalysis resistance, selecting discriminative features for training stego detectors.

7.2 Categorization of Metaheuristics

Metaheuristics can be categorized in various ways, such as based on their operation or their underlying concepts. In terms of operation, metaheuristics are divided into two main groups [104]:

1. Single solution-based approaches, such as Tabu Search (TS), Simulated Annealing (SA), and Variable Neighborhood Search (VNS).
2. Population-based approaches, such as Genetic Algorithms (GA), Artificial Bee Colony (ABC), Particle Swarm Optimization (PSO), and Ant Colony Optimization (ACO).

7.3 Key Characteristics of Metaheuristics

- Exploration and Exploitation: Efficiently balances global exploration with local exploitation to avoid premature convergence.
- Adaptability: Easily adaptable to different steganographic frameworks and image types.
- Scalability: Capable of handling large-scale, high-dimensional optimization problems.

7.4 Common Metaheuristic Algorithms Used

- **Genetic Algorithm (GA):** Uses evolutionary principles (selection, crossover, mutation) to evolve embedding positions or strategies.
- **Particle Swarm Optimization (PSO):** Models particles (candidate solutions) moving through a solution space influenced by local and global bests.
- **Ant Colony Optimization (ACO):** Based on pheromone trails in ant colonies, used to find optimal paths or sequences.
- **Grey Wolf Optimizer (GWO):** Mimics the social hierarchy and hunting behavior of grey wolves.
- **Firefly Algorithm, Bat Algorithm, Whale Optimization Algorithm:** Inspired by natural phenomena and effective in high-dimensional optimization.

7.5 Recent Trends

In this review, we focused on studies published within the last six years that explicitly apply metaheuristic algorithms in either steganography or steganalysis. The selection process prioritized high-quality contributions that demonstrated practical evaluation, rather than purely descriptive discussions, and that employed metaheuristics for well-defined purposes such as optimizing embedding positions, tuning classifier parameters, or selecting discriminative features. This ensured that only methodologically rigorous and experimentally validated works were included in Table V and VI, making its content representative of the state-of-the-art. Recent studies integrate metaheuristics with deep learning, transform domain methods (DWT, DCT), or hybridize multiple algorithms to enhance performance further. Additionally, adaptive or dynamic metaheuristic strategies are gaining traction for real-time steganographic systems. The following two tables summarize the applications of metaheuristic algorithms in image steganography and steganalysis.

TABLE V. APPLICATIONS OF METAHEURISTIC ALGORITHMS IN IMAGE STEGANOGRAPHY

Ref	Metaheuristic Algorithm	Domain	Purpose	Cover type	Performance
[105]	Harris Hawks Optimization (HHO)–IWT	Frequency (IWT)	Optimal pixel selection to maximize payload and imperceptibility	Images (256×256)	- **PSNR:** 36.66–38.05 dB - **SSIM:** 0.9144–0.9713 - **QI:** 0.9956–1.000 - **Capacity:** 50% - **Time:** 35 s (embed) /19 s (extract) - Robust to RS/PDH and image processing attacks
[106]	BESOPS–CE (Bald Eagle Search + Chaotic Encryption)	Frequency (IWT)	Optimal pixel selection (BES) with chaotic encryption of the secret image before k-LSB embedding; improves imperceptibility and robustness	Digital images (USC–SIPI)	- **PSNR:** 55.32–56.64 dB - **SSIM:** 0.9982–0.9998 - **MSE:** 0.1408–0.1912 - **RMSE:** 0.3752–0.4373 - **PSNR under attacks:** 54.83–55.92 dB - **NCC:** 0.9980–0.9993 - **Time**: 0.65–0.74 min(total)
[107]	Particle Swarm Optimization (PSO) with Integer Wavelet Transform (IWT)	Frequency	HMPSO for pixel selection with DDV embedding to enhance confidentiality and integrity	USC–SIPI images (color and grayscale)	Robust against χ^2 attack - **Payloads**: 6.25%, 12.5%, 18.75%, 25% - **PSNR:** 61.41–78.09 dB - **MSE**: 0.1012–0.8021 - **SSIM:** up to 1.000
[108]	Particle Swarm Optimization (PSO) with Integer Wavelet Transform (IWT)	Frequency domain (IWT)	PSO generates an optimal substitution matrix for embedding in IWT coefficients, with OPAP	Standard benchmark grayscale images (Lena, Baboon, Barbara, Jet)	- **Payload:** 589,824 bits - **PSNR:** 41.13–41.97 dB

Ref	Metaheuristic Algorithm	Domain	Purpose	Cover type	Performance
			minimizing distortion		
[109	Cuckoo Search (CS), Bee Colony Optimization (BCO), Cat Swarm Optimization (CSO), Genetic Algorithm (GA), Particle Swarm Optimization (PSO), Simulated Annealing (SA), Firefly Algorithm (FA)	Spatial domain	Bio-inspired optimization of pixel substitution; hybrid models (CS–GA–BCO for color, CS–GA–PSO for grayscale) achieve higher imperceptibility and robustness than LSB and DWTQ	Benchmark images (Lena,Baboon, Pepper; color and grayscale)	- **PSNR:** ~41.8 dB (best individual, CS color) - **PSNR:** ~42.1 dB (best individual, CS grayscale) - **Hybrid:** up to ~46 dB (CS–GA–BCO color) - **Hybrid:** up to ~45 dB (CS–GA–PSO grayscale)
[110]	Particle Swarm Optimization (PSO)	Spatial Domain	PSO determines the optimal starting pixel, scan order, and LSB plane for embedding; improves payload capacity and imperceptibility compared to GA	Standard benchmark grayscale images	- **Max payload:** (~40%) - **PSNR:** GA benchmark ≈ 45.13 dB → Proposed PSO: 56.60 dB - **Execution time (5 images):** 4.735 s (embed + extract)
[111]	Adaptive Genetic Algorithm (AGA)	Transform Domain (2-level DWT; block-wise)	AGA derives an optimal substitution matrix for LSB embedding after DWT, while OPAP refines pixel values to minimize distortion; AES+RSA strengthens confidentiality	Benchmark images (Lena, Baboon, Boat, Fundus1–4)	- **PSNR**: from ~50.76–59.06 dB (post-embedding) → 51.30–59.63 dB(post-optimization) - **Gain:** consistent ~0.5–2.1 improvement - **Execution time:** ~64.33–89.45 ms (encryption), ~33–45 ms (decryption) - **NPCR:** > 99% - **UACI:** 15–41% - **MAE:** ≈0.10–0.41%

Narrative summaries of studies listed in Table V

7.5.1 **Hassaballah et al. (2021)** — HHO–IWT for transform-domain embedding [105].. This study introduces a stegano graphic method for IoT security that combines Harris Hawks Optimization (HHO) with the Integer Wavelet Transform (IWT). The HHO algorithm searches for optimal encoding vectors and coefficient positions, enabling k-LSB embedding of secret images into IWT subbands while minimizing distortion through optimal pixel adjustment (OPAP). Experiments with 256 × 256 secret images embedded into 512 × 512 cover images show that the method achieves high visual quality even at the maximum tested payload of 50% of the cover image (k = 4). Reported performance includes PSNR in the range of 36.66–38.05 dB, SSIM between 0.9144–0.9713, and QI between 0.9956–1.000. In terms of efficiency, embedding and extraction at full payload require about 35.35 s and 19.36 s, respectively. The method also demonstrates robustness against image processing attacks, histogram analysis, and RS-steganalysis.

7.5.2 Bahaddad et al. (2023) — BESOPS–CE for pixel-level embedding with chaotic encryption [106].. This paper introduces a hybrid steganographic scheme that integrates the Bald Eagle Search (BES) algorithm for optimal pixel selection with chaotic encryption (Chen system) of the secret image. After encryption, the payload is embedde into selected IWT subbands (LH, HL, HH) using k-LSB substitution with OPAP refinement, followed by inverse IWT reconstruction. Experimental evaluation on the USC–SIPI image dataset shows very high imperceptibility (PSNR: 55.32–56.64 dB, SSIM: 0.9982–0.9998, with low

MSE and RMSE) and practical efficiency (embedding: ∼0.37–0.43 min, extraction: ∼0.28–0.32 min). Robustness tests confirm resilience under common image attacks (PSNR: 54.83–55.92 dB) with strong correlation (NCC: 0.9980–0.9993). Comparative studies demonstrate that BESOPS–CE consistently outperforms CE–GAN, GSO–SM, SSO–SM, and CSO–SM in terms of imperceptibility and security metrics.

7.5.3 Ali et al. (2024) — HMPSO with Distinction Disparity Value (DDV) [107].. This work presents an image steganography method that integrates Hénon Map–based Particle Swarm Optimization (HMPSO) with Distinction Disparity Value (DDV) embedding to enhance the confidentiality and integrity of hidden data. HMPSO guides the optimal pixel selection process, while DDV ensures controlled embedding that minimizes distortion. To further improve security, the secret message is compressed with Huffman coding prior to embedding. The method was evaluated on grayscale and color images from the USC–SIPI database at multiple payload levels (6.25%, 12.5%, 18.75%, and 25%). Experimental results show high imperceptibility with PSNR values up to 78.09 dB and SSIM reaching 1.000, while maintaining low MSE (0.1012–0.8021). Importantly, the scheme withstands statistical χ^2 attacks, making it more robust compared to conventional LSB and other PSO-based approaches. The key contribution lies in balancing payload capacity, image quality, and resistance to steganalysis through the combined use of HMPSO-driven pixel selection and DDV embedding.

7.5.4 Muhuri et al. (2020) — PSO–IWT for transform-domain embedding [108].. This work integrates Particle Swarm Optimization (PSO) with Integer Wavelet Transform (IWT) for image steganography. The key idea is that PSO evolves an optimal substitution matrix to guide the embedding of secret data into IWT coefficients. At the same time, an OPAP adjustment step minimizes distortion between cover and stego images. Experiments on standard benchmark images (Lena, Baboon, Barbara, Jet) under a fixed payload of 589,824 bits demonstrated consistent visual quality, achieving PSNR values between 41.13–41.97 dB. Comparative analysis confirmed that the proposed PSO–IWT scheme outperformed PSO–LSB and PSO–DWT variants in imperceptibility and robustness.

7.5.5 Rezaei et al. (2024) — Bio-inspired hybrids for spatial-domain embedding [109].. This study introduces a blind and attack-resistant steganography framework in the spatial domain, where a wide set of metaheuristics (CS, BCO, CSO, GA, PSO, SA, FA) are applied to optimize pixel substitution. Beyond evaluating individual algorithms, the authors emphasize hybrid designs: CS–GA–BCO proved most effective for color images, while CS–GA–PSO excelled on grayscale. The approach consistently improved imperceptibility (PSNR ∼41.8–42.1 dB for the best individuals, up to ∼45–46 dB with hybrids) and demonstrated stronger robustness compared to LSB and even competitive or superior results against DWT-based schemes. The method thus highlights the potential of hybrid bio-inspired optimization in balancing image quality with resistance to steganalysis.

7.5.6 Mohsin et al. (2019) — PSO-guided spatial-domain embedding [110].. This work addresses the challenge of achieving high payload capacity without degrading stego quality by casting pixel selection in the spatial domain as an optimization problem. The authors replace GA with Particle Swarm Optimization (PSO), which efficiently determines the best pixel positions, scan order, and LSB planes for embedding. By partitioning both cover and secret into four blocks, PSO balances embedding load across the image while preserving imperceptibility. Comparative experiments on standard grayscale benchmarks show a clear gain over GA, with PSNR rising from ∼45.1 dB (GA) to 56.6 dB under a maximum payload of 4 bpp (≈40%). The method further demonstrated practical feasibility with a total runtime of 4.735 s for embedding and extraction across five images.

7.5.7 Denis R and Madhubala P (2020) — AGA–OPAP for DWT-based embedding [111].. This work applies an Adaptive Genetic Algorithm (AGA) to derive an optimal substitution matrix for LSB embedding in the two-level DWT domain, with OPAP used to refine pixel values. Tested on benchmark images (Lena,

Baboon, Boat, Fundus1–4), the method improved PSNR from post-embedding ~50–58 dB to post-optimization 51.29–59.62 dB, yielding gains of +1–2 dB while maintaining robustness against RS steganalysis and low execution time.

TABLE VI : APPLICATIONS OF METAHEURISTIC ALGORITHMS IN IMAGE STEGANALYSIS

REF	Classifier Used	Metaheuristic Algorithm	Purpose	Cover type	Performance
[112]	Support Vector Machine (SVM)	Particle Swarm Optimization (PSO)	Blind statistical steganalysis; PSO tunes SVM hyperparameters (C, γ); 8×8 block-based features (first/second-order, extended DCT, Markov), optional calibration, PCA + 10-fold CV; spatial (LSB Replacement, LSB Matching, PVD) and transform (F5/DCT) schemes	JPEG (256×256); INRIA Holidays (1500, train) + UCID(800,test)	- Accuracy (LSB Replacement): 84.5% (ANOVA, strat./auto) - Accuracy (LSB Matching): 84.86% (ANOVA, shuffle) - Accuracy (PVD): 99.8% (ANOVA, linear) - Accuracy (F5): 97.6% (ANOVA, shuffle)
[113]	SVM, Ensemble, LDA, kNN	Multi-Island Lévy-Flight based Grasshopper Optimization Algorithm (MI–LFGOA)	Wrapper feature selection with PCA pre-processing followed by LFGOA using a multi-island strategy; fitness = detection error (SVM/ensemble). Objective: reduce SRM (34,671-D) and SPAM (686-D) dimensionality and computational cost while preserving or improving detection accuracy.	Spatial images (BOSSBase 1.01; grayscale)	Detection accuracy up to92.2% (SPAM, 0.7 bpp) and 94% (SRM,0.7bpp); 92–96% feature reduction; outperforms PSO, GWO, GOA, BA,FA.
[114]	Linear SVM, DT, NB, k-NN	APSO (adaptive inertia-weight PSO)	AUC-based wrapper feature selection for dimensionality reduction in steganalysis	Spatial images: BOSSBase1.01 (10k cover / 10k stego)	- **SPAM:** Accuracy = 82.62% (140 selected features out of 686) - **CC-PEV:** Accuracy = 87.72% (363 selected features out of 548)
[115]	SVM, LDA, RF, kNN, ZeroR	Levy Flight-based Grey Wolf Optimization (LFGWO)	selects the most relevant features from high-dimensional SPAM and AlexNet .	Spatial images (BOSSBase v1.01	- SPAM: 84 selected features (out of 686), accuracy = 69.12% (RF) - AlexNet: 89 selected features (out of 1000), accuracy = 67.11% (RF) - Reduced training time vs. full features; outperformed PSO and GWO in feature reduction and accuracy

REF	Classifier Used	Metaheuristic Algorithm	Purpose	Cover type	Performance
[116]	Xu-Net, Yedroudj-Net (Deep Learning Networks)	Evolutionary Algorithm	Enhancing steganalysis network training performance by applying a strengthening framework based on evolutionary algorithms.	Grayscale Images (BOSSBase 1.01, BOWS2)	Improved Xu-Net accuracy by over 1.1%, Yedroudj-Net by over 1.3%. Faster convergence and improved learning ability during training.
[117]	k-NN	BDA–SA (Binary Dragonfly Algorithm + Simulated Annealing)	Hybrid approach: BDA with SA to avoid local optima in BDA. Feature selection to reduce dimensionality and improve accuracy.	18 datasets from UCI repository	Largest gain: +37.4pp (Exactly: 100.0% vs 62.6% BALO) - **Also observed:** +33.4 pp vs BGWO, +32.8 pp vs BPSO (Exactly dataset) - **Smallest gain**: +3.1 pp (Breastcancer : 98.8% vs 95.7% BGWO)

Narrative summaries of steganalysis studies corresponding to Table VI

7.5.8 Shankar & Azhakath (2023) — Random-embedded, calibrated statistical blind JPEG steganalysis with SVM and SVM–PSO [112].. The authors conduct a random-embedded, calibrated statistical blind steganalysis study on JPEG images. Their pipeline applies DCT, then uses calibration to estimate the cover prior to feature extraction. Block (8 ×8) based analysis where first-order, second-order, extended DCT, and Markov features are extracted, with PCA for reduction. Embedding is evaluated across spatial (LSB Replacement, LSB Matching, PVD) and transform (F5) domains using random embedding percentages. For classification, they compare cross-validated SVM against SVM–PSO under multiple kernel functions and dataset resampling schemes (termed "sampling" in the paper: linear, shuffling, stratified, automatic). The datasets are INRIA Holidays (training) and UCID (testing), JPEG lossless, 256 × 256. Overall, they report better classification for SVM–PSO in several settings (notably on uncalibrated images) and note stable convergence characteristics of PSO—supporting the view that metaheuristics can assist not only with feature design but also with the practical configuration of classical detectors (e.g., via the kernels and sampling schemes examined in the study).

7.5.9 Chhikara & Kumar (2020) — MI–LFGOA for spatial rich-model steganalysis [113].. This work addresses the curse of dimensionality in spatial steganalysis, where descriptors such as SRM (34k+ features) and SPAM (686 features) impose high training cost with redundant information. The authors integrate PCA with a metaheuristic search, introducing a Lévy-flight variant of Grasshopper Optimization (LFGOA) and further extending it into a multi-island framework (MI–LFGOA) to maintain diversity and avoid premature convergence. On BOSSBase 1.01, their method reduces feature sets by over 90% while still achieving ∼92% (SPAM) and 94% (SRM) detection accuracy. Compared with PSO, GWO, GOA, BA, and FA, MI–LFGOA consistently produced more compact subsets without sacrificing accuracy. The key contribution is showing that multi-island search can make rich-model steganalysis computationally feasible, highlighting the potential of hybrid dimensionality reduction (PCA + metaheuristic) in digital forensics.

7.5.10 Adeli et al. (2018) — APSO for spatial image steganalysis [114].. The study introduces an adaptive inertia-weight PSO (APSO) as a wrapper-based selector using AUC as the fitness criterion. Experiments on BOSSBase 1.01 with SPAM and CC-PEV descriptors demonstrate that APSO can achieve competitive detection accuracy while substantially reducing the feature dimensionality: from 686 to 140 features in SPAM (82.6% accuracy) and from 548 to 363 features in CC-PEV (87.7% accuracy). In addition to accuracy gains, the method showed low computational cost, with execution times of about

248 ms for SPAM and 214 ms for CC-PEV, confirming that APSO is efficient compared to conventional feature selection approaches.

7.5.11 Pathak et al. (2019) — LFGWO for feature selection in steganalysis [115].. The authors proposed a Levy Flight based Grey Wolf Optimization (LFGWO) for feature selection. They evaluated it on the BOSSBase v1.01 dataset using SPAM and AlexNet features. According to Table 4, LFGWO reduced the SPAM feature set from 686 to 84 and achieved a classification accuracy of 69.12% with Random Forest. For AlexNet, the feature set was reduced from 1000 to 89 with an accuracy of 67.11% (RF). The comparative results further show that PSO selected 95 (SPAM) and 94 (AlexNet) features with accuracies of 59.63% and 56.35%, while GWO selected 87 (SPAM) and 92 (AlexNet) features with accuracies of 61.15% and 57.25%. In addition, Table 5 reports that training times were significantly reduced. For example, Random Forest required 4.12s (SPAM) and 7.31s (AlexNet) without feature selection, compared to only 0.67s and 0.71s after applying LFGWO. These results confirm that the method not only improves accuracy and reduces dimensionality but also enhances computational efficiency.

7.5.12 Ma et al. (2025) — Evolutionary Training Framework [116].. Ma et al. propose an evolutionary training framework that strengthens spatial CNN steganalyzers without changing their architectures. The method encodes the convolutional layer and the BN layer as block-level individuals, promotes model diversity via Xavier and Kaiming initialization, and triggers strengthening when training detection accuracy stalls according to a defined decision rule. It then applies an Elite plus Linear-rank selection strategy, adaptive crossover with probability controlled by population fitness, and a staged mutation scheme with decreasing amplitude. Experiments on BOSSBase 1.01 (10,000 grayscale images, resized from 512×512 to 256×256) with BOWS2 as supplemental data and a 4:5:1 train: test: validation split, using WOW, S-UNIWARD, and HILL at 0.2, 0.3, and 0.4 bpp, report consistent gains: Xu-Net improves by more than 1.1 percentage points and Yedroudj-Net by more than 1.3 percentage points, with faster convergence.

7.5.13 Chantar et al. (2021) — BDA-SA wrapper (general-purpose) [117].. Addressing local-optima pitfalls in single swarm selectors, this study hybridizes the Binary Dragonfly Algorithm (BDA) with Simulated Annealing (SA), embedding a local-refinement phase over the best binary solution. Although evaluated on diverse UCI datasets rather than steganalysis-specific corpora, the mechanism—global search plus local exploitation—transfers naturally to steganalysis pipelines that must compress very high-dimensional descriptors (e.g., SPAM/SRM or CNN features) without sacrificing detection accuracy.

8. DISCUSSION

The consolidated evidence in Table V and Table VI highlights how different metaheuristic families behave under specific embedding domains and analysis objectives, which provides actionable guidance for practitioners. In the spatial domain of steganography, swarm-based approaches such as PSO have shown clear advantages when imperceptibility and payload are the main concerns. For example, HMPSO combined with DDV embedding achieved PSNR values between 61.41 and 78.09 dB with SSIM up to 1.000, while maintaining robustness against the χ^2 attack across payloads ranging from 6.25% to 25% [107]. Similarly, Mohsin et al. reported that a PSO-driven steganography produced 56.60 dB PSNR compared to 45.13 dB with a GA baseline at around 40% payload, with a total runtime of only 4.735 s over five images [110]. These results suggest that PSO-based families represent a pragmatic choice for spatial-domain applications where high fidelity and moderate payload capacity are prioritized. For steganography, this is the opposite: robustness and stability are favored, and nature-inspired optimizers perform better. In case of HHO coupled with IWT, the PSNR values varied from 36.66 to 38.05 dB, and the range of SSIM was 0.9144 to 0.9713, and it is robust to RS/PDH and generic image processing attacks [105]. PSO–IWT delivered PSNR values of 41.13–41.97 dB for a fixed payload of 589,824 bits [108]. More notably, the BESOPS–CE hybrid scheme provided both high imperceptibility, with PSNR up to 56.64 dB and SSIM near 0.9998, and robustness, as indicated by PSNR values under attack conditions of about 55 dB and NCC above 0.998 [106]. This evidence indicates that when robustness to compression and noise is critical, HHO–IWT and PSO–IWT are suitable. At the same time, BES with chaotic

encryption is preferable when both imperceptibility and robustness are required in transform-domain embedding. Hybrid frameworks that combine metaheuristics with cryptographic or post-adjustment techniques further illustrate how balanced objectives can be achieved. For example, the AGA–DWT–OPAP method consistently improved PSNR by around 1–2 dB after optimization (up to 59.62 dB) while maintaining low timing overheads, demonstrating that evolutionary GA variants with distortion minimization can enhance transform-domain quality without compromising practicality [111]. BESOPS–CE similarly combines pixel selection with chaotic encryption to simultaneously improve imperceptibility and robustness [106]. Turning to steganalysis, Table VI shows that swarm and evolutionary algorithms are effective for feature selection and classifier configuration. MI–LFGOA reduced SRM and SPAM features by more than 90% while retaining detection accuracies of 94% and 92.2% respectively [113]. APSO achieved 82.62% with 140 selected SPAM features and 87.72% with 363 selected CC-PEV
features, with relatively low execution times [114]. LFGWO reduced SPAM to 84 features and AlexNet to 89 features, achieving 69.12% and 67.11% accuracy with Random Forest, outperforming PSO and GWO under the same conditions [115]. For classifier tuning, PSO optimized SVM parameters to reach 99.8% accuracy on PVD and 97.6% on F5, and improved the detection of LSB-based schemes [112]. At the deep learning level, evolutionary strengthening improved CNN steganalyzers such as Xu-Net and Yedroudj-Net by more than 1.1–1.3 percentage points, with faster convergence [116]. Collectively, these findings show that swarm/evolutionary selectors are practical tools for dimensionality reduction, PSO is effective for classical classifier optimization, and evolutionary training can incrementally improve deep architectures. Beyond metaheuristic-based approaches, Płachta et al. (2022) [118] provide a rigorous comparative study of JPEG image steganalysis on BOSSBase (QF = 75) using three embedding algorithms (nsF5, J-Uniward, UERD) at two payloads (0.1 and 0.4 bpnzac). They evaluated both shallow ensembles and deep learning models across DCTR, GFR, and PHARM feature spaces with balanced test sets and standard metrics (Accuracy, Precision, Recall, F1, AUC). Their results show that DCTR and GFR consistently outperform PHARM, with near-perfect detection for nsF5 at 0.4 bpnzac (∼99.9% accuracy). In contrast, J-Uniward at 0.1 bpnzac remains particularly challenging (maximum ≈ 56.3% accuracy). Importantly, their best ensemble (linear-regression fusion on DCTR) achieved mean Accuracy ≈ 80.1% and AUC ≈ 84.3%, slightly surpassing the best deep model (≈ 78.2% Accuracy, AUC ≈ 83.0%). The authors explicitly state that "the performance of the best deep learning algorithm was either similar or slightly inferior to that of the best ensemble classifier built on linear regression," concluding that carefully designed ensemble classifiers can serve as a strong alternative to deep learning in image steganalysis. Finally, evidence from hybrid search methods, although tested on general-purpose UCI datasets rather than image corpora, further supports the principle of combining global and local refinement. The BDA–SA wrapper achieved up to 100% accuracy on the Exactly dataset compared to 67.2–62.6% for competing methods, with its smallest gain still at +3.1 percentage points on the Breastcancer dataset [117]. This reinforces the general observation, already reflected in Table VI, that global exploration combined with local exploitation is beneficial in feature selection pipelines.

In summary, the comparative results in Tables V and VI underscore that swarm-based algorithms, especially PSO and its hybrids, are most reliable in spatial steganography where imperceptibility and payload matter, nature-inspired approaches such as HHO and BES perform better in the frequency domain where robustness is critical, and hybrid designs provide balanced trade-offs. For steganalysis, swarm and evolutionary algorithms are particularly effective for feature selection and classifier configuration, with global–local hybridization strategies further enhancing performance. The complementary evidence from Płachta et al. (2022) further emphasizes that ensemble classifiers can rival or even outperform deep learning in JPEG steganalysis, providing practitioners with an additional perspective for algorithm selection.

9. Research Gaps

Although recent contributions demonstrate remarkable progress, several gaps persist. First, the absence of unified datasets and standardized evaluation protocols hinders fair comparison and reproducibility across studies. Second, scalability to large-scale and high-resolution datasets has not been systematically addressed, limiting the applicability of current methods in real-world scenarios. Third, while robustness against common distortions has been achieved, resistance to advanced adversarial steganalysis tools remains weak. Fourth, the interpretability of metaheuristic-driven designs is rarely explored, leaving unclear why certain optimization strategies succeed. Finally, despite promising results of hybrid and ensemble-based approaches, the fundamental trade-offs among imperceptibility, robustness, payload, and detectability remain unresolved, underscoring the need for more adaptive and balanced frameworks.

10. Future Directions

The survey of recent contributions reveals that despite the impressive improvements achieved by metaheuristic-driven

image steganography and steganalysis, several challenges remain. As highlighted in Tables V and VI, spatial-domain approaches optimized with metaheuristics can reach very high imperceptibility (PSNR above 55 dB and SSIM close to 0.99). At the same time, transform-domain methods provide robustness with BER values below 0.01 and NCC near unity. On the analysis side, optimization-assisted steganalyzers frequently report detection accuracies higher than 90% together with competitive precision, recall, F1, and AUC scores. These observations confirm the progress of the field, but also point to open directions. One important perspective is the integration of deep models with metaheuristic optimization. While deep architectures have shown strong performance, comparative evidence [118] indicates that ensemble-based solutions may still outperform lightweight neural networks in terms of accuracy and AUC. Exploring synergies between these paradigms could improve both embedding adaptivity and detection reliability. Another direction concerns robustness against increasingly powerful steganalysis tools, since the reviewed results demonstrate that transform-domain approaches already gain advantages in this aspect, but further enhancement is required. The reviewed studies also show that algorithm performance varies significantly with domain and payload, which underlines the necessity of systematic benchmarking. The lack of unified datasets and evaluation protocols prevents fair comparison across methods, and the development of standard frameworks remains a priority. Finally, the consistent trade-offs observed in the survey (imperceptibility vs. robustness, payload vs. detectability) highlight that future research must focus on adaptive and hybrid strategies capable of balancing these conflicting requirements. In conclusion, image steganography and steganalysis remain fertile areas of research. Addressing the outlined challenges, guided by the performance evidence summarized in this review, will be crucial to moving towards more secure and practically deployable systems.

Conflicts of Interest

The authors declare no conflicts of interest.

Funding

This research received no external funding.

Acknowledgment

The authors extend their sincere thanks to the anonymous reviewers and the Editor-in-Chief for their insightful comments and valuable suggestions.

References

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. A, vol. 247, pp. 529–551, Apr. 1955.
[2] M. Wu and B. Liu, Multimedia Data Hiding. Berlin, Germany: Springer, 2003.
[3] A. Melman and O. Evsutin, "Image data hiding schemes based on metaheuristic optimization: A review," Artif. Intell. Rev., vol. 56, no. 12, pp. 15375–15447, 2023.
[4] H. Alyasiri, J. A. Clark, and D. Kudenko, "Evolutionary computation algorithms for detecting known and unknown attacks," in Proc. Int. Conf. Secur. Inf. Technol. Commun., Cham, Switzerland: Springer, 2018, pp. 170–184.
[5] A. Zeinalpour and C. P. McElroy, "Comparing metaheuristic search techniques in addressing the effectiveness of clustering-based DDoS attack detection methods," Electronics, vol. 13, no. 5, p. 899, 2024.
[6] E.-S. M. El-Kenawy et al., "Advanced dipper-throated meta-heuristic optimization algorithm for digital image watermarking," Appl. Sci., vol. 12, no. 20, p. 10642, 2022.
[7] M. F. Şahin and F. Anka, "Metaheuristics role in image processing and computer vision applications: A comprehensive review," Cluster Comput., vol. 28, no. 13, p. 871, 2025.
[8] F. A. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proc. IEEE, vol. 87, no. 7, pp. 1062–1078, Jul. 1999.
[9] S. Sharma, A. Gupta, M. C. Trivedi, and V. K. Yadav, "Analysis of different text steganography techniques: A survey," in Proc. Int. Conf. Comput. Intell. Commun. Technol. (CICT), 2016, pp. 130–133.
[10] N. Li, J. Qin, X. Xiang, and Y. Tan, "Robust coverless video steganography based on pose estimation and object tracking," J. Inf. Secur. Appl., vol. 87, p. 103912, 2024.
[11] J. Kunhoth, N. Subramanian, S. Al-Maadeed, and A. Bouridane, "Video steganography: Recent advances and challenges," Multimedia Tools Appl., vol. 82, no. 27, pp. 41943–41985, 2023.
[12] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels," J. Vis. Commun. Image Represent., vol. 28, pp. 21–27, 2015.

[13] A. K. Sahu and M. Sahu, "Digital image steganography and steganalysis: A journey of the past three decades," Open Comput. Sci., vol. 10, no. 1, pp. 296–342, 2020.
[14] F. Şahin, T. Çevik, and M. Takaoğlu, "Review of the literature on the steganography concept," Int. J. Comput. Appl., vol. 975, p. 8887, 2021.
[15] M. A. Majeed, R. Sulaiman, Z. Shukur, and M. K. Hasan, "A review on text steganography techniques," Mathematics, vol. 9, no. 21, p. 2829, 2021.
[16] B. Chauhan, S. Borikar, S. Aote, and V. Katankar, "A survey on image cryptography using lightweight encryption algorithm," Int. J. Sci. Res. Sci. Eng. Technol., vol. 4, no. 4, pp. 344–347, 2018.
[17] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography, 2nd ed. San Francisco, CA, USA: Morgan Kaufmann, 2007.
[18] N. Hamid, A. Yahya, R. B. Ahmad, and O. M. Al-Qershi, "Image steganography techniques: An overview," Int. J. Comput. Sci. Secur., vol. 6, no. 3, pp. 168–187, 2012.
[19] J. M. Jenifer, S. R. Ratna, J. S. Loret, and D. M. Gethsy, "A survey on different video steganography techniques," in Proc. Int. Conf. Trends Electron. Inform. (ICOEI), 2018, pp. 627–632.
[20] D. Pandey et al., "Secret data transmission using advanced steganography and image compression," Int. J. Nonlinear Anal. Appl., vol. 12, no. Special Issue, pp. 1243–1257, 2021.
[21] N. Jain, S. Meshram, and S. Dubey, "Image steganography using LSB and edge–detection technique," Int. J. Soft Comput. Eng., vol. 2, no. 3, pp. 217–222, 2012.
[22] R. Krenn, "Steganography and steganalysis," 2004.
[23] J. Kour and D. Verma, "Steganography techniques–A review paper," Int. J. Emerg. Res. Manag. Technol., vol. 3, no. 5, pp. 132–135, 2014.
[24] G. Kaur and A. Kochhar, "A review on image steganography techniques," Int. J. Adv. Res. Comput. Sci. Softw. Eng., vol. 5, no. 4, pp. 227–231, 2015.
[25] F. Q. A. Alyousuf, R. Din, and A. J. Qasim, "Analysis review on spatial and transform domain technique in digital steganography," Bull. Electr. Eng. Inform., vol. 9, no. 2, pp. 573–581, 2020.
[26] T. Morkel, J. H. Eloff, and M. S. Olivier, "An overview of image steganography," in Proc. Inf. Secur. South. Afr. Conf. (ISSA), 2005, pp. 1–11.
[27] R. Rădescu and R. Gliga, "An introduction to steganography," UPB Sci. Bull. Ser. C Electr. Eng., vol. 64, no. 1–4, pp. 17–24, 2004.
[28] J. M. Koelling, Digital Imaging: A Practical Approach. Walnut Creek, CA, USA: Altamira Press, 2004.
[29] M. Douglas, K. Bailey, M. Leeney, and K. Curran, "An overview of steganography techniques applied to the protection of biometric data," Multimedia Tools Appl., vol. 77, no. 13, pp. 17333–17373, 2018.
[30] N. Sharma and U. Batra, "A review on spatial domain technique based on image steganography," in Proc. Int. Conf. Comput. Commun. Technol. Smart Nation (IC3TSN), 2017, pp. 24–27.
[31] A. O. Aljahdali and O. A. Al-Harbi, "Double layer steganography technique using DNA sequences and images," PeerJ Comput. Sci., vol. 9, p. e1379, 2023.
[32] S. Sajasi and A.-M. E. Moghadam, "An adaptive image steganographic scheme based on noise visibility function and an optimal chaotic based encryption method," Appl. Soft Comput., vol. 30, pp. 375–389, 2015.
[33] C.-K. Chan and L.-M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit., vol. 37, no. 3, pp. 469–474, 2004.
[34] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," Pattern Recognit. Lett., vol. 24, no. 9–10, pp. 1613–1626, 2003.
[35] H.-C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods," IEE Proc. Vis. Image Signal Process., vol. 152, no. 5, pp. 611–615, 2005.
[36] C.-H. Yang, C.-Y. Weng, S.-J. Wang, and H.-M. Sun, "Adaptive data hiding in edge areas of images with spatial LSB domain systems," IEEE Trans. Inf. Forensics Security, vol. 3, no. 3, pp. 488–497, Sep. 2008.
[37] C.-H. Yang, "Varied PVD+LSB evading detection programs to spatial domain in data embedding systems," J. Syst. Softw., vol. 83, no. 10, pp. 1635–1643, 2010.
[38] X. Liao, Q.-Y. Wen, and J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," J. Vis. Commun. Image Represent., vol. 22, no. 1, pp. 1–8, 2011.
[39] Y.-P. Lee et al., "High-payload image hiding with quality recovery using tri-way pixel-value differencing," Inf. Sci., vol. 191, pp. 214–225, 2012.
[40] M. Khodaei and K. Faez, "New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing," IET Image Process., vol. 6, no. 6, pp. 677–686, 2012.
[41] J. Chen, "A PVD-based data hiding method with histogram preserving using pixel pair matching," Signal Process. Image Commun., vol. 29, no. 3, pp. 375–384, 2014.

[42] G. Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges," Multimedia Tools Appl., vol. 75, no. 21, pp. 13541–13556, 2016.
[43] D. A. Shehab and M. J. Alhaddad, "Comprehensive survey of multimedia steganalysis: Techniques, evaluations, and trends in future research," Symmetry, vol. 14, no. 1, p. 117, 2022.
[44] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," Signal Process., vol. 90, no. 3, pp. 727–752, 2010.
[45] J. Mielikainen, "LSB matching revisited," IEEE Signal Process. Lett., vol. 13, no. 5, pp. 285–287, May 2006.
[46] J. Al-Azzeh, Z. Alqadi, B. Ayyoub, and A. Sharadqh, "Improving the security of LSB image steganography," JOIV Int. J. Inform. Vis., vol. 3, no. 4, pp. 384–387, 2019.
[47] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," in Proc. Int. Conf. Image Process. (ICIP), vol. 3, 2001, pp. 1019–1022.
[48] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," Neurocomputing, vol. 335, pp. 299–326, 2019.
[49] D.-C. Wu and Z.-N. Shih, "Image steganography by pixel-value differencing using general quantization ranges," CMES-Comput. Model. Eng. Sci., vol. 141, no. 1, 2024.
[50] N.-I. Wu and M.-S. Hwang, "Data hiding: Current status and key issues," Int. J. Netw. Secur., vol. 4, no. 1, pp. 1–9, 2007.
[51] M. Alanzy, R. Alomrani, B. Alqarni, and S. Almutairi, "Image steganography using LSB and hybrid encryption algorithms," Appl. Sci., vol. 13, no. 21, p. 11771, 2023.
[52] S. Saha et al., "Extended exploiting modification direction based steganography using hashed-weightage array," Multimedia Tools Appl., vol. 79, no. 29, pp. 20973–20993, 2020.
[53] T. D. Nguyen, S. Arch-Int, and N. Arch-Int, "An adaptive multi bit-plane image steganography using block data-hiding," Multimedia Tools Appl., vol. 75, no. 14, pp. 8319–8345, 2016.
[54] K. Muhammad et al., "A secure method for color image steganography using gray-level modification and multi-level encryption," KSII Trans. Internet Inf. Syst., vol. 9, no. 5, pp. 1938–1962, 2015.
[55] M. Hassaballah, Digital Media Steganography: Principles, Algorithms, and Advances. Cambridge, MA, USA: Academic Press, 2020.
[56] V. M. Potdar and E. Chang, "Grey level modification steganography for secret communication," in Proc. IEEE Int. Conf. Ind. Inform. (INDIN), 2004, pp. 223–228.
[57] M. Safarpour and M. Charmi, "Capacity enlargement of the PVD steganography method using the GLM technique," arXiv:1601.00299, 2016.
[58] Y.-K. Lee and L.-H. Chen, "High capacity image steganographic model," IEE Proc. Vis. Image Signal Process., vol. 147, no. 3, pp. 288–294, 2000.
[59] P. C. Mandal, I. Mukherjee, G. Paul, and B. Chatterji, "Digital image steganography: A literature survey," Inf. Sci., vol. 609, pp. 1451–1488, 2022.
[60] M. Dalal and M. Juneja, "Steganography and steganalysis (in digital forensics): A cybersecurity guide," Multimedia Tools Appl., vol. 80, no. 4, pp. 5723–5771, 2021.
[61] T. Alobaidi and W. Mikhael, "An adaptive steganography insertion technique based on wavelet transform," J. Eng. Appl. Sci., vol. 70, no. 1, p. 144, 2023.
[62] J. Khandelwal, V. K. Sharma, D. Singh, and A. Zaguia, "DWT-SVD based image steganography using threshold value encryption method," Comput. Mater. Continua, vol. 72, no. 2, 2022.
[63] M. Hamidi, M. E. Haziti, H. Cherifi, and M. E. Hassouni, "Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform," Multimedia Tools Appl., vol. 77, no. 20, pp. 27181–27214, 2018.
[64] A. Raid, W. Khedr, M. A. El-Dosuky, and W. Ahmed, "JPEG image compression using discrete cosine transform—A survey," Int. J. Comput. Sci. Eng. Surv., vol. 5, no. 2, 2014.
[65] T. Rabie, M. Baziyad, and I. Kamel, "High-fidelity steganography: A covert parity bit model-based approach," Algorithms, vol. 17, no. 8, 2024.
[66] T. Alobaidi and W. Mikhael, "An adaptive steganography insertion technique based on cosine transform," Iraqi J. Electr. Electron. Eng., vol. 20, no. 2, 2024.
[67] M. K. Abdmouleh, A. Khalfallah, and M. S. Bouhlel, "A novel selective encryption scheme for medical images transmission based-on JPEG compression algorithm," Procedia Comput. Sci., vol. 112, pp. 369–376, 2017.
[68] M. C. Stamm, S. K. Tjoa, W. S. Lin, and K. J. R. Liu, "Anti-forensics of JPEG compression," in Proc. IEEE Int. Conf. Acoust. Speech Signal Process. (ICASSP), 2010, pp. 1694–1697.
[69] B. Bao and Y. Wang, "A robust blind color watermarking algorithm based on the Radon-DCT transform," Multimedia Tools Appl., vol. 83, no. 24, pp. 64663–64682, 2024.

[70] K. R. Malik et al., "A hybrid steganography framework using DCT and GAN for secure data communication in the big data era," Sci. Rep., vol. 15, no. 1, p. 19630, 2025.
[71] Y. Huang, Z. Liu, Q. Wu, and X. Liu, "Robust image steganography against JPEG compression based on DCT residual modulation," Signal Process., vol. 219, p. 109431, 2024.
[72] G. Savithri, Vinupriya, S. Mane, and J. Saira Banu, "Parallel implementation of RSA 2D-DCT steganography and chaotic 2D-DCT steganography," in Proc. Int. Conf. Comput. Vis. Image Process. (CVIP), vol. 1, Cham, Switzerland: Springer, 2017, pp. 593–605.
[73] P.-C. Su, Y.-H. Cheng, and T.-Y. Kuo, "JSN: Design and analysis of JPEG steganography network," Electronics, vol. 13, no. 23, p. 4821, 2024.
[74] V. K. Sharma, U. C. Pati, and K. Mahapatra, "A simple VLSI architecture for computation of 2D DCT, quantisation and zig-zag ordering for JPEG," Int. J. Signal Imag. Syst. Eng., vol. 5, no. 1, pp. 58–65, 2012.
[75] R. I. Yousif and N. H. Salman, "Image compression based on arithmetic coding algorithm," Iraqi J. Sci., pp. 329–334, 2021.
[76] J. H. Pujar and L. M. Kadlaskar, "A new lossless method of image compression and decompression using Huffman coding techniques," J. Theor. Appl. Inf. Technol., vol. 15, 2010.
[77] X. Liu, P. An, Y. Chen, and X. Huang, "An improved lossless image compression algorithm based on Huffman coding," Multimedia Tools Appl., vol. 81, no. 4, pp. 4781–4795, 2022.
[78] Y. Dong and W. D. Pan, "A survey on compression domain image and video data processing and analysis techniques," Information, vol. 14, no. 3, p. 184, 2023.
[79] J. Fridrich, T. Pevný, and J. Kodovský, "Statistically undetectable JPEG steganography: Dead ends challenges, and opportunities," in Proc. ACM Workshop Multimed. Secur., 2007, pp. 3–14.
[80] L. Guo, J. Ni, W. Su, C. Tang, and Y.-Q. Shi, "Using statistical image model for JPEG steganography: Uniform embedding revisited," IEEE Trans. Inf. Forensics Security, vol. 10, no. 12, pp. 2669–2680, Dec. 2015.
[81] D. Y. Mikhail, R. S. Hawezi, and S. W. Kareem, "An ensemble transfer learning model for detecting stego images," Appl. Sci., vol. 13, no. 12, p. 7021, 2023.
[82] R. Chandramouli, "A mathematical framework for active steganalysis," Multimedia Syst., vol. 9, pp. 303–311, 2003.
[83] S. A. Laskar and K. Hemachandran, "A review on image steganalysis techniques for attacking steganography," Int. J. Eng. Res. Technol., vol. 3, no. 1, 2014.
[84] K. Bailey and K. Curran, "An evaluation of image based steganography methods," Multimedia Tools Appl., vol. 30, pp. 55–88, 2006.
[85] K. D. Michaylov and D. K. Sarmah, "Steganography and steganalysis for digital image enhanced forensic analysis and recommendations," J. Cyber Secur. Technol., vol. 9, no. 1, pp. 1–27, 2025.
[86] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems: Breaking the steganographic utilities EzStego, JSteg, Steganos, and S-Tools—and some lessons learned," in Proc. Int. Workshop Inf. Hiding, Cham, Switzerland: Springer, 1999, pp. 61–76.
[87] K. F. Rafat and S. M. Sajjad, "Advancing reversible LSB steganography: Addressing imperfections and embracing pioneering techniques for enhanced security," IEEE Access, 2024.
[88] C. Chen and Y. Q. Shi, "JPEG image steganalysis utilizing both intrablock and interblock correlations," in Proc. IEEE Int. Symp. Circuits Syst. (ISCAS), 2008, pp. 3029–3032.
[89] R. Chhikara, P. Sharma, B. Chandra, and N. Malik, "Modified bird swarm algorithm for blind image steganalysis," Int. J. Inf. Technol., vol. 15, no. 6, pp. 2877–2888, 2023.
[90] J. Kodovský and J. Fridrich, "Steganalysis of JPEG images using rich models," in Media Watermarking, Security, and Forensics, vol. 8303, Bellingham, WA, USA: SPIE, 2012, pp. 81–93.
[91] D. D. Shankar, N. Khalil, and A. S. Azhakath, "Moderate embed cross validated and feature reduced steganalysis using principal component analysis in spatial and transform domain with support vector machine and support vector machine-particle swarm optimization," Multimedia Tools Appl., vol. 82, no. 7, pp. 10249–10276, 2023.
[92] X. Song, C. Yang, K. Han, and S. Ding, "Robust JPEG steganography based on DCT and SVD in nonsubsampled shearlet transform domain," Multimedia Tools Appl., vol. 81, no. 25, pp. 36453–36472, 2022.
[93] S. Chhikara and R. Kumar, "Image steganalysis with entropy hybridized with chaotic grasshopper optimizer," Multimedia Tools Appl., vol. 80, no. 21, pp. 31865–31885, 2021.
[94] A. K. Sahu and A. Gutub, "Improving grayscale steganography to protect personal information disclosure within hotel services," Multimedia Tools Appl., vol. 81, no. 21, pp. 30663–30683, 2022.
[95] Y. Chen, H. Wang, W. Li, and J. Luo, "Cost reassignment for improving security of adaptive steganography using an artificial immune system," IEEE Signal Process. Lett., vol. 29, pp. 1564–1568, 2022.
[96] H. Jeyaprakash, B. S. Chokkalingam, V. V, and S. Mohan, "Stego detection: Image steganalysis using a novel hidden stego visual geometry group–based CNN classification," J. Appl. Secur. Res., vol. 18, no. 4, pp. 979–999, 2023.

[97] J. Fridrich and J. Kodovský, "Rich models for steganalysis of digital images," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 868–882, Jun. 2012.
[98] A. C. Johnvictor, A. J. Amalanathan, R. M. Pariti Venkata, and N. Jethi, "Critical review of bio-inspired data optimization techniques: An image steganalysis perspective," Wiley Interdiscip. Rev. Data Min. Knowl. Discov., vol. 12, no. 4, p. e1460, 2022.
[99] F. Li, K. Wu, J. Lei, M. Wen, Z. Bi, and C. Gu, "Steganalysis over large-scale social networks with high-order joint features and clustering ensembles," IEEE Trans. Inf. Forensics Security, vol. 11, no. 2, pp. 344–357, Feb. 2015.
[100] Y. Wang, Y. Ma, R. Jin, P. Liu, and N. Ruan, "Comprehensive criteria-based generalized steganalysis feature selection method," IEEE Access, vol. 8, pp. 154418–154435, 2020.
[101] Y. Ma, L. Xu, Y. Zhang, T. Zhang, and X. Luo, "Steganalysis feature selection with multidimensional evaluation and dynamic threshold allocation," IEEE Trans. Circuits Syst. Video Technol., vol. 34, no. 3, pp. 1954–1969, Mar. 2023.
[102] L. Li, M. Fan, and D. Liu, "AdvSGAN: Adversarial image steganography with adversarial networks," Multimedia Tools Appl., vol. 80, no. 17, pp. 25539–25555, 2021.
[103] D. K. Sarmah, A. J. Kulkarni, and A. Abraham, Optimization Models in Steganography Using Metaheuristics. Cham, Switzerland: Springer, 2020.
[104] Z. N. Ansari and S. D. Daxini, "A state-of-the-art review on meta-heuristics application in remanufacturing," Arch. Comput. Methods Eng., vol. 29, no. 1, pp. 427–470, 2022.
[105] M. Hassaballah, M. A. Hameed, A. I. Awad, and K. Muhammad, "A novel image steganography method for industrial internet of things security," IEEE Trans. Ind. Informat., vol. 17, no. 11, pp. 7743–7751, Nov. 2021.
[106] A. A. Bahaddad, K. A. Almarhabi, and S. Abdel-Khalek, "Image steganography technique based on bald eagle search optimal pixel selection with chaotic encryption," Alex. Eng. J., vol. 75, pp. 41–54, 2023.
[107] A. S. Ali, S. Alsamaraee, and A. A. Hussein, "Optimize image steganography based on distinction disparity value and HMPSO to ensure confidentiality and integrity," J. Comput. Netw. Commun., vol. 2024, p. 2516567, 2024.
[108] P. K. Muhuri, Z. Ashraf, and S. Goel, "A novel image steganographic method based on integer wavelet transformation and particle swarm optimization," Appl. Soft Comput., vol. 92, p. 106257, 2020.
[109] S. Rezaei and A. Javadpour, "Bio-inspired algorithms for secure image steganography: Enhancing data security and quality in data transmission," Multimedia Tools Appl., vol. 83, no. 35, pp. 82247–82280, 2024.
[110] A. H. Mohsin et al., "New method of image steganography based on particle swarm optimization algorithm in spatial domain for high embedding capacity," IEEE Access, vol. 7, pp. 168994–169010, 2019.
[111] R. Denis and P. Madhubala, "Evolutionary computing assisted visually-imperceptible hybrid cryptography and steganography model for secure data communication over cloud environment," Int. J. Comput. Netw. Appl., vol. 7, no. 6, p. 208, 2020.
[112] D. D. Shankar and A. S. Azhakath, "Random embedded calibrated statistical blind steganalysis using cross validated support vector machine and support vector machine with particle swarm optimization," Sci. Rep., vol. 13, p. 2359, 2023.
[113] S. Chhikara and R. Kumar, "Mi-LFGOA: Multi-island Lévy-flight based grasshopper optimization for spatial image steganalysis," Multimedia Tools Appl., vol. 79, no. 39, pp. 29723–29750, 2020.
[114] A. Adeli and A. Broumandnia, "Image steganalysis using improved particle swarm optimization based feature selection," Appl. Intell., vol. 48, pp. 1609–1622, 2018.
[115] Y. Pathak, K. Arya, and S. Tiwari, "Feature selection for image steganalysis using Lévy flight-based grey wolf optimization," Multimedia Tools Appl., vol. 78, pp. 1473–1494, 2019.
[116] Y. Ma, X. Zhang, J. Wang, R. Jin, R. Nasimov, and H. Zhang, "Digital image steganalysis network strengthening framework based on evolutionary algorithm," Sci. Rep., vol. 15, p. 7472, 2025.
[117] H. Chantar, M. Tubishat, M. Essgaer, and S. Mirjalili, "Hybrid binary dragonfly algorithm with simulated annealing for feature selection," SN Comput. Sci., vol. 2, no. 4, p. 295, 2021.
[118] M. Płachta, M. Krzemiń, K. Szczypiorski, and A. Janicki, "Detection of image steganography using deep learning and ensemble classifiers," Electronics, vol. 11, no. 10, p. 1565, 2022.