Artificial Intelligence Review (2023) 56:15375–15447
https://doi.org/10.1007/s10462-023-10537-w

Image data hiding schemes based on metaheuristic optimization: a review

Anna Melman[1] · **Oleg Evsutin**[1]

Published online: 18 June 2023

Abstract

The digital content exchange on the Internet is associated with information security risks. Hiding data in digital images is a promising direction in data protection and is an alternative to cryptographic methods. Steganography algorithms create covert communication channels and protect the confidentiality of messages embedded in cover images. Watermarking algorithms embed invisible marks in images for further image authentication and proof of the authorship. The main difficulty in the development of data hiding schemes is to achieve a balance between indicators of embedding quality, including imperceptibility, capacity, and robustness. An effective approach to solving this problem is the use of metaheuristic optimization algorithms, such as genetic algorithm, particle swarm optimization, artificial bee colony, and others. In this paper, we present an overview of data hiding techniques based on metaheuristic optimization. We review and analyze image steganography and image watermarking schemes over the past 6 years. We propose three levels of research classification: embedding purpose level, optimization purpose level, and level of metaheuristics. The results demonstrate the high relevance of using metaheuristic optimization in the development of new data hiding algorithms. Based on the results of the review, we formulate the main problems of this scientific field and suggest promising areas for further research.

Keywords Digital images · Steganography · Watermarking · Data hiding · Metaheuristic optimization

1 Introduction

The exchange of multimedia files on the network is currently widespread and is used in a variety of fields. Millions of people share images, audio recordings and video files every day. However, there are a number of security aspects along with the many benefits of such communication and it is necessary to ensure the protection of transmitted information. Important areas of data protection are cryptography and hiding data in digital objects

✉ Oleg Evsutin
evsutin.oo@gmail.com

[1] Department of Cyber-Physical Systems Information Security, HSE University, 11 Pokrovsky Bulvar, Moscow, Russia 109028

(Fig. 1). It should be noted that we consider only data protection methods that involve some transformation of information, so Fig. 1 does not include password protection systems, access rights management, etc.

Many cybersecurity problems are solved using cryptography, including symmetric and asymmetric cryptography methods. However, it is appropriate to use data hiding methods in some cases. Such methods include digital steganography and digital watermarking. Steganography has the same goal as encryption, i.e. data privacy protection. Unlike encryption, steganography methods hide secret information inside digital objects so that an attacker cannot even know about its presence. An object with embedded information can be safely transmitted over an open communication channel because it does not attract attention. Important criteria of the embedding efficiency are imperceptibility and capacity. Encryption and steganography are often combined in data protection schemes to improve the security (Puteaux and Puech 2018; Yi and Zhou 2017; Elhoseny et al. 2018). There are linguistic and technical (images, text, video, audio) steganography (Cheddad et al. 2010).

Watermark is a special mark, such as a logo, a hash code, or a random string. It is embedded into a digital object in order to authenticate that object, control its integrity, or protect the authorship. Fragile watermarks are destroyed by any change in the digital object and are used to detect accidental distortions or attacks. Semi-fragile watermarks are usually used to detect and localize fake content. Robust watermarks are for copyright protection, so they can be detected even after post-processing of watermarked digital objects. Watermarking is widespread in various fields, such as medicine (Parah et al. 2017; Thakkar and Srivastava 2017a), science (Pizzolante et al. 2018), and cinema (Zhao et al. 2019; Dubey and Modi 2021).

Various digital objects can be used as containers for embedding, such as Internet traffic (Fathi-Kazerooni and Rojas-Cessa 2020; Lu et al. 2021), databases (Kumar et al. 2020;

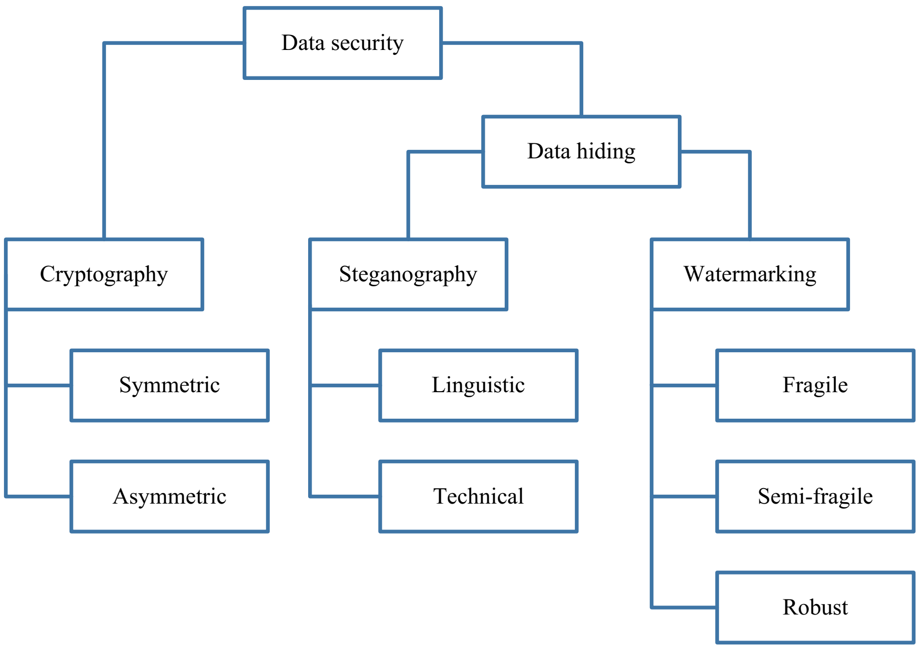


Fig. 1 Classification of digital data protection methods

Xiang and He 2018), sensor network data (Xiao and Gao 2019; Chen et al. 2019), and text documents (Xiang et al. 2018; Malik et al. 2017). However, hiding information in multimedia data is the most common (Dalal and Juneja 2021; AlSabhany et al. 2020; Subramanian et al. 2021). This is due to the nature of such data, including significant size, a high level of redundancy, and the prevalence of content-preserving post-processing methods. In this study, we focus on embedding additional information into digital images.

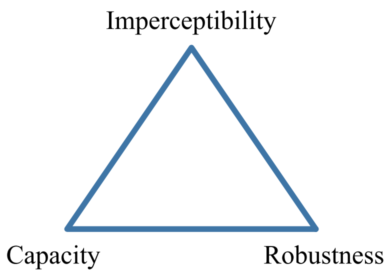
There are a wide variety of steganography and watermarking techniques for digital images (Evsutin et al. 2020; Singh et al. 2020; Wan et al. 2022; Kumar et al. 2022; Mandal et al. 2022). The authors use different methods to improve the efficiency of their schemes, such as interpolation (Zhang et al. 2017; Yang et al. 2017), edge detection (Parah et al. 2018; Ray et al. 2021), prediction errors (Chang et al. 2021; Bai et al. 2021), and neural networks (Mellimi et al. 2021; Liao et al. 2021).

The key performance indicators of information embedding, namely imperceptibility, capacity and robustness, cannot have maximum values at the same time. This idea is illustrated by the famous "magic triangle" (Dittmann et al. 2006), whose vertices contain each of the three criteria (Fig. 2). Maximizing any of the performance indicators leads to a decrease in the rest. Two of the three criteria located on the same side of the triangle can be quite high, but this leads to a significant decrease in efficiency for the criterion located on the opposite vertex. This simple figure shows that achieving a balance between different embedding characteristics is challenging.

Some authors use optimization methods in their data hiding algorithms to solve the described problem (Zhou et al. 2021; Wang et al. 2018b). A separate class consists of studies based on the use of metaheuristic optimization. Metaheuristic optimization effectively explores the search space regardless of the specific problem and finds solutions for a wide variety of problems, including non-linear and high-dimensional problems. The stochastic nature of metaheuristics makes it possible to find an optimal, or close to it solution in a reasonable time, excluding enumeration of all possible solutions. Therefore, authors of studies on data hiding often turn to this tool to find various embedding options. The first embedding schemes based on metaheuristics appeared quite a long time ago (Wang et al. 2001; Shih and Wu 2005; Huang et al. 2007; Yu et al. 2009), and they used the Genetic Algorithm (GA). However, the classic GA limits the scope of optimization problems to those for which the binary representation of individuals in the population is suitable. Modern steganography and watermarking algorithms use a large number of metaheuristics and different representations of individuals in a population (binary, integer, real values). This makes the algorithms more flexible and allows them to solve a wide range of data hiding problems.

In this paper, we present a review of studies on embedding information into digital images using metaheuristic optimization algorithms. It should be noted that despite the significant interest in this topic, a small number of review papers have been published. Abdul

Fig. 2 Magic triangle



Khalid et al. (2011) explore the application of bio-inspired algorithms as image processing techniques, but do not consider data hiding issues. Johnvictor et al. (2022) focus on the application of bio-inspired algorithms to image steganalysis. Soliman et al. (2014) include in the review only medical image watermarking schemes using metaheuristic optimization. Akay and Karaboga (2015) include several image and video watermarking schemes in an overview of the applications of the Artificial Bee Colony (ABC) algorithm. Huang et al. (2015) list a number of watermarking algorithms based on metaheuristics. Hanizan et al. (2017) consider several GA based steganography schemes. Singh et al. (2021a) and (2023) discuss some metaheuristic-based watermarking algorithms in their reviews of watermarking techniques; however they also do not discuss steganography schemes. Kapadia and Nithyanandam (2022) include only reversible data hiding schemes in the review.

Therefore, the main contribution of our study is as follows:

- We present an extensive research overview in the field of image steganography and watermarking using metaheuristic optimization over the past 6 years (2017–2022);
- We propose three levels of classification of studies in the field of image data hiding using metaheuristic optimization: embedding purpose level, optimization purpose level and metaheuristics level;
- We analyze optimization problems that are relevant to embedding information into digital images and show which of the metaheuristics are most often used to solve them;
- We formulate the problems of the subject area and indicate promising directions for further research.

The rest of the paper is organized as follows. In Sect. 2, we describe the background of our research. In Sect. 3, we present an overview of image data hiding schemes based on metaheuristic optimization, including steganography and watermarking ones. Section 4 contains a discussion of the review results, including an analysis of current trends and promising research directions. Section 5 summarizes our study.

2 Background

This section contains the background of our research. Here we provide basic information about image data hiding and key performance indicators of embedding. We also describe the basic concepts of metaheuristic optimization and provide a brief overview of the metaheuristics that different authors use in their data hiding schemes.

2.1 Data hiding in digital images

2.1.1 The general scheme

Data hiding is one of the information security areas. It consists in embedding additional information into some digital objects, in particular, images. As a result, such information becomes a part of the original image. The general scheme of this process is shown in Fig. 3. Data hiding methods are divided into steganography methods and digital watermarking methods depending on the embedding purpose.

Steganography techniques aim to ensure the confidentiality of embedded information. To do this, a secret message is imperceptibly embedded in the image. The presence of an

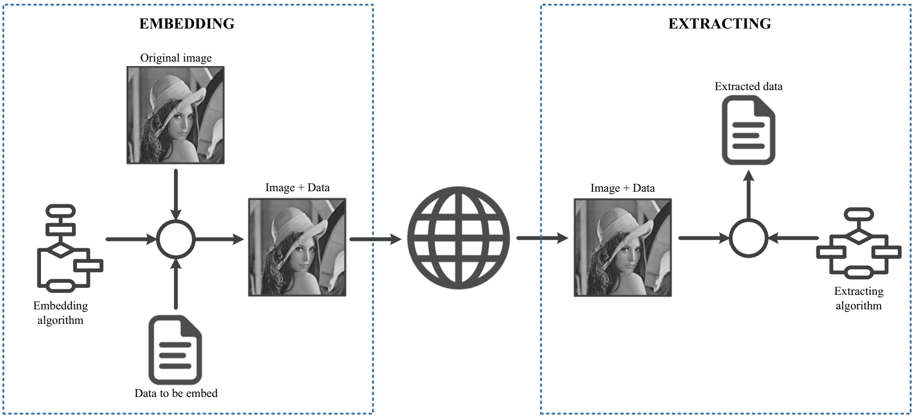


Fig. 3 The general scheme of image data hiding

attachment is not known to a third party, so an image with embedded information can be safely stored and transmitted over open communication channels. An efficient steganography scheme provides high embedding invisibility, due to which an attacker cannot detect a secret message.

Digital watermarking techniques are used to protect a cover image itself. A watermark is usually a logo or some information about an author of a digital object. Watermarking provides image authentication and the ability to verify copyright. Since many digital images are subject to various attacks, such as JPEG compression, many watermarking schemes provide for robust embedding to achieve a high level of security. In most cases, watermarking is done in an invisible way, but sometimes visible watermarks are used.

Steganography and watermarking methods are divided into spatial domain methods and frequency domain methods. Embedding information into the spatial domain of images consists in changing image pixels depending on information bits. Spatial domain schemes usually have a low level of robustness and are mainly used to solve steganography problems. Known methods include Least Significant Bit (LSB) (Muhammad et al. 2017; Zakaria et al. 2018), Quantization Index Modulation (QIM) (Chen and Wornell 2001; Zhang et al. 2018), Pixel Value Difference (PVD) (Pradhan et al. 2018; Ganguly et al. 2020), Histogram Shifting (HS) (Li and Li 2017; Ying et al. 2019), and others.

Frequency domain methods embed information in the frequency coefficients of images. Performing a frequency transform increases the computational complexity of the embedding scheme, but frequency domain embedding usually provides a higher level of robustness than spatial domain embedding. Most robust watermarking schemes work with the frequency domain of images. Such schemes can be based on the Discrete Wavelet Transform (DWT) (Liu et al. 2018; Chauhan et al. 2019) and other types of wavelet transforms, for example, the Integer Wavelet Transform (IWT) (Nazari and Mehrabian 2021; Zhang et al. 2020), on the Discrete Cosine Transform (DCT) (Ariatmanto and Ernawan 2020; Roy and Pal 2017), etc. Some authors propose hybrid schemes that combine several frequency transformations at once to form a hiding space (Hasan et al. 2021; Abdulrahman and Ozturk 2019). In many schemes, the authors apply Singular Value Decomposition (SVD) to the resulting array of frequency coefficients and use singular values for embedding to increase efficiency (Singh and Singh 2017; Anand and Singh 2020). A common embedding operation is a linear combination of the original image elements and the watermark according to the formula

$$I' = I * SF \times W, \tag{1}$$

where I is an original image, I' is a watermarked image, SF is a scaling factor, $*$ is a some linear operation, and W is a watermark. The scaling factor SF is also called the embedding strength. It affects the embedding robustness and the distortion level of the watermarked image. Increasing SF value increases the resistance of the watermark to various attacks, but worsens the embedding imperceptibility and vice versa. A parameter with a similar meaning is often used in watermarking schemes that use other embedding operations.

2.1.2 The key performance indicators

The key performance indicators of embedding additional information into digital images are imperceptibility, capacity, and robustness. The use of various optimization techniques in data hiding schemes is usually aimed at achieving the best values for one or more of these criteria.

Imperceptibility characterizes the visual quality of images with embedded information. The human eye is not very sensitive to small changes in pixel intensity, but it is able to distinguish more significant distortions. The high embedding imperceptibility means that the distortion caused by the embedding is not visible and does not affect the viewer's perception of the image. The main metrics of the imperceptibility are the Mean Squared Error (MSE), the Root Mean Square Error (RMSE), the Peak Signal-to-Noise Ratio (PSNR), and the Structural Similarity Index Measure (SSIM) (Kadhim et al. 2019).

The MSE metric evaluates the differences between two images and is calculated using the following formula:

$$MSE(I,I') = \frac{1}{m \times n} \sum_{i=1}^{m \times n} \left(I_i - I'_i\right)^2, \tag{2}$$

where m and n are width and height of an original image, I_i is an original image pixel value, I'_i is a stego or watermarked image pixel value. The RMSE metric is as follows:

$$RMSE(I,I') = \sqrt{MSE(I,I')}. \tag{3}$$

Low MSE and RMSE values indicate a similarity of images before and after embedding.

PSNR is the most common metric for assessing the invisibility of information embedding. The PSNR value is measured in decibels (dB). High values of the PSNR metric mean a high level of similarity between two images. $PSNR = 30$ dB is the lower limit of acceptable embedding quality (Cheddad et al. 2010). The following formula is used to calculate PSNR:

$$PSNR(I,I') = 10 \times \log_{10}\left(\frac{255^2}{MSE(I,I')}\right). \tag{4}$$

The SSIM metric is also quite widely used to assess the embedding invisibility. Some researchers show that SSIM more accurately characterizes the visual differences between two images (Setiadi 2021), but this metric is less common than PSNR for studies on data hiding. SSIM is calculated using the formula

$$SSIM(I,I') = \frac{\left(2\mu_C\mu_S + K_1\right) \times \left(2\sigma_{CS} + K_2\right)}{\left(\mu_C^2 + \mu_S^2 + K_1\right) \times \left(\sigma_C^2 + \sigma_S^2 + K_2\right)}, \tag{5}$$

where μ_C is a mean pixels value of a cover image, μ_S is a mean pixels value of a stego image, σ_C^2 is a variance of cover image pixel values, σ_S^2 is a variance of pixel values of stego image, σ_{CS} is a covariance of both images, K_1 and K_2 are constants.

Steganography schemes are characterized not only by visual invisibility, but also by statistical one, which means resistance to steganalysis. There are many different steganalysis methods. In the simplest case, differences between histograms of a cover image and a stego image are analyzed, or individual statistical indicators are investigated (Fridrich et al. 2001; Andriotis et al. 2013). More complex schemes use classifiers and neural networks to extract and analyze features (Singhal and Bedi 2021; Shojae Chaeikar and Ahmadi 2019). A steganography algorithm is considered resistant to stegoanalysis if the stegoanalyzer fails to detect the presence of embedded data in a stego image with accuracy better than random guessing. The most common methods of steganalysis are the following:

- Histogram analysis evaluates visual similarity between distributions of pixel values of a cover image and a stego image;
- The Regular-Singular (RS) steganalysis divides stego image pixel values into groups and determines the presence of a secret message by ratios in regular and singular groups;
- The chi-square test compares frequency distribution in a stego image with some sample distribution;
- The Kullback–Leibler (KL) divergence measures the distances between probability distributions and evaluates similarity of two images in steganalysis schemes;
- The sample pair analysis estimates message length after LSB embedding based on relationships among multi-sets pair;
- The feature-based steganalysis is a class of steganalysis schemes based on machine learning methods that analyze an extensive set of features.

Capacity indicates how much information is hidden in a digital image. Capacity can be expressed in absolute terms, such as the number of embedded bits, pixels, or characters, or in relative terms. The ratio of the total number of embedded bits to the image size in pixels is commonly used to estimate capacity and is measured in bits per pixel (bpp):

$$EC = \frac{B}{m \times n}, \tag{6}$$

where B is the total number of embedded bits.

Robustness refers to the stability of information extracting. In an ideal scenario, embedded information is extracted from the image without any errors, i.e. the extracted data is exactly the same as the original data. However, in practice, the number of incorrectly extracted bits is affected by various factors, such as rounding errors or post-processing of a stego image or watermarked one. Various post-processing operations such as JPEG compression, cropping, rotation, etc. are called attacks in the context of watermarking. Some authors use robustness benchmarks, such as StirMark (Petitcolas et al. 1998; Petitcolas 2000) or Checkmark (Pereira et al. 2001). StirMark 4.0 is the most well-known tool to benchmark watermarking algorithms. It simulates many common attacks to image watermarking algorithms. Typical tests (Petitcolas and Fatès 2004) are:

- Signal processing tests which typically apply transformation to the image but to not change its size (no resampling required);
- Geometric transformations which require the use of resampling algorithm as they change the size of the picture;
- Special transforms which basically include any other test not falling in the previous categories.

Checkmark is another solution to test the robustness and it includes attacks which take into account powerful prior information about the watermark and the watermarking algorithms.

An embedding algorithm is robust if it demonstrates the resistance to some number of attacks. Most authors use Bit Error Rate (BER), Bit Correct Rate (BCR), Normalized Correlation (NC), and Normalized Cross-Correlation (NCC) metrics to assess robustness. BER shows the ratio of a number of incorrectly extracted bits to a total size of the embedded data. BER can range from 0 to 1, where 0 means no extraction errors. This metric is calculated by the formula:

$$BER = \frac{B_e}{B}, \tag{7}$$

where B_e is a number of error bits. The BCR metric shows the ratio of correctly extracted bits to the total size of embedded data and is expressed by the following formula:

$$BCR = \frac{B_c}{B} = 1 - BER, \tag{8}$$

where B_c is a number of correct bits.

Digital images are often used as embedded information. For example, many watermarking schemes use a logo as a watermark. NC and NCC metric show the correlation between the original image (secret message or watermark) and the extracted image. They can range from 0 to 1, where 1 means two images match exactly. NC is calculated using the formula:

$$NC = \frac{\sum_{x=1}^{m} \sum_{y=1}^{n} \left(W(x,y) \times W'(x,y)\right)}{\sum_{x=1}^{m} \sum_{y=1}^{n} \left(W(x,y)^2\right)}, \tag{9}$$

where W is an original image (secret message or watermark), and W' is an extracted image. NCC is calculated using the formula:

$$NCC = \frac{\sum_{x=1}^{m} \sum_{y=1}^{n} \left(W(x,y) \times W'(x,y)\right)}{\sqrt{\sum_{x=1}^{m} \sum_{y=1}^{n} \left(W(x,y)^2\right)}\sqrt{\sum_{x=1}^{m} \sum_{y=1}^{n} \left(W'(x,y)^2\right)}}. \tag{10}$$

In some studies, the authors use the Correlation Coefficient (CC):

$$CC = \frac{\sum_{x=1}^{m} \sum_{y=1}^{n} \left(W(x,y) - \overline{W}\right) \times \left(W'(x,y) - \overline{W'}\right)}{\sqrt{\sum_{x=1}^{m} \sum_{y=1}^{n} \left(\left(W(x,y) - \overline{W}\right)^2\right)}\sqrt{\sum_{x=1}^{m} \sum_{y=1}^{n} \left(\left(W'(x,y) - \overline{W'}\right)^2\right)}}, \tag{11}$$

where $\overline{W}$ and $\overline{W'}$ are the mean of values in W and W', respectively.

2.2 Metaheuristic optimization

2.2.1 The general scheme of metaheuristic optimization

Optimization chooses the best solution from a set of options under certain constraints. However, in some problems solution space of the problem is infinite or it is too large for assessment of all the solutions (Akyol and Alatas 2017). Metaheuristic optimization is a class of optimization algorithms that finds solutions to such problems in a reasonable time using a directed search mechanism. Metaheuristic algorithms or metaheuristics are not guaranteed to find an optimal solution, but choosing a solution that is close to optimal is a good compromise between optimization quality and computational complexity in many problems.

The general scheme of metaheuristic optimization is illustrated in Fig. 4. The optimization process can be divided into an initial phase and a solution search phase. At the initial phase, an initial set of solutions, called the population, is formed. The initial population is usually generated randomly. The number of individuals in the population and its

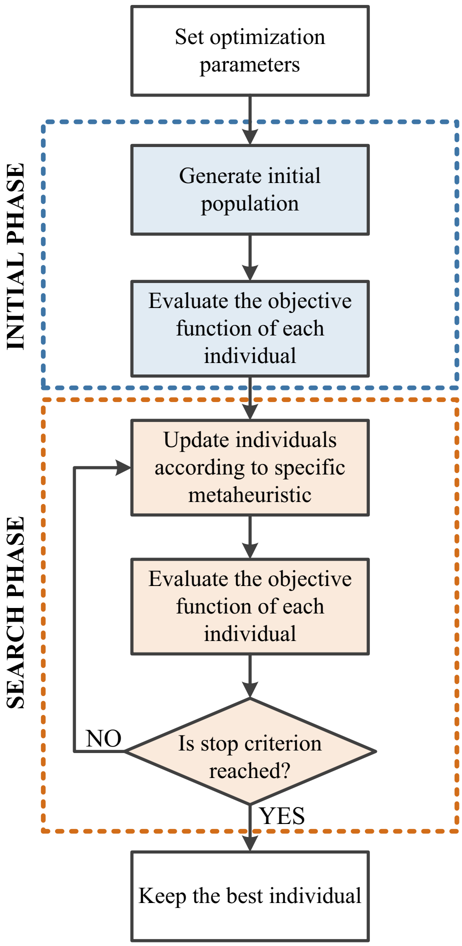


Fig. 4 The general scheme of metaheuristic optimization

dimension is determined by the optimization parameters and depends on each specific task. For each individual of the population, the calculation of the objective function, also called the fitness function, is performed. Next, the search for the optimization problem solution is performed. This is an iterative process that repeats until a certain stopping condition is reached. Such a condition can be the achievement of a certain number of generations or objective function estimates, as well as the achievement of a certain value of the objective function. The optimization process changes the individuals of a population according to the rules of a specific metaheuristic algorithm in order to get closer to the best solution. There are exploration and exploitation phases of the search. Exploration expands the scope of the search to explore new areas while exploitation focuses on discovered promising areas (Hussain et al. 2019). The objective function is estimated for the modified individuals of the population at each generation, and usually individuals with better objective function values form a new generation of solutions. Finally, the individual of the population corresponding to the best value of the objective function becomes the solution of the optimization problem.

It is worth noting that single-objective optimization problems are solved in most data hiding schemes based on metaheuristics. The target of single-objective optimization is to find the best solution that corresponds to either minimum or maximum value of a single objective function (Halim et al. 2021). However, metaheuristic optimization can also be used to solve multi-objective optimization problems.

2.2.2 Brief overview of metaheuristics

There are many different metaheuristics (Fan et al. 2020; Azad et al. 2020; Stegherr et al. 2022). In this subsection, we provide a brief overview of the metaheuristics that authors of data hiding scheme use to solve various optimization problems. Their classification is shown in Fig. 5.

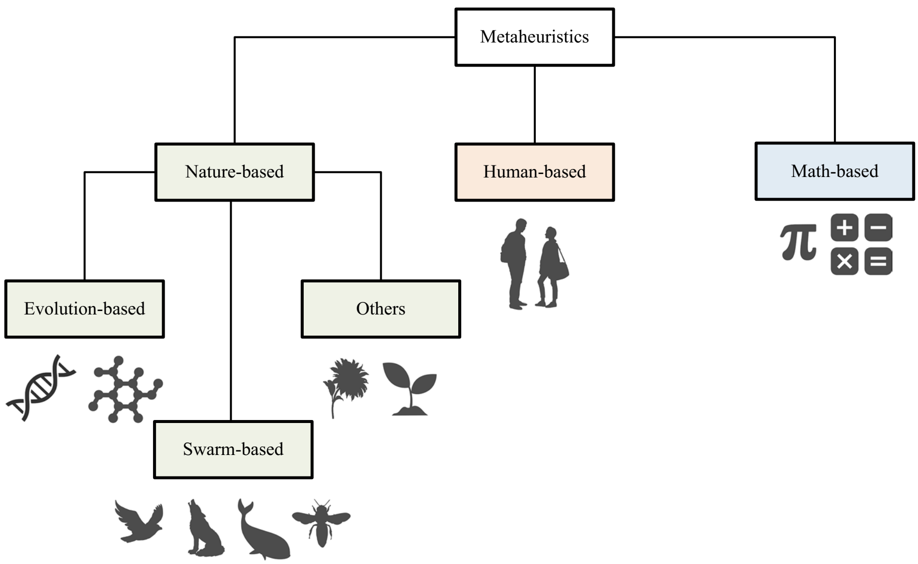


Fig. 5 Classification of metaheuristics

Most metaheuristics are inspired by various natural phenomena. For example, in data hiding schemes, Genetic Algorithm (GA) (Deb 2000) and Differential Evolution (DE) (Storn and Price 1997) are often used, which are inspired by evolutionary processes and natural selection. Principles similar to GA are used in Genetic Programming (GP) (Koza 1994), which finds a computer program of unspecified size and shape to solve or approximately solve a problem.

Swarm-based algorithms are inspired by the group behavior (swarm intelligence) of individuals in nature. This class of algorithms is most common for solving various data hiding problems. The most commonly used algorithm is Particle Swarm Optimization (PSO) (Trelea 2003), which is inspired by the behavior of flocks of birds in nature. Competitive Swarm Optimizer (CSO) (Cheng and Jin 2015) is similar to PSO but uses a pairwise competition mechanism during optimization. Artificial Bee Colony (ABC) (Karaboga and Basturk 2007) is based on the intelligent behavior of honey bee swarm. Firefly Algorithm (FA) (Yang 2010) is inspired by the flashing lights of fireflies in nature. Ant Colony Optimization (ACO) (Dorigo et al. 2006) takes inspiration from the foraging behavior of some ant species. The main inspiration of Harris Hawks Optimization (HHO) (Heidari et al. 2019) is the cooperative behavior and chasing style of Harris' hawks in nature called surprise pounce. Grey Wolf Optimizer (GWO) (Mirjalili et al. 2014) algorithm mimics the leadership hierarchy and hunting mechanism of grey wolves in nature. Whale Optimization Algorithm (WOA) (Mirjalili and Lewis 2016) mimics the social behavior of humpback whales. Fruit fly Optimization Algorithm (FOA) (Pan 2012) is based on the food finding behavior of the fruit fly. Cuckoo Search (CS) (Gandomi et al. 2013) is based on the obligate brood parasitic behavior of some cuckoo species. Bat Algorithm (BA) (Yang and Gandomi 2012) is based on the echolocation behavior of bats. Artificial Immune System (AIS) (Alonso et al. 2015) is based on the manner in which immune systems respond to perceived threats to the system. Monarch Butterfly Optimization (MBO) (Wang et al. 2018a) simulates the migration behavior of monarch butterflies in nature. Elephant Herding Optimization (EHO) (Wang et al. 2016) algorithm is inspired by the social skills and structural independence of the elephants in herds. The main inspiration of Salp Swarm Algorithm (SSA) (Mirjalili et al. 2017) is the swarming behavior of salps when navigating and foraging in oceans. Bacterial Foraging Optimization Algorithm (BFOA) (Das et al. 2009) is inspired by the social foraging behavior of Escherichia coli. Dragonfly Algorithm (DA) (Mirjalili 2016a) is inspired by the static and dynamic swarming behaviors of dragonflies in nature. Grasshopper Optimisation Algorithm (GOA) (Saremi et al. 2017) mimics the behavior of grasshopper swarms in nature. Slime Mould Algorithm (SMA) (Li et al. 2020) is aroused by the diffusion and foraging conduct of slime mould. Dipper Throated Optimization (DTO) (Takieldeen et al. 2022) algorithm is inspired by the dipper throated bird. Manta Ray Foraging Optimization (MRFO) (Zhao et al. 2020) is based on intelligent behaviors of manta rays. Shark Smell Optimization (SSO) (Abedinia et al. 2016) is based on the ability of shark, as a superior hunter in the nature, for finding prey. Antlion Optimization (ALO) (Mirjalili 2015) mimics the hunting mechanism of antlions in nature. Beetle Swarm Optimisation (BSO) (Chen et al. 2018) is based the foraging principle of the beetle.

Some nature-inspired algorithms are based on natural phenomena that cannot be attributed to imitation of the evolutionary process or examples of swarm intelligence. For example, Invasive Weed Optimization (IWO) (Mehrabian and Lucas 2006) mimic robustness, adaptation and randomness of colonizing weeds. The inspiration for the Sunflower Optimization Algorithm (SFO) (Gomes et al. 2019) comes from sunflowers' motion to capture solar radiation.

Some metaheuristics are inspired by the behavior of individuals and social groups. For example, Seeker Optimization Algorithm (SOA) (Dai et al. 2009) is based on the concept of simulating the act of human searching. Imperialist Competitive Algorithm (ICA) (Lin et al. 2012) is inspired by human's socio-political evolution. Cohort Intelligence (CI) (Kulkarni et al. 2016) is inspired by the candidates' self supervised learning behavior in a cohort. Teaching–Learning-Based Optimization (TLBO) (Rao et al. 2011) is inspired by teaching–learning process. Social Group Optimization (SGO) (Satapathy and Naik 2016) is inspired from the concept of social behavior of human toward solving a complex problem.

Some of the metaheuristic optimization algorithms do not have any prototype in the real world and are based on some mathematical concepts. For example, Bayesian Optimization Algorithm (BOA) (Pelikan et al. 2002) is based on constructing, learning, and sampling of Bayesian probabilistic networks. The Jaya (Venkata Rao 2016) algorithm is based on the general idea of heuristic search and is distinguished by the absence of configurable parameters. Sine Cosine Algorithm (SCA) (Mirjalili 2016b) is based on sine and cosine mathematical functions. Archimedes Optimization Algorithm (AOA) (Hashim et al. 2021) is devised with inspirations from Archimedes' Principle. Stochastic Fractal Search (SFS) (Salimi 2015) uses a mathematic concept called the fractal.

3 Overview of data hiding schemes based on metaheuristic optimization

3.1 Classification

In this paper, we present an overview of data hiding schemes based on metaheuristic optimization over the past 6 years. We considered 147 studies published from 2017 to 2022. We included "Article" type publications from peer-reviewed scientific journals such as "Multimedia Tools and Applications", "IEEE Access", "Future Generation Computer Systems", "Optik", "Expert Systems with Applications", and others. The research includes publications from Springer (69 studies), Elsevier (31 studies), IEEE (14 studies), MDPI (8 studies), Taylor & Francis (3 studies), and other publishers. The distribution of publications by year is as follows: 2017—12 studies; 2018—19 studies; 2019—18 studies; 2020—24 studies; 2021—31 studies; 2022—43 studies.

We propose the following classification of the considered studies (Fig. 6):

(1) The first level of classification is related to the purpose of information embedding. We separately analyze steganography methods and digital watermarking methods.
(2) The second level of classification is related to the purpose of applying metaheuristic optimization. Our research shows that optimization goals depend significantly on the embedding goal. In the case of steganography, the authors use metaheuristics to find the optimal arrangement of information bits in the cover image. In the field of image watermarking, the most common problem is choosing the optimal scaling factor. We also separately consider studies whose authors solve other problems using metaheuristics.
(3) The third level of classification is the level of metaheuristics. We group the considered studies according to the frequency of using metaheuristics within the first and second level classification.

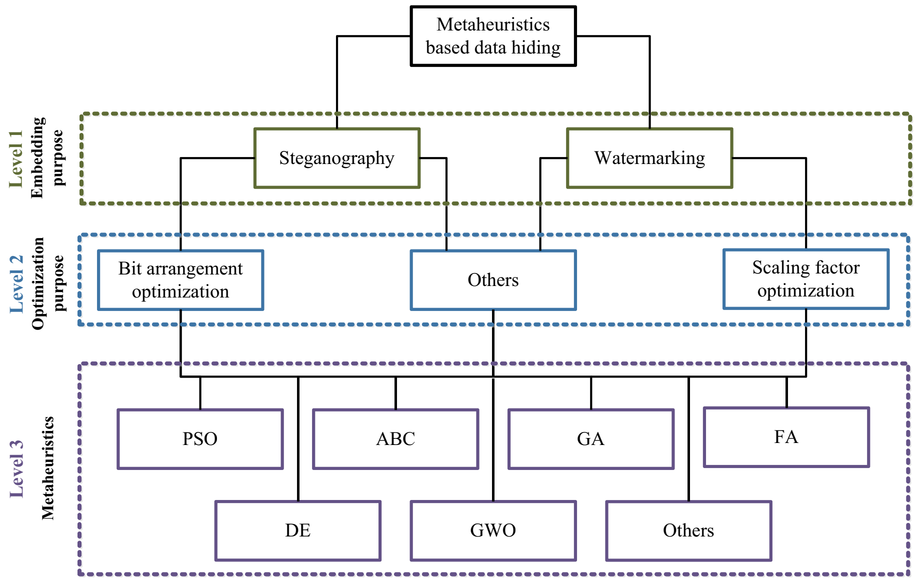


Fig. 6 Classification of reviewed studies

We note the embedding domain, features of data hiding schemes, and embedding performance indicators in research analysis. We also indicate the objective function if it is described in the relevant study.

3.2 Image steganography schemes based on metaheuristics

In this subsection, we discuss the use of metaheuristic optimization to improve the efficiency of steganographic embedding of information into digital images.

3.2.1 Bit arrangement optimization

The efficiency of steganography schemes significantly depends on the message bit location in the image pixels or in the frequency coefficients. Embedding additional data in some elements can lead to more noticeable distortion of the stego image than in others. Metaheuristic optimization is a good solution to the problem of finding the best arrangement of message bits within a cover image.

An illustration of this process is shown in Fig. 7. It shows a schematic representation of an image pixel block. White "pixels" are not used for embedding information, while blue "pixels" contain embedded data. A different arrangement of message bits in the pixel block leads to a different quality of embedding. Note that in this example, the PSNR values are chosen arbitrarily, they are not related to any particular image and embedding algorithm, but only illustrate a possible relationship between the location of the message bits in the image block and the invisibility of the embedding. As the figure shows, optimization allows us to find a better location for the message and significantly improve the embedding efficiency.

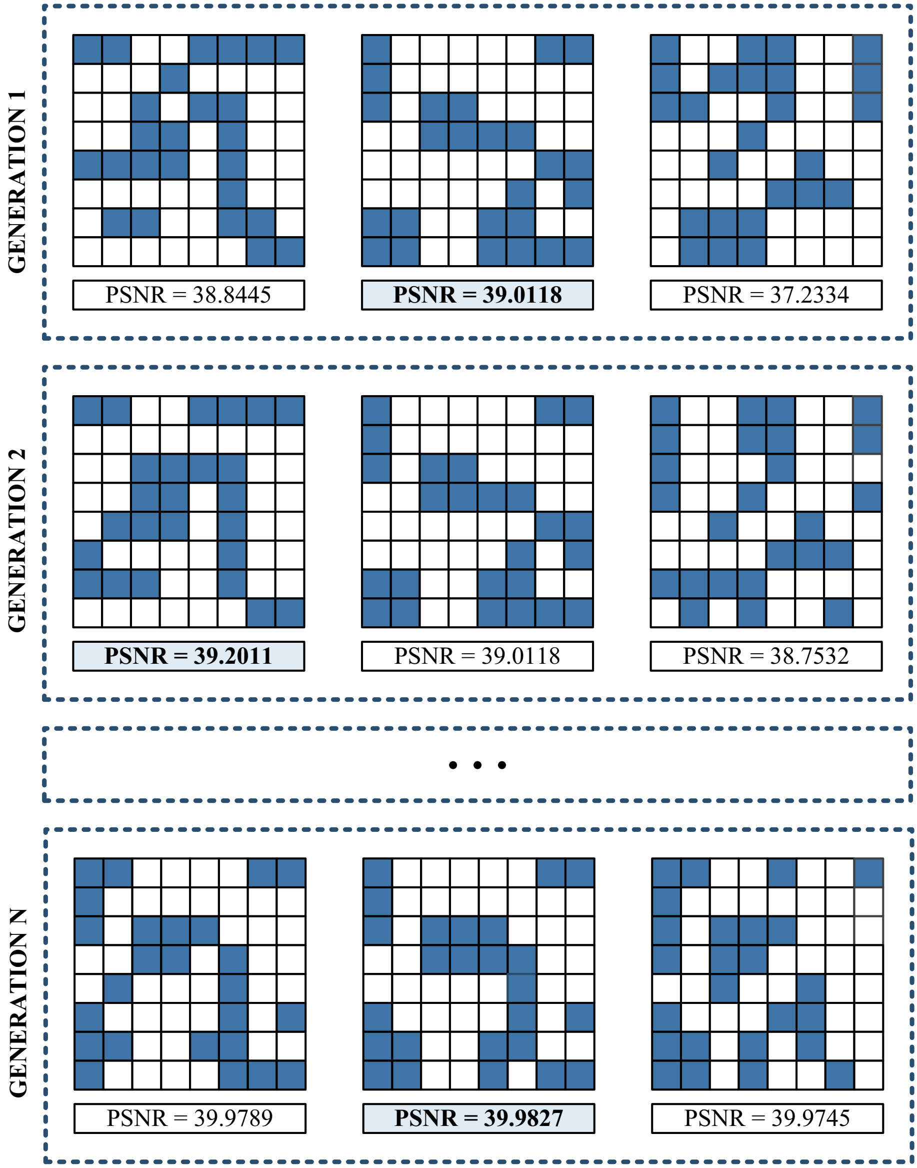


Fig. 7 Finding the best arrangement of message bits within a cover image block

The PSO algorithm is the most popular among steganography schemes that use metaheuristics to optimize the position of message bits in the elements of a cover image. The authors of various studies prefer PSO due to its fast convergence and high efficiency, despite the problem of choosing optimization parameters. Data hiding schemes in the spatial domain of images usually combine metaheuristics with classic LSB embedding. In this case, the optimization is aimed at selecting suitable pixels or blocks of pixels for embedding. For example, Shukur and Jabbar (2018) embed secret message bits into optimal image elements using LSB substitution. They use PSO to achieve high embedding imperceptibility. Mohsin et al. (2019) use PSO to provide high-capacity embedding in the spatial domain of images. In particular, metaheuristics are used to find the best embedding starting point and pixel scan direction. In another study, Mohsin et al. (2021) propose to use LSB steganography in a blockchain-based system for exchanging medical data between hospitals. PSO is used to find the best bit locations for hiding secret data in host images. The optimization goal is to achieve the maximum PSNR value. Jaradat et al. (2021) use chaotic PSO. The optimization goal is also to maximize the PSNR metric value. Li and He (2018) use PSO to improve the quality of PVD-embedding. Optimization algorithm selects the ideal pixel gray values among numerous modulus function solutions. The authors propose to use two different objective functions. One of them ensures the successful embedding and extraction of the secret information and is calculated using the following formula:

$$Minimize\, f = \left|\left(g_1' + g_0'\right) \mod 2^{t_1} - b_1\right| + \left|\left(g_2' + g_0'\right) \mod 2^{t_2} - b_2\right| + \left|\left(g_3' + g_0'\right) \mod 2^{t_3} - b_3\right|, \tag{12}$$

where g_0', g_1', g_2', g_3' are pixel values of a stego image, t_i is a number of embedded secret bits, and b_i is a decimal value of t_i. The other objective function chooses the best solution among the solutions found by the first objective function. PSNR is used as the second objective function.

Most of the studies belongs to the frequency embedding. In this case, the optimization process searches for the most suitable frequency coefficients or their blocks for embedding. For example, a scheme for embedding a secret message into the DWT domain is proposed by Sharma and Batra (2021). The pre-processing stage uses Huffman encoding to compress data and improve security. Metaheuristic optimization is used to find the best positions to embed information. Nipanikar et al. (2018) use PSO to hide the speech signal in the DWT domain of digital images. Speech signal is first converted to sparse representation and then to binary form. PSO finds suitable embedding positions. The authors use the cost function to evaluate the fitness of each pixel position. The proposed cost function depends on the intensity, entropy, and edge of the individual seed points of the chromosomes. Muhuri et al. (2020) present a steganography method that hides information in IWT coefficients. The authors apply PSO to find the optimal substitution matrix for converting secret data into their substituted forms. The PSNR metric is used as the objective function. The proposed scheme embeds information in the *k* LSBs of the IWT coefficients. An optimal pixel adjustment procedure minimizes the variations in the modified coefficient values from the original values. Wang and Li (2022) propose an image steganography algorithm for underwater acoustic communication based on IWT and PSO. The secret information is generated using the interleaved packing method and then embedded in the transform coefficients whose positions are found using PSO. The objective function is defined as the number of bits of the secret data that match the lowest significant bits of the high frequency coefficients. Jeevitha and Amutha Prabha (2020) propose a solution for the medical data protection based on steganography. Canny edge detection method implemented to detect the smooth edges to hide the secret data. The embedding domain is Hidden Markov Tree (HMT) Contourlet Transform (CT) domain.

GA optimization is also quite widespread in the considered class of image steganography schemes. An example of a spatial domain embedding scheme can be found in (Wazirali et al. 2019). This scheme is based on LSB substitution. GA is used to find the best sequence of operations in the process of executing a steganographic algorithm, such as pixel scanning, pixel shifting flipping secret bits, and others. This scheme provides the optimal arrangement of the secret message bits in the cover image. The PSNR metric is used as an objective function. Wang et al. (2017) propose a reversible data hiding scheme in the spatial domain based on the HS technique. GA is employed to search the nearly optimal zero and peak bins. The fitness function is the difference between the possible maximal distortion for the given HS-based multiple embedding in one generation and the current distortion. Zhang et al. (2022) also propose a reversible scheme based on the HS technique. K-means clustering is used for contrast enhancement was employed to generate seven sharply-distributed clusters. GA is used to adaptively search for the optimal embedding points for each clustering. The objective function matches the embedding distortion of each chromosome. Vazquez et al. (2022) proposes a data hiding scheme that does not involve direct embedding and uses one-to-one correspondence between the bits that make up the secret image and the host pixels. The extraction step requires a seed value for the initial population of the GA search. The objective function shows the number of bits for which a one-to-one correspondence is established between the secret image and the cover image.

A number of studies are devoted to frequency domain embedding using GA optimization. Biswas and Bandyapadhay (2020) use GA when embedding information into the DCT domain of digital images using the LSB method. GA optimization increases the robustness of the algorithm and allows it to withstand any rigorous testing and brutal attack. The insertion position value is used as the fitness function. Sabeti and Aghabagheri (2022) propose an embedding scheme for JPEG images based on variant embedding rate for all non-zero DCT coefficients. GA finds the best embedding locations and maximizes PSNR during optimization. Almawgani et al. (2022) embed information into the DWT domain. GA is used to find the optimal mapping function for each block in the image. PSNR is used as a fitness function. The secret message is encoded and compressed using the Lempel–Ziv–Welch (LZW) algorithm to increase the embedding capacity. The embedding is done using the LSB method and the optimal pixel adjustment process reduces the embedding error between the cover image and the stego image. Sabeti et al. (2022) use the edge intensity criterion to select appropriate DWT or IWT coefficients for embedding and obtain the highest PSNR value. Uma Maheswari and Jude Hemanth (2017) choose Fresnelet Transform (FT) or CT to create a hiding space. They explain this choice by the ability of these transformations to provide higher capacity and security. Metaheuristics are used to find the best coefficients for embedding. In particular, the authors evaluate the performance of GA and PSO. The PSNR metric is an objective function. Jude Hemanth et al. (2018) apply a modified version of GA to find the optimal frequency coefficients of FT or Discrete Ripplet Transform (DRT) for data hiding. Hossain et al. (2022) use the Ballot Transform (BaT) to transform non-overlapping groups of pixels into an integer polynomial sequence in coefficient form. The motivation for choosing BaT to form the hiding space is to increase the speed of the embedding algorithm. GA is used to find the embedding positions of the secret message bits in the coefficients obtained after the transformation. The optimization aims to maximize the PSNR value.

Some researchers use FA optimization. For example, a matrix XOR encoding steganography technique is proposed by Khari et al. (2020). Adaptive FA is used to optimize the selection of cover blocks within the image. A reversible steganography algorithm based on Fractional Fourier Transform (FrFT) is presented by Amsaveni and Bharathi (2021). The authors solve the problem of finding the best positions for HS technique embedding using FA. The objective function is as follows:

$$Minimize\, f = \lambda \times \left(1 - SSIM(I, I')\right) + (1 - \lambda) \times BER, \tag{13}$$

where λ is the weighting constant.

There are examples of the application of another swarm-based metaheuristics. Khan (2018) uses ACO to detect complex region of cover image to embed information in the spatial domain using the LSB method. The study compare 4 versions of the algorithm using different function: Flat, Gaussian, Sine and Wave function. In another study, Khan et al. (2020) propose a double asymmetric data hiding technique based on ACO. Sharma et al. (2022a) use the Huffman encoding algorithm to convert the secret information into a bitstream, which is further embedded in the frequency domain of images. A hybrid metaheuristic optimization scheme combining FA and ACO is applied to select the best embedding positions.

Walia et al. (2018) improve the performance of LSB steganography by using CS optimization and maximizing the PSNR value. As a result, an optimal stego key is obtained, which determines the order of permutation within the cover image, the scanning direction, and bit replacement parameters. Gurunathan and Rajagopalan (2020) propose an algorithm combining steganographic embedding and JPEG compression. The CS algorithm is used for searching an optimal substitution matrix for LSB embedding in the domain of quantized DCT coefficients. The standard PSNR metric is also used as the objective function.

Sarmah and Kulkarni (2018) propose a steganography scheme for compressed JPEG images based on human-based metaheuristic. The scheme hides the secret message bits in the quantized DCT coefficients. The CI optimization algorithm is used to identify the optimal substitution matrix. The PSNR metric is used as the objective function. In another study, Sarmah and Kulkarni (2019) propose an improved CI to reduce the computational complexity of the optimization process.

Weng et al. (2022) propose a reversible data hiding scheme for JPEG images with multiple two-dimensional histograms. Metaheuristic optimization is used to find the optimal complexity threshold and two-dimensional histogram mapping for each selected two-dimensional histogram. The authors combine PSO and DE to reduce the computational complexity of the algorithm. Wang et al. (2022) propose an algorithm that not only hides data in digital images, but also turn ordinary samples into adversarial samples. Information embedding is performed using the LSB method. The boundary position DE metaheuristic algorithm proposed by the authors is used to select the effective embedding region with adversarial effect. The authors note that the optimization algorithm is distinguished by its simplicity and efficiency, combined with fast convergence.

Other metaheuristics are less popular for this class of steganography algorithms. For example, Banharnsakun (2018) uses ABC to optimize the block assignment for a secret image embedding. The evaluation of the objective function consists in calculating the MSE metric. The study demonstrates that the algorithm resists some noise attacks better than similar steganography schemes. Ding et al. (2020) propose an image steganography scheme based on evolutionary multi-objective optimization for implementation in the Internet of Things (IoT) using mobile edge computing. This scheme uses AIS-based optimization and the Pareto optimal method to search perturbation locations on the cover image. A high-pass filters bank is used to preprocess the cover image to form the candidate locations of the perturbation. The fitness function is

$$Maximize\, f = \frac{1}{1 - SSIM + KL}, \tag{14}$$

where KL is a KL divergence. Hassaballah et al. (2021) propose to use the HHO algorithm to improve the efficiency of LSB embedding for industrial IoT applications. The HHO algorithm is used to select the most appropriate image pixels that can be used to hide the secret data bits in the IWT coefficients. The proposed method converts secret data into an encoded form based on optimal encoding vectors created by the HHO algorithm. The optimal pixel adjustment process is used to improve the visual quality of stego images. Hameed et al. (2022) also combine LSB and HHO. The optimization is aimed at finding the encoding vector to convert the secret message to its encoded form. The encoded form corresponds to the best position of the message in the cover image. The HHO based data encoding operation uses the PSNR metric as an objective function. Molaei and Ebrahimzadeh (2019) use BOA to find the optimal mapping vector for optimum embedding of information into the low-order bits of the host image using modulus function. The authors use a composite objective function consisting of the sum of squared errors and the average SSIM value between images before and after embedding. Ambika et al. (2019) propose to increase the security of steganography in the DWT domain by separately encrypting each bit plane of the secret image. 'R' component is encrypted by Blowfish algorithm; 'G' component is encrypted using advanced encryption standard, and 'B' component is encrypted using signcryption algorithm. Multiobjective WOA is used to select the elements of the cover image that are most suitable for hiding information. The objective function maximizes the PSNR value. In another study, Ambika and Biradar (2020) propose a scheme combining EHO and MBO to protect the confidentiality of information transmitted over communication channels. Metaheuristic optimization solves the problem of choosing suitable image elements for embedding. The fitness function depends on the cost function, which calculates the edge, entropy, and intensity of the pixel. Ambika et al. (2022) use GWO to find the best pixel positions of the cover image when embedding a secret image into an IWT domain. The secret image is encrypted using the signcryption algorithm before embedding. Roselin Kiruba and Sree Sharmila (2021) use a hybrid of FOA and SOA called the fruit fly optimization hybridized improved seeker algorithm to find optimal locations for hiding data in the spatial domain. The embedding scheme hides the secret message in the LSBs of the respective quantized DCT coefficients. Ben Ali (2019) proposes a novel nature-inspired Smell Bees Optimization Algorithm (SBOA) that strongly mimics the behavior of the honey bees olfactory perception, as well as a scheme for embedding information into the spatial domain of images based on a new metaheuristic. The objective function is the MSE between the cover image and the stego image. Eshmawi et al. (2022) use CSO for better message localization. The optimization aims to maximize the PSNR value.

A summary of each of the reviewed studies, including key performance indicator values, are presented in Table 1. In the "Performance indicators" column, we show the values of the main quality metrics and brief information about robustness and resistance to steganalysis. We use data that have been experimentally evaluated by the authors of relevant studies. Note that robust schemes can provide resistance to a large number of attacks, so in this study we use three levels of robustness or the name of the benchmark (if available) to avoid excessive increase in the size of the paper. A low level of robustness corresponds to resistance to no more than 5 types of attacks, a medium robustness level includes from 6 to 10 types of attacks, and a high robustness level includes 11 or more types of attacks. We do not separately consider attacks that belong to the same type, but have different parameters, for example, JPEG compression with different quality factors. We also provide NC, NCC, CC, BER, and BCR values under attacks. We indicate the capacity calculated by formula (6) for comparison of different studies. If the authors of the relevant study provide only the

Table 1 Steganographic schemes with optimized message bit arrangement

Reference	Embedding domain	Metaheuristic	Performance indicators
Shukur and Jabbar (2018)	Spatial	PSO	EC: 0.0305 bpp (CLR) PSNR: 42.93–44.87 dB
Mohsin et al. (2019)	Spatial	PSO	EC: 0.5–4.5 bpp (GS) PSNR: 53.3743–59.1227 dB Steganalysis: histogram analysis, RS steganalysis
Mohsin et al. (2021)	Spatial	PSO	–
Jaradat et al. (2021)	Spatial	Chaotic PSO	EC: 0.5–3.125 bpp (GS) PSNR: 56.15–69.20 dB SSIM: 0.9973–0.9998 Steganalysis: histogram analysis
Li and He (2018)	Spatial	PSO	EC: 2.1104–2.6388 bpp (GS) PSNR: 36.63–43.69 dB Steganalysis: RS steganalysis
Sharma and Batra (2021)	DWT	PSO	EC: 0.1953–0.7813 bpp (CLR) PSNR: 78.12–81.95 dB SSIM: 0.981–0.999 BER: 0.042–0.054 Steganalysis: histogram analysis
Nipanikar et al. (2018)	DWT	PSO	PSNR: 47.6 dB
Muhuri et al. (2020)	IWT	PSO	EC: 2 bpp (GS) PSNR: 41.13–41.97 dB SSIM: ≈ 0.997 Steganalysis: RS steganalysis, chi–square test, KL divergence
Wang and Li (2022)	IWT	PSO	EC: 0.25–0.75 bpp (GS) PSNR: 50.56–65.01 dB SSIM: 0.9998–0.9999 Steganalysis: RS steganalysis
Jeevitha and Amutha Prabha (2020)	HMT-CT	PSO	EC: 0.0673–0.1050 bpp (GS) PSNR: 43.460–49.536 dB Robustness: medium CC: 0.8930–0.9958

Table 1 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Wazirali et al. (2019)	Spatial	GA	EC: 0.125–2.7466 bpp PSNR: 51.36–66.36 dB Steganalysis: histogram analysis
Wang et al. (2017)	Spatial	GA	EC: 0.1–0.6 bpp (GS) PSNR: ≈ 32–64 dB
Zhang et al. (2022)	Spatial	GA	PSNR: 23.60–45.85 dB
Vazquez et al. (2022)	Spatial	GA	PSNR: ∞ SSIM: 1
Biswas and Bandyapadhay (2020)	DCT	GA	EC: 2.00 bpp (CLR) PSNR: 38.27 dB Robustness: StirMark 4.0 Steganalysis: sample pair analysis, dual statistical method, KL divergence
Sabeti and Aghabagheri (2022)	DCT	GA	EC: 0.0011–0.0763 bpp (GS) PSNR: 40–65 dB SSIM: ≈ 0.985–1.0 Steganalysis: feature-based steganalysis
Almawgani et. al. (2022)	DWT	GA	EC: 4 bpp (GS) PSNR: 44.98–52.83 dB Steganalysis: histogram analysis
Sabeti et al. (2022)	DWT, IWT	GA	EC: 0.25–0.5722 bpp (GS) PSNR: 51.37–56.19 dB SSIM: 0.9968–0.9996 Steganalysis: RS steganalysis, histogram analysis, feature-based steganalysis
Uma Maheswari and Jude Hemanth (2017)	FT, CT	GA, PSO	EC: 2.3897–13.7655 bpp (GS) PSNR: 45.95– 52.91 dB Steganalysis: chi–square test
Jude Hemanth et al. (2018)	FT, DRT	GA	EC: 8.2308–8.5107 bpp (GS) PSNR: 50.14–50.57 dB SSIM: 0.99

Table 1 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Hossain et al. (2022)	BaT	GA	EC: 1–4 bpp (GS) PSNR: 32.18–49.458 dB SSIM: 0.694–0.99 Steganalysis: histogram analysis, RS analysis, sample pair analysis, chi-square test, feature-based steganalysis, primary sets
Khari et al. (2020)	Spatial	Adaptive FA	PSNR: ≈ 70 dB
Amsaveni and Bharathi (2021)	FrFT	FA	EC: 0.125–1.0 bpp (GS) PSNR: 40.12–53.40 dB SSIM: 0.9788–0.9988 Robustness: medium BER: 0.0009–0.0021
Khan (2018)	Spatial	ACO	EC: 0.36–0.44 bpp (GS) PSNR: > 45 dB
Khan et al. (2020)	Spatial	ACO	EC: 2.1455–6.2538 bpp (GS) PSNR: 53.3739–61.4498 dB SSIM: 0.9997– 0.9999
Sharma et al. (2022a)	DWT	FA and ACO	PSNR: 68.06 dB SSIM: 0.994 Steganalysis: histogram analysis
Walia et al. (2018)	Spatial	CS	EC: 0.3966–3.6113 bpp (GS) PSNR: 33.66–55.31 dB SSIM: 0.90–1.0
Gurunathan and Rajagopalan (2020)	DCT	CS	EC: 1.125 bpp (GS) PSNR: 33.48–37.92 dB
Sarmah and Kulkarni (2018)	DCT	CI	EC: 1.125 bpp (GS) PSNR: 29.935–42.4212 dB
Sarmah and Kulkarni (2019)	DCT	Improved CI	EC: 1.125 bpp (GS) PSNR: 29.9355– 42.4019 dB

Table 1 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Weng et al. (2022)	DCT	PSO and DE	EC: 0.0229–0.0610 bpp (GS) PSNR: ≈ 35–53 dB
Wang et al. (2022)	Spatial	Boundary position DE	PSNR: 41 dB SSIM: 0.9562
Banharnsakun (2018)	Spatial	ABC	EC: 0.5 bpp (GS) PSNR: 56.3605– 56.4024 dB Robustness: low BER: 0.072–0.0075
Ding et al. (2020)	Spatial	AIS	PSNR: 82.7501 dB SSIM: 1.0 Steganalysis: sample pair analysis
Hassaballah et al. (2021)	IWT	HHO	EC: 3 bpp (GS) PSNR: 36.92–37.81 dB Robustness: medium NCC: 0.9514–1.0 Steganalysis: histogram analysis, RS steganalysis
Hameed et al. (2022)	Spatial	HHO	EC: 6–12 bpp (CLR) PSNR: 35.1188–45.3950 dB SSIM: 0.9054–0.9960 Steganalysis: histogram analysis, RS analysis, sample pairs, chi-square test, feature-based steganalysis Robustness: medium NCC: 0.9514–1.000
Molaei and Ebrahimzadeh (2019)	Spatial	BOA	EC: 1–2 bpp (GS) PSNR: 46.40–51.18 dB SSIM: 0.9939–0.9994
Ambika et al. (2019)	DWT	WOA	PSNR: 57.6226–66.3084 dB
Ambika and Biradar (2020)	DWT	EH and MBO	PSNR: 34.9369–38.0144 dB
Ambika et al. (2022)	IWT	GWO	PSNR: 48.59–54.93 dB

Table 1 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Roselin Kiruba and Sree Sharmila (2021)	DCT	FOA and SOA	EC: 0.625–2.5 bpp (GS) PSNR: 58.0563–64.4216 dB SSIM: 0.9707–0.998
Ben Ali (2019)	Spatial	SBOA	EC: 0.5–1 bpp (GS) PSNR: 53.74–57.74 dB Robustness: low CC: 0.8835–0.9868 Steganalysis: feature–based steganalysis
Eshmawi et al. (2022)	IWT	CSO	PSNR: 54.5135–56.6695 dB SSIM: 0.9980–0.9984 Robustness: low NCC: 0.9958–0.9981

cover size or only the message size, the capacity is not specified. “CLR” indicates a color cover image, and “GS” indicates a grayscale cover image.

3.2.2 Other optimization purposes

This subsection provides an overview of steganography schemes in which metaheuristic optimization is used to solve problems other than the choice of message bit placement. For example, Karakus and Avci (2020) use an improved pixel similarity-based LSB method using GA optimization to embed doctors’ comments in medical images. Parameters to be optimized by using GA in this study are navigating window size, navigating window direction, layer selection, bit planes detection, normalization coefficient, secret bit direction value, bit planes direction value, secret bit pole value, and threshold value. The PSNR metric is used as an objective function. Reshma et al. (2022) propose a steganography scheme based on the pixel prediction approach. The support vector neural network classifier is used to identify suitable pixels. The authors apply GA to set the neural network, and the optimization task is to minimize the error. The CT coefficients are used to embed information. Alsalhi (2019) presents a quantum steganography scheme based on adaptive neural networks. A modified version of PSO is involved in the neural network training process. Kasana et al. (2017) hide secret information in the LWT domain of digital images after pre-scrambling by Arnold transform. The authors apply GA to find the optimal scaling factor. The objective function is calculated by the formula:

$$Maximize\,f = PSNR(I, I') + NC(W, W'). \tag{15}$$

Pandey (2020) uses steganography in a scheme for the secure transmission of medical data. First, confidential information is encrypted using a new algorithm based on a bit mask oriented GA. The protected data is then embedded into the DWT domain of medical images. Du and Yin (2022) propose a reversible scheme for embedding data into JPEG images. Unlike most research in the field of image data hiding, in this scheme, the embedding is done directly into the bitstream. GA optimization is aimed at reducing the size of a stego file.

Some authors use metaheuristics for the rate allocation. A scheme for reversible data hiding based on multiple histograms modification is presented by Wang et al. (2020). The authors use GA for the rate allocation among multiple histograms to minimize distortions. Prabha and Jagadeeswari (2020) solve a similar optimization problem. The authors describe a scheme for reversible information embedding into images that are compressed using vector quantization and side match vector quantization. The hybrid embedding domain combines DCT and Burrows Wheeler Transform (BWT). The enhanced ICA optimization algorithm is used to signify the embedding rate of each region in a cover image by choosing a threshold value. Contrast sensitive function is used as a fitness function. Tang et al. (2022) propose an adaptive steganography technique based on edge detection and matrix coding. Edge detection is based on fuzzy logic. GA is used to optimize the number of secret bits depending on the size of the message, the number of edge regions, and the sensitivity of the human eye to changing RGB components. The optimization aims to minimize the difference between the embedding capacity and the secret message size. Mehbodniya et al. (2022) propose a reversible embedding scheme based on the difference expansion method using multilevel thresholding. The authors divide the cover image pixels into several classes using SMA and then embed the data into the pixels of each class using difference expansion. Increasing the correlation between pixels of each class is used to increase the capacity and reduce the distortion level of the stego image.

In some schemes, metaheuristics are used to form the hiding space. Pramanik et al. (2020) propose a steganography scheme for the secure transmission of a user's secret passwords. The scheme combines GA and PSO while embedding information in the coefficients of the Bi-Orthogonal Wavelet Transform (BOWT). PSO is used to get an enhanced version of the original cover image. The GA selects the best hidden image among a set of hidden images which are created after mutation. Jaya Prakash and Mahalakshmi (2022) use neural networks and AOA to create a mosaic image. The neural network is applied for style transfer of images and the AOA is used to optimize the tile fitting process. The resulting mosaic image is used for reversible data hiding based on the LSB method.

Another possible optimization problem is edge detection. Dhawan et al. (2021) propose an IoT data security solution based on image steganography. SSA is used to localize the edge and smooth blocks of cover image. Embedding information in areas with different properties is carried out with different parameters. The authors also use a hybrid fuzzy neural network to improve the quality of the stego image. The objective function is the Manhattan distance of 8-neighboring pixels from the center pixel. The maximum value of the objective function represents the higher chance of edges. In (Dhawan et al. 2022), the authors propose an embedding scheme in the IWT domain, where SSA is used for edge detection in a similar way. A deep enhanced stacked auto encoder is used to enhance the quality of the stego images.

Table 2 provides a summary of the reviewed studies.

3.3 Image watermarking schemes based on metaheuristics

In this subsection, we present an overview of research that uses metaheuristic optimization to improve the efficiency of embedding watermarks in digital images.

3.3.1 Scaling factor optimization

The efficiency of image watermarking schemes often depends on an optimal embedding parameter, called the scaling factor or embedding strength factor, which provides a balance between embedding imperceptibility and robustness. Metaheuristic optimization can find a suitable value of the scaling factor. In most studies, various attacks affect the watermark in the optimization process in order to select solutions with increased robustness.

The scheme for finding the best value of the scaling factor using metaheuristic optimization is shown in Fig. 8. As the figure shows, the minimum value of the scaling factor provides high embedding imperceptibility, but also leads to low embedding resistance to attacks. The maximum value of the scaling factor provides high robustness, but the visual quality of the image is significantly degraded. Optimization allows us to find such a value of the scaling factor that provides an acceptable level of imperceptibility and robustness at the same time. To do this, in many schemes, authors combine the imperceptibility and robustness metrics in the objective function. PSNR or SSIM metrics evaluate the similarity of the original and watermarked images, while NC, NCC, CC, BER or BCR metrics evaluate the similarity of the original watermark and the extracted watermark after applying various attacks.

We present an overview of studies in which metaheuristics are used to optimize the scaling factor or embedding strength factor. In almost all cases, the hiding space is a

Table 2 Other steganographic schemes based on metaheuristic optimization

Reference	Embedding domain	Metaheuristic	Optimization purpose	Performance indicators
Karakus and Avci (2020)	Spatial	GA	Data hiding method selection	EC: 0.0038–0.1526 character per pixel (GS) PSNR: 47.4113–66.5374 dB
Reshma et al. (2022)	CT	GA	Neural network setup	PSNR: 89.325 dB SSIM: 1.0
Alsalhi (2019)	IWT	PSO	Neural network setup	PSNR: 65.6543 dB
Kasana et al. (2017)	LWT	GA	Scaling factor selection	EC: 1.9844 bpp (GS) PSNR: 50.2078–51.1673 dB Steganalysis: histogram analysis, chi–square test
Pandey (2020)	DWT	BMOGA	Secret message encryption	PSNR: 44.23–58.24 dB SSIM: 1.0 Steganalysis: histogram analysis
Du and Yin (2022)	Bitstream	GA	Code mapping	EC: 0.0076–0.0648 bpp (GS)
Wang et al. (2020)	Spatial	GA	Rate allocation	EC: 0.05–0.7 bpp (GS) PSNR: ≈ 35–65 dB
Prabha and Jagadeeswari (2020)	DCT-BWT	Enhanced ICA	Rate allocation	EC: 0.1813–0.1963 bpp (GS) PSNR: 35.8–39.8 dB SSIM: 0.91–0.93
Tang et al. (2022)	Spatial	GA	Rate allocation	EC: 0.0770–6 bpp (CLR) PSNR: 45.7096–71.8569 dB SSIM: 0.9984–1.0 Steganalysis: RS analysis
Mehbodniya et al. (2022)	Spatial	SMA	Rate allocation	EC: 0.1–6.0 bpp (GS) PSNR: 26.00–55.18 dB
Pramanik et al. (2020)	BOWT	PSO and GA	Creating a hiding space	EC: 1.5 bpp (CLR) PSNR: 50.88–54.51 dB
Jaya Prakash and Mahalakshmi (2022)	Spatial	AOA	Creating a hiding space	EC: 0.017–0.1897 bpp (CLR)
Dhawan et al. (2021)	Spatial	SSA	Edge detection	EC: 0.7–2.3 bpp (GS) PSNR: 55.907–60.822 SSIM: 0.9969–0.9992 Steganalysis: KL divergence

Table 2 (continued)

Reference	Embedding domain	Metaheuristic	Optimization purpose	Performance indicators
Dhawan et al. (2022)	IWT	SSA	Edge detection	EC: 0.7–6.0 bpp (GS) PSNR: 45–60 dB Robustness: medium Steganalysis: KL divergence

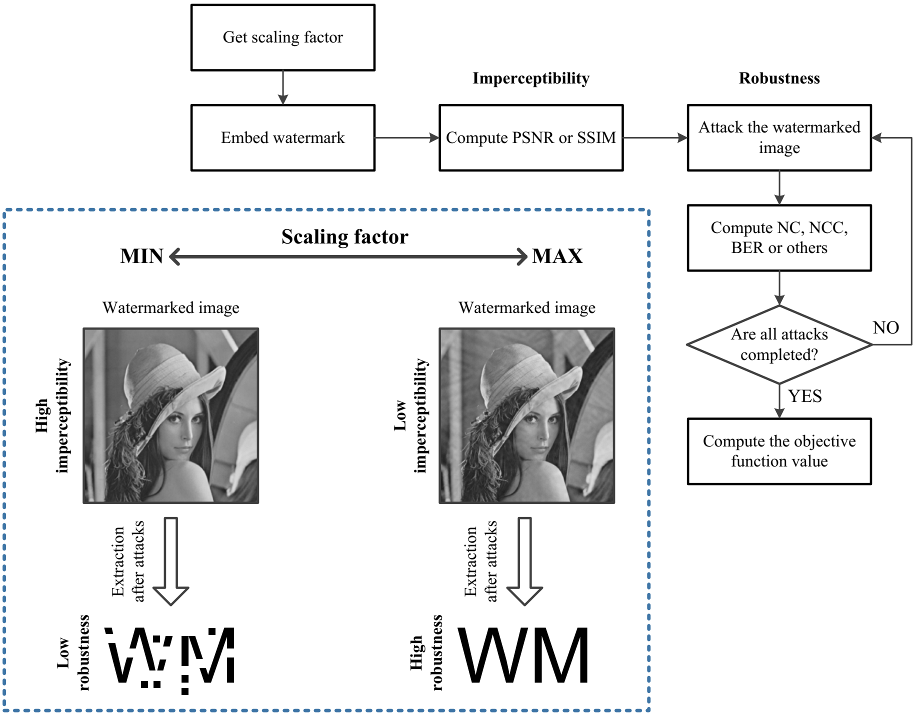


Fig. 8 Scaling factor optimization

frequency domain. We group studies by metaheuristics. The largest number of studies contains schemes that combine the embedding of a watermark into the DWT domain, SVD and PSO. For example, Ahmadi et al. (2021a) propose a scheme that combines robust and fragile watermarks. The robust watermark is embedded into the blue channel of RGB color space based on DWT, Human Visual System (HVS) and SVD using PSO optimization. A fragile watermark is embedded into all RGB channels by manipulating the diagonal singular values for the purpose of authentication. The objective function is as follows:

$$Maximize\, f = SSIM\left(I, I'\right) + \frac{1}{N} \times \sum_{i=1}^{N} NC_i\left(W, W'\right), \tag{16}$$

where N is a number of attacks. In another study, Ahmadi et al. (2021b) present DWT-SVD-PSO watermarking scheme. Its feature is implementing HVS as a sum of visual and edge entropies to select the most suitable embedding block regions. PSO finds the scaling factor value. The objective function maximizes the robustness for a fixed target value of PSNR. The objective function is calculated by the formula

$$Maximize\, f = NC(I, I') + \frac{1}{N} \times \sum_{i=1}^{N} NC_i\left(W, W'\right). \tag{17}$$

In Kumar et al. (2021), the magic square scrambling method is applied to the watermark before embedding. After that, the watermark is embedded into the hybrid domain of the Fractional Quaternion Wavelet Transform (FrQWT) and SVD. PSO is applied to optimize the performance of the watermarking scheme, an objective function is defined as

$$Maximize\, f = \alpha \times BCR(I, I') + \beta \times BCR(W, W_1') + \gamma \times BCR(W, W_2'), \tag{18}$$

where α, β, and γ are weighting parameters, W_1' is an extracted watermark without attack, and W_2' is an extracted watermark after attack. Mohan et al. (2021) also embed the watermark in the DWT-SVD domain. Before embedding, the watermark is scrambled by using a step space-filling curve to improve security. The combination of the PSO and FA metaheuristics finds the optimal values for the embedding parameters. The objective function is as follows:

$$Minimize\, f = \alpha \times \frac{1}{PSNR(I, I')} + \frac{1}{N} \times \sum_{i=1}^{N} \frac{1}{NC_i(W, W')}, \tag{19}$$

where α is a balancing factor. Shen et al. (2021) combine PSO and GWO to effectively implement adaptive color multi-watermarking embedding. They hide 4 watermarks in the DWT-SVD domain after pre-transforms such as Arnold transform and gyrator transform. The hybrid optimization scheme finds the optimal embedding regions and embedding strengths, and the objective function is calculated using the following formula:

$$Maximize\, f = CC\left(I, I'\right) + \frac{1}{N} \times \sum_{i=1}^{N} \sum_{j=1}^{N_w} CC_i^j\left(W, W'\right), \tag{20}$$

where N_w represents the number of watermarks. Another example of DWT-SVD schemes is presented by Thakkar and Srivastava (2017b). The authors propose the following expression for the objective function:

$$Maximize\, f = \frac{CC(I, I') + CC(W, W')}{2}. \tag{21}$$

In another study, Thakkar and Srivastava (2019) embed watermarks into the Complex Wavelet Transform (CWT) and SVD domain. The authors use Jaya and PSO algorithms to improve embedding efficiency. The comparison of the algorithms shows that Jaya is better for finding the optimal scaling factor. In a later study, Thakkar and Srivastava (2021) compare the performance of PSO-based image watermarking with and without Arnold transform applied to the watermark. Experimental results show that a scrambled watermark is more suitable for robust embedding. The objective function is

$$Maximize\, f = CC(I, I') + \frac{1}{N} \times \sum_{i=1}^{N} CC_i\left(W, W'\right). \tag{22}$$

A modified version of the multi-objective PSO is proposed by Saxena and Mishra (2017). The authors note that their algorithm is characterized by increased performance due to the new leader selection strategy and personal best replacement scheme. They also investigate the applicability of the proposed algorithm for improving the image watermarking quality. In the optimization process, it is necessary to simultaneously maximize $CC(I, I')$ and $CC(W, W')$. Zheng et al. (2018) propose a new modification of the PSO algorithm called guided dynamic-PSO. They demonstrate the efficiency of this algorithm on the example of embedding watermarks in the DWT-SVD domain. The objective function is the sum of correlation coefficients:

$$Maximize\, f = CC(I, I') + CC(W, W'). \tag{23}$$

Bansal et al. (2022) combine PSO and fuzzy logic. The watermark is obtained from fuzzy inference system using luminance sensitivity, edge sensitivity, and contrast sensitivity. The embedding is done in DWT-SVD coefficients using the scaling factor found by PSO. The objective function is given below:

$$Maximize\, f = PSNR(I, I') + \alpha \times \sum_{i=0}^{N} NC_i(W, W'), \tag{24}$$

where $i = 0$ means no attack, α is a balancing factor. Anand and Singh (2022) use a combination of Redundant Discrete Wavelet Transform (RDWT) and randomized SVD (RSVD) to form the watermark hiding space and a combination of PSO and FA to find the optimal scaling factor.

A number of studies present a combination of several transforms and SVD to form a watermark hiding space. Zhou et al. (2019) and Wu et al. (2020) use a set of transformations including LWT, DCT, Discrete Fractional Angular Transform (DFAT), and SVD to form the hiding space. The optimization of the watermark embedding parameters is carried out using PSO, while the objective function is as follows:

$$Maximize\, f = \left[\eta \times PSNR(I, I')\right] \times \left[\frac{1}{N}\sum_{i=1}^{N} \eta_t \times CC_i(W, W')\right], \tag{25}$$

where η_t and η are the weight coefficients. Kang et al. (2020) propose a robust blind watermarking scheme combining multi-dimensional PSO, intertwining chaotic map-based watermark image encryption, and hybrid DWT-DCT-SVD domain. The objective function is calculated using the following formula:

$$Maximize\, f = PSNR\left(I, I'\right) + \left\{1 - \frac{\left[\sum_{i=1}^{N} BER_i\left(W, W'\right)\right]}{N}\right\} \times \lambda, \tag{26}$$

where λ is used to adjust the balance of PSNR and BER. A semi-blind image watermarking scheme is proposed by Cheema et al. (2020). It is based on Finite Ridgelet Transform (FRT), DWT, SVD, and PSO. The scheme hides one pixel of the color watermark in one pixel of the color image. The objective function is:

$$Minimize\, f = \frac{N}{PSNR(I, I') + \sum_{i=1}^{N} NCC_i(W, W')}. \tag{27}$$

Zhang and Wei (2019) embed watermarks into a hybrid DCT-DWT-SVD domain. The authors use PSO with the following objective function:

$$Minimize\, f = -\frac{1}{N} \times \left(PSNR\left(I, I'\right) + \sum_{i=1}^{N} NCC_i\left(W, W'\right)\right). \tag{28}$$

A robust double-encrypted watermarking algorithm based on the Redistributed Invariant Wavelet Transform (RIDWT) and DCT is proposed by Li et al. (2021). Arnold transform and FrFT are applied to the watermark before embedding. PSO is used to obtain optimal embedding factors that provide a balance between imperceptibility and robustness. The objective function is as follows:

$$Minimize\, f = r_1 \times \log \left| PSNR\left(I, I'\right) - PSNR_{\text{target}}\left(I, I'\right) \right| + r_2 \times \frac{N}{\sum_{i=1}^{N} NCC_i(W, W')}, \tag{29}$$

where $PSNR_{\text{target}}\left(I, I'\right)$ is the expected PSNR value, and r_1, r_2 are random numbers between 0 and 1. Laxmanika and Singh (2022) apply bi-dimensional empirical mode decomposition to watermark before singular decomposition to decompose from higher frequency to lower frequency. PSO is used in the embedding and extracting steps to get the scaling factor matrix. Awasthi and Srivastava (2022) propose and compare two watermarking schemes: in the LWT-DCT-SVD hybrid domain and in the DWT-DCT-SVD hybrid domain. The authors also compare the performance of two metaheuristics for choosing the optimal scaling factor: Jaya and PSO. The objective function is given by the expression

$$Minimize\, f = \frac{\frac{1}{N}\sum_{i=1}^{N} CC_i(W, W') - \frac{1}{50} PSNR(I, I')}{\left[\left(\frac{N}{K}\right) - 1\right]}, \tag{30}$$

where K is a number of images used. The results of the comparison show that PSO is more effective in improving robustness, while Jaya provides better embedding imperceptibility. The choice of DWT or LWT affects the running time of the algorithm. Mahto et al. (2022) use each color image channel to store additional information. They embed the PAN number in the DWT domain of the red channel, they embed the account number in the spatial domain of the green channel, and the blue channel is used to embed the watermark image into the domain combining LWT, Schur decomposition and the Tensor SVD (TSVD). Finding the best scaling factor value for watermark embedding is done with a hybrid optimization scheme based on PSO and FA. The objective function has the following form:

$$Minimize\, f = \gamma \times \frac{1}{PSNR(I, I')} + \left[\frac{1}{n} \times \sum_{i=1}^{n} \frac{1}{NC_i(W, W')}\right], \tag{31}$$

where γ is a stabilising factor which balances the quality and robustness effects. In Mahto and Singh (2022), a similar principle is followed for other frequency transforms. FA is used to select the scaling factor.

Some watermarking schemes do not use SVD. For example, Balasamy and Ramakrishnan (2019) propose an authentication scheme for medical images in which the PSO finds the optimal weights of each watermarked bit. The DWT domain is used to embed the watermark. Swaraja et al. (2020) propose a blind dual medical image watermarking framework based on DWT and Schur Decomposition (SD). The authors use a hybrid scheme that combines metaheuristics such as PSO and BFO to find optimum threshold parameters. Global exploration is done by PSO and local exploration done by BFO. The objective function is calculated as follows:

$$Minimize\, f = \lambda \times \left| PSNR\left(I, I'\right) - PSNR_{\text{target}}\left(I, I'\right) \right| + \left(1 - \frac{1}{N}\sum_{i=1}^{N} NC_i\left(W, W'\right)\right), \tag{32}$$

where λ is a coefficient.

A number of studies do not use wavelet transforms when forming the watermark hiding space. An approach for copyright protection of multi-spectral images using PSO and Kernel Extreme Learning Machine (KELM) is described by Sisaudia and Vishwakarma (2021). KELM is applied as a non-linear regression model for prediction of DCT coefficients where watermark bits are embedded. PSO is used to optimize the strength of the embedding of watermark bits in the DCT domain. The objective function is as follows:

$$Minimize\, f = -NCC\left(I, I'\right) + \frac{N}{\sum_{i=1}^{N} NCC_i(W, W')}. \tag{33}$$

Cedillo-Hernandez et al. (2021) propose to generate a pseudo-random watermark using secret keys. The spread spectrum method is used to embed the watermark in the annular middle frequency region of the DFT coefficients. PSO is used to optimize embedding parameter values including a strength factor and two radiuses defining the embedding area. The objective function is as follows:

$$Maxixize\, f = VIF(I, I') + \frac{\sum_{i=1}^{N} BCR_i\,(W, W')}{N}, \tag{34}$$

where the VIF metric measures the imperceptibility between the original image I and its watermarked version I'. The VIF metric is defined as

$$VIF = \frac{\sum\limits_{k \in channels} I\left(\vec{C}^{Z,k}; \vec{G}^{Z,k} \middle| s^{Z,k}\right)}{\sum\limits_{k \in channels} I\left(\vec{C}^{Z,k}; \vec{E}^{Z,k} \middle| s^{Z,k}\right)}, \tag{35}$$

where $\vec{C}^{Z,k}$ represents Z elements of the random field, E and G denote the visual signal at the output of the HVS model from the original and watermarked images respectively. Hsu and Hu (2020) propose a scheme based on crisscross inter-block Quaternion Discrete Fourier Transform (QDFT). The authors apply PSO to optimize the embedding parameters and use the following objective function:

$$Minimize\, f = -F\left(PSNR(I, I')\right) \times SSIM(I, I') \times \left(\varepsilon - \frac{1}{N}\sum_{i=1}^{N} BER(W, W')\right), \tag{36}$$

where ε represents the acceptable upper bound BER value (%), the sigmoid function F is defined as

$$F(\chi) = \frac{1}{1 + e^{-2(\chi - \beta)}}, \tag{37}$$

where β indicate the acceptable lower bound of SSIM. Li et al. (2018) propose a watermarking scheme based on the Quaternion Discrete Cosine Transform (QDCT) and SVD. They use an encrypted binary computer-generated hologram as a watermark. In this scheme, the PSO algorithm solves two different problems. First, the authors use PSO when generating the watermark to improve the reconstructed image quality. The objective function is the BCR metric. Second, the authors use PSO to optimize the embedding strength factor. In this case the objective function is:

$$Maximize\, f = PSNR(I, I') + 2 \times \left[\sum_{i=1}^{10} (NC_i(W, W') + BCR_i(W, W')) \right]. \tag{38}$$

Hsu et al. (2022) form an embedding space using QR Decomposition (QRD). The authors combine PSO with a super-resolution convolutional neural network to increase efficiency. Metaheuristic optimization aims to find the optimal embedding parameters, while the neural network improves the visual recognition of extracted watermarks. The objective function is given below:

$$\begin{aligned} Minimize\, f = {} & \min \left(PSNR(I, I')/38, 1 \right) \times SSIM(I, I') \\ & \times \frac{1}{N} \sum_{i=1}^{N} NCC_i(W, W') \times \left(\frac{1}{N} \sum_{i=1}^{N} 1 - BER_i(W, W') \right). \end{aligned} \tag{39}$$

Various researchers use the ABC metaheuristic in watermarking schemes. For example, Ansari and Pant (2017, 2018) find optimal embedding parameters in the DWT-SVD domain using the ABC metaheuristic. The authors explain the choice of this optimization algorithm by a small number of parameters and fast convergence. The objective function is

$$Maximize\, f = BCR(I, I') + \frac{1}{N} \times \sum_{i=1}^{N} BCR_i\left(W, W'\right). \tag{40}$$

Gao and Chen (2021) propose a watermarking scheme in the DWT-SVD domain. Arnold transformation is applied to randomize the watermark before embedding. Speed-Up Robust Feature (SURF) and random sample consensus algorithms are used to increase the robustness of the embedding against geometric attacks. The improved ABC algorithm is used to optimize the embedding strength. The objective function is as follows:

$$Minimize\, f = -BCR(I, I') + \frac{N}{\sum_{i=1}^{N} BCR_i(W, W')}. \tag{41}$$

Sharma et al. (2019) combine RDWT and SVD with ABC optimization, and the objective function is as (16). In later work, Sharma et al. (2021d) use ABC to achieve a balance between imperceptibility and robustness when embedding watermarks in a hybrid LWT-DCT domain. The objective function is as (40). A DWT-SVD-ABC scheme is presented by Sharma et al. (2021e). The following objective function is applied to optimize the strength factor using ABC:

$$Minimize\, f = \frac{100}{PSNR(I, I')} + \frac{1}{BCR(I, I')} + \frac{N}{\sum_{i=1}^{N} BCR_i(W, W')}. \tag{42}$$

Another scheme combining wavelet transform, SVD and ABC optimization is presented by Salehnia and Fathi (2021). The authors suggest using Arnold transform to encrypt the watermark and LWT to reduce the number of errors when extracting a watermark. ABC optimization selects three scaling factors. The objective function is as follows:

$$Maximaze\, f = PSNR\left(I, I'\right) / \left(1 - \frac{\sum_{i=1}^{N} NC_i\left(W, W'\right)}{N_A}\right), \tag{43}$$

where N_A indicates a number of unintentional attacks. Singh et al. (2021b) use the IWT-SVD hybrid block transform. The proposed scheme encrypts the watermark using a pseudo-random key that is adaptively generated from the host image and the watermark. Blocks with low entropy are selected for embedding using a pseudo-random number generator. A scaling factor α is chosen adaptively for each image to improve the visual quality of the embedding. The authors compare the performance of GA, ABC, and FA to optimize the scaling factor. Experimental results show that GA provides the best embedding quality. The objective function is calculated as follows:

$$Maximize\, f = \frac{\left(PSNR\left(I, I'\right) \times SSIM\left(I, I'\right)\right)}{\alpha} + \frac{\left(Cor\left(W, W'\right) \times BER\left(W, W'\right)\right)}{\alpha}, \tag{44}$$

$$Cor\left(W, W'\right) = \frac{\sum_{x=1}^{m} \sum_{y=1}^{n} \left(W(x, y) - W'(x, y)\right)^2}{\sqrt{\sum_{x=1}^{m} \sum_{y=1}^{n} \left(W(x, y)^2\right)} \sqrt{\sum_{x=1}^{m} \sum_{y=1}^{n} \left(W'(x, y)^2\right)}}. \tag{45}$$

Lei et al. (2019) use the IWT domain to embed two watermarks. The low frequency coefficients are used to embed a robust watermark for copyright protection, and the high frequency coefficients are used to embed a fragile watermark for content authentication. The objective function combines metrics of imperceptibility, capacity, and robustness and is calculated as follows:

$$Maximize\, f = \frac{3 \times PSNR(I, I') \times (1 - EC) \times BCR_{av}(W, W')}{PSNR(I, I') + (1 - EC) \times BCR_{av}(W, W') + (1 - EC) \times PSNR(I, I')}, \tag{46}$$

$$BCR_{av}(W, W') = \frac{1}{N} \times \sum_{i=1}^{N} \alpha_i \times BCR_i\left(W, W'\right), \tag{47}$$

where α is a weighting factor. In Kasana and Kasana (2017), a feature is that singular values of LWT coefficients of the cover image are utilized to create reference image instead of embedding the watermark. ABC is used to find an optimal embedding strength, the objective function is formed as follows:

$$Minimize\, f = \frac{1}{CC(W, W') + CC(I, I')}. \tag{48}$$

Garg and Kishore (2022a) propose a blind scheme that hides the watermark in the hybrid DWT-DCT domain using ABC. The objective function is

$$Minimize\, f = 10 \times \left|PSNR\left(I, I'\right) - PSNR_{\text{target}}\left(I, I'\right)\right| + \left(1 - \frac{1}{N} \sum_{i=1}^{N} NCC_i\left(W, W'\right)\right). \tag{49}$$

Abdelhakim et al. (2018) propose a block embedding scheme that embeds watermarks in the FrFT and SVD domain. The quality threshold-based fitness function evaluates the fitness of each solution according to its rank within the solutions. Ansari et al.

(2017) hide watermarks in Slantlet Transform (ST) coefficients. The authors explain the choice of this transformation by the increased resistance to image processing attacks. The ABC algorithm is used to achieve the optimal balance between robustness and imperceptibility. The objective function is calculated as follows:

$$Minimize\, f = \frac{20}{PSNR(I, I')} + \frac{1}{N} \sum_{i=1}^{N} BER_i\left(W, W'\right). \tag{50}$$

A watermarking scheme for color images based on DCT and Non-Negative Matrix Factorization (NNMF) is proposed by Sharma et al. (2022c). The optimal embedding strength factor is found using the multi-objective ABC. The set of objective values for each color channel is described as follows:

$$Minimize\, f = \left(\frac{100}{PSNR(I, I')} \frac{1}{BCR(W, W')} \frac{1}{BCR_1(W, W')} \frac{1}{BCR_2(W, W')} \cdots \frac{1}{BCR_N(W, W')} \right). \tag{51}$$

There are several watermarking schemes that use GA optimization. Sivananthamaitrey and Kumar (2022a) combine Stationary Wavelet Transform (SWT), SVD and GA in their dual watermarking scheme. A grayscale watermark is embedded in the frequency coefficients of the green RGB component of the cover image to provide copyright protection. A binary watermark is embedded into the spatial domain of the blue component of the cover image to localize distortion. The objective function is as (17). In another paper, Sivananthamaitrey and Kumar (2022b) compare the performance of GA, IWO, and TLBO for a watermarking scheme in the SWT-SVD domain. The results show the superiority of the new metaheuristics compared to the classical GA in terms of embedding robustness, capacity, and running time. Barlaskar et al. (2022) use the sequential two-stage correction module to provide high robustness. Geometric correction module improves resistance to geometric attacks and uses a hybrid deep convolution neural network model integrated with support vector regressor. Non-geometric correction module corrects the watermark embedded region by computing the global mean, block mean, and variance of the DCT mid-band frequency components of the watermarked image. GA finds an optimal scaling factor, and the objective function is the sum of PSNR and the product of NC' and the weighting factor, where

$$NC' = \frac{\sum_{i=1}^{m} \sum_{j=1}^{n} W(i,j) \times W'(i,j)}{m \times n} \tag{52}$$

and watermark bit is set to 1 if the watermark bit is 1 otherwise it is set to -1. Kumari and Mustafi (2022) propose an embedding scheme based on the blind source separation technique that mixes the original image and the scaled and padded watermark image. The authors find the optimal coefficients of the mixing matrix using GA and the RMSE metric as an objective function.

Some researchers use DE optimization. Ali et al. (2020) propose a watermarking scheme in the spatial domain. In this scheme, DC-coefficients of DCT are computed in the spatial domain without using a real DCT. The embedding efficiency of the quantization-based watermarking is controlled by DE. The objective function is as (49). A similar objective function is used by Vali et al. (2018). The authors embed the watermark into the RDWT and SVD domain. The self-adaptive DE algorithm is used to optimize the scaling factor values. This version of DE saves the user from choosing optimization options, since they are configured in an adaptive way. Salimi et al. (2020) use DE twice. First, DE is used to find suitable locations for watermark blocks and to select optimal values for alpha-blending coefficients. In this case, the objective function is formed as follows:

$$Minimize\, f = -\left(k_1 PSNR(I, I') + k_2 PSNR(W, W')\right) + k_{p_1} h_1 + k_{p_2} h_2, \tag{53}$$

where k_1 and k_2 are weight coefficients, and k_{pi} are penalty coefficients, h_j values depend on the ratio of the current PSNR value to an acceptable lower bound for PSNR. Next, DE is applied again to select the best embedding parameters for the found optimal values. The objective function is:

$$Minimize\, f = -PSNR(I, I') + k_{p_3} h_3. \tag{54}$$

Cui et al. (2018) embed watermarks into the DWT-SVD domain. However, before doing frequency transformation, they convert the host image from RGB space to YIQ space, which is more suitable for HVS. The objective function combines imperceptibility and robustness metrics:

$$Maximize\, f = NCC(I, I') + NCC(W, W'). \tag{55}$$

A small group of studies is devoted to the combination of GWO and image watermarking. For example, Pandey et al. (2020) use GWO when embedding a watermark into singular values of LWT coefficients. The objective function is as follows:

$$Minimize\, f = \frac{100}{PSNR(I, I')} + \frac{100}{SSIM(I, I')} + \sum_{i=1}^{N} \left[1 - NCC_i(W, W')\right]. \tag{56}$$

Hsu and Hu (2021) embed a watermark in the QDCT coefficients. GWO is used to increase robustness and imperceptibility, and denoising convolutional neural network is used to make the extracted binary watermark more visually recognizable. The objective function is as follows:

$$Minimize\, f = -\min\left(\frac{PSNR\left(I, I'\right)}{40}, 1\right) \times SSIM\left(I, I'\right) \times \left(1 - BER\left(W, W'\right)\right). \tag{57}$$

Sharma et al. (2021a) propose a video watermarking technique, but individual frames are used as cover objects. The hiding space is formed by applying Graph-Based Transform (GBT) and SVD. The hybrid GWO-GA optimization technique is used to find the main embedding parameter, while the PSNR metric is considered as a fitness function. Dappuri et al. (2020) use enhanced GWO in their watermarking algorithm based on SVD in Translation Invariant Wavelet (TIW) domain. The authors choose TIW as frequency transform for its increased robustness to image processing operations.

There are several examples of watermarking schemes based on FA optimization. For example, Kazemivash and Moghaddam (2018) propose an image watermarking scheme based on predictive model using regression tree. The low frequency subband of the LWT is used to embed the watermark after the Fibonacci-Q transformation. FA is applied to find the best scaling factor and the objective function is calculated using the following formula:

$$Maximize\,f = \left[PSNR_{AF}\left(I, I'\right) + NC(W, W')_{AF}\right] + \left[\omega \times \left(\frac{1}{N} \times \sum_{i=1}^{N} NC_i(W, W')\right)\right], \tag{58}$$

where AF means an attack-free phase, and ω is used for balancing effect of PSNR and NC. Altay and Ulutaş (2021) apply the Fibonacci-Lucas transform to the watermark to improve security. A modified version of FA called self-adaptive step FA is used to select the optimal embedding parameters in the DWT-SVD domain. The objective function is as follows:

$$Maximaze\,f = 0.01 \times PSNR\left(I, I'\right) + \frac{1}{N} \times \sum_{i=1}^{N} NC_i\left(W, W'\right). \tag{59}$$

Moeinaddini and Afsari (2018) use opposition and dimensional based modified FA (Verma et al. 2016), which differs from the classical FA in less computational complexity. The embedding procedure is based on changing the differences between image elements, and optimization is used to find the best threshold value. The objective function is as follows:

$$Minimize\,f = \left|PSNR_{\text{target}}\left(I, I'\right) - PSNR\left(I, I'\right)\right| + \sum_{i=1}^{N} \left(1 - NC_i\left(W, W'\right)\right). \tag{60}$$

Devi et al. (2022b) optimize the scaling factor using a combination of Jaya and FA metaheuristics to achieve a better balance between exploration and exploitation search. The choice of a specific metaheuristic for each new generation of optimization depends on the value of the objective function. If it cannot be improved by Jaya, FA is used instead. The objective function is given by the following expression:

$$Maximize\,f = (PSNR(I, I') + SSIM(I, I'))/\gamma + \left(\sum_{i=1}^{N} Cor_i(W, W') + \sum_{i=1}^{N} BER_i(W, W')\right)/\gamma, \tag{61}$$

where γ is the chosen population value.

FOA-based scheme is proposed by Zhang and Ma (2019). Algorithm is designed for virtual reality technology, but its general scheme is similar to the classical image watermarking. In particular, the authors use the quantization-based embedding approach. FOA is used to adaptively determine the embedding strength of watermarking. The objective function is formed as follows:

$$Minimize\,f = \frac{1}{PSNR(I, I')} + \sum_{i=1}^{N} \frac{1}{NC_i(W, W')}. \tag{62}$$

Liu et al. (2019) and Nazir et al. (2021) also combine image watermarking and FOA. The authors hide the watermark in a hybrid domain based on DWT, Hessenberg Decomposition (HD), and SVD. FOA is used to find the optimal scaling factor. The objective function is as follows:

$$Maximize\,f = \omega_1 \frac{1}{\lambda} PSNR(I, I') + \omega_2 SSIM(I, I') + \omega_3 \frac{1}{N} \sum_{i=1}^{N} NCC(W, W'), \tag{63}$$

where λ is the weighting factor, ω_1, ω_2, ω_3 are the proportion coefficients.

We also note examples of using other metaheuristics to optimize the scaling factor. A multi-objective ACO is used by Makbol et al. (2017). The authors use IWT coefficients as a watermark hiding space to counter the false positive problem. The aim of the optimization is to achieve a high PSNR value and a maximum CC value. CS is applied to optimize the watermark embedding parameters by Ali and Ahn (2018). The authors explain the prospects of this metaheuristic for image watermarking by a small number of customizable optimization parameters. The objective function is as (49). Swaraja et al. (2021) present a hierarchical layered watermark structure for medical images. The authors use RDWT and QR decomposition to form the hiding space. A robust watermark is used to protect the copyright, while a fragile watermark is used to detect distortion and recover damaged areas. The particle swarm BFO algorithm is used to increase the embedding robustness. Pourhadi and Mahdavi-Nasab (2020) propose a BA based scheme. A feature of the scheme is the use of the SURF technique. SURF corrects geometric distortions both at the stage of embedding watermark into the Stationary Wavelet Transform (SWT) domain and at the watermark extracting stage. BA is applied to optimize the embedding strength factors and the objective function is constructed as follows:

$$Minimize\,f = \alpha \times f_1 + (10 - \alpha) \times f_2, \tag{64}$$

where α is a weighting factor,

$$f_1 = \frac{40}{PSNR(I, I')} + \frac{1}{NC(I, I')}, \tag{65}$$

$$f_2 = \frac{1}{N} \times \sum_{i=1}^{N} \frac{1}{NC_i(W, W')} + \frac{10}{N} \times \sum_{i=1}^{N} BER_i(W, W'). \tag{66}$$

Koley (2022) proposes a watermarking scheme for 3D red-cyan anaglyph stereo. The hiding space is formed using the Shearlet Transform (ST) and Maximum Noise Fraction (MNF) transform. The author applies Henon chaotic encryption to the watermark to improve security. BA is used to select the embedding strength factor in order to strike a balance between stealth and robustness. The objective function is given by the expression

$$Minimize\,f = SSIM(W, W')^{-1}_{avg} - SSIM(I, I'), \tag{67}$$

where *avg* is a mean value for N attacks. Devi et al. (2022a) propose an encrypted watermark embedding scheme for protecting aerial remote sensing images. Embedding procedure uses a hybrid RDWT and SVD domain. Embedding strength optimization also uses a hybrid scheme that combines 2 swarm intelligence algorithms: GOA and BA. The objective function is as (61). Chakravarthy et al. (2019) use SCA to select the best scaling factor when embedding a watermark into the IWT-SVD domain. The objective function is as (33). TLBO-based scheme is proposed by Moosazadeh and Ekbatanifard (2019). An embedding operation is based on the relationships between the DCT coefficients. TLBO is used to optimize embedding parameters and select the appropriate watermark location. The objective function is as follows:

$$Maximize\, f = PSNR(I, I') + \sum_{i=1}^{N} \lambda_i NC_i(W, W'), \tag{68}$$

where λ_i is a weighted factor. Chacko and Chacko (2022) propose a watermarking scheme for medical imaging that uses a neural network to extract data. The authors use HHO to find embed options. The objective function is:

$$Maximize\, f = PSNR(I, I') + \frac{1}{N} \sum_{i=0}^{N} \left(NCC_i(W, W') \times \alpha_i \right), \tag{69}$$

where α is a weighting factor. Sharma et al. (2021b) use DA to optimize watermarking in a hybrid DWT-DCT domain. In another study, Sharma et al. (2021c) use GOA to solve a similar problem. Both metaheuristics show the same efficiency in optimizing the embedding strength. In (Sharma et al. 2022b), the authors apply MRFO to optimize the locally relevant multiple embedding strengths in a Dual Tree Complex Wavelet Transform (DTCWT) based watermarking scheme. After optimization, the authors apply a bi-directional extreme learning machine to learn the values of multiple embedding strengths. This design of the algorithm speeds up its operation and improves performance. The objective function of the optimization algorithm is as follows:

$$Maximize\, f = \log \left[SSIM(I, I') + \frac{1}{N} \sum_{i=1}^{N} NC_i(W, W') \right]. \tag{70}$$

El-Kenawy et al. (2022) combine the DTO algorithm with the SFS algorithm for DCT-DWT image domain. The SFS is used with the DTO to improve the exploration of the search space to efficiently find the best set of parameters. Rai and Goyal (2022) combine fuzzy inference systems, Back Propagation Neural Network (BPNN) and SSO to embed a watermark into the DCT frequency domain. Fuzzy-BPNN finds suitable areas for imperceptible embedding and the optimal embedding parameters are determined using the SSO algorithm. The objective function is as (68). Sinhal and Ansari (2022) use Q-factor Wavelet Transform (TQWT) and DCT to form an embedding domain. ALO is used to get optimal values for TQWT and watermark embedding parameters such as Q-factor, redundancy and embedding strength. To avoid increasing the computational complexity of the algorithm due to the use of metaheuristic search, the authors suggest using the general values of optimized parameters obtained for a large number of different images. The optimization process uses the following objective function:

$$Minimize\, f = \frac{1}{N} \sum_{i=1}^{N} BER_i(W, W') + \frac{1}{PSNR(I, I')}. \tag{71}$$

A summary of each of the reviewed studies, including embedding efficiency indicators, is presented in Table 3.

3.3.2 Other optimization purposes

There are also studies in the field of image watermarking that use metaheuristic optimization to solve other problems. They are mainly aimed at choosing the optimal

Table 3 Watermarking schemes with the scaling factor optimization

Reference	Embedding domain	Metaheuristic	Performance indicators
Ahmadi et al. (2021a)	DWT-SVD	PSO	EC: 0.0312 bpp (CLR) PSNR: 43.2199–57.0541 dB SSIM: 0.707–0.9952 Robustness: high NC: 0.7367–1.0
Ahmadi et al. (2021b)	DWT-SVD	PSO	EC: 0.0039–0.0312 bpp (GS) PSNR: 40.0008–51.8600 dB Robustness: high NC: 0.4393–1.0
Kumar et al. (2021)	FrQWT-SVD	PSO	EC: 0.0156 bpp (GS) PSNR: 32.44–40.27 dB SSIM: 0.8324–0.9323 Robustness: high BCR: 0.817–0.9932
Mohan et al. (2021)	DWT-SVD	PSO and FA	EC: 2 bpp (CLR) PSNR: 54.5625–56.1661 dB Robustness: medium NC: 0.7192–0.9956
Shen et al. (2021)	DWT-SVD	GWO and PSO	EC: 6 bpp (CLR) PSNR: 55.9214–59.7229 dB Robustness: high CC: 0.8128–0.9819
Thakkar and Srivastava (2017b)	DWT-SVD	PSO	EC: 0.0156 bpp (GS) Robustness: Checkmark CC: 0.838–1.0
Thakkar and Srivastava (2019)	CWT-SVD	PSO or Jaya	EC: 0.25 bpp (GS) CC: 0.7681–0.9994 Robustness: low
Thakkar and Srivastava (2021)	DWT-SVD	PSO	EC: 0.25 bpp (GS) Robustness: medium CC: 0.9593–0.9999

Table 3 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Saxena and Mishra (2017)	DWT-SVD	Modified PSO	EC: 24 bpp (CLR) Robustness: medium
Zheng et al. (2018)	DWT-SVD	Guided Dynamic PSO	EC: 24 bpp (CLR) PSNR: 39.7923 dB Robustness: medium
Bansal et al. (2022)	DWT-SVD	PSO	PSNR: 50.4534–68.4423 dB SSIM: 0.9871–0.9983 Robustness: medium NC: 0.7502–1.0
Anand and Singh (2022)	RDWT-RSVD	PSO and FA	EC: 0.2504 bpp (GS) PSNR: 45.5891 dB SSIM: 0.9961 Robustness: medium NC: 0.7185–0.9995
Zhou et al. (2019)	LWT-DCT-DFAT-SVD	PSO	EC: 0.0312 bpp (GS) PSNR: 42.2268–44.0828 dB Robustness: high CC: 0.8564–0.9994
Wu et al. (2020)	LWT–DCT–DFAT–SVD	PSO	EC: 0.0312 bpp (GS) PSNR: 42.2875–46.0327 dB Robustness: medium CC: 0.8891–0.9962
Kang et al. (2020)	DWT-DCT-SVD	PSO	EC: 9.8×10^{-4} bpp (GS) PSNR: 39.9004–43.8502 dB Robustness: high NCC: 0.692–1.0 BER: 0.0–0.168

Table 3 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Cheema et al. (2020)	FRT-DWT-SVD	PSO	EC: 24 bpp (CLR) PSNR: 45.0325–45.9059 dB SSIM: 0.9970–0.9990 Robustness: high NCC: 0.7712–0.999
Zhang and Wei (2019)	DCT-DWT-SVD	PSO	EC: 0.5 bpp (GS) PSNR: 43.9023–48.9906 dB Robustness: high NCC: 0.9432–0.9998
Li et al. (2021)	RIDWT-DCT-SVD	PSO	EC: 0.125 bpp (GS) PSNR: 41.5647–42.3596 dB Robustness: high NCC: 0.9615–1.0
Laxmanika and Singh (2022)	DWT-DCT-SVD	PSO	EC: 2 bpp (GS) PSNR: 41.7053–49.4254 Robustness: medium NC: 0.9364–0.9967
Awasthi and Srivastava (2022)	LWT-DCT-SVD, DWT-DCT-SVD	Jaya, PSO	EC: 2 bpp (GS) PSNR: 42.3417–44.9488 dB Robustness: high CC: 0.7183–1.0
Mahto et al. (2022)	LWT-Schur-TSVD	PSO and FA	EC: 0.5 bpp (CLR) PSNR: 56.0407–59.5111 dB SSIM: 0.9898–0.9979 Robustness: medium NC: 0.6901–1.0 BER: 0.0–0.4231

Table 3 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Mahto and Singh (2022)	DWT-CT-TSVD	FA	EC: 0.5 bpp (CLR) PSNR: 30.8420–45.3162 dB Robustness: medium NC: ≈ 0.70–0.95 BER: 0.0–0.45
Balasamy and Ramakrishnan (2019)	DWT	PSO	EC: 0.1467 bpp (GS) PSNR: 49.0055 dB SSIM: 0.9999 Robustness: medium BER: ≈0.01–0.16
Swaraja et al. (2020)	DWT-SD	PSO and BFO	EC: 0.8128 bpp (CLR, GS) PSNR: 34.55–37.24 dB Robustness: Checkmark NC: 0.89–1.0
Sisaudia and Vishwakarma (2021)	DCT	PSO	EC: 0.0039 bpp (GS and CLR) PSNR: 44.6396–45.8695 dB Robustness: medium NCC: 0.772–1.0 BER: 0.0–0.2460
Cedillo-Hernandez et al. (2021)	DFT	PSO	EC: 1.04×10^{-4} bpp (CLR) PSNR: 43.17–44.96 dB Robustness: high BCR: 0.81–0.99
Hsu and Hu (2020)	QDFT	PSO	EC: 0.0469 bpp (CLR) PSNR: 39.04–39.41 dB SSIM: 0.954–0.958 Robustness: high BER: 0–0.49

Table 3 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Li et al. (2018)	QDCT-SVD	PSO	EC: 1 bpp (CLR) PSNR: 42.476–42.801 dB Robustness: high NC: 0.817–1.0 BER: 0.0–0.142
Hsu et al.(2022)	QRD	PSO	EC: 0.1875–0.375 bpp (CLR) PSNR: 37.95–38.02 dB SSIM: 0.914–0.915 Robustness: high NCC: ≈ 0.75–1.0 BER: ≈ 0.0–0.25
Ansari and Pant (2017)	DWT-SVD	ABC	EC: 0.5 bpp PSNR: 35.3840–37.4815 dB Robustness: high BCR: 0.6205–0.9968
Ansari and Pant (2018)	DWT-SVD	ABC	EC: 2 bpp (GS) PSNR: 35.0029–35.8038 dB Robustness: high BCR: 0.6066–0.9994
Gao and Chen (2021)	DWT-SVD	Improved ABC	EC: 0.125 bpp (GS) PSNR: 31.1279–39.2776 dB Robustness: high NCC: ≈0.85–1.0
Sharma et al. (2019)	RDWT-SVD	ABC	EC: 24 bpp (CLR) PSNR: 59.3682–77.4875 dB SSIM: 0.9834–0.9998 Robustness: high NC: 0.7563–0.9969

Table 3 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Sharma et al. (2021d)	LWT-DCT	ABC	EC: 0.0937 bpp (CLR) PSNR: 41.0428–42.4077 dB SSIM: 0.8994–0.9942 Robustness: high BCR: ≈0.7–0.99
Sharma et al. (2021e)	DWT-SVD	ABC	EC: 0.0938–0.375 bpp (CLR) PSNR: 44.3693–47.6391 dB SSIM: 0.9140–0.9986 Robustness: high BCR: 0.7517–0.9986
Salehnia and Fathi (2021)	LWT-SVD	ABC	EC: 0.0312 bpp (GS) PSNR: 50.37–53.10 dB SSIM: 0.991–0.998 Robustness: high NC: 0.9338–1.0 BER: 0.0005–0.0624
Singh et al. (2021b)	IWT-SVD	GA, ABC, FA	EC: 0.0156 bpp (GS and CLR) PSNR: 52.52–58.42 dB SSIM: 0.9669–0.9989 Robustness: high Cor (45): 0.6859–1.0 BER: 0.0–0.5708
Lei et al. (2019)	IWT	ABC	EC: 0.0312 bpp (GS) PSNR: 32–37 dB Robustness: medium BCR: 0.9688–0.9981
Kasana and Kasana (2017)	LWT	ABC	PSNR: 40.47–42.31 dB Robustness: medium CC: 0.6573–0.9987

Table 3 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Garg and Kishore (2022a)	DWT-DCT	ABC	PSNR: 39.8989–49.7581 dB Robustness: high NCC: 0.9431–1.0
Abdelhakim et al. (2018)	FrFT-SVD	ABC	EC: 0.0156 bpp (GS) PSNR: 44.52–52.53 dB Robustness: high BCR: 0.645–1.0
Ansari et al. (2017)	ST	ABC	EC: 0.0625 bpp (GS) PSNR: 42.889–48.557 dB Robustness: medium BER: 0.0–0.2757
Sharma et al. (2022c)	NNMF-DCT	ABC	EC: 0.0938–1.5 bpp (CLR) PSNR: 45.0189–49.3731 dB Robustness: high BCR: 0.6010–0.9972
Sivananthamaitrey and Kumar (2022a)	SWT-SVD	GA	EC: 9 bpp (CLR) PSNR: 37.57–54.47 dB SSIM: 0.9812–0.9999 Robustness: high NC: 0.9553–1.0 BER: 0.0048–0.0598
Sivananthamaitrey and Kumar (2022b)	SWT-SVD	GA, IWO, TLBO	EC: 9 bpp (CLR) PSNR: 36.41–54.47 dB SSIM: 0.9954–0.9999 Robustness: high NC: 0.9553–1.0

Table 3 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Barlaskar et al. (2022)	DWT-DCT	GA	EC: 0.0039 bpp (GS) PSNR: 36.89–55.06 dB SSIM: 0.9379–0.9999 Robustness: high NC' (64): 0.9452–0.9938 BER: 0.0019–0.3208
Kumari and Mustafi (2022)	FrFT	GA	PSNR: 50.6–53.9 dB SSIM: ≈ 0.95–0.98 Robustness: medium CC: 0.93–1.0 BER: 0.0–0.14
Ali et al. (2020)	Spatial	DE	EC: 0.0156 bpp (GS) PSNR: 44.9996–45.0031 dB SSIM: 0.9870–0.9969 Robustness: high NCC: 0.6022–1.0
Vali et al. (2018)	RDWT-SVD	Self-adaptive DE	EC: 8 bpp (GS) PSNR: 52.9371–54.6852 dB Robustness: high CC: 0.8924–0.9973
Salimi et al. (2020)	DWT	DE	EC: 8 bpp (GS) PSNR: 58.42–83.16 dB SSIM: 0.9824–0.9968 Robustness: medium NCC: 0.6936–0.9987
Cui et al. (2018)	DWT-SVD	DE	EC: 0.5 bpp (GS) PSNR: 44.1288–68.9824 dB Robustness: medium NCC: ≈ 0.94–1.0

Table 3 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Pandey et al. (2020)	LWT-SVD	GWO	PSNR: 38.99–39.59 dB SSIM: 0.99 Robustness: medium NCC: 0.79–0.99
Hsu and Hu (2021)	QDCT	GWO	EC: 0.0156–0.0625 bpp (CLR) PSNR: 38.03–38.12 dB SSIM: 0.943–0.945 Robustness: high NCC: 0.464–1.0
Sharma et al. (2021a)	GBT-SVD	GWO and GA	PSNR: 52.5768–55.4184 dB SSIM: 0.9997–0.9999 Robustness: low NC: ≈ 0.85–1.0 BER: 0.02–0.055
Dappuri et al. (2020)	TIW-SVD	Enhanced GWO	PSNR: ≈ 75 dB SSIM: ≈ 1 Robustness: medium NCC: ≈ 0.99
Kazemivash and Moghaddam (2018)	LWT	FA	EC: 0.0039 bpp (GS) PSNR: 37.7955–38.9708 dB Robustness: high NC: 0.6236–1.0 BER: 0.0–0.1709
Altay and Ulutaş (2021)	DWT-SVD	Self-Adaptive Step FA	EC: 0.0039 bpp (GS) PSNR: 40.4597–45.5527 dB Robustness: high NC: 0.7131–1.0 BER: 0.0–0.2998

Table 3 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Moeinaddini and Afsari (2018)	DWT-SVD	Modified FA	EC: 0.0039 bpp (GS) PSNR: 51.0125–54.1380 dB SSIM: 0.9814–0.9896 Robustness: medium NC: 0.8830–1.0
Devi et al. (2022b)	RDWT-SVD	Jaya and FA	EC: 0.0323 bpp (GS, CLR) PSNR: 39.43–46.98 dB SSIM: 0.7425–0.9989 Robustness: high Cor (45): 0.8915–1.0 BER: 0.0–0.1221
Zhang and Ma (2019)	Spatial	FOA	PSNR: 86.4859–87.0142 dB Robustness: medium NC: 0.9527–1.0
Liu et al. (2019)	DWT-HD-SD	FOA	EC: 0.125–2.0 bpp (GS) PSNR: 38.1295–38.2477 dB SSIM: 0.9989–0.9992 Robustness: high NCC: 0.8322–1.0
Nazir et al. (2021)	DWT-HbD-SVD	FOA	EC: 0.375–6 bpp (CLR) PSNR: 29.2385–41.1389 dB SSIM: 0.9941–0.9987 Robustness: high NC: ≈0.75–0.99
Makbol et al. (2017)	IWT-SVD	Multi-objective ACO	EC: 2 bpp (GS) PSNR: 42.9159–43.0108 dB Robustness: high CC: 0.9220–0.9938

Table 3 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Ali and Ahn (2018)	DWT	CS	EC: 0.0625–0.25 bpp (GS) PSNR: 38.0358 dB Robustness: high BCR: 0.6720–1.0
Swaraja et al. (2021)	RDWT-QR	Particle Swarm BFO	PSNR: 55.97–60.78 dB Robustness: medium
Pourhadi and Mahdavi-Nasab (2020)	SWT	BA	EC: 0.0039 bpp (GS) PSNR: 39.791–40.476 dB Robustness: high NC: 0.724–1.0
Koley (2022)	ST-MNF	BA	EC: 1.28 bpp (CLR) PSNR: $\approx$ 60 dB SSIM: 0.9928–0.9989 Robustness: high CC: 0.9582–1.0 BER: 0.0–0.0587
Devi et al. (2022a)	RDWT-SVD	GOA and BA	EC: 0.0625 bpp (CLR, GS) PSNR: 56.92–74.24 dB SSIM: 1.0 Robustness: high Cor (45): 0.7027–0.9993 BER: 0.0012–0.3016
Chakravarthy et al. (2019)	IWT-SVD	SCA	PSNR: 31.1455–46.5912 dB SSIM: 0.9653–0.9951
Moosazadeh and Ekbatanifard (2019)	DCT	TLBO	EC: 0.0039 bpp (CLR) PSNR: 39.95–40.76 dB Robustness: high NC: 0.6606–1.0 BER: 0.0–0.1816

Table 3 (continued)

Reference	Embedding domain	Metaheuristic	Performance indicators
Chacko and Chacko (2022)	DCT	HHO	PSNR: ≈ 40–50 dB Robustness: medium NCC: ≈ 0.93–1.0 BER: ≈ 0.0–0.09
Sharma et al. (2021b)	DWT-DCT	DA	PSNR: 44.2–51.2 dB
Sharma et al. (2021c)	DWT-DCT	GOA	PSNR: 42.2250–50.1064 dB
Sharma et al. (2022b)	DTCWT-SVD	MRFO	EC: 0.0156 bpp (GS) PSNR: 50.605–57.444 dB SSIM: 0.991–1.0 Robustness: high NC: 0.847–1.0 BER: 0.0–0.098
El-Kenawy et al. (2022)	DCT-DWT	DTO and SFS	PSNR: 63.87–65.11 dB Robustness: low NC: 0.886–0.989
Rai and Goyal (2022)	DCT	SSO	EC: 0.0039 bpp (GS) PSNR: 51.872–52.994 dB Robustness: high NC: 0.9821–1.0
Sinhal and Ansari (2022)	TQWT-DCT	ALO	EC: 0.0039 bpp (GS, CLR) PSNR: 38.51–40.50 dB SSIM: 0.9658–0.9974 Steganalysis: histogram analysis Robustness: high NCC: 0.86–1.0 BER: 0.0–0.08

arrangement of watermark bits in data elements of a host image. Such studies mainly use FA-optimization. For example, Kazemivash and Moghaddam (2017) embed watermarks into the LWT domain, and FA optimization selects suitable image blocks. In particular, FA finds blocks that need to be ignored during embedding in order to achieve the greatest efficiency. The objective function combines the imperceptibility and robustness metrics and is constructed as follows:

$$Minimize\, f = \left[\omega \times \left(\frac{1}{PSNR(I,I')} + BER(W,W')\right)\right] + \\ + \left[\left(\frac{1}{N} \times \sum_{i=1}^{N} \frac{1}{NC_i(W,W')}\right) + \left(\frac{1}{N} \times \sum_{i=1}^{N} BER_i(W,W')\right)\right], \tag{72}$$

where first bracket is for attack free phase and second one for attacked phase, and ω is used for balancing effect of PSNR, BER and NC. Moeinaddini (2019) combines Hadamard Transform (HT) and distinct discrete FA for selecting suitable blocks to balance transparency and robustness. Fitness function is as follows:

$$Minimize\, f = \frac{\gamma}{PSNR(I,I')} + \frac{1}{SSIM(I,I')} + \frac{1}{\frac{1}{N}\sum_{i=1}^{N} NC_i(W,W')}, \tag{73}$$

where γ is used for balancing effect of PSNR.

In some papers, the authors use other metaheuristics. A robust watermarking method for high dynamic range images is presented by Bakhsh and Moghaddam (2018). An RGB-to-LogLUV transform is performed at the beginning of the embedding procedure to improve resistance to the tone mapping attacks. The watermark bits are embedded into the DWT coefficients. ABC is employed to find the best block for watermark embedding. The HDRVDP metric is used to calculate the fitness function (Mantiuk et al. 2011). Li et al. (2017) propose a watermarking approach for 3D scenes. A holographic watermark is embedded in a Multi-level Cellular Automata (MCA) transform and GA optimization is used to search for optimal embedding blocks. The objective function is calculated as follows:

$$Maximize\, f = PSNR(I,I') + \gamma_1 SSIM(I,I') + \gamma_2 \sum_{i=1}^{K} BCR_i\left(W,W'\right), \tag{74}$$

where K represents the number of watermarks, γ_1 and γ_2 are the weighting factors. Hemamalini and Nagarajan (2020) use DA to select suitable areas for embedding. The objective function is based on edge level, neighbourhood strength, gradient energy, and wavelet energy of the pixels. Lydia et al. (2021) combine Discrete Shearlet Transform (DST) and Discrete Curvelet Transform (DCurT) to form an embedding domain. Random GOA algorithm selects optimal DCurT coefficients for embedding. The optimization goal is to achieve the maximum value of the PSNR metric. Basu et al. (2022) use DE to look for an optimized location of the watermark in the spatial domain in order to embed it into the cognitively insignificant regions. The same scaling factor is used for both DE optimization and embedding and extracting operations. The value of the objective function is a vector whose elements are the sums of the squares of the pixel values for the corresponding lines of the image. Optimization is aimed at finding the minimum values of the target vector. Soppari and Chandra (2022) propose a blind digital image watermarking model based on the multi-objective hybrid metaheuristic-based clustering approach. Metaheuristic optimization is used for watermark region selection. The scheme combines SFO and BSO algorithms. The objective function is as follows:

$$Minimize\, f = \frac{1}{SSIM} + MSE + \frac{1}{PC}, \tag{75}$$

where PC (Pearson Coefficient) is the covariance of the two images divided by the product of their standard deviations. Garg and Kishore (2022b) optimize watermark embedding positions in a hybrid DWT-DCT domain using SGO. The objective function is defined by the following expression:

$$Maximize\, f = PSNR(I, I') + \alpha \times \sum_{i=1}^{N} NCC_i(W, W'), \tag{76}$$

where α is a weighting factor.

Shih et al. (2018) use PSO to find the optimal capacity. The content of the host image is automatically analyzed to determine the unchanging regions of interest. The rest of the image is used to embed the watermark. The objective function is calculated as follows:

$$Maximize\, f = \omega_1 Q + \omega_2 EC, \tag{77}$$

where ω_1, ω_2 are weighting factors, and EC is the number of bits to be embedded,

$$Q = \frac{2\mu_C \mu_S \times \sigma_{CS} \times \sigma_C \sigma_S}{\left(\mu_C^2 + \mu_S^2\right) \times \left(\sigma_C^2 + \sigma_S^2\right)}. \tag{78}$$

Embedding parameters optimization is a common task, however, in some cases, it is necessary to optimize extraction parameters. Anis et al. (2021) use ABC optimization in a watermarking scheme based on the QIM method. The authors investigate the model of the channel distortion and modify the extraction process to increase the robustness. The ABC algorithm is used to determine the optimal channel distortion parameters. The objective function is formed as follows:

$$Maximize\, f = \frac{1}{BER(R, \hat{R})}, \tag{79}$$

where R is a reference message (known sample of watermark), and $\hat{R}$ is the extracted reference message. Saadati et al. (2021) hide watermarks in the ST-SVD domain. WOA is used at the information extraction stage to optimize the scaling factor. The objective function is the PSNR between the original and extracted watermark.

Arsalan et al. (2017) propose a reversible watermarking technique for protecting medical data in the IWT domain. The key feature of this scheme is the use of high-frequency IWT coefficients compading before embedding to combat rounding errors. GP is used to find the companding factor, the fitness function is based on the PSNR metric.

Table 4 provides a summary of the reviewed studies.

4 Discussion

In this section, we analyze and discuss the results of the review, as well as highlight promising areas of research in the field of image data hiding.

Table 4 Other watermarking schemes based on metaheuristic optimization

Reference	Embedding domain	Metaheuristic	Optimization purpose	Performance indicators
Kazemivash and Moghaddam (2017)	LWT	FA	Bit arrangement selection	EC: 0.0039 bpp (GS) PSNR: 33.1430–39.1184 dB Robustness: high NC: 0.7681–1.0 BER: ≈ 0.0–0.4
Moeinaddini (2019)	HT	Distinct discrete FA	Bit arrangement selection	EC: 0.0156 bpp (GS) PSNR: 46.410–48.493 dB SSIM: 0.9924–0.9964 Robustness: high NC: 0.72–1.0
Bakhsh and Moghaddam (2018)	DWT	ABC	Bit arrangement selection	EC: 7.89×10^{-4}–0.0124 bpp (CLR) Robustness: high BER: 0.0–0.328
Li et al. (2017)	MCA	GA	Bit arrangement selection	EC: 2 bpp (CLR) PSNR: 33.79 dB SSIM: 0.9850 Robustness: low BCR: 0.6730–0.9143
Hemamalini and Nagarajan (2020)	DWT	DA	Bit arrangement selection	PSNR: 53.5305–60.8998 dB Robustness: low CC: 0.9367–0.9831
Lydia et al. (2021)	DST-DCurT	Random GOA	Bit arrangement selection	PSNR: 49.22–58.07 dB SSIM: 0.96–0.999 Robustness: low
Basu et al. (2022)	Spatial	DE	Bit arrangement selection	EC: 0.25 bpp (GS) PSNR: 57.0673–57.2301 dB SSIM: 0.9994–0.9999 Robustness: medium NC: 0.7661–0.8262
Soppari and Chandra (2022)	DWT	SFO and BSO	Bit arrangement selection	PSNR: 41.79–52.019 dB Robustness: low

Table 4 (continued)

Reference	Embedding domain	Metaheuristic	Optimization purpose	Performance indicators
Garg and Kishore (2022b)	DWT-DCT	SGO	Bit arrangement selection	EC: 0.0156 bpp (GS) PSNR: 43.3247–46.9499 dB Robustness: high NCC: 0.8268–1.0 BER: 0.0–0.0938
Shih et al. (2018)	DWT-SVD-DCT	PSO	Rate allocation	EC: 0.3467 bpp (GS) PSNR: 57.33 dB
Anis et al. (2021)	DWT	ABC	Extraction parameter selection	PSNR: 39.28–43.56 dB Robustness: medium BER: 0.0–0.376
Saadati et al. (2021)	ST-SVD	WOA	Extraction parameter selection	EC: 1.5 bpp (CLR) Robustness: high NCC: 0.5901–0.9976
Arsalan et al. (2017)	IWT	GP	Companding	EC: 0.1–0.7 bpp PSNR: 41.87–56.79 dB SSIM: 0.9707–0.9984

4.1 Analysis

We have considered 147 data hiding schemes based on metaheuristic optimization; 57 of them are steganography schemes (38.78%), and 90 are watermarking schemes (61.22%). The use of metaheuristic optimization to improve the efficiency of watermarking schemes is more common.

According to the review, 26 steganographic schemes (45.61%) perform embedding in the spatial domain (or bitstream), and 31 steganographic schemes (54.39%) perform embedding in the frequency domain. The spatial and frequency schemes of steganography use metaheuristic optimization in approximately equal proportions. The vast majority of watermarking schemes are frequency domain embedding schemes. Only three watermarking algorithms work in the spatial domain. This is mainly due to the fact that frequency embedding is more robust than spatial embedding, and watermarking efficiency directly depends on the robustness level.

Metaheuristics were used for the message bit arrangement optimization in 43 steganography schemes (75.44%). In 14 cases (24.56%), the authors used optimization algorithms to solve other problems, including data hiding method selection (1), neural network setup (2), scaling factor selection (1), secret message encryption (1), rate allocation (4), creating a hiding space (2), edge detection (2), and code mapping (1). Thus, in the field of steganography, metaheuristics are mainly used for the optimal message bit arrangement in the embedding area.

Optimization was used to select the scaling factor in 77 watermarking schemes (85.56%). In 13 cases (14.44%), the authors used metaheuristics to solve other problems, including bit arrangement selection (9), rate allocation (1), extraction parameter selection (2), companding (1). Thus, in the field of watermarking, metaheuristics are mainly used to optimize the scaling factor or embedding strength.

Figure 9 illustrates the proportion of the optimization purposes in the total number of studies. Summarizing the review of all research in the field of image data hiding based on metaheuristics, we can note the following main optimization purposes:

- scaling factor selection (78, 53.06%);
- bit arrangement selection (52, 35.38%);
- rate allocation (5, 3.40%);
- neural network setup (2, 1.36%);
- extraction parameter selection (2, 1.36%);
- creating a hiding space (2, 1.36%);
- edge detection (2, 1.36%);
- data hiding method selection (1, 0.68%);
- secret message encryption (1, 0.68%);
- companding (1, 0.68%);
- code mapping (1, 0.68%).

The reviewed studies use 40 different metaheuristics. It should be noted that we do not consider modifications as individual algorithms, and in the case of hybrid schemes, we consider each component separately.Steganography schemes use 23 different metaheuristics. Some authors use more than one metaheuristic in their schemes, so the total number of metaheuristic use cases is greater than the number of papers devoted to steganography, and is equal to 63 (48—bit arrangement selection and 15—others). Authors most often choose

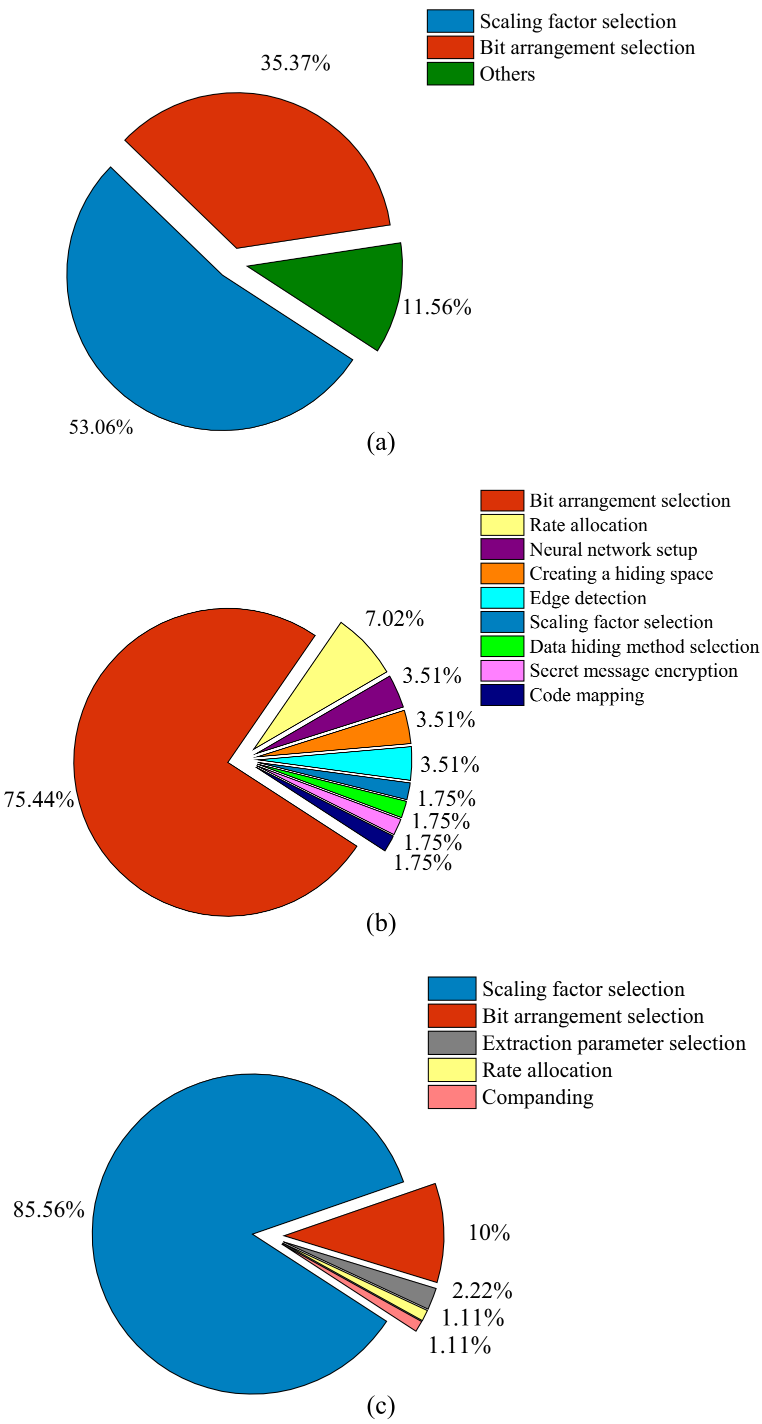


Fig. 9 Optimization purposes: among all studies (**a**); among steganography schemes (**b**); among watermarking schemes (**c**)

GA and PSO when developing steganography schemes. GA is used 19 times (30.16%), and PSO is used 14 times (22.22%). PSO is used to select the bit arrangement for steganography algorithms 12 times (25.00%), and GA is used to solve the same problem 11 times (22.92%). In the context of other optimization problems, PSO is used 2 times (13.33%) and GA is used 8 times (53.33%). This indicates the high flexibility of GA optimization, and the ability to adapt the algorithm to a variety of tasks. The other 21 metaheuristics are used in no more than three different studies. Figure 10a shows the frequency of using various metaheuristics for steganography embedding.

Image watermarking schemes use 28 metaheuristics. The total number of metaheuristic use cases is 106 (92—scaling factor selection and 14—others). PSO is the most popular algorithm among authors of watermarking methods and is used 29 times (27.36%). The second and third places are occupied by other algorithms based on swarm intelligence, in particular, ABC is used in 16 cases (15.09%) and FA is used in 11 cases (10.38%). The top three look similar among studies where optimization is applied to the scaling factor selection: PSO (28, 30.43%), ABC (14, 15.22%), and FA (9, 9.78%). Swarm intelligence algorithms are also popular in watermarking schemes for other optimization problems.

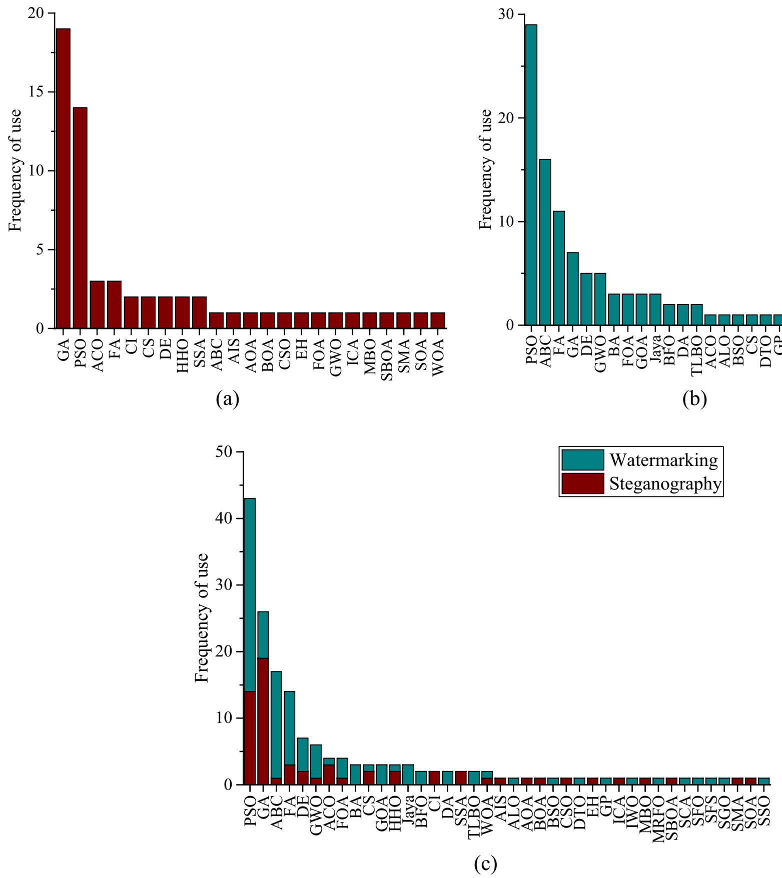


Fig. 10 Frequency of use of metaheuristics in image data hiding schemes: steganography (**a**); watermarking (**b**); all schemes (**c**)

However, their choice is not systematic. Figure 10b shows the frequency of using various metaheuristics for image watermarking.

Thus, the most popular strategy for applying metaheuristics for steganography is to find optimal embedding positions using GA or PSO. A popular metaheuristic-based watermarking strategy is to choose a scaling factor using PSO.

Figure 10c illustrates the use of metaheuristics for all of the studies. PSO is the most popular algorithm among authors of data hiding methods (43, 25.44%), GA comes in second (26, 15.38%), and ABC comes in third (17, 10.06%). These are classic metaheuristics. Since their development, a large number of studies have been published on the practical application of these optimization algorithms, including the estimation of optimization parameters. It is also worth noting that over the past 6 years there has been an increase in research interest in the use of metaheuristics to solve problems in the field of image data hiding. Figure 11 shows the frequency of use of metaheuristics in image data hiding schemes by year. As can be seen, there is a tendency to evaluate the performance of new optimization algorithms for data hiding. However, the proportion of classic algorithms such as PSO and GA remains high.

4.2 Promising areas of research

As the review shows, the use of metaheuristics to improve the efficiency of hiding data in digital images attract the attention of researchers, and interest in this topic has been growing in recent years. Here we formulate a list of promising research areas in the field of metaheuristic optimization application for image steganography and watermarking.

(1) *Comparing the efficiency of metaheuristics for data hiding areas* In most of the considered works, there is no detailed argumentation for the choice of one or another

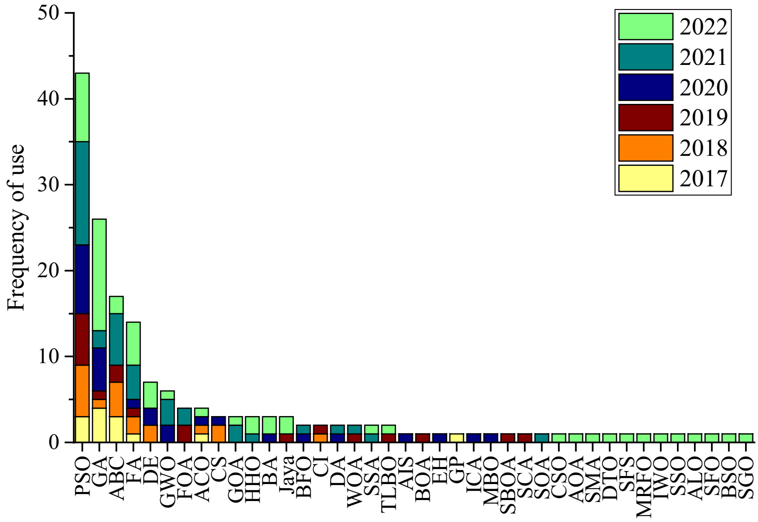


Fig. 11 Frequency of use of metaheuristics in image data hiding schemes by year

metaheuristic. However, it is obvious that different metaheuristics can demonstrate different efficiency in solving the same problem (Uma Maheswari and Jude Hemanth 2017; Thakkar and Srivastava 2019; Singh et al. 2021b). Comparison of the efficiency of different optimization algorithms on the example of one embedding algorithm or one class of embedding algorithms seems to be a promising task.

(2) *Combining metaheuristics* There are hybrid schemes that combine different metaheuristics to solve an optimization problem (Ambika and Biradar 2020; Pramanik et al. 2020). This approach provides flexibility in optimization settings and the ability to choose optimal solutions or close to them at different stages of the data hiding algorithm. The search for effective combinations of different metaheuristics can also be considered as a possible direction of research.

(3) *Evaluation of efficiency dependence on objective function* Basically, the authors use the classical embedding imperceptibility and robustness metrics and their combinations to construct the objective function. However, the design of the objective function can have a significant impact on the optimization quality. Evaluation of the efficiency for different objective functions in solving one problem seems to be a promising research direction. The object of study can be both the construction of the objective function and the setting of weight coefficients, which are often used in composite objective functions. New objective functions may include, for example, different metrics of similarity of pixel histograms and frequency coefficients before and after embedding, blockiness, image quality index, and others. It is expedient to evaluate the efficiency of new objective functions both for different embedding operations and for different embedding domains.

(4) *Increasing the robustness of steganography schemes and their resistance to steganalysis* Many authors use PSNR and MSE metrics as objective functions to maximize embedding imperceptibility. However, improving robustness can significantly increase the practical applicability of embedding schemes, and inclusion of robustness metrics in the objective function is relevant not only for watermarking schemes, but also for steganography. Another interesting approach is to increase the resistance of embedding to steganalysis using metaheuristic optimization. In the considered studies, resistance to steganalysis is mainly determined by the basic embedding method (basic operation), and optimization is aimed at improving the visual invisibility of embedding. The development of new constructions of objective functions, which include statistical invisibility metrics, is a promising direction.

(5) *Adjustment of the metaheuristic optimization algorithm parameters* The efficiency of finding the best solution depends on the choice of metaheuristic parameters, such as population size, number of generations, and others. However, in some of the considered works, the authors do not indicate the optimization parameters, and also do not present the results of experiments to estimate the best parameter values. Such an experimental study can determine the appropriate parameter values for various metaheuristics and optimization problems.

(6) *Application of new metaheuristics in data hiding tasks* In recent years, the authors of various studies have often turned to new algorithms for metaheuristic optimization. However, the pace of creation of new metaheuristics and effective modifications of known metaheuristics is far ahead of the pace of new data hiding scheme development. Thus, performance evaluation of metaheuristic optimization algorithms developed in recent years for steganography and watermarking is a promising area of research. Researchers should focus not only on the assessment of imperceptibility, robustness and other indicators of the embedding quality, but also on the assessment of the statistical

significance of the results obtained using metaheuristics, the assessment of convergence, the relationship between the obtained increase in efficiency and computational complexity.

(7) *Development of new metaheuristics* It should be noted that the growing interest in the use of metaheuristic optimization in solving any scientific and applied problems indicates the high relevance of the development of new metaheuristics. As shown in Fig. 11, researchers have increasingly used new algorithms, the applicability of which for steganography and watermarking has not yet been evaluated. The development of new metaheuristics will allow researchers to find new options for solving the problems of embedding additional information in digital images.

5 Conclusion

The use of metaheuristic optimization to improve the efficiency of image data hiding schemes is quite widespread. A review of current studies showed that this area is actively developing at the present time. Steganography algorithms mainly use metaheuristics to choose the best location of the secret message bits in the cover image. Watermarking schemes mainly apply metaheuristic optimization to find the optimal scaling factor. Authors often use well-known metaheuristics in their schemes, such as GA and PSO. Recently, the use of new metaheuristics has also been noted.

The data hiding schemes of recent years show high rates of embedding efficiency. However, some problems associated with the development, configuration and application of metaheuristics for data hiding have not yet been solved. Based on the results of the review, we noted a number of promising areas that may be interest to researchers in the field of image steganography and watermarking. We expect that the trend towards an increase in the number of studies combining image data hiding and metaheuristic optimization will continue, and new effective solutions will be obtained in the future.

Acknowledgements This research was funded by Russian Science Foundation, project No 21-71-10113. We are very grateful to the anonymous referees for their constructive comments and helpful suggestions to improve the quality of this paper.

Data availability Data sharing not applicable to this article as no datasets were generated or analyzed during the current study.

Declarations

Conflict of interest The authors declare that they have no conflict of interest.

References

Abdelhakim AM, Saad MH, Sayed M, Saleh HI (2018) Optimized SVD-based robust watermarking in the fractional Fourier domain. Multimed Tools Appl 77:27895–27917. https://doi.org/10.1007/s11042-018-6014-5

Abedinia O, Amjady N, Ghasemi A (2016) A new metaheuristic algorithm based on shark smell optimization. Complexity 21:97–116. https://doi.org/10.1002/cplx.21634

Abdul Khalid NE, Md Ariff N, Yahya S, Mohamed Noor N (2011) A review of bio-inspired algorithms as image processing techniques. Commun Comput Inf Sci 179:660–673. https://doi.org/10.1007/978-3-642-22170-5_57

Abdulrahman AK, Ozturk S (2019) A novel hybrid DCT and DWT based robust watermarking algorithm for color images. Multimed Tools Appl 78:17027–17049. https://doi.org/10.1007/s11042-018-7085-z
Ahmadi SBB, Zhang G, Rabbani M et al (2021a) An intelligent and blind dual color image watermarking for authentication and copyright protection. Appl Intell 51:1701–1732. https://doi.org/10.1007/s10489-020-01903-0
Ahmadi SBB, Zhang G, Wei S, Boukela L (2021b) An intelligent and blind image watermarking scheme based on hybrid SVD transforms using human visual system characteristics. Vis Comput 37:385–409. https://doi.org/10.1007/s00371-020-01808-6
Akay B, Karaboga D (2015) A survey on the applications of artificial bee colony in signal, image, and video processing. SIViP 9:967–990. https://doi.org/10.1007/s11760-015-0758-4
Akyol S, Alatas B (2017) Plant intelligence based metaheuristic optimization algorithms. Artif Intell Rev 47:417–462. https://doi.org/10.1007/s10462-016-9486-6
Ali M, Ahn CW (2018) An optimal image watermarking approach through cuckoo search algorithm in wavelet domain. Int J Syst Assur Eng Manage 9:602–611. https://doi.org/10.1007/s13198-014-0288-4
Ali M, Ahn CW, Pant M et al (2020) An optimized digital watermarking scheme based on invariant DC coefficients in spatial domain. Electronics 9:1428. https://doi.org/10.3390/electronics9091428
Almawgani AHM, Alhawari ARH, Hindi AT et al (2022) Hybrid image steganography method using Lempel Ziv Welch and genetic algorithms for hiding confidential data. Multidimension Syst Signal Process 33:561–578. https://doi.org/10.1007/s11045-021-00793-w
Alonso FR, Oliveira DQ, Zambroni De Souza AC (2015) Artificial immune systems optimization approach for multiobjective distribution system reconfiguration. IEEE Trans Power Syst 30:840–847. https://doi.org/10.1109/TPWRS.2014.2330628
AlSabhany AA, Ali AH, Ridzuan F et al (2020) Digital audio steganography: systematic review, classification, and analysis of the current state of the art. Comput Sci Rev 38:100316. https://doi.org/10.1016/j.cosrev.2020.100316
Alsalhi Y (2019) An accurate and high-efficient QuBits steganography scheme based on hybrid neural networks. Multimed Tools Appl 78:17077–17093. https://doi.org/10.1007/s11042-018-7061-7
Altay ŞY, Ulutaş G (2021) Self-adaptive step firefly algorithm based robust watermarking method in DWT-SVD domain. Multimed Tools Appl 80:23457–23484. https://doi.org/10.1007/s11042-020-10251-7
Ambika, Biradar RL (2020) Secure medical image steganography through optimal pixel selection by EH-MB pipelined optimization technique. Health Technol 10:231–247. https://doi.org/10.1007/s12553-018-00289-x
Ambika, Biradar RL, Burkpalli V (2019) Encryption-based steganography of images by multiobjective whale optimal pixel selection. Int J Comput Appl. https://doi.org/10.1080/1206212X.2019.1692442
Ambika, Virupakshappa, Lim S-J (2022) Hybrid image embedding technique using Steganographic Signcryption and IWT-GWO methods. Microprocess Microsyst. https://doi.org/10.1016/j.micpro.2022.104688
Amsaveni A, Bharathi M (2021) Use of firefly optimization algorithm for fractional fourier transform based reversible data hiding. J Intell Fuzzy Syst 40:415–425. https://doi.org/10.3233/JIFS-191911
Anand A, Singh AK (2020) An improved DWT-SVD domain watermarking for medical information security. Comput Commun 152:72–80. https://doi.org/10.1016/j.comcom.2020.01.038
Anand A, Singh AK (2022) Hybrid nature-inspired optimization and encryption-based watermarking for E-healthcare. IEEE Trans Comput Soc Syst. https://doi.org/10.1109/TCSS.2022.3140862
Andriotis P, Oikonomou G, Tryfonas T (2013) JPEG steganography detection with Benford's Law. Digit Investig 9:246–257. https://doi.org/10.1016/j.diin.2013.01.005
Anis K, Zied K, Anis S (2021) A reframed watermark extraction approach using the ABC algorithm. Chin J Electron 30:736–742. https://doi.org/10.1049/cje.2021.05.016
Ansari IA, Pant M (2017) Multipurpose image watermarking in the domain of DWT based on SVD and ABC. Pattern Recogn Lett 94:228–236. https://doi.org/10.1016/j.patrec.2016.12.010
Ansari IA, Pant M (2018) Quality assured and optimized image watermarking using artificial bee colony. Int J Syst Assur Eng Manage 9:274–286. https://doi.org/10.1007/s13198-016-0568-2
Ansari IA, Pant M, Ahn CW (2017) Artificial bee colony optimized robust-reversible image watermarking. Multimed Tools Appl 76:18001–18025. https://doi.org/10.1007/s11042-016-3680-z
Ariatmanto D, Ernawan F (2020) An improved robust image watermarking by using different embedding strengths. Multimed Tools Appl 79:12041–12067. https://doi.org/10.1007/s11042-019-08338-x
Arsalan M, Qureshi AS, Khan A, Rajarajan M (2017) Protection of medical images and patient related information in healthcare: using an intelligent and reversible watermarking technique. Appl Soft Comput 51:168–179. https://doi.org/10.1016/j.asoc.2016.11.044
Awasthi D, Srivastava VK (2022) LWT-DCT-SVD and DWT-DCT-SVD based watermarking schemes with their performance enhancement using Jaya and Particle swarm optimization and comparison

of results under various attacks. Multimed Tools Appl 81:25075–25099. https://doi.org/10.1007/s11042-022-12456-4
Azad AS, Rahaman MSA, Watada J et al (2020) Optimization of the hydropower energy generation using meta-heuristic approaches: a review. Energy Rep 6:2230–2248. https://doi.org/10.1016/j.egyr.2020.08.009
Bai Y, Jiang G, Zhu Z et al (2021) Reversible data hiding scheme for high dynamic range images based on multiple prediction error expansion. Signal Process: Image Commun 91:116084. https://doi.org/10.1016/j.image.2020.116084
Bakhsh FY, Moghaddam ME (2018) A robust HDR images watermarking method using artificial bee colony algorithm. J Inf Secur Appl 41:12–27. https://doi.org/10.1016/j.jisa.2018.05.003
Balasamy K, Ramakrishnan S (2019) An intelligent reversible watermarking system for authenticating medical images using Wavelet and PSO. Cluster Comput 22:4431–4442. https://doi.org/10.1007/s10586-018-1991-8
Banharnsakun A (2018) Artificial bee colony approach for enhancing LSB based image steganography. Multimed Tools Appl 77:27491–27504. https://doi.org/10.1007/s11042-018-5933-5
Bansal M, Mishra A, Sharma A (2022) Multiple scaling Fuzzy-PSO watermarking scheme for gray-scale and colored images. Multimed Tools Appl 81:15219–15248. https://doi.org/10.1007/s11042-022-12526-7
Barlaskar SA, Singh SV, Anish MK, Laskar RH (2022) Genetic algorithm based optimized watermarking technique using hybrid DCNN-SVR and statistical approach for watermark extraction. Multimed Tools Appl 81:7461–7500. https://doi.org/10.1007/s11042-021-11798-9
Basu S, Debnath A, Basu A, Das TS (2022) An image data hiding technique using differential evolution. Multimed Tools Appl 81:39995–40012. https://doi.org/10.1007/s11042-022-12557-0
Ben Ali YM (2019) Smell Bees Optimization for new embedding steganographic scheme in spatial domain. Swarm Evol Comput 44:584–596. https://doi.org/10.1016/j.swevo.2018.08.003
Biswas R, Bandyapadhay SK (2020) Random selection based GA optimization in 2D-DCT domain color image steganography. Multimed Tools Appl 79:7101–7120. https://doi.org/10.1007/s11042-019-08497-x
Cedillo-Hernandez M, Cedillo-Hernandez A, Garcia-Ugalde FJ (2021) Improving DFT-based image watermarking using particle swarm optimization algorithm. Mathematics 9:1795. https://doi.org/10.3390/math9151795
Chacko A, Chacko S (2022) Deep learning-based robust medical image watermarking exploiting DCT and Harris hawks optimization. Int J Intell Syst 37:4810–4844. https://doi.org/10.1002/int.22742
Chakravarthy S, Jagannathan MA, Ranjani JJ et al (2019) An optimized hierarchical encryption technique for tamper recognition. Multimed Tools Appl 78:18693–18712. https://doi.org/10.1007/s11042-019-7265-5
Chang Q, Li X, Zhao Y, Ni R (2021) Adaptive pairwise prediction-error expansion and multiple histograms modification for reversible data hiding. IEEE Trans Circuits Syst Video Technol 31:4850–4863. https://doi.org/10.1109/TCSVT.2021.3055612
Chauhan DS, Singh AK, Kumar B, Saini JP (2019) Quantization based multiple medical information watermarking for secure e-health. Multimed Tools Appl 78:3911–3923. https://doi.org/10.1007/s11042-017-4886-4
Cheddad A, Condell J, Curran K, Mc Kevitt P (2010) Digital image steganography: survey and analysis of current methods. Signal Process 90:727–752. https://doi.org/10.1016/j.sigpro.2009.08.010
Cheema AM, Adnan SM, Mehmood Z (2020) A novel optimized semi-blind scheme for color image watermarking. IEEE Access 8:169525–169547. https://doi.org/10.1109/ACCESS.2020.3024181
Chen B, Wornell GW (2001) Quantization index modulation: a class of provably good methods for digital watermarking and information embedding. IEEE Trans Inf Theory 47:1423–1443. https://doi.org/10.1109/18.923725
Chen T, Zhu Y, Teng J (2018) Beetle swarm optimisation for solving investment portfolio problems. J Eng 2018:1600–1605. https://doi.org/10.1049/joe.2018.8287
Chen T-S, Hou K-N, Beh W-K, Wu A-Y (2019) Low-complexity compressed-sensing-based watermark cryptosystem and circuits implementation for wireless sensor networks. IEEE Trans Very Large Scale Integr (VLSI) Syst 27:2485–2497. https://doi.org/10.1109/TVLSI.2019.2933722
Cheng R, Jin Y (2015) A competitive swarm optimizer for large scale optimization. IEEE Trans Cybern 45:191–204. https://doi.org/10.1109/TCYB.2014.2322602
Cui X, Niu Y, Zheng X, Han Y (2018) An optimized digital watermarking algorithm in wavelet domain based on differential evolution for color image. PLoS ONE 13:e0196306. https://doi.org/10.1371/journal.pone.0196306
Dai C, Chen W, Zhu Y, Zhang X (2009) Seeker optimization algorithm for optimal reactive power dispatch. IEEE Trans Power Syst 24:1218–1231. https://doi.org/10.1109/TPWRS.2009.2021226

Dalal M, Juneja M (2021) A survey on information hiding using video steganography. Artif Intell Rev 54:5831–5895. https://doi.org/10.1007/s10462-021-09968-0
Dappuri B, Rao MP, Sikha MB (2020) Non-blind RGB watermarking approach using SVD in translation invariant wavelet space with enhanced Grey-wolf optimizer. Multimed Tools Appl 79:31103–31124. https://doi.org/10.1007/s11042-020-09433-0
Das S, Biswas A, Dasgupta S, Abraham A (2009) Bacterial foraging optimization algorithm: theoretical foundations, analysis, and applications. Stud Comput Intell 203:23–55. https://doi.org/10.1007/978-3-642-01085-9_2
Deb K (2000) An efficient constraint handling method for genetic algorithms. Comput Methods Appl Mech Eng 186:311–338. https://doi.org/10.1016/S0045-7825(99)00389-8
Devi KJ, Singh P, Dash JK et al (2022a) A new robust and secure 3-level digital image watermarking method based on G-BAT hybrid optimization. Mathematics. https://doi.org/10.3390/math10163015
Devi KJ, Singh P, Thakkar HK, Kumar N (2022b) Robust and secured watermarking using Ja-Fi optimization for digital image transmission in social media. Appl Soft Comput. https://doi.org/10.1016/j.asoc.2022.109781
Dhawan S, Chakraborty C, Frnda J et al (2021) SSII: secured and high-quality steganography using intelligent hybrid optimization algorithms for IoT. IEEE Access 9:87563–87578. https://doi.org/10.1109/ACCESS.2021.3089357
Dhawan S, Gupta R, Bhuyan HK et al (2022) An efficient steganography technique based on S2OA & DESAE model. Multimed Tools Appl. https://doi.org/10.1007/s11042-022-13798-9
Ding X, Xie Y, Li P et al (2020) Image steganography based on artificial immune in mobile edge computing with internet of things. IEEE Access 8:136186–136197. https://doi.org/10.1109/ACCESS.2020.3010513
Dittmann J, Megías D, Lang A, Herrera-Joancomartí J (2006) Theoretical framework for a practical evaluation and comparison of audio watermarking schemes in the triangle of robustness, transparency and capacity. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 4300 LNCS, 1–40. https://doi.org/10.1007/11926214_1
Dorigo M, Birattari M, Stützle T (2006) Ant colony optimization artificial ants as a computational intelligence technique. IEEE Comput Intell Mag 1:28–39. https://doi.org/10.1109/CI-M.2006.248054
Du Y, Yin Z (2022) New framework for code-mapping-based reversible data hiding in JPEG images. Inf Sci 609:319–338. https://doi.org/10.1016/j.ins.2022.07.071
Dubey N, Modi H (2021) A robust discrete wavelet transform based adaptive watermarking scheme in ycbcr color space against camcorder recording in cinema/movie theatres. Eng Sci 15:116–128. https://doi.org/10.30919/es8d491
Elhoseny M, Ramírez-González G, Abu-Elnasr OM et al (2018) Secure medical data transmission model for IoT-based healthcare systems. IEEE Access 6:20596–20608. https://doi.org/10.1109/ACCESS.2018.2817615
El-Kenawy E-SM, Khodadadi N, Khoshnaw A et al (2022) Advanced dipper-throated meta-heuristic optimization algorithm for digital image watermarking. Appl Sci (switzerland). https://doi.org/10.3390/app122010642
Eshmawi AA, Alsuhibany SA, Abdel-Khalek S, Mansour RF (2022) Competitive swarm optimization with encryption based steganography for digital i.security. Comput Mater Contin 72:4173–4184. https://doi.org/10.32604/cmc.2022.028008
Evsutin O, Melman A, Meshcheryakov R (2020) Digital steganography and watermarking for digital images: a review of current research directions. IEEE Access 8:166589–166611. https://doi.org/10.1109/ACCESS.2020.3022779
Fan X, Sayers W, Zhang S et al (2020) Review and classification of bio-inspired algorithms and their applications. J Bionic Eng 17:611–631. https://doi.org/10.1007/s42235-020-0049-9
Fathi-Kazerooni S, Rojas-Cessa R (2020) GAN tunnel: network traffic steganography by using GANs to counter internet traffic classifiers. IEEE Access 8:125345–125359. https://doi.org/10.1109/ACCESS.2020.3007577
Fridrich J, Goljan M, Du R (2001) Detecting LSB steganography in color, and gray-scale images. IEEE Multimed 8:22–28. https://doi.org/10.1109/93.959097
Gandomi AH, Yang X-S, Alavi AH (2013) Cuckoo search algorithm: a metaheuristic approach to solve structural optimization problems. Eng Comput 29:17–35. https://doi.org/10.1007/s00366-011-0241-y
Ganguly NM, Paul G, Saha SK, Burman D (2020) A PVD based high capacity steganography algorithm with embedding in non-sequential position. Multimed Tools Appl 79:13449–13479. https://doi.org/10.1007/s11042-019-08178-9

Gao H, Chen Q (2021) A robust and secure image watermarking scheme using SURF and improved Artificial Bee Colony algorithm in DWT domain. Optik 242:166954. https://doi.org/10.1016/j.ijleo.2021.166954

Garg P, Kishore RR (2022a) An efficient and secured blind image watermarking using ABC optimization in DWT and DCT domain. Multimed Tools Appl 81:36947–36964. https://doi.org/10.1007/s11042-021-11237-9

Garg P, Kishore RR (2022b) A robust and secured adaptive image watermarking using social group optimization. Visual Comput. https://doi.org/10.1007/s00371-022-02631-x

Gomes GF, da Cunha SS Jr, Ancelotti AC Jr (2019) A sunflower optimization (SFO) algorithm applied to damage identification on laminated composite plates. Eng Comput 35:619–626. https://doi.org/10.1007/s00366-018-0620-8

Gurunathan K, Rajagopalan SP (2020) A stegano—visual cryptography technique for multimedia security. Multimed Tools Appl 79:3893–3911. https://doi.org/10.1007/s11042-019-7471-1

Halim AH, Ismail I, Das S (2021) Performance assessment of the metaheuristic optimization algorithms: an exhaustive review. Artif Intell Rev 54:2323–2409. https://doi.org/10.1007/s10462-020-09906-6

Hameed MA, Abdel-Aleem OA, Hassaballah M (2022) A secure data hiding approach based on least-significant-bit and nature-inspired optimization techniques. J Ambient Intell Human Comput. https://doi.org/10.1007/s12652-022-04366-y

Hanizan HS, Din R, Hafiza AS et al (2017) A review of artificial intelligence techniques in image steganography domain. J Eng Sci Technol 12:103–113

Hasan N, Islam MS, Chen W et al (2021) Encryption based image watermarking algorithm in 2DWT-DCT domains. Sensors 21:5540. https://doi.org/10.3390/s21165540

Hashim FA, Hussain K, Houssein EH et al (2021) Archimedes optimization algorithm: a new metaheuristic algorithm for solving optimization problems. Appl Intell 51:1531–1551. https://doi.org/10.1007/s10489-020-01893-z

Hassaballah M, Hameed MA, Awad AI, Muhammad K (2021) A novel image steganography method for industrial internet of things security. IEEE Trans Ind Inf 17:7743–7751. https://doi.org/10.1109/TII.2021.3053595

Heidari AA, Mirjalili S, Faris H et al (2019) Harris hawks optimization: algorithm and applications. Future Gener Comput Syst 97:849–872. https://doi.org/10.1016/j.future.2019.02.028

Hemamalini B, Nagarajan V (2020) Wavelet transform and pixel strength-based robust watermarking using dragonflyoptimization. Multimed Tools Appl 79:8727–8746. https://doi.org/10.1007/s11042-018-6096-0

Hossain S, Mukhopadhyay S, Ray B et al (2022) A secured image steganography method based on ballot transform and genetic algorithm. Multimed Tools Appl 81:38429–38458. https://doi.org/10.1007/s11042-022-13158-7

Hsu L-Y, Hu H-T (2020) Blind watermarking for color images using EMMQ based on QDFT. Expert Syst Appl 149:113225. https://doi.org/10.1016/j.eswa.2020.113225

Hsu L-Y, Hu H-T (2021) QDCT-based blind color image watermarking with aid of GWO and DnCNN for performance improvement. IEEE Access 9:155138–155152. https://doi.org/10.1109/ACCESS.2021.3127917

Hsu L-Y, Hu H-T, Chou H-H (2022) A high-capacity QRD-based blind color image watermarking algorithm incorporated with AI technologies. Expert Syst Appl. https://doi.org/10.1016/j.eswa.2022.117134

Huang H-C, Pan J-S, Huang Y-H et al (2007) Progressive watermarking techniques using genetic algorithms. Circuits Syst Signal Process 26:671–687. https://doi.org/10.1007/s00034-006-0104-z

Huang H-C, Chang F-C, Chen Y-H, Chu S-C (2015) Survey of bio-inspired computing for information hiding. J Inf Hiding Multimed Signal Process 6:430–443

Hussain K, Mohd Salleh MN, Cheng S, Shi Y (2019) Metaheuristic research: a comprehensive survey. Artif Intell Rev 52:2191–2233. https://doi.org/10.1007/s10462-017-9605-z

Jaradat A, Taqieddin E, Mowafi M (2021) A high-capacity image steganography method using chaotic particle swarm optimization. Secur Commun Netw 2021:e6679284. https://doi.org/10.1155/2021/6679284

Jaya Prakash S, Mahalakshmi K (2022) Improved reversible data hiding scheme employing dual image-based least significant bit matching for secure image communication using style transfer. Visual Comput 38:4129–4150. https://doi.org/10.1007/s00371-021-02285-1

Jeevitha S, Amutha Prabha N (2020) Effective payload and improved security using HMT Contourlet transform in medical image steganography. Health Technol 10:217–229. https://doi.org/10.1007/s12553-018-00285-1

Johnvictor AC, Amalanathan AJ, Pariti Venkata RM, Jethi N (2022) Critical review of bio-inspired data optimization techniques: an image steganalysis perspective. Wiley Interdisc Rev: Data Min Knowl Discov. https://doi.org/10.1002/widm.1460

Jude Hemanth D, Anitha J, Popescu DE, Son LH (2018) A modified genetic algorithm for performance improvement of transform based image steganography systems. J Intell Fuzzy Syst 35:197–209. https://doi.org/10.3233/JIFS-169580

Kadhim IJ, Premaratne P, Vial PJ, Halloran B (2019) Comprehensive survey of image steganography: techniques, evaluations, and trends in future research. Neurocomputing 335:299–326. https://doi.org/10.1016/j.neucom.2018.06.075

Kang X, Chen Y, Zhao F, Lin G (2020) Multi-dimensional particle swarm optimization for robust blind image watermarking using intertwining logistic map and hybrid domain. Soft Comput 24:10561–10584. https://doi.org/10.1007/s00500-019-04563-6

Kapadia AM, Nithyanandam P (2022) A review: reversible information hiding and bio-inspired optimization. Lect Notes Electr Eng 806:489–506. https://doi.org/10.1007/978-981-16-6448-9_48

Karaboga D, Basturk B (2007) A powerful and efficient algorithm for numerical function optimization: artificial bee colony (ABC) algorithm. J Glob Optim 39:459–471. https://doi.org/10.1007/s10898-007-9149-x

Karakus S, Avci E (2020) A new image steganography method with optimum pixel similarity for data hiding in medical images. Med Hypotheses 139:109691. https://doi.org/10.1016/j.mehy.2020.109691

Kasana G, Kasana SS (2017) Reference based semi blind image watermarking scheme in wavelet domain. Optik 142:191–204. https://doi.org/10.1016/j.ijleo.2017.05.027

Kasana G, Singh K, Bhatia SS (2017) Data hiding using lifting scheme and genetic algorithm. Int J Inf Comput Secur 9:271–287. https://doi.org/10.1504/IJICS.2017.087561

Kazemivash B, Moghaddam ME (2017) A robust digital image watermarking technique using lifting wavelet transform and firefly algorithm. Multimed Tools Appl 76:20499–20524. https://doi.org/10.1007/s11042-016-3962-5

Kazemivash B, Moghaddam ME (2018) A predictive model-based image watermarking scheme using Regression Tree and Firefly algorithm. Soft Comput 22:4083–4098. https://doi.org/10.1007/s00500-017-2617-4

Khan S (2018) Ant Colony Optimization (ACO) based data hiding in image complex region. Int J Electr Comput Eng (IJECE) 8:379–389. https://doi.org/10.11591/ijece.v8i1.pp379-389

Khan S, Irfan MA, Khan K et al (2020) ACO based variable least significant bits data hiding in edges using IDIBS algorithm. Symmetry 12:781. https://doi.org/10.3390/sym12050781

Khari M, Garg AK, Gandomi AH et al (2020) Securing data in internet of things (IoT) using cryptography and steganography techniques. IEEE Trans Syst Man Cybern: Syst 50:73–80. https://doi.org/10.1109/TSMC.2019.2903785

Koley S (2022) Bat optimized 3D anaglyph image watermarking based on maximum noise fraction in the digital Shearlet domain. Multimed Tools Appl 81:19491–19523. https://doi.org/10.1007/s11042-021-11861-5

Koza JR (1994) Genetic programming as a means for programming computers by natural selection. Stat Comput 4:87–112. https://doi.org/10.1007/BF00175355

Kulkarni AJ, Baki MF, Chaouch BA (2016) Application of the cohort-intelligence optimization method to three selected combinatorial optimization problems. Eur J Oper Res 250:427–447. https://doi.org/10.1016/j.ejor.2015.10.008

Kumar S, Singh BK, Yadav M (2020) A Recent survey on multimedia and database watermarking. Multimed Tools Appl 79:20149–20197. https://doi.org/10.1007/s11042-020-08881-y

Kumar S, Singh MK, Saini D (2021) An image watermarking framework based on PSO and FrQWT. J Discr Math Sci Cryptogr 24:1293–1308. https://doi.org/10.1080/09720529.2021.1936901

Kumar S, Gupta A, Walia GS (2022) Reversible data hiding: a contemporary survey of state-of-the-art, opportunities and challenges. Appl Intell 52:7373–7406. https://doi.org/10.1007/s10489-021-02789-2

Kumari R, Mustafi A (2022) The spatial frequency domain designated watermarking framework uses linear blind source separation for intelligent visual signal processing. Front Neurorobot. https://doi.org/10.3389/fnbot.2022.1054481

Laxmanika, Singh PK (2022) Robust and imperceptible image watermarking technique based on SVD, DCT, BEMD and PSO in wavelet domain. Multimed Tools Appl 81:22001–22026. https://doi.org/10.1007/s11042-021-11246-8

Lei B, Zhao X, Lei H et al (2019) Multipurpose watermarking scheme via intelligent method and chaotic map. Multimed Tools Appl 78:27085–27107. https://doi.org/10.1007/s11042-017-4743-5

Li Z, He Y (2018) Steganography with pixel-value differencing and modulus function based on PSO. J Inf Secur Appl 43:47–52. https://doi.org/10.1016/j.jisa.2018.10.006

Li M, Li Y (2017) Histogram shifting in encrypted images with public key cryptosystem for reversible data hiding. Signal Process 130:190–196. https://doi.org/10.1016/j.sigpro.2016.07.002

Li X-W, Liu Y, Kim S-T, Wang Q-H (2017) Designing a genetic watermarking approach for 3D scenes. Opt Lasers Eng 93:83–91. https://doi.org/10.1016/j.optlaseng.2017.01.013
Li J, Lin Q, Yu C et al (2018) A QDCT- and SVD-based color image watermarking scheme using an optimized encrypted binary computer-generated hologram. Soft Comput 22:47–65. https://doi.org/10.1007/s00500-016-2320-x
Li S, Chen H, Wang M et al (2020) Slime mould algorithm: a new method for stochastic optimization. Future Gener Comput Syst 111:300–323. https://doi.org/10.1016/j.future.2020.03.055
Li Y-M, Wei D, Zhang L (2021) Double-encrypted watermarking algorithm based on cosine transform and fractional Fourier transform in invariant wavelet domain. Inf Sci 551:205–227. https://doi.org/10.1016/j.ins.2020.11.020
Liao X, Peng J, Cao Y (2021) GIFMarking: the robust watermarking for animated GIF based deep learning. J vis Commun Image Represent 79:103244. https://doi.org/10.1016/j.jvcir.2021.103244
Lin J-L, Tsai Y-H, Yu C-Y, Li M-S (2012) Interaction enhanced imperialist competitive algorithms. Algorithms 5:433–448. https://doi.org/10.3390/a5040433
Liu X-L, Lin C-C, Yuan S-M (2018) Blind dual watermarking for color images' authentication and copyright protection. IEEE Trans Circuits Syst Video Technol 28:1047–1055. https://doi.org/10.1109/TCSVT.2016.2633878
Liu J, Huang J, Luo Y et al (2019) An optimized image watermarking method based on HD and SVD in DWT domain. IEEE Access 7:80849–80860. https://doi.org/10.1109/ACCESS.2019.2915596
Lu J, Zhang W, Deng Z et al (2021) Research on information steganography based on network data stream. Neural Comput Appl 33:851–866. https://doi.org/10.1007/s00521-020-05260-4
Lydia EL, Raj JS, Pandi Selvam R et al (2021) Application of discrete transforms with selective coefficients for blind image watermarking. Trans Emerg Telecommun Technol 32:e3771. https://doi.org/10.1002/ett.3771
Mahto DK, Singh AK (2022) Firefly optimization-based dual watermarking for colour images with improved capacity. Multimed Tools Appl. https://doi.org/10.1007/s11042-022-13795-y
Mahto DK, Anand A, Singh AK (2022) Hybrid optimisation-based robust watermarking using denoising convolutional neural network. Soft Comput 26:8105–8116. https://doi.org/10.1007/s00500-022-07155-z
Makbol NM, Khoo BE, Rassem TH, Loukhaoukha K (2017) A new reliable optimized image watermarking scheme based on the integer wavelet transform and singular value decomposition for copyright protection. Inf Sci 417:381–400. https://doi.org/10.1016/j.ins.2017.07.026
Malik A, Sikka G, Verma HK (2017) A high capacity text steganography scheme based on LZW compression and color coding. Eng Sci Technol Int J 20:72–79. https://doi.org/10.1016/j.jestch.2016.06.005
Mandal PC, Mukherjee I, Paul G, Chatterji BN (2022) Digital image steganography: a literature survey. Inf Sci 609:1451–1488. https://doi.org/10.1016/j.ins.2022.07.120
Mantiuk R, Kim KJ, Rempel AG, Heidrich W (2011) HDR-VDP-2: a calibrated visual metric for visibility and quality predictions in all luminance conditions. ACM Trans Graph 30(4):1–14. https://doi.org/10.1145/2010324.1964935
Mehbodniya A, Douraki BK, Webber JL et al (2022) Multilayer reversible data hiding based on the difference expansion method using multilevel thresholding of host images based on the slime mould algorithm. Processes. https://doi.org/10.3390/pr10050858
Mehrabian AR, Lucas C (2006) A novel numerical optimization algorithm inspired from weed colonization. Ecol Inform 1:355–366. https://doi.org/10.1016/j.ecoinf.2006.07.003
Mellimi S, Rajput V, Ansari IA, Ahn CW (2021) A fast and efficient image watermarking scheme based on Deep Neural Network. Pattern Recogn Lett 151:222–228. https://doi.org/10.1016/j.patrec.2021.08.015
Mirjalili S (2015) The ant lion optimizer. Adv Eng Softw 83:80–98. https://doi.org/10.1016/j.advengsoft.2015.01.010
Mirjalili S (2016a) Dragonfly algorithm: a new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems. Neural Comput Appl 27:1053–1073. https://doi.org/10.1007/s00521-015-1920-1
Mirjalili S (2016b) SCA: a sine cosine algorithm for solving optimization problems. Knowl-Based Syst 96:120–133. https://doi.org/10.1016/j.knosys.2015.12.022
Mirjalili S, Lewis A (2016) The whale optimization algorithm. Adv Eng Softw 95:51–67. https://doi.org/10.1016/j.advengsoft.2016.01.008
Mirjalili S, Mirjalili SM, Lewis A (2014) Grey wolf optimizer. Adv Eng Softw 69:46–61. https://doi.org/10.1016/j.advengsoft.2013.12.007

Mirjalili S, Gandomi AH, Mirjalili SZ et al (2017) Salp Swarm Algorithm: a bio-inspired optimizer for engineering design problems. Adv Eng Softw 114:163–191. https://doi.org/10.1016/j.advengsoft.2017.07.002

Moeinaddini E (2019) Selecting optimal blocks for image watermarking using entropy and distinct discrete firefly algorithm. Soft Comput 23:9685–9699. https://doi.org/10.1007/s00500-018-3535-9

Moeinaddini E, Afsari F (2018) Robust watermarking in DWT domain using SVD and opposition and dimensional based modified firefly algorithm. Multimed Tools Appl 77:26083–26105. https://doi.org/10.1007/s11042-018-5838-3

Mohan A, Anand A, Singh AK et al (2021) Selective encryption and optimization based watermarking for robust transmission of landslide images. Comput Electr Eng 95:107385. https://doi.org/10.1016/j.compeleceng.2021.107385

Mohsin AH, Zaidan AA, Zaidan BB et al (2019) New method of image steganography based on particle swarm optimization algorithm in spatial domain for high embedding capacity. IEEE Access 7:168994–169010. https://doi.org/10.1109/ACCESS.2019.2949622

Mohsin AH, Zaidan AA, Zaidan BB et al (2021) PSO–blockchain-based image steganography: towards a new method to secure updating and sharing COVID-19 data in decentralised hospitals intelligence architecture. Multimed Tools Appl 80:14137–14161. https://doi.org/10.1007/s11042-020-10284-y

Molaei AM, Ebrahimzadeh A (2019) Optimal steganography with blind detection based on Bayesian optimization algorithm. Pattern Anal Appl 22:205–219. https://doi.org/10.1007/s10044-018-00773-0

Moosazadeh M, Ekbatanifard G (2019) A new DCT-based robust image watermarking method using teaching-learning-based optimization. J Inf Secur Appl 47:28–38. https://doi.org/10.1016/j.jisa.2019.04.001

Muhammad K, Ahmad J, Rehman NU et al (2017) CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. Multimed Tools Appl 76:8597–8626. https://doi.org/10.1007/s11042-016-3383-5

Muhuri PK, Ashraf Z, Goel S (2020) A novel image steganographic method based on integer wavelet transformation and particle swarm optimization. Appl Soft Comput 92:106257. https://doi.org/10.1016/j.asoc.2020.106257

Nazari M, Mehrabian M (2021) A novel chaotic IWT-LSB blind watermarking approach with flexible capacity for secure transmission of authenticated medical images. Multimed Tools Appl 80:10615–10655. https://doi.org/10.1007/s11042-020-10032-2

Nazir H, Bajwa IS, Samiullah M et al (2021) Robust secure color image watermarking using 4D hyperchaotic system, DWT, HbD, and SVD based on improved FOA algorithm. Secur Commun Netw 2021:e6617944. https://doi.org/10.1155/2021/6617944

Nipanikar SI, Hima Deepthi V, Kulkarni N (2018) A sparse representation based image steganography using particle swarm optimization and wavelet transform. Alex Eng J 57:2343–2356. https://doi.org/10.1016/j.aej.2017.09.005

Pan W-T (2012) A new Fruit Fly Optimization Algorithm: taking the financial distress model as an example. Knowl-Based Syst 26:69–74. https://doi.org/10.1016/j.knosys.2011.07.001

Pandey HM (2020) Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography. Future Gener Comput Syst 111:213–225. https://doi.org/10.1016/j.future.2020.04.034

Pandey MK, Parmar G, Gupta R, Sikander A (2020) Lossless robust color image watermarking using lifting scheme and GWO. Int J Syst Assur Eng Manage 11:320–331. https://doi.org/10.1007/s13198-019-00859-w

Parah SA, Ahad F, Sheikh JA, Bhat GM (2017) Hiding clinical information in medical images: a new high capacity and reversible data hiding technique. J Biomed Inform 66:214–230. https://doi.org/10.1016/j.jbi.2017.01.006

Parah SA, Sheikh JA, Akhoon JA et al (2018) Information hiding in edges: a high capacity information hiding technique using hybrid edge detection. Multimed Tools Appl 77:185–207. https://doi.org/10.1007/s11042-016-4253-x

Pelikan M, Sastry K, Goldberg DE (2002) Scalability of the Bayesian optimization algorithm. Int J Approx Reason 31:221–258. https://doi.org/10.1016/S0888-613X(02)00095-6

Pereira S, Voloshynovskiy S, Madueno M et al (2001) Second generation benchmarking and application oriented evaluation. In: Moskowitz IS (ed) Information hiding. Springer, Berlin, pp 340–353

Petitcolas FAP (2000) Watermarking schemes evaluation. IEEE Signal Process Mag 17:58–64. https://doi.org/10.1109/79.879339

Petitcolas FAP, Fatès N (2004) StirMark Benchmark manual. https://www.petitcolas.net/watermarking/stirmark/. Accessed 30 May 2023

Petitcolas FAP, Anderson RJ, Kuhn MG (1998) Attacks on copyright marking systems. In: Aucsmith D (ed) Information hiding. Springer, Berlin, pp 218–238

Pizzolante R, Castiglione A, Carpentieri B et al (2018) On the protection of consumer genomic data in the Internet of Living Things. Comput Secur 74:384–400. https://doi.org/10.1016/j.cose.2017.06.003

Pourhadi A, Mahdavi-Nasab H (2020) A robust digital image watermarking scheme based on bat algorithm optimization and SURF detector in SWT domain. Multimed Tools Appl 79:21653–21677. https://doi.org/10.1007/s11042-020-08960-0

Prabha KR, Jagadeeswari M (2020) Enhanced imperialist competitive algorithm based efficient reversible data hiding technique. Multimed Tools Appl 79:4057–4074. https://doi.org/10.1007/s11042-019-07772-1

Pradhan A, Sekhar KR, Swain G (2018) Digital image steganography using LSB substitution, PVD, and EMD. Math Probl Eng 2018:e1804953. https://doi.org/10.1155/2018/1804953

Pramanik S, Singh RP, Ghosh R (2020) Application of bi-orthogonal wavelet transform and genetic algorithm in image steganography. Multimed Tools Appl 79:17463–17482. https://doi.org/10.1007/s11042-020-08676-1

Puteaux P, Puech W (2018) An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images. IEEE Trans Inf Forensics Secur 13:1670–1681. https://doi.org/10.1109/TIFS.2018.2799381

Rai M, Goyal S (2022) A hybrid digital image watermarking technique based on fuzzy-BPNN and shark smell optimization. Multimed Tools Appl 81:39471–39489. https://doi.org/10.1007/s11042-022-12712-7

Rao RV, Savsani VJ, Vakharia DP (2011) Teaching-learning-based optimization: a novel method for constrained mechanical design optimization problems. CAD Comput Aided Des 43:303–315. https://doi.org/10.1016/j.cad.2010.12.015

Ray B, Mukhopadhyay S, Hossain S et al (2021) Image steganography using deep learning based edge detection. Multimed Tools Appl 80:33475–33503. https://doi.org/10.1007/s11042-021-11177-4

Reshma VK, Vinod Kumar RS, Shahi D, Shyjith MB (2022) Optimized support vector neural network and contourlet transform for image steganography. Evol Intell 15:1295–1311. https://doi.org/10.1007/s12065-020-00387-8

Roselin Kiruba R, Sree Sharmila T (2021) Secure data hiding by fruit fly optimization improved hybridized seeker algorithm. Multimed Syst Signal Process 32:405–430. https://doi.org/10.1007/s11045-019-00697-w

Roy S, Pal AK (2017) A blind DCT based color watermarking algorithm for embedding multiple watermarks. AEU-Int J Electron C 72:149–161. https://doi.org/10.1016/j.aeue.2016.12.003

Saadati M, Vahidi J, Seydi V, Sheikholharam Mashhadi P (2021) Proposing a new image watermarking method using shearlet transform and whale optimization algorithm. Int J Eng Trans A 34:843–853. https://doi.org/10.5829/ije.2021.34.04a.10

Sabeti V, Aghabagheri A (2022) Developing an adaptive DCT-based steganography method using a genetic algorithm. Multimed Tools Appl. https://doi.org/10.1007/s11042-022-14166-3

Sabeti V, Sobhani M, Hasheminejad SMH (2022) An adaptive image steganography method based on integer wavelet transform using genetic algorithm. Comput Electr Eng. https://doi.org/10.1016/j.compeleceng.2022.107809

Salehnia T, Fathi A (2021) Fault tolerance in LWT-SVD based image watermarking systems using three module redundancy technique. Expert Syst Appl 179:115058. https://doi.org/10.1016/j.eswa.2021.115058

Salimi H (2015) Stochastic fractal search: a powerful metaheuristic algorithm. Knowl-Based Syst 75:1–18. https://doi.org/10.1016/j.knosys.2014.07.025

Salimi L, Haghighi A, Fathi A (2020) A novel watermarking method based on differential evolutionary algorithm and wavelet transform. Multimed Tools Appl 79:11357–11374. https://doi.org/10.1007/s11042-019-08455-7

Saremi S, Mirjalili S, Lewis A (2017) Grasshopper optimisation algorithm: theory and application. Adv Eng Softw 105:30–47. https://doi.org/10.1016/j.advengsoft.2017.01.004

Sarmah DK, Kulkarni AJ (2018) JPEG based steganography methods using cohort intelligence with cognitive computing and modified multi random start local search optimization algorithms. Inf Sci 430–431:378–396. https://doi.org/10.1016/j.ins.2017.11.027

Sarmah DK, Kulkarni AJ (2019) Improved cohort intelligence—a high capacity, swift and secure approach on JPEG image steganography. J Inf Secur Appl 45:90–106. https://doi.org/10.1016/j.jisa.2019.01.002

Satapathy S, Naik A (2016) Social group optimization (SGO): a new population evolutionary optimization technique. Complex Intell Syst 2:173–203. https://doi.org/10.1007/s40747-016-0022-8
Saxena N, Mishra KK (2017) Improved multi-objective particle swarm optimization algorithm for optimizing watermark strength in color image watermarking. Appl Intell 47:362–381. https://doi.org/10.1007/s10489-016-0889-5
Setiadi DRIM (2021) PSNR vs SSIM: imperceptibility quality assessment for image steganography. Multimed Tools Appl 80:8423–8444. https://doi.org/10.1007/s11042-020-10035-z
Sharma N, Batra U (2021) An enhanced Huffman-PSO based image optimization algorithm for image steganography. Genet Program Evolvable Mach 22:189–205. https://doi.org/10.1007/s10710-020-09396-z
Sharma S, Sharma H, Sharma JB (2019) An adaptive color image watermarking using RDWT-SVD and artificial bee colony based quality metric strength factor optimization. Appl Soft Comput 84:105696. https://doi.org/10.1016/j.asoc.2019.105696
Sharma C, Bagga A, Singh BK, Shabaz M (2021a) A novel optimized graph-based transform watermarking technique to address security issues in real-time application. Math Probl Eng 2021:e5580098. https://doi.org/10.1155/2021/5580098
Sharma S, Chauhan U, Khanam R, Singh KK (2021b) Digital watermarking using dragonfly optimization algorithm. J Inf Technol Manage 12:36–47. https://doi.org/10.22059/JITM.2020.78888
Sharma S, Chauhan U, Khanam R, Singh KK (2021c) Digital watermarking using grasshopper optimization algorithm. Open Comput Sci 11:330–336. https://doi.org/10.1515/comp-2019-0023
Sharma S, Sharma H, Sharma JB (2021d) Artificial bee colony based perceptually tuned blind color image watermarking in hybrid LWT-DCT domain. Multimed Tools Appl 80:18753–18785. https://doi.org/10.1007/s11042-021-10610-y
Sharma S, Sharma H, Sharma JB, Poonia RC (2021e) A secure and robust color image watermarking using nature-inspired intelligence. Neural Comput Appl. https://doi.org/10.1007/s00521-020-05634-8
Sharma N, Chakraborty C, Kumar R (2022a) Optimized multimedia data through computationally intelligent algorithms. Multimed Syst. https://doi.org/10.1007/s00530-022-00918-6
Sharma NK, Kumar S, Rajpal A, Kumar N (2022b) MantaRayWmark: an image adaptive multiple embedding strength optimization based watermarking using Manta Ray Foraging and bi-directional ELM. Expert Syst Appl. https://doi.org/10.1016/j.eswa.2022.116860
Sharma S, Sharma H, Sharma JB (2022c) A new optimization based color image watermarking using nonnegative matrix factorization in discrete cosine transform domain. J Ambient Intell Humaniz Comput 13:4297–4319. https://doi.org/10.1007/s12652-021-03408-1
Shen Y, Tang C, Xu M et al (2021) A DWT-SVD based adaptive color multi-watermarking scheme for copyright protection using AMEF and PSO-GWO. Expert Syst Appl 168:114414. https://doi.org/10.1016/j.eswa.2020.114414
Shih FY, Wu Y-T (2005) Robust watermarking and compression for medical images based on genetic algorithms. Inf Sci 175:200–216. https://doi.org/10.1016/j.ins.2005.01.013
Shih FY, Zhong X, Chang I-C, Satoh S (2018) An adjustable-purpose image watermarking technique by particle swarm optimization. Multimed Tools Appl 77:1623–1642. https://doi.org/10.1007/s11042-017-4367-9
Shojae Chaeikar S, Ahmadi A (2019) Ensemble SW image steganalysis: a low dimension method for LSBR detection. Signal Process: Image Commun 70:233–245. https://doi.org/10.1016/j.image.2018.10.004
Shukur WA, Jabbar KK (2018) Information hiding using LSB technique based on developed PSO algorithm. Int J Electr Comput Eng (IJECE) 8:1156–1168. https://doi.org/10.11591/ijece.v8i2.pp1156-1168
Singh D, Singh SK (2017) DWT-SVD and DCT based robust and blind watermarking scheme for copyright protection. Multimed Tools Appl 76:13001–13024. https://doi.org/10.1007/s11042-016-3706-6
Singh L, Singh AK, Singh PK (2020) Secure data hiding techniques: a survey. Multimed Tools Appl 79:15901–15921. https://doi.org/10.1007/s11042-018-6407-5
Singh OP, Singh AK, Srivastava G, Kumar N (2021a) Image watermarking using soft computing techniques: a comprehensive survey. Multimed Tools Appl 80:30367–30398. https://doi.org/10.1007/s11042-020-09606-x
Singh P, Devi KJ, Thakkar HK, Santamaría J (2021b) Blind and secured adaptive digital image watermarking approach for high imperceptibility and robustness. Entropy 23:1650. https://doi.org/10.3390/e23121650
Singh R, Saraswat M, Ashok A et al (2023) From classical to soft computing based watermarking techniques: a comprehensive review. Future Gener Comput Syst 141:738–754. https://doi.org/10.1016/j.future.2022.12.015
Singhal A, Bedi P (2021) Multi-class blind steganalysis using deep residual networks. Multimed Tools Appl 80:13931–13956. https://doi.org/10.1007/s11042-020-10353-2

Sinhal R, Ansari IA (2022) Tunable Q-factor wavelet transform-based robust image watermarking scheme using logistic mapping and antlion optimization. Circuits Syst Signal Process 41:6370–6410. https://doi.org/10.1007/s00034-022-02090-8

Sisaudia V, Vishwakarma VP (2021) Copyright protection using KELM-PSO based multi-spectral image watermarking in DCT domain with local texture information based selection. Multimed Tools Appl 80:8667–8688. https://doi.org/10.1007/s11042-020-10028-y

Sivananthamaitrey P, Kumar PR (2022a) Optimal dual watermarking of color images with SWT and SVD through genetic algorithm. Circuits Syst Signal Process 41:224–248. https://doi.org/10.1007/s00034-021-01773-y

Sivananthamaitrey P, Kumar PR (2022b) Performance analysis of meta-heuristics on dual watermarking of color images based on SWT and SVD. Multimed Tools Appl 81:1001–1027. https://doi.org/10.1007/s11042-021-11204-4

Soliman MM, Hassanien AE, Onsi HM (2014) Bio-inspiring techniques in watermarking medical images: a review. Intell Syst Ref Libr 70:93–114. https://doi.org/10.1007/978-3-662-43616-5_4

Soppari K, Chandra NS (2022) Automated digital image watermarking based on multi-objective hybrid meta-heuristic-based clustering approach. Int J Intell Robot Appl. https://doi.org/10.1007/s41315-022-00241-3

Stegherr H, Heider M, Hähner J (2022) Classifying metaheuristics: towards a unified multi-level classification system. Nat Comput 21:155–171. https://doi.org/10.1007/s11047-020-09824-0

Storn R, Price K (1997) Differential evolution—a simple and efficient heuristic for global optimization over continuous spaces. J Global Optim 11:341–359. https://doi.org/10.1023/A:1008202821328

Subramanian N, Elharrouss O, Al-Maadeed S, Bouridane A (2021) Image steganography: a review of the recent advances. IEEE Access 9:23409–23423. https://doi.org/10.1109/ACCESS.2021.3053998

Swaraja K, Meenakshi K, Kora P (2020) An optimized blind dual medical image watermarking framework for tamper localization and content authentication in secured telemedicine. Biomed Signal Process Control 55:101665. https://doi.org/10.1016/j.bspc.2019.101665

Swaraja K, Meenakshi K, Kora P (2021) Hierarchical multilevel framework using RDWT-QR optimized watermarking in telemedicine. Biomed Signal Process Control 68:102688. https://doi.org/10.1016/j.bspc.2021.102688

Takieldeen AE, El-Kenawy E-SM, Hadwan M, Zaki RM (2022) Dipper throated optimization algorithm for unconstrained function and feature selection. Comput Mater Contin 72:1465–1481. https://doi.org/10.32604/cmc.2022.026026

Tang L, Xie J, Wu D (2022) An interval type-2 fuzzy edge detection and matrix coding approach for color image adaptive steganography. Multimed Tools Appl 81:39145–39167. https://doi.org/10.1007/s11042-022-13127-0

Thakkar FN, Srivastava VK (2017a) A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications. Multimed Tools Appl 76:3669–3697. https://doi.org/10.1007/s11042-016-3928-7

Thakkar FN, Srivastava VK (2017b) A particle swarm optimization and block-SVD-based watermarking for digital images. Turk J Electr Eng Comput Sci 25:3273–3288. https://doi.org/10.3906/elk-1603-17

Thakkar FN, Srivastava VK (2019) Performance comparison of recent optimization algorithm Jaya with particle swarm optimization for digital image watermarking in complex wavelet domain. Multidimens Syst Sign Process 30:1769–1791. https://doi.org/10.1007/s11045-018-0627-8

Thakkar FN, Srivastava VK (2021) An adaptive, secure and imperceptive image watermarking using swarm intelligence, Arnold transform, SVD and DWT. Multimed Tools Appl 80:12275–12292. https://doi.org/10.1007/s11042-020-10220-0

Trelea IC (2003) The particle swarm optimization algorithm: convergence analysis and parameter selection. Inf Process Lett 85:317–325. https://doi.org/10.1016/S0020-0190(02)00447-7

Uma Maheswari S, Jude Hemanth D (2017) Performance enhanced image steganography systems using transforms and optimization techniques. Multimed Tools Appl 76:415–436. https://doi.org/10.1007/s11042-015-3035-1

Vali MH, Aghagolzadeh A, Baleghi Y (2018) Optimized watermarking technique using self-adaptive differential evolution based on redundant discrete wavelet transform and singular value decomposition. Expert Syst Appl 114:296–312. https://doi.org/10.1016/j.eswa.2018.07.004

Vazquez E, Torres S, Sanchez G et al (2022) Confidentiality in medical images through a genetic-based steganography algorithm in artificial intelligence. Front Robot AI. https://doi.org/10.3389/frobt.2022.1031299

Venkata Rao R (2016) Jaya: a simple and new optimization algorithm for solving constrained and unconstrained optimization problems. Int J Ind Eng Comput 7:19–34. https://doi.org/10.5267/j.ijiec.2015.8.004

Verma OP, Aggarwal D, Patodi T (2016) Opposition and dimensional based modified firefly algorithm. Expert Syst Appl 44:168–176. https://doi.org/10.1016/j.eswa.2015.08.054

Walia GS, Makhija S, Singh K, Sharma K (2018) Robust stego-key directed LSB substitution scheme based upon cuckoo search and chaotic map. Optik 170:106–124. https://doi.org/10.1016/j.ijleo.2018.04.135

Wan W, Wang J, Zhang Y et al (2022) A comprehensive survey on robust image watermarking. Neurocomputing 488:226–247. https://doi.org/10.1016/j.neucom.2022.02.083

Wang W, Li Q (2022) An image steganography algorithm based on PSO and IWT for underwater acoustic communication. IEEE Access 10:107376–107385. https://doi.org/10.1109/ACCESS.2022.3212691

Wang R-Z, Lin C-F, Lin J-C (2001) Image hiding by optimal LSB substitution and genetic algorithm. Pattern Recogn 34:671–683. https://doi.org/10.1016/S0031-3203(00)00015-7

Wang G-G, Deb S, Gao X-Z, Dos Santos CL (2016) A new metaheuristic optimisation algorithm motivated by elephant herding behaviour. Int J Bio-Inspired Comput 8:394–409. https://doi.org/10.1504/IJBIC.2016.081335

Wang J, Ni J, Zhang X, Shi Y-Q (2017) Rate and distortion optimization for reversible data hiding using multiple histogram shifting. IEEE Trans Cybern 47:315–326. https://doi.org/10.1109/TCYB.2015.2514110

Wang G-G, Deb S, Zhao X, Cui Z (2018a) A new monarch butterfly optimization with an improved crossover operator. Oper Res Int J 18:731–755. https://doi.org/10.1007/s12351-016-0251-z

Wang Z, Zhang X, Yin Z (2018b) Joint cover-selection and payload-allocation by steganographic distortion optimization. IEEE Signal Process Lett 25:1530–1534. https://doi.org/10.1109/LSP.2018.2865888

Wang J, Chen X, Ni J et al (2020) Multiple histograms-based reversible data hiding: framework and realization. IEEE Trans Circuits Syst Video Technol 30:2313–2328. https://doi.org/10.1109/TCSVT.2019.2915584

Wang D, Li M, Zhang Y (2022) Adversarial data hiding in digital images. Entropy. https://doi.org/10.3390/e24060749

Wazirali R, Alasmary W, Mahmoud MMEA, Alhindi A (2019) An optimized steganography hiding capacity and imperceptibly using genetic algorithms. IEEE Access 7:133496–133508. https://doi.org/10.1109/ACCESS.2019.2941440

Weng S, Zhou Y, Zhang T et al (2022) General framework to reversible data hiding for JPEG images with multiple two-dimensional histograms. IEEE Trans Multimed. https://doi.org/10.1109/TMM.2022.3198877

Wu J-Y, Huang W-L, Zuo M-J, Gong L-H (2020) Optical watermark scheme based on singular value decomposition ghost imaging and particle swarm optimization algorithm. J Mod Opt 67:1059–1071. https://doi.org/10.1080/09500340.2020.1810346

Xiang S, He J (2018) Database authentication watermarking scheme in encrypted domain. IET Inf Secur 12:42–51. https://doi.org/10.1049/iet-ifs.2017.0092

Xiang L, Li Y, Hao W et al (2018) Reversible natural language watermarking using synonym substitution and arithmetic coding. Comput Mater Contin 55:541–559. https://doi.org/10.3970/cmc.2018.03510

Xiao Y, Gao G (2019) Digital watermark-based independent individual certification scheme in WSNs. IEEE Access 7:145516–145523. https://doi.org/10.1109/ACCESS.2019.2945177

Yang X-S (2010) Firefly algorithm, stochastic test functions and design optimization. Int J Bio-Inspired Comput 2:78–84. https://doi.org/10.1504/IJBIC.2010.032124

Yang X-S, Gandomi AH (2012) Bat algorithm: a novel approach for global engineering optimization. Eng Comput (swansea, Wales) 29:464–483. https://doi.org/10.1108/02644401211235834

Yang C-N, Hsu S-C, Kim C (2017) Improving stego image quality in image interpolation based data hiding. Comput Stand Interfaces 50:209–215. https://doi.org/10.1016/j.csi.2016.10.005

Yi S, Zhou Y (2017) Binary-block embedding for reversible data hiding in encrypted images. Signal Process 133:40–51. https://doi.org/10.1016/j.sigpro.2016.10.017

Ying Q, Qian Z, Zhang X, Ye D (2019) Reversible data hiding with image enhancement using histogram shifting. IEEE Access 7:46506–46521. https://doi.org/10.1109/ACCESS.2019.2909560

Yu L, Zhao Y, Ni R, Zhu Z (2009) PM1 steganography in JPEG images using genetic algorithm. Soft Comput 13:393–400. https://doi.org/10.1007/s00500-008-0327-7

Zakaria AA, Hussain M, Wahab AWA et al (2018) High-capacity image steganography with minimum modified bits based on data mapping and LSB substitution. Appl Sci 8:2199. https://doi.org/10.3390/app8112199

Zhang Y, Ma X-L (2019) Research on image digital watermarking optimization algorithm under virtual reality technology. Discr Contin Dyn Syst—S 12:1427. https://doi.org/10.3934/dcdss.2019098

Zhang L, Wei D (2019) Dual DCT-DWT-SVD digital watermarking algorithm based on particle swarm optimization. Multimed Tools Appl 78:28003–28023. https://doi.org/10.1007/s11042-019-07902-9

Zhang X, Sun Z, Tang Z et al (2017) High capacity data hiding based on interpolated image. Multimed Tools Appl 76:9195–9218. https://doi.org/10.1007/s11042-016-3521-0
Zhang Y, Ye D, Gan J et al (2018) An image steganography algorithm based on quantization index modulation resisting scaling attacks and statistical detection. Comput Mater Contin 56:151–167. https://doi.org/10.3970/cmc.2018.02464
Zhang X, Zhang W, Sun W et al (2020) A robust watermarking scheme based on roi and IWT for remote consultation of covid-19. Comput Mater Contin 64:1435–1452. https://doi.org/10.32604/cmc.2020.011359
Zhang T, Yang C, Weng S, Hou T (2022) Adaptive multi-histogram reversible data hiding with contrast enhancement. J vis Commun Image Represent. https://doi.org/10.1016/j.jvcir.2022.103637
Zhao B, Fang L, Zhang H et al (2019) Y-DWMS: a digital watermark management system based on smart contracts. Sensors 19:3091. https://doi.org/10.3390/s19143091
Zhao W, Zhang Z, Wang L (2020) Manta ray foraging optimization: an effective bio-inspired optimizer for engineering applications. Eng Appl Artif Intell 87:103300. https://doi.org/10.1016/j.engappai.2019.103300
Zheng Z, Saxena N, Mishra KK, Sangaiah AK (2018) Guided dynamic particle swarm optimization for optimizing digital image watermarking in industry applications. Future Gener Comput Syst 88:92–106. https://doi.org/10.1016/j.future.2018.05.027
Zhou NR, Luo AW, Zou WP (2019) Secure and robust watermark scheme based on multiple transforms and particle swarm optimization algorithm. Multimed Tools Appl 78:2507–2523. https://doi.org/10.1007/s11042-018-6322-9
Zhou L, Han H, Wu H (2021) Generalized reversible data hiding with content-adaptive operation and fast histogram shifting optimization. Entropy 23:917. https://doi.org/10.3390/e23070917