

Received August 15, 2020, accepted September 4, 2020, date of publication September 8, 2020, date of current version September 23, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3022779

Digital Steganography and Watermarking for Digital Images: A Review of Current Research Directions

OLEG EVSUTIN^{1,3}, ANNA MELMAN²,
AND ROMAN MESHCHERYAKOV³, (Senior Member, IEEE)

¹Department of Cyber-Physical Systems Information Security, National Research University Higher School of Economics, 123458 Moscow, Russia

²Department of Information Systems Security, Tomsk State University of Control Systems and Radioelectronics, 634050 Tomsk, Russia

³Laboratory of Cyber-Physical Systems, V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, 117997 Moscow, Russia

Corresponding author: Oleg Evsutin (evsutin.oo@gmail.com)

This work was supported by the Russian Science Foundation under Grant 19-71-00106.

ABSTRACT The development of information technology has led to a significant increase in the share of multimedia traffic in data networks. This has necessitated to solve the following information security tasks in relation to multimedia data: protection against leakage of confidential information, as well as identifying the source of the leak; ensuring the impossibility of unauthorized changes; copyright protection for digital objects. To solve such kind of problems, methods of steganography and watermarking are designed that implement embedding in digital objects hidden information sequences for various purposes. In this paper, an overview of promising research in the specified area is provided. First of all, we provide basic information about this field of research and consider the main applications of its methods. Next, we review works demonstrating current trends in the development of methods and algorithms for data hiding in digital images. This review is not exhaustive; it focuses on contemporary works illustrating current research directions in the field of information embedding in digital images. This is the main feature of review, which distinguishes it from previously published reviews. The paper concludes with an analysis of identified problems in the field of digital steganography and digital watermarking.

INDEX TERMS Information security, digital image steganography, digital watermarking, data hiding.

I. INTRODUCTION


In the modern world, the importance of protecting digital data is very high. One of the ways to ensure the security of digital data is using steganography and digital watermarking techniques. This is particularly relevant for various multimedia data, such as images, audio recordings, video files. Concealing information with the help of steganography and digital watermark embedding is a well-established and developing scientific field.

Steganography involves the protection of some additional information that is embedded in a digital cover object. Information itself, as well as the cover object hiding it, can be different digital objects themselves. The main idea of steganographic methods is to make embedded information invisible to an attacker. Due to this statement, secret information could be safely transmitted through an open

communication channel, because only the sender and receiver will know about its presence inside the transmitted cover object [1].

Digital watermarking methods are used to protect the digital cover objects themselves. The functions of a digital watermark are similar to the functions of an electronic digital signature. A digital watermark is a label that allows, for example, to identify the author of a digital object, or to confirm the authenticity and integrity of this object. Digital watermarks are often used to protect the authorship of multimedia files, to control the integrity of data, and to authenticate the sources of this data. The classic digital watermark application is connected with multimedia protection. However, at present, the application of such methods to protect data of a different type [2] is becoming relevant.

It is worth noting that in some cases the difference between these two directions of data hiding in digital objects lies solely in the purpose of application since many algorithms for steganographic embedding and embedding of digital

The associate editor coordinating the review of this manuscript and approving it for publication was Ahmed Farouk .

watermarks are based on the same operations. Nevertheless, there are many specific algorithms that explicitly apply only to steganography or only to digital watermarking. On such occasions, the main differences are in the requirements for the effectiveness of data embedding. In general, the main requirement for the effectiveness of steganographic algorithms is the invisibility of embedding, since the idea of steganography lies in the invisibility of the embedding. In the meantime, digital watermark hiding algorithms are often developed as robust embedment algorithms that can detect embedded data even after distortions of a digital object. Although, various authors are developing algorithms with additional quality indicators that expand the possibilities of applying such algorithms in practice.

Among the many possible covers for embedding additional information, the most common are digital images. This is facilitated by the widespread dissemination of digital images in various fields of activity, from everyday communication on social networks to medicine, the army, and space. It should be noted that frames of video sequences are also images, so the use of steganography and digital watermarking methods for video data is often based on processing individual frames as images. In this paper, digital images are considered as digital cover objects, and the review is limited to relevant studies.

This review is aimed at studying current trends in the development of methods and algorithms for data hiding in digital images. Its main goal is to identify current problems and challenges in the field of digital steganography and digital watermarking in the context of the current state of this scientific field. It is non-exhaustive but notes modern works illustrating the current research directions in the field of information embedding in digital images. This is the key feature of this review, which distinguishes it from previously published review papers.

The rest of the paper is organized as follows. Section 2 introduces the basic concepts of digital steganography and digital watermarking. Section 3 describes the spatial and frequency domain of embedding and provides an overview of current work on spatial and frequency embedding. Section 4 provides an overview of research in priority areas of data hiding in digital images. Section 5 presents an analysis of the work reviewed and formulates a list of current issues. The conclusion summarizes the review.

II. BASIC CONCEPTS AND APPLICATIONS

As noted in the introduction, this review does not purport to be called comprehensive. Instead, it focuses on the most promising and relevant research areas in the field of digital steganography and digital watermarking. Nevertheless, it is necessary to determine the basic concepts used in these areas of knowledge, to describe the basic methods and applications.

A. CLASSIFICATION OF METHODS FOR DATA HIDING IN DIGITAL IMAGES

One of the two main areas of data hiding in digital data is digital steganography. Methods of digital steganography are

used to ensure the confidentiality of information due to its imperceptible transmission inside digital objects, in particular digital images.

When steganographic embedding, information is hidden inside the cover image according to some algorithm. Frequently, to increase the security of embedding, a secret key or special algorithm parameters known to the sender and receiver of information are used. An image with information embedded in it is called a stego image. Inasmuch as the steganographic embedding algorithms ensure the invisibility of embedded data and hide the fact of the presence of such data, the transmission of stego image is usually carried out over an open communication channel. A scheme of this process is presented in Fig. 1.

The receiver uses the information extraction algorithm and extracts the embedded message from the stego image. The information can be extracted in its original form, and may contain distortions associated with the features of the embeddable procedure or with any destructive effects that arose when transmitting a stego image over a communication channel. Fig. 1 also shows that on the receiver side, the original image can be restored. It is indicated by a dashed line, since such a possibility does not always exist. For this purpose, the embedding algorithm must have the property of reversibility, i.e. the ability to totally restore the original image after extracting the embedded information.

A detailed classification of steganographic algorithms can be found in review papers [3], [4].

Additional information embedding in a digital image leads to its distortion. Therefore, the stealth of steganographic embedding is characterized, first of all, by the absence of visible distortions of stego images. The absence of noticeable distortions of a digital image containing embedded information is estimated using various similarity metrics.

A stronger requirement is resistance to steganalysis: an image containing an attachment and a “clean” image without an attachment should be statistically indistinguishable.

An illustration of the steganalysis idea is shown in Fig. 2. In general, it is assumed that the attacker does not know whether any embedded information is contained in some digital image. In some scenarios, an attacker may be more aware. For example, he knows that some image contains a secret message, but does not know by what algorithm it was embedded. In most cases, steganalysis methods are used to establish the fact of the presence or absence of embedded information, however, if the attacker is sufficiently informed, the embedded information itself can also be obtained. Steganalysis is a separate rather extensive area with its own methods and approaches. Their detailed description can be found in [5], [6].

Another additional requirement for steganographic algorithms can be robustness – resistance to various destructive effects, which allows you to extract embedded information with minimal distortion even when exposed to any distorting effects on stego images. Though, more often embedding algorithms for digital watermarks have the robustness property.

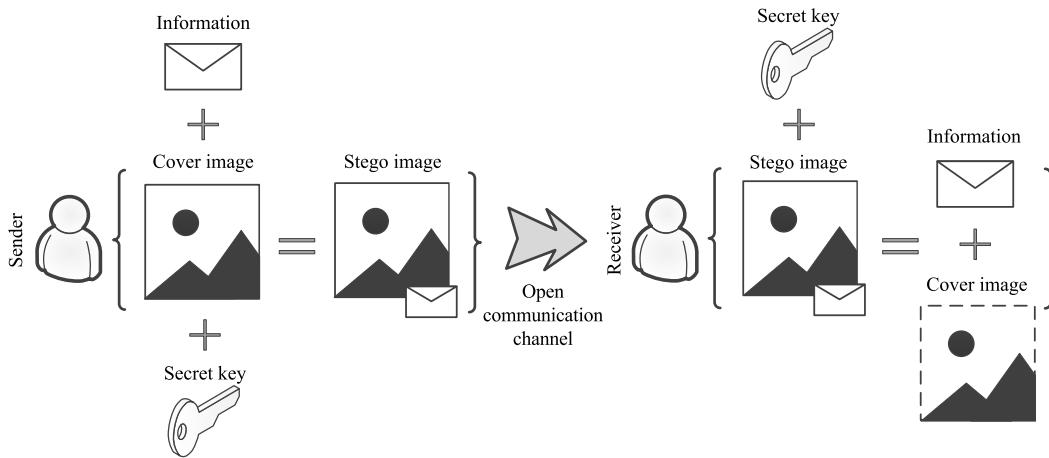


FIGURE 1. Information embedding and extracting.

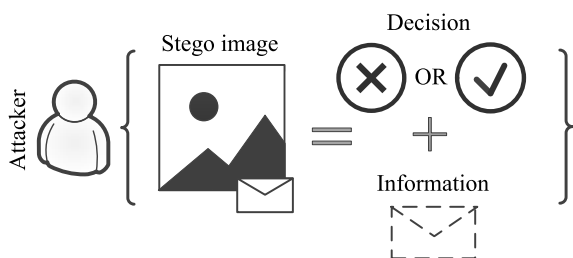


FIGURE 2. Steganalysis.

A digital watermark is some additional information that is embedded in a digital object for authentication or integrity purposes. This can be, for example, text, a logo, a hash code, or other information. In most cases digital watermarking methods are used to protect the cover image itself, and not the embedded information, because embedded information is not a secret message, but serves to identify the owner of the image or to control the integrity of the image. Extraction of such information occurs if it is necessary to confirm the authorship of an image, verify its authenticity, assess the presence of any random or intentional distortions, while the ultimate goal of steganographic embedding is precisely the hidden transmission of some message to the addressee. The most widely digital watermarks are used in the field of copyright protection for digital content, in particular, digital images: illustrations, photographs. But digital watermarking methods can also be used in other areas, for example, for patient data embedding in medical images. Many embedding algorithms allow not only to detect changes in the image, but also to localize them and restore the damaged area. Articles [7], [8] are examples of review papers on digital watermarking techniques.

Sometimes the watermarking algorithms completely coincide with the steganography algorithms, in which case their difference lies only in the purpose of use. There are also a large number of specific algorithms for digital watermarks

embedding that are not suitable for embedding a large amount of data, as is assumed in steganographic applications. However, in general, the watermarking mechanism is similar to that shown in Fig. 1. Sometimes it is not necessary to completely extract the built-in watermark. It is enough to convince that a specific watermark is indeed contained in this image. Embedding invisibility and capacity are important for watermarking techniques as for steganography, but in some cases watermarks can be visible and high capacity is not always required. Table 1 illustrates the differences between steganography and watermarking methods.

TABLE 1. Steganography and watermarking.

Characteristics	Steganography	Watermarking
Purpose of use	Hidden data transmission	Control of integrity, authenticity, authorship protection
Protected object	Secret message	Cover image
Result of embedding	Stego image	Watermarked image
Main security threat	Steganalysis	Image distortion
Main security criterion	Resistance to steganalysis	Robustness
Imperceptibility of embedding	High	Usually high, but in some cases not required
Embedding capacity	Usually high	May be different
Need to extract embedded information	Yes	Not in all cases

Digital watermarks differ in their degree of resistance to distortion: fragile digital watermarks are destroyed with any change of the marked image, semi-fragile digital watermarks can withstand some attacks, for example, moderate JPEG compression, and robust digital watermarks are also detectable after more significant cover image distortions. Typically, fragile watermarks are used to control image

integrity and localize distortions, while robust watermarks are used to validate authorship and authenticity control. Semi-fragile watermarks can partially solve both problems. For example, some distortions are considered acceptable and the watermarking algorithm provides resistance to such distortions, while other distortions are considered unauthorized and localized when attempting to check the watermark.

In the context of embedding information, various distortions of images containing embedded information are commonly referred to as attacks. The most common attacks on the digital watermarks are:

- rotation – turning the image to some angle,
- scaling – reducing or increasing the size of the image,
- compression – application to the image of some compression algorithm, such as JPEG, JPEG 2000, etc.,
- noise overlay – adding noise to an image, such as Gaussian noise, salt and pepper noise, etc.,
- changing the brightness and / or contrast,
- cropping – cropping part of an image,
- deleting / adding of content on an image,
- histogram equalization – align the image histogram, etc.

Abstract examples of typical attacks on digital watermarks are shown in Fig. 3. Note that the same attacks are relevant for digital steganography methods, but robustness is often not considered when developing steganographic algorithms. Instead, resistance to steganalysis is investigated, which in turn is usually not considered in the case of watermarking.

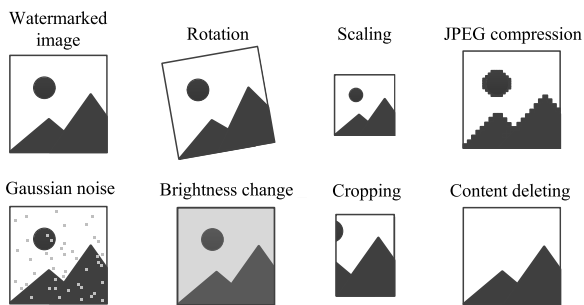


FIGURE 3. Typical attacks on digital watermarks.

Both steganography techniques and watermarking techniques can work with a variety of image types: uncompressed, compressed with different compression techniques, encrypted, stereo images. The direction of quantum image processing has also been developing recently.

It was noted above that the main performance indicators that characterize the algorithms of embedding information in digital images are: the invisibility of embedding, capacity, robustness, resistance to steganalysis and reversibility. In practice, computational complexity is also important. Computational complexity depends on the embedding domain, the embedding operation, and the methods that the algorithm’s authors use to increase its efficiency.

The embedding domain determines which elements of the image data are embedded with the information. It is

customary to allocate a spatial and frequency domain. The frequency domain is in turn defined by some frequency conversion. More information about embedding domains will be provided in the next section of this paper. Embedding operation means how the data element of a digital image was modified when embedding information. In addition to direct embedding, authors of concealment algorithms often employ various additional techniques, such as confusing transformations, optimization techniques, error prediction, interpolation, machine learning, edge detection, etc. This increases the computational complexity of the algorithms but improves one or more other quality measures.

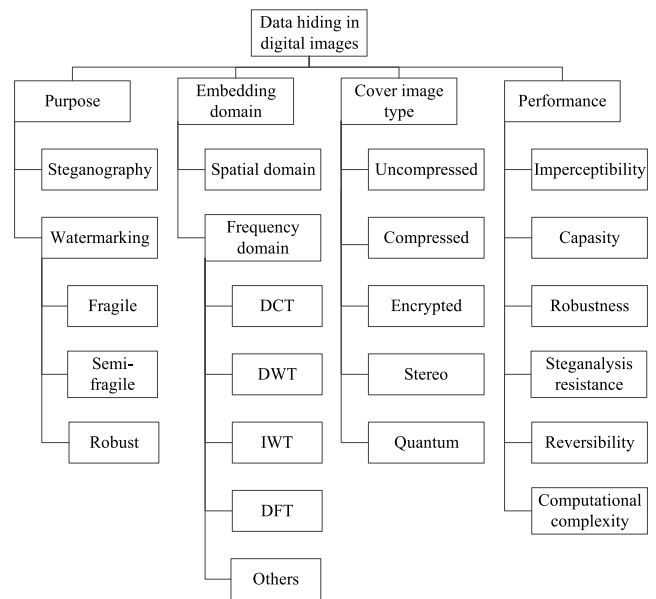


FIGURE 4. Classification of methods for data hiding in digital images.

Fig. 4 presents a diagram illustrating the classification of data hiding methods in digital images according to various criteria, such as purpose of use, embedding domain, container type, and performance indicators. In this case, the purpose of use is understood as the entire set of areas of application of steganography and watermarking methods.

As can be seen from Fig. 4, modern methods of data hiding in digital images differ even at the level of basic criteria. The next sections will highlight the currently most relevant research areas as well as outstanding issues that merit the attention of researchers.

B. KEY EMBEDDING PERFORMANCE INDICATORS

Consider the key embedding performance indicators that authors use to assess the quality of the algorithms developed.

One of the main criteria for assessing the quality of embedding is invisibility. In most of the algorithms for concealing information in digital images (except for some watermark embedding algorithms), the embedded information should not be visible to the naked eye. For numerical estimation of invisibility, the vast majority of works use peak signal to noise ratio (PSNR). To calculate the PSNR between a container

image and an embedded image, use the formula

$$\text{PSNR (dB)} = 10 \times \log_{10} \left(\frac{255^2}{\text{MSE}} \right), \quad (1)$$

$$\text{MSE} = \frac{1}{M \times N} \sum_{i=1}^{N \times M} (C_i - S_i)^2, \quad (2)$$

where $M \times N$ is the height and width of cover the image, C_i the intensity of pixel in the cover image, S_i is the intensity of pixel in the image with attachment.

The MSE value is sometimes used as a self-standing quality metric. Sometimes, the value RMSE is also used, which is calculated by the formula

$$\text{RMSE} = \sqrt{\text{MSE}}. \quad (3)$$

Another metric to assess the similarity of the two images is the structural similarity index measure (SSIM). This metric is often found in the works of various authors, but is used less frequently than PSNR. The SSIM metric is computed using the formula

$$\text{SSIM} = \frac{(2\mu_C \mu_S + K_1) \times (2\sigma_{CS} + K_2)}{(\mu_C^2 + \mu_S^2 + K_1) \times (\sigma_C^2 + \sigma_S^2 + K_2)}, \quad (4)$$

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

There are many other metrics that can numerically assess the visual invisibility of embedding, such as normalized cross-correlation (NCC), weighted peak signal to noise ratio (WPSNR), Euclidean distance (ED), image fidelity (IF) and others, but their use is much less frequent.

The metrics listed above are also used to prove the reversibility of embedding. In this case, the original cover image and the image from which the embedded information was extracted should be the same. For example, in this case the PSNR value will aim for $+\infty$.

Another important characteristic is the capacity of the embedding. In different sources, authors indicate the capacity of the embedding differently. In some works, the total number of built-in bits is given as capacity, in others the size and color space of the embedded image can be specified, and in others the ratio of embedded bits to the total number of image pixels is given. In the last variant, the EC can be expressed by the formula

$$\text{EC (bpp)} = \frac{B}{M \times N}, \quad (5)$$

where B is the total number of bits embedded in the image.

There are two main approaches for assessing robustness. If an image was used as a secret message or as a watermark, the metrics described above for estimating the visual similarity of the two images may be used to estimate robustness. In this case, the metrics are calculated between the original message/watermark and the retrieved message/watermark.

Another approach is to use bit error rate (BER) metric to quantify the robustness of embedding regardless of the type of embedded data:

$$\text{BER} = \frac{B_e}{B}, \quad (6)$$

where B_e is the number of errors (changed bits) that occurred during extraction.

To assess the resistance to steganalysis used a variety of methods. Statistical steganalysis involves the study of the statistical characteristics of stego image. In the simplest case, histogram analysis is used, in which the histograms of the pixels of the container image and the image with an attachment are compared with each other. Other popular methods of statistical steganalysis are regular and singular analysis (RS-analysis) [9], based on the study of pixel changes and their classification into regular and singular groups, chi-square analysis [10] based on analysis of pairs of values that are exchanged after embedding, and others. Feature-based steganalysis involves extracting many different features from images, which then form a set for training the classifier, such as the support vector machine (SVM) classifier. The classifier then determines whether an image contains an attachment or not. Examples of such steganalysis technique are described in [11]–[13].

There are two different ways to evaluate the computational complexity of an embedding. In a number of papers, the authors perform a theoretical assessment of the complexity of the algorithm. The advantage of this approach is its versatility and independence from the specific software implementation, but it does not allow you to find out any numerical values and fully assess the applicability of the algorithm in practice, where the difference of a few seconds can be very important. Another approach, which is more often used by research authors, is based on conducting computational experiments. In this case, the authors measure the running time of the software implementation of their algorithm (usually in seconds). This allows you to know the running time of the algorithm with high accuracy, but the obtained time characteristics are relevant only for the implementation of the program in a specific programming environment and for its execution on a computer with certain technical characteristics. Sometimes the authors use both versions of the computational complexity assessment, which allows us to comprehensively study the effectiveness of the algorithm by this criterion.

In individual studies, authors can enter additional performance indicators, but the main indicators described are found in most works on hiding information in digital images, and allow researchers to compare their results.

III. FREQUENCY AND SPATIAL DATA HIDING

Before proceeding to the latest research areas in the field of hiding of information in digital images, it is worth reflecting the current state of affairs in the field of steganography and digital watermarking in general.

Currently active development of algorithms for data hiding in digital images is underway, which differs in interesting and effective approaches to improving the embedding quality. To do this, the current section will consider the spatial and frequency domains of embedding, as well as examples of recent work related to information embedding in the spatial or frequency domain.

A. SPATIAL DATA HIDING

All the methods and algorithms for information embedding developed to date can be divided into two classes, depending on which elements of the digital image data undergo changes during embedding. The first class includes data hiding in the spatial domain, and the second class includes data hiding in the frequency domain.

Information embedding in the spatial domain of digital images involves changing the elements of image data without applying any frequency transformations. Most often, such algorithms use image pixels to hide message bits. For example, in the simplest case, one or more of the least significant bits of a pixel is replaced by bits of a secret message, this is the classic LSB method. A diagram illustrating the basic idea of embedding digital images in the spatial domain is shown in Fig. 5. Data hiding in the spatial domain of digital images also includes concealment of data in palette indices, in pixel values encoded in any way, in pixel values obtained by interpolation or prediction.

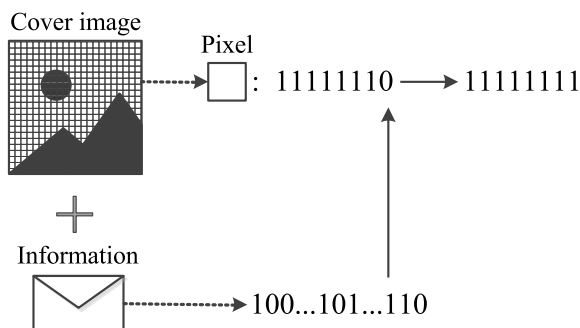


FIGURE 5. Information embedding in the spatial domain.

Spatial data hiding has several advantages. Firstly, we are talking about the high capacity and invisibility of embedding. Secondly, the implementation of spatial embedding does not require large computational resources, which makes such algorithms more preferable for applications for which performance is important. For example, most algorithms for data embedding in digital images in the “Internet of things” are based on the LSB method in the spatial domain [14]–[16]. The main disadvantage of spatial methods is weak robustness. In most cases, the embedded information will be completely destroyed during any image processing with an attachment. However, many algorithms have been developed for which this problem has been successfully solved.

Here are some examples of recent studies of this class.

[17] proposed an embedding method designed to hide text or digital images in pixels of RGB images. To implement embedding, secret data is previously converted into a sequence of two-digit numbers. One digit of this number is embedded in one pixel by changing the pixel value of the cover image to the nearest possible value depending on the difference between the least significant bit of the pixel in the message digit.

The authors of article [18] propose an algorithm for information embedding in binary images. To reduce distortion of stego images, which are especially noticeable when embedding in binary images, a fused distortion measurement using both global statistical characteristics and local structured features and flipping position optimization is used. In [19] there is another embedding scheme in binary (halftone) images, which is based on pair swapping and distortion measurement. It uses syndrome-trellis code.

A common solution in the field of modern digital steganography and digital watermarking is to increase the efficiency of installation on any criteria by optimization. For example, article [20] uses the particle swarm optimization (PSO) to improve the visual quality of steganographic embedding of information by the LSB method. In particular, the PSO searches for the best location for a secret message. In [21], a genetic algorithm (GA) is used to solve a similar problem. In [22], [23] research reviews are presented, that use bioinspired optimization algorithms are used to increase the efficiency of information embedding in digital images.

In [24], a scheme for watermark embedding in a spatial domain based on texture analysis and association rules mining is described. The authors suggest embedding the watermark in highly textured places on the cover image to increase the invisibility and robustness of embedding. Four grayscale histogram-based image features are chosen and then the Apriori algorithm is used to mine the association rules between these features.

Another example of robust watermarking in a spatial domain is presented in [25]. A distinctive feature of the proposed scheme is the calculation of the direct current (DC) coefficient of discrete Fourier transform (DFT) when embedded, and the DC-coefficient is obtained in the spatial domain without the true 2D-DFT.

The article [26] is an example of the direction of hiding data in quantum images that has emerged in recent years. The author offers a scheme for embedding digital watermarks in color quantum images based on the LSB method. Gray code transform is used to improve embedding security.

The article [27] is also devoted to the processing of quantum images. This paper describes embedding techniques for both digital watermarking and steganographic applications. The steganographic scheme starts with an extension of the secret image, which then needs to be encrypted. The watermark embedding scheme uses the Arnold’s cat map to create confusion in the expanded watermark image. When embedding information in a cover image, the least significant and most significant qubits and XORING techniques are used.

TABLE 2. Spatial data hiding.

Ref. no.	Purpose of use	Embedding operation	Key features	Cover image	PSNR, dB	Capacity	Robustness	Steganalysis resistance
[14]	Steganography	LSB	Embedding in different pixels positions in different channels	Color 512×512, JPEG	> 40	1.25 – 1.97 bpp	–	Histogram analysis, RS analysis
[15]	Watermarking	LSB	Pseudo-randomly embedding	Color 512×512	38.20 – 36.98	2 bpp	Fragile	–
[16]	Steganography	LSB	Vector quantization, two-level encoding	Grayscale 512×512, VQ-compressed	33.59 – 32.86	497849 – 515602 bits	–	Chi-square analysis, AUMP LSB detector
[17]	Steganography	Altering the pixel’s digits to the nearest pixel value possible	Encryption the secret data into a sequence of two-digit decimal values	Color 512×512	38.85 – 38.57	3145728 bits	–	Weighted stegoimage analysis
[18]	Steganography	Flipping pixels	Fused distortion measurement, flipping position optimization	Binary 256x256	–	200-1000 bits	–	Feature based analysis (SVM classifier)
[19]	Steganography	Syndrome-trellis code	Pair swapping, distortion measurement	Binary (halftone) 256×256	–	1024 bits	–	Feature based analysis (SVM classifier)
[20]	Steganography	LSB	PSO	Color 128×128	44.87 – 43.97	500 bits	Salt & pepper noise, Gaussian noise	–
[21]	Steganography	LSB	GA	Grayscale 256×256	66.46 – 45.23	8192 – 524288 bits	–	Histogram analysis
[24]	Watermarking	Additive embedding	Texture analysis, association rules mining	Color Grayscale 512×512	50.38 – 47.48	Grayscale 64×64	High	–
[25]	Watermarking	Additive embedding	Arnold transform, DC coefficient of 2D-DFT is obtained in the spatial domain	Color 512×512	38.0 – 36.5	Color 32×32	Medium	–
[26]	Watermarking	LSB	Gray code transform, neighbor interpolation	Quantum Color 256×256, 512×512	≈ 58	Quantum Binary 128×128, 256×256	–	Histogram analysis
[27]	Steganography Watermarking	LSQb XORing techniques and MSQb	Novel enhanced quantum representation, logistic map, Arnold’s cat map	Quantum grayscale 256×256	≈ 48 – 46	Quantum grayscale 128×128	–	–

Table 2 provides basic information about the above examples of research on information embedding in the spatial domain of images. This table shows the purpose of embedding (steganography or watermarking), the embedding operation, key features of the embedding algorithm, the type and size of the cover image, the PSNR value, the corresponding capacity value, and information about resistance to steganalysis and robustness. To characterize the visual invisibility of embedding, the PSNR metric was chosen, since it is the most common and is specified in the vast majority of works. In the “Capacity” column, the capacity is indicated in the same way as in the corresponding paper. In the “Robustness” column, “Fragile” is indicated, if the digital watermark is designed as fragile, or the level of robustness is marked. If the corresponding article describes resistance to 1-4 types of attacks, they are listed in the table. If the authors

note resistance to 5-9 types of attacks in the table, the level of robustness is indicated as “Medium”, if 10 or more types of attacks – “High”. If the specified information is not reflected in some paper, the corresponding cell has a “–” sign.

As it can be seen from Table 2, among the algorithms for spatial domain information embedding, there are both algorithms for steganographic embedding and watermarking algorithms. Among the embedding operations, the LSB replacement operation prevails, but a variety of ways to improve efficiency, including optimization methods, can significantly improve the quality of embedding. Note the presence of resistance to some types of steganalysis in most of the listed researches. Robustness is not analyzed in most of the studies, however, there are examples of robust watermark embedding among the mentioned studies.

B. FREQUENCY DATA HIDING

Frequency embedding methods in the general case are more resistant to destructive effects on the image with an investment due to the fact that embedding is performed not in the image pixels, but in the coefficients of a certain frequency transformation. Most often, when developing steganographic algorithms, a discrete cosine transform (DCT), a discrete wavelet transform (DWT), integer wavelet transform (IWT), and a DFT are used. There are studies whose authors work with other transformations, for example, contourlet transform [28], [29], Hadamard transform [30], [31], curvelet transform [32]. The general frequency embedding scheme is shown in Fig. 6.

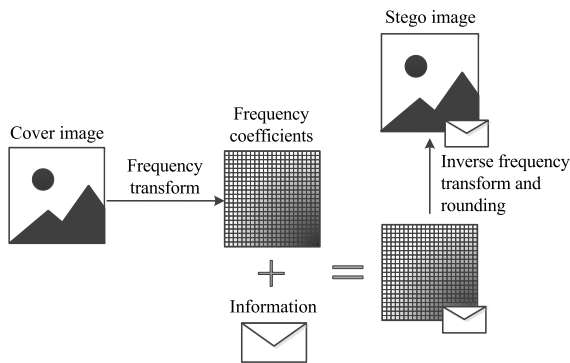


FIGURE 6. Information embedding in the frequency domain.

Data hiding in the frequency domain as well as data hiding in the spatial domain allows you to hide different amounts of information while maintaining high imperceptibility of embedding. In this case, the frequency embedding has increased robustness. However, a significant disadvantage of the frequency embedding is the greater computational complexity compared to spatial embedding. Therefore, embedding algorithms operating with image frequency coefficients are less suitable for real-time systems and applications with limited computing resources.

Let's note examples of works devoted to digital images frequency domain information embedding.

In [33], an algorithm for steganographic embedding of information in color images is presented. Embedding using the LSB method is performed in DCT coefficients. In this case, the RGB plane of the image is pre-processed to select random pixels that will be used for embedding. Random selection of pixels protects the algorithm from brutal attacks and withstands against benchmark steganalysis tools. A GA is used to increase the robustness and invisibility of embedding.

In the articles [34]–[36] a series of studies aimed at achieving the highest embedment capacity in a DCT domain are presented. In [34], the original algorithm is presented; later studies [35], [36] describe improved modifications to this algorithm.

The research [37] is aimed at ensuring the safe transmission of medical images. Information is embedded using DCT-singular value decomposition (SVD) based embedding

process. The medical images are encrypted using compressed sensing encryption before embedding.

In [38] embedding is carried out in the IWT coefficients of a digital image. Additionally, this algorithm uses chaotic mapping to transform an embedded secret message. [39] also used an IWT, but in combination with DCT. The embedded image is pre-encrypted, and then DCT is applied to both the encrypted image and the matrix of wavelet transform coefficients. SVD is used to embed information. Another work that uses a combination of IWT and DCT is described in [40]. In this case, it is proposed to use these transformations to hide digital watermarks in images containing text.

Article [41] proposed a graph wavelet-based steganography scheme to hide a secret image inside a cover image. Graph wavelet is used to increase the imperceptibility of embedding, as it uses an inter-pixel relationship. For preprocessing a secret message, Arnold's transformation is used.

In [42], an algorithm for steganographic embedding in the DFT phase spectrum is described. To achieve error-free retrieval of embedded information, the authors suggest implementing embedding iteratively. To do this, information is extracted at the embedding stage and checked for errors that need to be corrected by re-embedding the already changed block of phase value.

The paper [43] proposes a hybrid algorithm for watermark embedding. The watermark is inserted in the DCT middle band of the DFT magnitude. The authors argue that the combination of two transformations increases the invisibility due to the use of DFT and increases the robustness due to the use of DCT. Before embedding, the watermark is encrypted using Arnold transform, and during embedding, the watermark bits are replaced with pseudo-random sequence elements to increase security.

Recently, the use of neural networks in hiding data in digital images has been actively investigated. For example, in [44] neural networks are used for embedding and extracting digital watermarks. Moreover, embedding can be implemented in the area of different frequency transformations, which provides flexibility of the proposed scheme. The method presented in [45] works with the DCT domain and is claimed to be universal. It is designed for both steganographic applications and for digital watermarks embedding. The paper [46] provides an overview of various strategies for digital image data hiding using the generative adversarial network: cover modification, cover selection, and cover synthesis.

The main characteristics of these studies are shown in Table 3. In comparison with Table 2, the "Domain" column has been added to Table 3, which indicates the frequency conversion area where information is embedded.

According to Table 3, we can see that currently the authors have obtained a large number of different solutions to the problem of increasing the efficiency of hiding of data in the frequency domain of digital images. Many authors use optimization and machine learning methods to optimize embedding parameters or build a hiding space

TABLE 3. Frequency data hiding.

Ref. no.	Purpose of use	Domain	Embedding operation	Key features	Cover image	PSNR, dB	Capacity	Robustness	Steganalysis resistance
[28]	Steganography	Contourlet transform, Fresnelet transform	Additive embedding	GA, PSO, QR code	Grayscale 256×256	≈ 46 – 52	156750 – 902136 bits	–	Chi-square analysis
[29]	Steganography	Contourlet transform	Additive embedding	SVD, QR factorization, nonnegative matrix factorization	Grayscale 512×512	56.95 – 29.37	Grayscale 512×512	High	Feature based analysis (SVM classifier)
[30]	Watermarking	Hadamard transform	Prediction error expansion	Adaline neural network	Grayscale 512×512	≈ 48 – 40	0.1 – 0.5 bpp	Fragile	–
[31]	Watermarking	Hadamard transform	Additive embedding	Dynamic embedding vector	Quantum grayscale 64×64	80.09 – 64.29	Quantum grayscale 64×64	–	Probability analysis
[32]	Steganography	Curvelet transform	LSB	Curvelet denoising technique	Grayscale 255×255	40.26 – 37.13	Grayscale 255×255	–	–
[33]	Steganography	DCT	LSB	GA, random selection of pixels	Color	38.27	2 bpp	Benchmark testing tool StirMark 4.0	Quantitative, statistical, sample pair analysis
[36]	Steganography	DCT, DWT	DCT or DWT coefficients replacing	Quad-tree dividing of image, curve-fitting technique	Color 512×512	43.41 – 28.15	18.77 – 22.70 bpp	Medium	–
[37]	Steganography	DCT	Additive embedding	SVD, compressive sensing encryption	Grayscale 256×256	70.80 – 63.40	Grayscale 256×256 pixels	–	Histogram analysis
[38]	Steganography	IWT	LSB	Modified logistic chaotic map	Color 512×512	58.05 – 54.39	39 – 384 Kbytes	–	Histogram analysis
[39]	Steganography	Redundant IWT+DCT	Additive embedding	SVD, logistic chaotic map	Grayscale 512×512	50.18 – 49.26	Grayscale 256×256	High	Histogram analysis, feature based analysis (SVM classifier)
[40]	Watermarking	IWT+DCT	Additive embedding	For text-images	Grayscale 512×512	58.17 – 57.45	Grayscale 96×96 – 192×192	Medium	–
[41]	Steganography	Transform domain	Alpha blending	Graph wavelet-based analysis, Arnold cat map	Grayscale 256×256	56.03 – 48.03	Grayscale 403×327 – 864×540	–	–
[42]	Steganography	DFT	DFT coefficients phases replacing	Iterative embedding, minimization of changes quantity	Grayscale 512×512	39.55 – 36.79	44996 – 151987 bits	–	–
[43]	Watermarking	DFT+DCT	Additive embedding	Arnold transform, pseudo-random sequences embedding	Grayscale 512×512	66.37 – 57.31	Binary 19×52	High	Histogram analysis
[44]	Watermarking	Transform domain	Additive embedding	Neural networks	Grayscale 512×512	47.52 – 35.93	1024 bits	High	–
[45]	Steganography Watermarking	DCT	Without changing the cover image	Neural networks	Color 504×504	51.00 – 30.00	1 – 19 characters (8 – 152 bits)	Medium	Histogram analysis

that provides the best embedding performance. The most commonly used embedding operation is additive embedding, which is the addition of values of cover image data elements and embedded information, including using a

certain coefficient. It also follows from Table 3 that among the algorithms for embedding of information in the frequency domain, algorithms with the property of robustness are much more common, and this is relevant not only for

digital watermark embedding, but also for steganographic embedding. A number of authors cite the results of research of their algorithms both by the criterion of robustness and resistance to steganalysis.

IV. OVERVIEW OF CURRENT RESEARCH IN DIGITAL STEGANOGRAPHY AND DIGITAL WATERMARKING

In this section, we'll look at some of the most topical ways of digital image data hiding that have been actively developing over the last few years. Each subsection provides a general description of the relevant area of study, examples of current studies in this area and summary tables illustrating the considered area.

A. REVERSIBLE EMBEDDING

The actual direction of data hiding in the last few years is reversible embedding. Reversibility means that after extracting the embedded information, the original cover object can be restored to its original form. This property is especially important for those applications in which some kind of intelligent processing of images containing embedded data is supposed: classification, pattern recognition, edge detection, etc. In this case, even with high imperceptibility of embedding, the additional information contained in the image may distort the result of processing. Therefore, the only solution is to extract the embedded data and restore the cover image in its original form. Reversible embedding algorithms can work with both spatial data and frequency coefficients. Researches on reversible embedding have been published for quite some time [47]–[49], but in recent years their number has increased significantly. Consider in more detail a number of current studies.

For example, in the paper [50], the authors propose a reversible scheme for data hiding in color indexes of a digital image. All indices are divided into three types according to relations with their neighbors. Embedding of secret information is carried out in the indices of one or two types, depending on the required capacity.

The authors of [51] propose their steganography technique of data hiding in the least significant bits of pixels. Embedding occurs in two stages. At the first stage, 2 bits of information are embedded in each pixel of the image, and two changed pixels are combined into a pair of intermediate pixels. At the second stage, using a pair of intermediate pixels, two identical separate pairs are obtained to hide 4 more secret bits, due to which it is possible to achieve a large embedment capacity.

Reference [52] presented an algorithm for reversible steganographic embedding information in compressed JPEG images, which differs in an original approach to the selection of DCT coefficients, the change of which leads to less distortion of the cover image during embedding. To ensure reversibility, the length of the message and the coefficients used to embed the message are hidden inside the image together with the message itself.

Another example of reversible embedding in JPEG images is presented in [53]. In this case, the authors propose using zero DCT coefficients for embedding in order to increase the embedding capacity. To keep the JPEG file size from increasing, and the quality of the stego image remains high, it is proposed to choose only the most suitable zero coefficients for embedding.

The study [54] also focuses on increasing the invisibility of reversible steganographic embedding. Thus, the authors of the study propose a method of reversible data hiding based on the difference value and with statistical features maintained.

A distinctive feature of the method [55] is the generation of three interconnected stego images as a result of embedding the message in the original image. The embedding operations use the pixel value ordering and the prediction error histogram shifting.

In [56], an algorithm is proposed for information embedding in similar blocks of DCT coefficients of stereo pairs. The similarity of the blocks is determined by comparing the low-frequency regions of the DCT spectrum, and embedding is carried out in the mid-frequency region. When the bits are embedded, the messages are converted to two integer values in the range $[-1; 1]$. A pseudo-random number generator is used to select one embedding coefficient from the left or right image of stereo pair.

In most cases, reversible embedding methods and algorithms have a steganographic application. However, in some cases we are talking about the reversible embedding of digital watermarks. For example, an improved reversible contrast mapping algorithm for reversible invisible watermarking is proposed in [57]. The watermark is fragile and is embedded into the spatial domain of the image.

Another example of a reversible watermark embedding algorithm is presented in work [58]. The study [58] proposes an algorithm for reversible information embedding in color images that is invariant to the transition to grayscale. The idea of this algorithm is that information is embedded in a color image, but its grayscale version does not change. Information is embedded only in the blue and red channels, while the green channel is adjusted adaptively to remove the offsets from the gray version. To ensure reversibility, error-correcting bits are used.

A detailed review of research in the field of reversible watermark embedding is presented in [59].

Currently actively developing direction of hiding information in digital images is embedding in combination with secret sharing. The main idea of these methods is that all information is not embedded in a single image, but is divided between several shadow images. As a result, a complete message can be restored having only the required number of parts. Several examples of recent studies on the sharing of secrets, among other things, provide the reversibility of information.

In [60], authors propose a scheme for steganographic data hiding, designed to ensure secure image transmission in the infrastructure of the “Internet of things”. The basis of this

scheme is the Shamir's secret sharing scheme. The proposed scheme consists of two modules: a module for generating encrypted or shadow images and a key module for embedding shadow images in containers. The secret image is divided into several shadow images that are embedded in cover images.

The authors of the paper [61] suggest a secret separation scheme, in which the embedding of secret information is performed during image encoding. This scheme is based on Gray code and absolute moment block truncation coding compression.

In [62], the main focus is on ensuring high embedding capacity. The secret message is embedded in the 4-LSB bit planes by the combination of LSB substitution and XOR operation. First, part of the message is embedded in 3-LSB bit planes, and two shadow images are obtained. Then you need to calculate the complexity of each pixel in the first of the resulting shadow images. If the complexity of a certain pixel exceeds a pre-set threshold, the pixel is complex, and an additional secret message bit is embedded in it.

The study [63] is an example of a combination of secret sharing and digital watermarking. First comes the generation of obfuscated shares of cover image. Then part of the obfuscated shares is subjected to DWT, and the reference image is formed from the most significant coefficients. SVD is applied to the resulting reference image, and a watermark is embedded in the singular values in an additive way.

The above-mentioned studies are listed in Table 4 along with brief characteristics and performance indicators.

According to Table 4, it can be concluded that algorithms for reversible embedding of information primarily work with the spatial domain of digital images. This is also due to the fact that most studies lack any analysis of robustness. A common embedding operation is histogram shifting in which image pixels are changed by modifying the histogram.

Special mention should be made of the studies on embedding additional information in encrypted images. The specificity of this embedding is that the image containing the embedded message or digital watermark is encrypted and inaccessible to without the knowledge of the secret key. Moreover, the presence of a key in the general case allows not only to extract the embedded data, but also to restore the image in its original form. This means that the algorithms implementing this approach are reversible. To extract information and restore the original image, you usually need two keys: a data hiding key and an encryption key. With only the data hiding key, the recipient can retrieve the embedded data, but cannot restore the image. On the contrary, having only the encryption key, it is impossible to extract and decrypt data, but you can restore the original image. Thus, in such works, the image encryption technique is combined with digital steganography and digital watermarking methods. The general operation scheme of such algorithms is presented in Fig. 7.

It should be noted that in some schemes of reversible embedding of information in encrypted images, it is possible to get a stego image similar to the original image after

decryption, but not matching it. While in other schemes, either the decryption and retrieval of embedded information occur simultaneously, or obtaining a stego image is simply not provided, so the restored image always matches the original one.

For the correct extraction of information and restoration of the original cover image, some additional information is also usually required, which is generated during embedding and is unique for each cover image and attachment pair. In most cases, it becomes part of the embedded message and is transmitted inside the image, however, some authors suggest transmitting it separately.

Consider examples of such work.

In [64], information embedding is carried out in the spatial domain of encrypted images. When embedding information, the most significant bits of a part of the pixels are zeroed, and in order to completely restore the original image, you need to know which pixels this procedure was applied to. To do this, a location map is generated, which is compressed using arithmetic coding and embedded in the cover image along with the encrypted message.

A similar method is presented in [65]. It is based on a median-edge detector, which predicts image pixels. Embedding is done in pixels for which the prediction error does not exceed a certain threshold. To retrieve a message, you also need to know the label map, which is generated before embedding, is compressed using Huffman coding, and is embedded in the image along with the message.

The authors of [66] propose an embedding method based on MSB (most significant bit) prediction. Within the framework of this method, two different approaches are described. The first of them, the high-capacity reversible data hiding approach with correction of prediction errors, does not allow to completely restore the original data, but it has high capacity, and the restored image is very close to the original. The second one, the high-capacity reversible data hiding approach with embedded prediction errors, has a slightly lower capacity due to the built-in location map, but it has full reversibility.

Another algorithm combining image encryption and steganography is described in the paper [67]. As a result of image encryption, two blocks of additional information are formed, one of which is compressed. Further, additional information, combined in one sequence with the message, is embedded in the encrypted image, while for encryption and embedding only one key is needed – the encryption key.

Reference [68] deals with spatial embedding in encrypted images. However, the algorithm proposed there also requires knowledge of the embed key and encryption key to extract information and completely restore the original image, respectively. Additional information needed to extract data and restore the cover image is embedded in fixed locations of blocks, and when extracted, it is extracted first of all, before the main payload is extracted.

In study [69], an approach to additional information embedding in encrypted images is implemented for binary

TABLE 4. Reversible data hiding.

Ref. no.	Purpose of use	Domain	Embedding operation	Key features	Cover image	PSNR, dB	Capacity	Robustness	Steganalysis resistance
[50]	Steganography	Spatial	Changing index position code	Hiding secret data into the index tables of palette images, lossless index coding	Color 512×512	40.10 – 34.49	0.5 – 0.98 bit/index	–	–
[51]	Steganography	Spatial	LSB	Dual-layer based embedding, obtaining of 4 stego images	Grayscale 512×512	48.14 – 46.51	1572864 bits	–	RS, pixel difference histogram analysis
[52]	Steganography	DCT	Histogram shifting	Block selection according to simulated distortions	Grayscale 512×512, JPEG	≈ 55 – 40	6000 – 40000 bits	–	–
[53]	Steganography	DCT	Additive embedding	Zero coefficients is used for embedding, distortion cost function	Grayscale 512×512, JPEG	> 36	≈ 17000 – 230000 bits	Fragile	–
[54]	Steganography	Spatial	Difference histogram shifting	Difference values shifting, statistical features maintained	Grayscale 512×512	> 55	0.1 – 0.2 bpp	–	Histogram analysis
[55]	Steganography	Spatial	Prediction error histogram shifting	Pixel value ordering, obtaining of 3 stego images	Grayscale 512×512	≈ 46 – 41	≈ 1300000 bits	–	RS analysis
[56]	Steganography	DCT	Changing difference of a coefficients pair	Conversion of secret data into a sequence of integer value pairs	Color stereo images	43.24 – 31.91	0.12 – 0.38 bpp	–	Chi-square analysis
[57]	Watermarking	Spatial	LSB	Contrast mapping, software and hardware implementation	Color and grayscale 256×256	≈ 43 – 30	≈ 3.5 – 4 bpp	Fragile	–
[58]	Watermarking	Spatial	LSB, difference expansion	Polynomial predictor of R and B components, error correcting bits, pixel selection	Color 510×510	≈ 55 – 40	10000 – 130000 bits	Grayscale invariance	–
[60]	Steganography	Spatial	Pixel replacement	Shamir's polynomials	Grayscale 512×512	46.75	518964 bits	–	Histogram analysis
[61]	Steganography	Spatial	Encoding	Gray code, absolute moment block truncation coding compression	Grayscale 512×512	≈ 45 – 36	49152 – 196608 bits	–	–
[62]	Steganography	Spatial	LSB + XOR	Pixel complexity computing	Grayscale 512×512	≈ 37	≈ 800000 bits	–	–
[63]	Watermarking	DWT	Additive embedding	Shamir's polynomials, SVD	Color 512×512	≈ 60	Grayscale 64×64	High	Histogram analysis

images with low redundancy. The authors propose reordering image blocks, dividing them into homogeneous and heterogeneous, and creating a type image whose white pixels correspond to homogeneous regions, and black ones to heterogeneous ones. Before encrypting the original image, type image is embedded in the image in order to further provide the ability to restore the original image.

The authors of [70] also consider binary images, but as digital watermarks that need to be embedded in some other images. To increase the imperceptibility of embedding, data

embedding positions are adaptively selected using the visual perceptual model. With encryption and embedding keys, the digital watermark can be successfully extracted, while the original image will be completely restored.

The embedding scheme presented in [71], based on homomorphism and matrix embedding. The matrix embedding option is based on the Golay code.

Information embedding in encrypted digital images is most often spatial. However, some studies suggest embedding information in the frequency domain of an encrypted image.

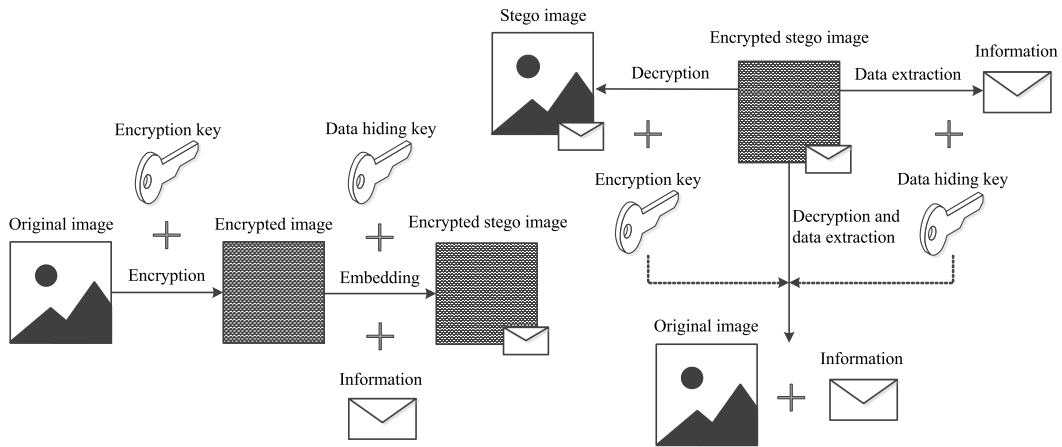


FIGURE 7. Reversible information embedding in encrypted images.

In [72], an IWT is used for this. Location maps are generated according to the most significant bit planes of high frequency coefficients. Location maps are additionally losslessly compressed and, together with secret data, are embedded in the most significant bits of high-frequency wavelet coefficients by changing bits. In this case, the original image can be completely restored only if both the encryption key and the embed key are known. Having only an encryption key, you can access the image, however it will contain embedded data and will not match the original. The use of IWT is explained by the absence of information loss, which is characteristic of other frequency transforms. The method presented in [73] also works in the field of IWT of encrypted images.

All the above-mentioned works are summarized in Table 5. It should be noted that for schemes for invertible embedding of information in encrypted images, the PSNR value is calculated either between the cover image and the stego image, or between the cover image and the totally restored image. In some cases schemes are described in which decryption and retrieval occur simultaneously. Since the original image is exactly the same as the original one, the PSNR value tends to $+\infty$. In other embedding schemes, a similar situation occurs only after sequentially decoding the image and extracting the embedded information. If only decryption was performed, access to the stego image occurs, which still contains embedded data.

Also note that the “Purpose” column is missing from Table 5. The purpose of embedding in this case can be understood as embedding information in encrypted images in general, since in most cases, the authors do not specify whether their algorithm refers to steganography or watermarking.

Table 5 shows that the current algorithms for reversible embedding of information in encrypted images differ in diversity both in the context of embedding operations and in the context of approaches to improving the efficiency of embedding. Most algorithms involve data hiding in the spatial

domain, but the frequency domain is also used for reversible embedding. Resistance to steganalysis is not analyzed in any of the studies. This is due to the specifics of embedding in encrypted images, since image encryption itself is already a feature that can draw attention to the fact that secret information is being transmitted over the communication channel. In this case, the statistical characteristics of the original cover image are violated, and can not give a specialist in steganalysis any information. Robustness is also almost nowhere considered.

B. IMAGE CONTENT BASED EMBEDDING

A specific direction in the field of digital watermarking is embedding information generated from the content of the same image into the image. As noted above, digital watermarks are most often used to protect authorship of digital content. However, this is not the only possible digital watermark application. To ensure integrity monitoring, detection and localization of deliberate changes some information unique to each image is often used as digital watermark. This information is essentially an electronic signature for a digital image. Such a signature is generated on the basis of image data and any additional information, such as a timestamp or a logo, and then embedded in the image as a digital watermark. A diagram of this process is shown in Fig. 8.

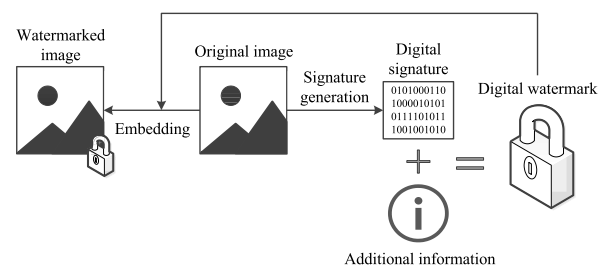


FIGURE 8. Digital signature embedding in digital images.

Let us consider a number of works implementing this approach.

TABLE 5. Reversible data hiding in encrypted images.

Ref. no.	Domain	Embedding operation	Key features	Cover image	PSNR, dB	Capacity	Robustness	Steganalysis resistance
[64]	Spatial	Pixel value expansion	Location map, arithmetic coding	Grayscale 512×512	+∞	0.88 – 0.99 bpp	–	–
[65]	Spatial	MSB	Embedding in encrypted images, median-edge detector predictor, label map	Grayscale 512×512	+∞	1.57 – 3.06 bpp	–	–
[66]	Spatial	MSB	MSB prediction error detection, error location map	Grayscale 512×512	+∞ – 29	0.38 – 1 bpp	–	–
[67]	Spatial	LSB	Rearranging the original image to construct a redundancy image, local smoothness adjustment	Grayscale 512×512	+∞	0.34 – 0.44 bpp	–	–
[68]	Spatial	Concatenation	Run-length coding, matrix-based LSB compression, location map	Grayscale 512×512	51.41 – 41.50	0.99 – 0.98 bpp	–	–
[69]	Spatial	Pixels substitution	Rearranging the original image, type image, pixel prediction	Binary 256×256	+∞ – 18	0.36 – 0.54 bpb	–	–
[70]	Spatial	Pixel bits substituting	Content-adaptive embedding, data embedding position selection	Grayscale 512×512	50.15 – 27.16	Binary 32×32 – 256×256	JPEG compression	–
[71]	Spatial	Matrix embedding	Homomorphism, Golay code	Grayscale 512×512	≈ 57 – 54	0.1 – 0.5 bpp	–	–
[72]	IWT	MSB	Ratio correction, adaptive correction, location map	Grayscale 512×512	+∞	0.68 – 0.83 bpp	–	–
[73]	IWT	Histogram shifting	Orthogonal decomposition	Grayscale 512×512	64.19 – 57.73	0.005 – 0.04 bpp	–	–

Reference [74] is the only example of steganographic embedding in this subsection. It proposed a scheme for the secure transmission of one image inside another, based on the use of a structural digital signature obtained on the basis of stego image data and subsequently determining whether the stego image change was accidental or intentional. To perform the authentication procedure, the image must be transmitted along with the associated digital signature.

Reference [75] proposes a copyright protection scheme based on a combination of the digital watermark implemented in DCT coefficients and cryptography. In this scheme, the DC coefficients of all blocks of the DCT of size 8×8 are combined into one pseudo-image, and the binary map is formed on the basis of the values of blocks of data «pixels». A digital signature is formed from the data of the original image, watermark and time stamp.

The authors of [76] propose using a reversible embedding of the digital watermark based on using of position, intensity and number (PIN) pattern matrix for the authentication of grayscale and color images with the additional use of a digital signature. The signature is formed on the basis of the image data already containing the digital watermark, and then it is also embedded in the signed image. A similar idea was implemented in [77]. In this case, the DWT is first applied to the blue component of the RGB image, then one of the subbands is decomposed according to SVD, and

the digital watermark is embedded in the obtained singular values. A digital signature is generated based on an image already containing a digital watermark and a secret key, and is further embedded in the image.

The authors of [78] propose an algorithm for fragile watermarks embedding, which allows localizing changes made to images and restoring distorted fragments. To do this, at the stage of generating a digital watermark, bit sequences are generated that will be used later if restoration is necessary. For effective recovery of distorted image fragments, K-means clustering is used.

The study [79] describes a system for marking medical images in order to verify their authenticity and access control. This system combines a watermarking method based on quantization index modulation and a joint watermarking-decryption approach. It allows you to embed a watermark on the side of the sender as evidence of the reliability of the image before sending it in encrypted form. Then, on the receiver side, in the decryption process, another watermark should be built in to track access to the image.

The work [80] proposes a fragile watermarking scheme for color image tampering detection and self-recovery. A digital watermark is generated from cover image data and is divided into recovery and authentication watermarks. The recovery watermark is generated using a halftoning algorithm and a block-based method. The XOR operation is additionally used

to create the authentication watermark. Then the watermarks are embedded in the LSB pixels for subsequent authentication and localization of distortions in the images. A similar approach is implemented in [81], but in this work, a digital watermark is generated using the DWT. The authors of the paper [82] apply a similar principle to protect stereo images.

In [83], a watermark is generated based on the highest Faber-Schauder DWT coefficients of a container image combined with a logo image. The resulting watermark is then embedded in the cover's spatial domain using the LSB method.

The research [84] presents a hybrid scheme that combines invisible and zero watermarking techniques to protect medical data. An invisible watermark is formed based on information about the patient and embedded in the medical image. Zero-watermark code is generated based on the invisible watermark and the medical image itself and stored separately. To perform the authentication procedure, the XOR operation is applied to it and the feature pattern obtained from the current image.

In [85], the authors' attention is also focused on the protection of medical data. The watermark consists of authenticity data, which is the result of hashing some logo, and integrity data including tamper detection, localization, and recovery information. A distinctive feature of the proposed algorithm is that region of interest and region of none interest are divided for watermark generation to design an effective recovery function. When embedding a watermark in a medical image, using Slantlet transform, SVD and recursive dither modulation are used.

The algorithm described in [86] is aimed at protecting images containing text (for example, scanned copies of documents). The watermark is formed by averaging the values of the image pixels-containers of the 2×2 pixel block. Then it is embedded in the protected image by applying the linear interpolation technique.

In [87], the chaos based watermarking scheme for effective tamper detection in images is proposed. A watermark is generated for each specific image using the Ikeda chaotic system and Arnold cat map. To increase the security of this scheme, a logical map is used to generate a chaotic sequence. The final watermark is generated by applying the XOR operation to the watermark received during the generation stage and this chaotic sequence.

The authors of [88] propose a technique for fragile digital watermarks embedding in the least significant bits of pixels to provide authentication and integrity control of digital images. A digital watermark is generated based on image data using the SHA-256 hash function.

Paper [89] proposes a column-level authentication technique. For this, a unique digital signature is generated for each column of pixels using a hash function. To hide the signature in the corresponding columns, pixels are selected that were not used when creating the signature.

It should be noted that in most of these works, a digital signature is understood as the result of hashing a data string

containing some information about a digital image without using a private signature key and PKI infrastructure. The use of such a digital signature as a digital watermark cannot guarantee non-repudiation of authorship. In cases where this property is critical, it is necessary to use a full-fledged digital signature generated using the private signature key.

Table 6 provides a list of all the studies listed in this subsection, with key characteristics.

Table 6 shows that almost all of the papers presented relate to methods for the introduction of digital watermarks. A popular embedding operation is the replacement of the LSB in the spatial area. It is easy to see that today authors have proposed many approaches to the creation of unique watermarks for each specific image, based on the content of the image, both with and without the use of cryptographic transformations. Image content based embedding can be both fragile and robust. Resistance to steganalysis is not analysed in any of the studies listed.

C. EDGE DETECTION BASED EMBEDDING

As noted earlier, additional information embedding in digital images using methods of steganography and digital watermarking in many studies is accompanied by the use of various approaches and techniques to increase the efficiency of embedding. A large number of studies in this area are based on the assertion that information embedding in some fragments of images is often more effective than in others. A common approach to increasing the imperceptibility of embedding is to hide data in the edges found in the image. To implement this approach, it is necessary to perform image preprocessing, which consists of edge detection in the image, as a result of which the image pixels will be defined as edge or non-edge. This information is used during embedding as a kind of instruction that allows you to determine which pixels you want to embed information in. A schematic illustration of this process is presented in Fig. 9.

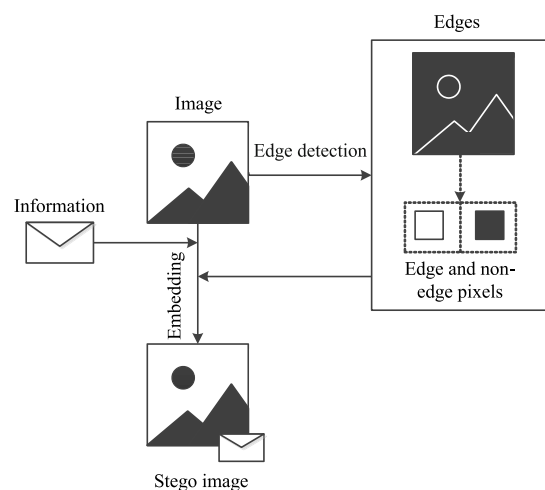


FIGURE 9. Edge detection based information embedding scheme.

Here are examples of such works.

TABLE 6. Image content based data hiding.

Ref. no.	Purpose of use	Domain	Embedding operation	Key features	Cover image	PSNR, dB	Capacity	Robustness	Steganalysis resistance
[74]	Steganography	Spatial	LSB	Fuzzy filtering, color quantization	Color	42.91 – 42.56	Equal to cover size	–	–
[75]	Watermarking	DCT	XOR	Logistic map, binary map, timestamping	Grayscale 512×512	–	Binary 64×64	High	–
[76]	Watermarking	Spatial	LSB	Position, intensity and number (PIN) pattern matrix	Color, Grayscale	49.65 – 49.62	Color, Grayscale $[(M \times 12) / 128] \times N$ pixels, where $M \times N$ – cover size	–	–
[77]	Watermarking	DWT	Additive embedding	SVD	Color 512×512	53.44	Color 256×256	Medium	–
[78]	Watermarking	Spatial + DCT	LSB	Distorted image fragments recovery using K-means clustering	Grayscale 512×512	39.01 – 38.53	96 Kbytes	Fragile	–
[79]	Watermarking	Spatial	Quantization index modulation	Joint watermarking / decryption	Grayscale 576×688, 1008×1280	47.3 – 44.75	498 – 161 Kbits	Additive white Gaussian noise	–
[80]	Watermarking	Spatial	LSB	Halftoning algorithm, digest image, bit adjustment	Color 512×512	≈ 44.6	2 bpp	Fragile	–
[81]	Watermarking	Spatial	LSB	Chaotic map, DWT-based watermark generation	Grayscale 512×512	≈ 44	2 bpp	Fragile	–
[82]	Watermarking	Spatial	LSB	Block classification, DCT-based watermark generation	Stereo 640×480	51.89 – 48.93	2 bpp	Fragile	–
[83]	Watermarking	Spatial	LSB	DWT-based watermark generation	Grayscale 256×2556	≈ 51	$(M \times N) / 2$ bits, where $M \times N$ – cover size	Fragile	–
[84]	Watermarking	DCT	QIM-DM	Zero-watermarking, halftoning algorithm, spread spectrum, seam carving procedure	Grayscale 512×512, 1024×1024	59.05	66088 bits	High	–
[85]	Watermarking	Slantlet transform	Recursive dither modulation	SHA-1, cyclic redundancy check, IWT-based watermark generation, SVD	Grayscale	41.30	Depends on region of interest	High	–
[86]	Watermarking	Spatial	Linear interpolation	For text-images, average value based watermark generation	Grayscale 256×2556	53.63 – 48.41	$(M \times N) / 2$ pixels, where $M \times N$ – cover size	Medium	–
[87]	Watermarking	Spatial	LSB	Arnold cat map, logistic map, Ikeda chaotic system	Grayscale 256×2556	51.14	Binary 256×256	Fragile	–
[88]	Watermarking	Spatial	LSB	SHA-256	Grayscale 512×512	≈ 57	65536 bits	Fragile	–
[89]	Watermarking	Spatial	LSB	Column based signature, MD5	Grayscale 512×512	> 70	65536 bits	Fragile	–

Reference [90] presented a watermark embedding method based on a two-level contourlet transform. To increase the imperceptibility of embedding, when hiding information, the authors prefer more “complex” image blocks, where “complexity” is determined by the high concentration of edges detected using the Canny edge detector.

The [91] work presents an algorithm for the embedding of digital watermarks, based on a combination of a SVD, a GA, and a Canny edge detector. The embedding of watermark bits is done in an additive way, with two different scaling factors being used to improve embedding efficiency.

In [92], in order to ensure a good balance between imperceptibility and reliability, as well as to improve the ability to withstand geometric attacks, the digital watermarks embedding algorithm is proposed, based on the separation of texture blocks and edges in the image in a DWT domain.

In [93], an algorithm is proposed that masks the distortions introduced at the stage of concealing the digital watermark into the edges of image, determined by the combination of Total Variation decomposition and the Canny edge detector. The message bits are embedded in the Haar wavelet transform coefficients.

In [94], on the contrary, it is proposed to ignore the edges and neighboring areas when embedding information. This is because the watermark extracted from the edges is subject to great distortion.

The authors of the work [95] propose a scheme of image authentication using a semi-fragile watermarking system. Developed by the author’s algorithm exploits the Zernike moments to authenticate an image and the Sobel edge map to perform tamper detection. The algorithm combines embedding into the frequency and spatial domains of images.

The edge detection is used not only to embed digital watermarks, but also to hide secret messages using steganography methods. For example, in [96], to increase the efficiency of steganographic embedding, it is proposed to use a fuzzy detector that allows you to determine a larger number of edges than, for example, the classic Canny and Sobel edge detectors. The number of bits that must be embedded in a particular pixel is different for different pixels and depends on whether the pixel is edge-pixel or not. Steganography methods described in the papers [97], [98] are also based on the use of a fuzzy edge detector.

The algorithm presented in [99] embeds into the frequency DWT coefficients corresponding to the edges of the image. To improve the quality of embedding, a GA is used.

In [100], message bits are embedded in the sharp regions by local reference pixels which are detected by the Canny edge detector and optimized by dilation morphological operator. For embedding, a hybrid XOR technique is used, according to which the least significant bits of edge pixels are divided into two groups and transformed according to certain rules.

The article [101] proposes an algorithm for steganographic embedding of information in the spatial domain of images, based on the Sobel edge detector. The main feature of the

algorithm is variable threshold value, which increases the security and capacity of embedding.

The authors of [102] use the modified median edge detector to determine edges on an image. This allows you to hide information in the selected area of an image which reduces the probability of detection.

In [103], an algorithm for high-capacity data hiding in digital images using the Laplacian of Gaussian edge detector is described. The cover image is decomposed into the pair of pixels and then secret bits are embedded into each pair of pixels in an additive way.

In [104], the embedding domain is the coefficients of the dual-tree complex wavelet transform. The authors justify the choice of this frequency conversion by the fact that the presence of a real and imaginary part increases the hiding space and allows for a large embedding capacity. The k -nearest neighbor based machine learning and Canny edge detector is used to improve embedding efficiency.

In [105], a secret sharing scheme is presented to ensure the security of a secret image. This scheme uses optimal asymmetric encryption padding to provide confidentiality for the secret image and a systematic Reed–Solomon based information dispersal algorithms to generate the shares. At the generation stage, noise-like shadow images are generated and then embedded in covers using the fully exploiting modification direction method, which embeds information in a block of two pixels by increasing or decreasing each pixel in the block by a certain amount. Embedding is only performed in blocks that belong to the edges of the image.

These examples illustrate that the edge detection is successfully used to increase the efficiency of information embedding in digital images. Table 7 shows the studies listed in this subsection with the main characteristics.

As follows from Table 7, the most popular in the development of data hiding algorithms is the Canny edge detector, and the most common embedding operations are LSB and additive embedding, both in the spatial domain and in the frequency domain. Edge detection is used in a variety of embedding schemes aimed at achieving various performance indicators. In the schemes of steganography, resistance to various methods of steganalysis is noted, and in the schemes of embedding the digital watermark in some works, there is a high stability to various distortions.

V. ANALYSIS

Despite the variety of existing algorithms for data hiding in digital images, which differ in interesting and original scientific and technical solutions, a number of unsolved problems can be noted.

In some works, imperceptibility of embedding is characterized exclusively through the absence of significant distortions, estimated using various quality metrics. It is worth noting that it is clear from the studies presented in this review that the achievement of high invisibility in the human eye is now being achieved in the vast majority of

TABLE 7. Edge detection based data hiding.

Ref. no.	Purpose of use	Domain	Embedding operation	Key features	Cover image	PSNR, dB	Capacity	Robustness	Steganalysis resistance
[90]	Watermarking	Contourlet transform, DCT	Change in differences between pairs of coefficients	Block complexity, Canny edge detector	Grayscale 512×512	44.06 – 40.06	1024 bits	Medium	–
[91]	Watermarking	Spatial	Additive embedding	GA, SVD, Canny edge detector	Grayscale 512×512	45.22 – 43.80	Binary 32×32	High	–
[92]	Watermarking	DWT	Additive embedding	Arnold scrambling, Canny edge detector	Grayscale 256×256	–	Binary 32×32	Medium	–
[93]	Watermarking	DWT	Additive embedding	Total variation decomposition, Canny edge detector	Grayscale 512×512	46.60 – 44.14	Grayscale 64×32	Additive noise, cropping, rotation, JPEG compression	–
[94]	Watermarking	Spatial	Additive embedding	Canny edge detector, error prediction	Color 256×256	> 35	Binary 256×256	High	–
[95]	Watermarking	Spatial + DWT	Additive embedding	Zernike moments, Sobel edge detector	Grayscale 512×512	40.9	3404 bits	Medium	–
[96]	Steganography	Spatial	LSB	Fuzzy edge detector, Gaussian function	Grayscale 256×256	41.40 – 25.71	1.39 – 3.99 bpp	–	–
[97]	Steganography	Spatial	LSB	Fuzzy edge detector, gradient filter	Grayscale 512×512	56.73 – 48.59	26214 – 183500 bits	–	Feature based analysis (SVM classifier)
[98]	Steganography	Spatial	LSB	Fuzzy edge detector, chaotic method	Grayscale 128×128	50.01 – 48.87	16632 – 21488 bits	–	Histogram analysis
[99]	Steganography	DWT	LSB	GA, mother wavelet matrix based edge detector	Grayscale 512×512	69.04 – 51.92	6.3 – 67.7 Kb	–	–
[100]	Steganography	Spatial	XOR	Dilation morphological operator, Canny edge detector	Color 512×512	54.38 – 43.62	0.10 – 1.24 bpp	–	Histogram analysis, RS analysis
[101]	Steganography	Spatial	LSB	Sobel edge detector, variable threshold value	Color 128×128 – 512×512	47.64 – 46.78	2 bpp	–	RS analysis, sample pair analysis
[102]	Steganography	Spatial	XOR	Modified median edge detector	Grayscale 100×100	≈ 60 – 45	≈ 0.2 – 1 bpp	–	RS analysis, feature based analysis (FLD classifier)
[103]	Steganography	Spatial	Additive embedding	Laplacian of Gaussian edge detector	Grayscale 128×128	45.59 – 38.37	2.08 – 3.10 bpp	–	–
[104]	Steganography	Dual-Tree Complex Wavelet Transform	Batch by batch pixel value embedding	Machine learning, Canny edge detector	Color 256×256 – 512×512	> 50	Color 64×64 – 384×384	–	Histogram analysis
[105]	Steganography	Spatial	Fully exploiting modification direction	Information dispersal algorithms, threshold value based edge detector	Grayscale 512×512	51.42 – 49.74	Grayscale 256×256	–	Feature based analysis (SVM classifier)

cases. Furthermore, the absorption capacity can be very high and can reach several bits per pixel. However, defining the imperceptibility of embedding only through the absence of noticeable distortion is insufficient when it comes to the reliable protection of digital data. The absence of visible distortion does not guarantee the imperceptibility of embedding information in a digital image. Therefore, resistance to various methods of steganalysis is an important criterion for the quality of embedding, primarily when it comes to problems of steganography. It is relevant to search for new approaches to organizing the steganographic embedding of information in digital images that can ensure the achievement of statistical invisibility of embedding and requiring reasonable computational costs. This is also true for digital watermarking, as vulnerability to steganalysis can lead to a situation in which an attacker, being confident in the presence of a digital watermark in a particular image, can change or destroy it. However, the vast majority of watermark embedding algorithms do not address this aspect. Therefore, when creating new watermarking methods, it is also advisable to provide for the possibility of ensuring the statistical invisibility of embedding.

Another problem of many modern algorithms is the possibility of errors when extracting embedded information, in the absence of any destructive effects on the image with the embedding. In some cases, the occurrence of a certain proportion of errors during data extraction is not a problem, for example, when transmitting a digital image as a message, the distortion of several pixels will most likely not even be visible to the naked eye. But the occurrence of errors is completely unacceptable if the information before embedding was compressed or converted using a cryptographic algorithm. This is also true for fragile watermark embedding algorithms that use a hash code or an electronic signature as a watermark. An error even in one bit of the hash code or electronic signature will lead to the compromise of the corresponding digital watermark even in the absence of external destructive influences and attempts to counterfeit. This problem must be taken into account by researchers when developing data hiding algorithms.

The solution of a problem of errors when extracting embedded information is proposed by some researchers, especially those working with reversible information embedding. In a number of cases, it is proposed at the embedding stage to generate some additional information that allows, when extracting, for example, to use the desired order of data elements for extraction. The disadvantage of this solution is that the amount of such additional information can be quite large, in some cases it is comparable in size to the container image itself. If such information is embedded in the image, it reduces the maximum cover image capacity. If this information is transmitted separately from the image with the attachment, this contradicts the idea of steganography imperceptibility and robustness of digital watermarks. For the reason that in the case of steganographic applications, the transfer of additional information that is unique for

each cover image and attachment pair will reveal the existence of a secret data channel, and in the case of digital watermarks, such additional information may be completely lost or distorted by the time it is required to implement the authentication procedure or integrity checks.

It is also worth noting that in a number of studies on digital watermarking, the robustness criterion is not analyzed. Also, in some works where the watermark is supposed to withstand various image processing operations, the resistance to a small number of attacks is stated, which implies that significant distortions of the container will entail the destruction of the watermark and the inability to use it for authentication tasks. Therefore, the improvement of approaches to increase the stability of embedding to various distortions, as well as the development of new ones, are urgent tasks, the solution of which will significantly increase the applicability of digital watermarking algorithms to protect data in information systems. Improving robustness embedding under the influence of destructive influences on stego image is also relevant for steganographic algorithms, the development of which this issue is often not addressed. However, it is obvious that the transmission of information through steganography methods can result in both random and intentional steganography distortions aimed at destroying the built-in message and preventing the hidden exchange of information.

Also on the basis of a large number of different studies on the concealment of information in digital images, it was noted that in most cases the authors did not pay attention to the exchange of keys and parameters of algorithms. At the moment there is no generally accepted key exchange protocol for steganography and watermarking. This problem is most relevant for steganographic embedding. The very idea of steganographic embedding in its complete invisibility to third parties. However, the transmission of keys, for example, in encrypted form over an open communication channel, is an unambiguous unmasking sign. In the case of the presence of some protected channel, the use of steganographic embedding is in principle impractical. However, in the case of keys or parameters unique to the sender-receiver pair, their secure exchange is much easier to implement than when additional information is generated during the embedding process and is unique for each new image with embedded information.

VI. CONCLUSION

Currently, methods of steganography and digital watermarking are actively developing, and many researchers from different countries offer many new algorithms that differ in different quality characteristics. Despite the variety of developed algorithms, in the field of information embedding in digital images, there are still a number of unsolved problems. The overwhelming majority of modern embedding algorithms provide high imperceptibility of embedding, therefore, the attention of researchers working in this field should be aimed at achieving other embedding efficiency

indicators: reversibility, robustness, and resistance to steganalysis. The review showed that work in these areas is underway, but there are still a lot of problems that require new original solutions.

REFERENCES

- [1] J. Fridrich, *Steganography in Digital Media: Principles, Algorithms, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
- [2] A. S. Panah, R. Van Schyndel, T. Sellis, and E. Bertino, "On the properties of non-media digital watermarking: A review of state of the art techniques," *IEEE Access*, vol. 4, pp. 2670–2704, 2016, doi: [10.1109/ACCESS.2016.2570812](https://doi.org/10.1109/ACCESS.2016.2570812).
- [3] M. Hussain, A. W. A. Wahab, Y. I. B. Idris, A. T. S. Ho, and K.-H. Jung, "Image steganography in spatial domain: A survey," *Signal Process., Image Commun.*, vol. 65, pp. 46–66, Jul. 2018, doi: [10.1016/j.image.2018.03.012](https://doi.org/10.1016/j.image.2018.03.012).
- [4] I. J. Kadhim, P. Premaratne, P. J. Vial, and B. Halloran, "Comprehensive survey of image steganography: Techniques, evaluations, and trends in future research," *Neurocomputing*, vol. 335, pp. 299–326, Mar. 2019, doi: [10.1016/j.neucom.2018.06.075](https://doi.org/10.1016/j.neucom.2018.06.075).
- [5] K. Karampidis, E. Kavallieratou, and G. Papadourakis, "A review of image steganalysis techniques for digital forensics," *J. Inf. Secur. Appl.*, vol. 40, pp. 217–235, Jun. 2018, doi: [10.1016/j.jisa.2018.04.005](https://doi.org/10.1016/j.jisa.2018.04.005).
- [6] T.-S. Reinel, R.-P. Raul, and I. Gustavo, "Deep learning applied to steganalysis of digital images: A systematic review," *IEEE Access*, vol. 7, pp. 68970–68990, 2019, doi: [10.1109/ACCESS.2019.2918086](https://doi.org/10.1109/ACCESS.2019.2918086).
- [7] A. F. Qasim, F. Meziane, and R. Aspin, "Digital watermarking: Applicability for developing trust in medical imaging workflows state of the art review," *Comput. Sci. Rev.*, vol. 27, pp. 45–60, Feb. 2018, doi: [10.1016/j.cosrev.2017.11.003](https://doi.org/10.1016/j.cosrev.2017.11.003).
- [8] S. Kumar, B. K. Singh, and M. Yadav, "A recent survey on multimedia and database watermarking," *Multimedia Tools Appl.*, vol. 79, nos. 27–28, pp. 20149–20197, Jul. 2020, doi: [10.1007/s11042-020-08881-y](https://doi.org/10.1007/s11042-020-08881-y).
- [9] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB steganography in color, and gray-scale images," *IEEE MultimediaMag.*, vol. 8, no. 4, pp. 22–28, Oct. 2001, doi: [10.1109/93.959097](https://doi.org/10.1109/93.959097).
- [10] A. Westfeld and A. Pfitzmann, "Attacks on steganographic systems," in *Information Hiding*. Berlin, Germany: Springer, 2000, pp. 61–76, doi: [10.1007/10719724_5](https://doi.org/10.1007/10719724_5).
- [11] P. Wang, Z. Wei, and L. Xiao, "Spatial rich model steganalysis feature normalization on random feature-subsets," *Soft Comput.*, vol. 22, no. 6, pp. 1981–1992, Mar. 2018, doi: [10.1007/s00500-016-2459-5](https://doi.org/10.1007/s00500-016-2459-5).
- [12] T. Denmark, M. Boroumand, and J. Fridrich, "Steganalysis features for content-adaptive JPEG steganography," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1736–1746, Aug. 2016, doi: [10.1109/TIFS.2016.2555281](https://doi.org/10.1109/TIFS.2016.2555281).
- [13] Y. Pathak, K. V. Arya, and S. Tiwari, "Feature selection for image steganalysis using Levy flight-based grey wolf optimization," *Multimedia Tools Appl.*, vol. 78, no. 2, pp. 1473–1494, Jan. 2019, doi: [10.1007/s11042-018-6155-6](https://doi.org/10.1007/s11042-018-6155-6).
- [14] A. K. Bairagi, R. Khondoker, and R. Islam, "An efficient steganographic approach for protecting communication in the Internet of Things (IoT) critical infrastructures," *Inf. Secur. J., Global Perspective*, vol. 25, nos. 4–6, pp. 197–212, Dec. 2016, doi: [10.1080/19393555.2016.1206640](https://doi.org/10.1080/19393555.2016.1206640).
- [15] S. A. Parah, J. A. Sheikh, F. Ahad, and G. M. Bhat, "High capacity and secure electronic patient record (EPR) embedding in color images for IoT driven healthcare systems," in *Internet of Things and Big Data Analytics Toward Next-Generation Intelligence*, N. Dey, A. E. Hassanien, C. Bhatt, A. S. Ashour, and S. C. Satapathy, Eds. Cham, Switzerland: Springer, 2018, pp. 409–437.
- [16] C.-T. Huang, M.-Y. Tsai, L.-C. Lin, W.-J. Wang, and S.-J. Wang, "VQ-based data hiding in IoT networks using two-level encoding with adaptive pixel replacements," *J. Supercomput.*, vol. 74, no. 9, pp. 4295–4314, Sep. 2018, doi: [10.1007/s11227-016-1874-9](https://doi.org/10.1007/s11227-016-1874-9).
- [17] V. Verma, S. K. Muttou, and V. B. Singh, "Enhanced payload and trade-off for image steganography via a novel pixel digits alteration," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7471–7490, Mar. 2020, doi: [10.1007/s11042-019-08283-9](https://doi.org/10.1007/s11042-019-08283-9).
- [18] W. Lu, L. He, Y. Yeung, Y. Xue, H. Liu, and B. Feng, "Secure binary image steganography based on fused distortion measurement," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 6, pp. 1608–1618, Jun. 2019, doi: [10.1109/TCSVT.2018.2852702](https://doi.org/10.1109/TCSVT.2018.2852702).
- [19] W. Liu, X. Yin, W. Lu, J. Zhang, J. Zeng, S. Shi, and M. Mao, "Secure halftone image steganography with minimizing the distortion on pair swapping," *Signal Process.*, vol. 167, Feb. 2020, Art. no. 107287, doi: [10.1016/j.sigpro.2019.107287](https://doi.org/10.1016/j.sigpro.2019.107287).
- [20] W. A. Shukur and K. K. Jabbar, "Information hiding using LSB technique based on developed PSO algorithm," *Int. J. Electr. Comput. Eng.*, vol. 8, no. 2, pp. 1156–1168, Apr. 2018, doi: [10.11591/ijece.v8i2.pp1156-1168](https://doi.org/10.11591/ijece.v8i2.pp1156-1168).
- [21] R. Wazirali, W. Alasmary, M. M. E. A. Mahmoud, and A. Alhindi, "An optimized steganography hiding capacity and imperceptibly using genetic algorithms," *IEEE Access*, vol. 7, pp. 133496–133508, 2019, doi: [10.1109/ACCESS.2019.2941440](https://doi.org/10.1109/ACCESS.2019.2941440).
- [22] H. C. Huang, F. C. Chang, Y. H. Chen, and S. C. Chu, "Survey of bio-inspired computing for information hiding," *J. Inf. Hiding Multimedia Signal Process.*, vol. 6, no. 3, pp. 430–443, May 2015.
- [23] B. Akay and D. Karaboga, "A survey on the applications of artificial bee colony in signal, image, and video processing," *Signal, Image Video Process.*, vol. 9, no. 4, pp. 967–990, May 2015, doi: [10.1007/s11760-015-0758-4](https://doi.org/10.1007/s11760-015-0758-4).
- [24] M. Ghadi, L. Laouamer, L. Nana, and A. Pasqu, "A blind spatial domain-based image watermarking using texture analysis and association rules mining," *Multimedia Tools Appl.*, vol. 78, no. 12, pp. 15705–15750, Jun. 2019, doi: [10.1007/s11042-018-6851-2](https://doi.org/10.1007/s11042-018-6851-2).
- [25] Q. Su, D. Liu, Z. Yuan, G. Wang, X. Zhang, B. Chen, and T. Yao, "New rapid and robust color image watermarking technique in spatial domain," *IEEE Access*, vol. 7, pp. 30398–30409, 2019, doi: [10.1109/ACCESS.2019.2895062](https://doi.org/10.1109/ACCESS.2019.2895062).
- [26] W. Hu, R.-G. Zhou, J. Luo, and B. Liu, "LSBs-based quantum color images watermarking algorithm in edge region," *Quantum Inf. Process.*, vol. 18, no. 1, p. 16, Nov. 2018, doi: [10.1007/s11128-018-2138-9](https://doi.org/10.1007/s11128-018-2138-9).
- [27] A. A. A. El-Latif, B. Abd-El-Atty, M. S. Hossain, M. A. Rahman, A. Alamri, and B. B. Gupta, "Efficient quantum information hiding for remote medical image sharing," *IEEE Access*, vol. 6, pp. 21075–21083, 2018, doi: [10.1109/ACCESS.2018.2820603](https://doi.org/10.1109/ACCESS.2018.2820603).
- [28] S. U. Maheswari and D. J. Hemant, "Performance enhanced image steganography systems using transforms and optimization techniques," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 415–436, Jan. 2017, doi: [10.1007/s11042-015-3035-1](https://doi.org/10.1007/s11042-015-3035-1).
- [29] M. S. Subhedar and V. H. Mankar, "Image steganography using contourlet transform and matrix decomposition techniques," *Multimedia Tools Appl.*, vol. 78, no. 15, pp. 22155–22181, Aug. 2019, doi: [10.1007/s11042-019-7512-9](https://doi.org/10.1007/s11042-019-7512-9).
- [30] Z. Pakdaman, S. Saryazdi, and H. Nezamabadi-Pour, "A prediction based reversible image watermarking in Hadamard domain," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 8517–8545, Mar. 2017, doi: [10.1007/s11042-016-3490-3](https://doi.org/10.1007/s11042-016-3490-3).
- [31] X. Song, S. Wang, A. A. A. El-Latif, and X. Niu, "Dynamic watermarking scheme for quantum images based on Hadamard transform," *Multimedia Syst.*, vol. 20, no. 4, pp. 379–388, Jul. 2014, doi: [10.1007/s00530-014-0355-3](https://doi.org/10.1007/s00530-014-0355-3).
- [32] H. Mostafa, A. F. Ali, and G. El Taweal, "Hybrid curvelet transform and least significant bit for image steganography," in *Proc. IEEE 7th Int. Conf. Intell. Comput. Inf. Syst. (ICICIS)*, Dec. 2015, pp. 300–305, doi: [10.1109/IntelCIS.2015.7397238](https://doi.org/10.1109/IntelCIS.2015.7397238).
- [33] R. Biswas and S. K. Bandyapadhyay, "Random selection based GA optimization in 2D-DCT domain color image steganography," *Multimedia Tools Appl.*, vol. 79, nos. 11–12, pp. 7101–7120, Mar. 2020, doi: [10.1007/s11042-019-08497-x](https://doi.org/10.1007/s11042-019-08497-x).
- [34] T. Rabie and I. Kamel, "On the embedding limits of the discrete cosine transform," *Multimedia Tools Appl.*, vol. 75, no. 10, pp. 5939–5957, May 2016, doi: [10.1007/s11042-015-2557-x](https://doi.org/10.1007/s11042-015-2557-x).
- [35] T. Rabie and I. Kamel, "Toward optimal embedding capacity for transform domain steganography: A quad-tree adaptive-region approach," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 8627–8650, Mar. 2017, doi: [10.1007/s11042-016-3501-4](https://doi.org/10.1007/s11042-016-3501-4).
- [36] T. Rabie, I. Kamel, and M. Baziyad, "Maximizing embedding capacity and stego quality: Curve-fitting in the transform domain," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8295–8326, Apr. 2018, doi: [10.1007/s11042-017-4727-5](https://doi.org/10.1007/s11042-017-4727-5).

- [37] R. Thanki, S. Borra, V. Dwivedi, and K. Borisagar, "A steganographic approach for secure communication of medical images based on the DCT-SVD and the compressed sensing (CS) theory," *Imag. Sci. J.*, vol. 65, no. 8, pp. 457–467, Nov. 2017, doi: [10.1080/13682199.2017.1367129](https://doi.org/10.1080/13682199.2017.1367129).
- [38] M. Y. Valandar, P. Ayubi, and M. J. Barani, "A new transform domain steganography based on modified logistic chaotic map for color images," *J. Inf. Secur. Appl.*, vol. 34, pp. 142–151, Jun. 2017, doi: [10.1016/j.jisa.2017.04.004](https://doi.org/10.1016/j.jisa.2017.04.004).
- [39] S. Arunkumar, V. Subramaniaswamy, V. Vijayakumar, N. Chilamkurti, and R. Logesh, "SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images," *Measurement*, vol. 139, pp. 426–437, Jun. 2019, doi: [10.1016/j.measurement.2019.02.069](https://doi.org/10.1016/j.measurement.2019.02.069).
- [40] R. A. Alotaibi and L. A. Elrefaei, "Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT)," *Appl. Comput. Informat.*, vol. 15, no. 2, pp. 191–202, Jul. 2019, doi: [10.1016/j.aci.2018.06.003](https://doi.org/10.1016/j.aci.2018.06.003).
- [41] V. K. Sharma, D. K. Srivastava, and P. Mathur, "Efficient image steganography using graph signal processing," *IET Image Process.*, vol. 12, no. 6, pp. 1065–1071, Jun. 2018, doi: [10.1049/iet-ipc.2017.0965](https://doi.org/10.1049/iet-ipc.2017.0965).
- [42] O. Evsutin, A. Kokurina, R. Meshcheryakov, and O. Shumskaya, "The adaptive algorithm of information unmistakable embedding into digital images based on the discrete Fourier transformation," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 28567–28599, Nov. 2018, doi: [10.1007/s11042-018-6055-9](https://doi.org/10.1007/s11042-018-6055-9).
- [43] M. Hamidi, M. E. Haziti, H. Cherifi, and M. E. Hassouni, "Hybrid blind robust image watermarking technique based on DFT-DCT and Arnold transform," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 27181–27214, Oct. 2018, doi: [10.1007/s11042-018-5913-9](https://doi.org/10.1007/s11042-018-5913-9).
- [44] M. Ahmadi, A. Norouzi, N. Karimi, S. Samavi, and A. Emami, "ReDMark: Framework for residual diffusion watermarking based on deep networks," *Expert Syst. Appl.*, vol. 146, May 2020, Art. no. 113157, doi: [10.1016/j.eswa.2019.113157](https://doi.org/10.1016/j.eswa.2019.113157).
- [45] R. Jarusek, E. Volna, and M. Kotyrba, "Robust steganographic method based on unconventional approach of neural networks," *Appl. Soft Comput.*, vol. 67, pp. 505–518, Jun. 2018, doi: [10.1016/j.asoc.2018.03.023](https://doi.org/10.1016/j.asoc.2018.03.023).
- [46] J. Liu, Y. Ke, Z. Zhang, Y. Lei, J. Li, M. Zhang, and X. Yang, "Recent advances of image steganography with generative adversarial networks," *IEEE Access*, vol. 8, pp. 60575–60597, 2020, doi: [10.1109/ACCESS.2020.2983175](https://doi.org/10.1109/ACCESS.2020.2983175).
- [47] J. Fridrich, M. Goljan, and R. Du, "Invertible authentication," *Proc. SPIE*, vol. 4314, pp. 197–208, Aug. 2001, doi: [10.1117/12.435400](https://doi.org/10.1117/12.435400).
- [48] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 890–896, Aug. 2003, doi: [10.1109/TCSVT.2003.815962](https://doi.org/10.1109/TCSVT.2003.815962).
- [49] A. M. Alattar, "Reversible watermark using the difference expansion of a generalized integer transform," *IEEE Trans. Image Process.*, vol. 13, no. 8, pp. 1147–1156, Aug. 2004, doi: [10.1109/TIP.2004.828418](https://doi.org/10.1109/TIP.2004.828418).
- [50] J.-C. Chuang, Y.-C. Hu, C.-M. Chen, Y.-H. Lin, and Y. Chen, "Joint index coding and reversible data hiding methods for color image quantization," *Multimedia Tools Appl.*, vol. 78, no. 24, pp. 35537–35558, Dec. 2019, doi: [10.1007/s11042-019-08193-w](https://doi.org/10.1007/s11042-019-08193-w).
- [51] A. K. Sahu and G. Swain, "Reversible image steganography using dual-layer LSB matching," *Sens. Imag.*, vol. 21, no. 1, p. 1, Dec. 2019, doi: [10.1007/s11220-019-0262-y](https://doi.org/10.1007/s11220-019-0262-y).
- [52] D. Hou, H. Wang, W. Zhang, and N. Yu, "Reversible data hiding in JPEG image based on DCT frequency and block selection," *Signal Process.*, vol. 148, pp. 41–47, Jul. 2018, doi: [10.1016/j.sigpro.2018.02.002](https://doi.org/10.1016/j.sigpro.2018.02.002).
- [53] F. Di, M. Zhang, F. Huang, J. Liu, and Y. Kong, "Reversible data hiding in JPEG images based on zero coefficients and distortion cost function," *Multimedia Tools Appl.*, vol. 78, no. 24, pp. 34541–34561, Dec. 2019, doi: [10.1007/s11042-019-08109-8](https://doi.org/10.1007/s11042-019-08109-8).
- [54] T. Li, H. Li, L. Hu, and H. Li, "A reversible steganography method with statistical features maintained based on the difference value," *IEEE Access*, vol. 8, pp. 12845–12855, 2020, doi: [10.1109/ACCESS.2020.2964830](https://doi.org/10.1109/ACCESS.2020.2964830).
- [55] X.-Z. Xie, C.-C. Chang, and C.-C. Lin, "A hybrid reversible data hiding for multiple images with high embedding capacity," *IEEE Access*, vol. 8, pp. 37–52, 2020, doi: [10.1109/ACCESS.2019.2961764](https://doi.org/10.1109/ACCESS.2019.2961764).
- [56] W.-C. Yang and L.-H. Chen, "Reversible DCT-based data hiding in stereo images," *Multimedia Tools Appl.*, vol. 74, no. 17, pp. 7181–7193, Sep. 2015, doi: [10.1007/s11042-014-1958-6](https://doi.org/10.1007/s11042-014-1958-6).
- [57] S. Das, A. K. Sunaniya, R. Maity, and N. P. Maity, "Parallel hardware implementation of efficient embedding bit rate control based contrast mapping algorithm for reversible invisible watermarking," *IEEE Access*, vol. 8, pp. 69072–69095, 2020, doi: [10.1109/ACCESS.2020.2986134](https://doi.org/10.1109/ACCESS.2020.2986134).
- [58] D. Hou, W. Zhang, K. Chen, S.-J. Lin, and N. Yu, "Reversible data hiding in color image with grayscale invariance," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 29, no. 2, pp. 363–374, Feb. 2019, doi: [10.1109/TCSVT.2018.2803303](https://doi.org/10.1109/TCSVT.2018.2803303).
- [59] A. Menendez-Ortiz, C. Feregrino-Urbe, R. Hasimoto-Beltran, and J. J. Garcia-Hernandez, "A survey on reversible watermarking for multimedia content: A robustness overview," *IEEE Access*, vol. 7, pp. 132662–132681, 2019, doi: [10.1109/ACCESS.2019.2940972](https://doi.org/10.1109/ACCESS.2019.2940972).
- [60] L. Li, M. S. Hossain, A. A. A. El-Latif, and M. F. Alhamid, "Distortion less secret image sharing scheme for Internet of Things system," *Cluster Comput.*, vol. 22, no. S1, pp. 2293–2307, Jan. 2019, doi: [10.1007/s10586-017-1345-y](https://doi.org/10.1007/s10586-017-1345-y).
- [61] T.-F. Cheng, C.-C. Chang, and L. Liu, "Secret sharing: Using meaningful image shadows based on Gray code," *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 9337–9362, Apr. 2017, doi: [10.1007/s11042-016-3535-7](https://doi.org/10.1007/s11042-016-3535-7).
- [62] C.-C. Chang, Y. Liu, and K. Chen, "Real-time adaptive visual secret sharing with reversibility and high capacity," *J. Real-Time Image Process.*, vol. 16, no. 4, pp. 871–881, Aug. 2019, doi: [10.1007/s11554-018-0813-9](https://doi.org/10.1007/s11554-018-0813-9).
- [63] P. Singh and B. Raman, "Reversible data hiding based on Shamir's secret sharing for color images over cloud," *Inf. Sci.*, vol. 422, pp. 77–97, Jan. 2018, doi: [10.1016/j.ins.2017.08.077](https://doi.org/10.1016/j.ins.2017.08.077).
- [64] D. Huang and J. Wang, "High-capacity reversible data hiding in encrypted image based on specific encryption process," *Signal Process., Image Commun.*, vol. 80, Feb. 2020, Art. no. 115632, doi: [10.1016/j.image.2019.115632](https://doi.org/10.1016/j.image.2019.115632).
- [65] L. Liu, A. Wang, and C.-C. Chang, "Separable reversible data hiding in encrypted images with high capacity based on median-edge detector prediction," *IEEE Access*, vol. 8, pp. 29639–29647, 2020, doi: [10.1109/ACCESS.2020.2972736](https://doi.org/10.1109/ACCESS.2020.2972736).
- [66] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE Trans. Inf. Forensics Security*, vol. 13, no. 7, pp. 1670–1681, Jul. 2018, doi: [10.1109/TIFS.2018.2799381](https://doi.org/10.1109/TIFS.2018.2799381).
- [67] Z.-L. Liu and C.-M. Pun, "Reversible image reconstruction for reversible data hiding in encrypted images," *Signal Process.*, vol. 161, pp. 50–62, Aug. 2019, doi: [10.1016/j.sigpro.2019.03.016](https://doi.org/10.1016/j.sigpro.2019.03.016).
- [68] C. Qin, Z. He, X. Luo, and J. Dong, "Reversible data hiding in encrypted image with separable capability and high embedding capacity," *Inf. Sci.*, vol. 465, pp. 285–304, Oct. 2018, doi: [10.1016/j.ins.2018.07.021](https://doi.org/10.1016/j.ins.2018.07.021).
- [69] H. Ren, W. Lu, and B. Chen, "Reversible data hiding in encrypted binary images by pixel prediction," *Signal Process.*, vol. 165, pp. 268–277, Dec. 2019, doi: [10.1016/j.sigpro.2019.07.020](https://doi.org/10.1016/j.sigpro.2019.07.020).
- [70] Y. Yao, W. Zhang, H. Wang, H. Zhou, and N. Yu, "Content-adaptive reversible visible watermarking in encrypted images," *Signal Process.*, vol. 164, pp. 386–401, Nov. 2019, doi: [10.1016/j.sigpro.2019.06.034](https://doi.org/10.1016/j.sigpro.2019.06.034).
- [71] S. Chen, C.-C. Chang, and Q. Liao, "Fidelity preserved data hiding in encrypted images based on homomorphism and matrix embedding," *IEEE Access*, vol. 8, pp. 22345–22356, 2020, doi: [10.1109/ACCESS.2020.2968577](https://doi.org/10.1109/ACCESS.2020.2968577).
- [72] G. Ma and J. Wang, "Efficient reversible data hiding in encrypted images based on multi-stage integer wavelet transform," *Signal Process., Image Commun.*, vol. 75, pp. 55–63, Jul. 2019, doi: [10.1016/j.image.2019.03.013](https://doi.org/10.1016/j.image.2019.03.013).
- [73] L. Xiong, Z. Xu, and Y.-Q. Shi, "An integer wavelet transform based scheme for reversible data hiding in encrypted images," *Multidimensional Syst. Signal Process.*, vol. 29, no. 3, pp. 1191–1202, Jul. 2018, doi: [10.1007/s11045-017-0497-5](https://doi.org/10.1007/s11045-017-0497-5).
- [74] F. I. Alam and M. M. Islam, "An investigation into image hiding steganography with digital signature framework," in *Proc. Int. Conf. Informat., Electron. Vis. (ICIEV)*, May 2013, pp. 1–6, doi: [10.1109/ICIEV.2013.6572548](https://doi.org/10.1109/ICIEV.2013.6572548).
- [75] S. Rawat and B. Raman, "A publicly verifiable lossless watermarking scheme for copyright protection and ownership assertion," *AEU-Int. J. Electron. Commun.*, vol. 66, no. 11, pp. 955–962, Nov. 2012, doi: [10.1016/j.aeue.2012.04.004](https://doi.org/10.1016/j.aeue.2012.04.004).
- [76] S. K. Singh, N. Poria, and P. Palanisamy, "Reversible watermarking with embedded digital signature," in *Proc. Int. Conf. Comput. Power, Energy, Inf. Commun. (ICCPEIC)*, Apr. 2014, pp. 478–481, doi: [10.1109/ICCPEIC.2014.6915411](https://doi.org/10.1109/ICCPEIC.2014.6915411).

- [77] X. Cui, Y. Wang, X. Zheng, Y. Han, H. Qiao, and S. Li, "A novel color image watermarking algorithm based on digital signature," in *Proc. Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber. Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2019, pp. 267–274, doi: 10.1109/iThings/GreenCom/CPSCom/SmartData.2019.00065.
- [78] A. Abdelhakim, H. I. Saleh, and M. Abdelhakim, "Fragile watermarking for image tamper detection and localization with effective recovery capability using K-means clustering," *Multimedia Tools Appl.*, vol. 78, no. 22, pp. 32523–32563, Nov. 2019, doi: 10.1007/s11042-019-07986-3.
- [79] D. Bouslimi and G. Coatrieux, "A crypto-watermarking system for ensuring reliability control and traceability of medical images," *Signal Process., Image Commun.*, vol. 47, pp. 160–169, Sep. 2016, doi: 10.1016/j.image.2016.05.021.
- [80] J. Molina-Garcia, B. P. Garcia-Salgado, V. Ponomaryov, R. Reyes-Reyes, S. Sadovnychiy, and C. Cruz-Ramos, "An effective fragile watermarking scheme for color image tampering detection and self-recovery," *Signal Process., Image Commun.*, vol. 81, Feb. 2020, Art. no. 115725, doi: 10.1016/j.image.2019.115725.
- [81] W.-L. Tai and Z.-J. Liao, "Image self-recovery with watermark self-embedding," *Signal Process., Image Commun.*, vol. 65, pp. 11–25, Jul. 2018, doi: 10.1016/j.image.2018.03.011.
- [82] M. Yu, J. Wang, G. Jiang, Z. Peng, F. Shao, and T. Luo, "New fragile watermarking method for stereo image authentication with localization and recovery," *AEU-Int. J. Electron. Commun.*, vol. 69, no. 1, pp. 361–370, Jan. 2015, doi: 10.1016/j.aeue.2014.10.006.
- [83] A. Azeroual and K. Afdel, "Real-time image tamper localization based on fragile watermarking and faber-schauder wavelet," *AEU-Int. J. Electron. Commun.*, vol. 79, pp. 207–218, Sep. 2017, doi: 10.1016/j.aeue.2017.06.001.
- [84] M. Cedillo-Hernandez, A. Cedillo-Hernandez, M. Nakano-Miyatake, and H. Perez-Meana, "Improving the management of medical imaging by using robust and secure dual watermarking," *Biomed. Signal Process. Control*, vol. 56, Feb. 2020, Art. no. 101695, doi: 10.1016/j.bspc.2019.101695.
- [85] X. Liu, J. Lou, H. Fang, Y. Chen, P. Ouyang, Y. Wang, B. Zou, and L. Wang, "A novel robust reversible watermarking scheme for protecting authenticity and integrity of medical images," *IEEE Access*, vol. 7, pp. 76580–76598, 2019, doi: 10.1109/ACCESS.2019.2921894.
- [86] L. Laouamer and O. Tayan, "Performance evaluation of a document image watermarking approach with enhanced tamper localization and recovery," *IEEE Access*, vol. 6, pp. 26144–26166, 2018, doi: 10.1109/ACCESS.2018.2831599.
- [87] O. Benrhouma, H. Hermassi, A. A. A. El-Latif, and S. Belghith, "Chaotic watermark for blind forgery detection in images," *Multimedia Tools Appl.*, vol. 75, no. 14, pp. 8695–8718, Jul. 2016, doi: 10.1007/s11042-015-2786-z.
- [88] E. Gul and S. Ozturk, "A novel hash function based fragile watermarking method for image integrity," *Multimedia Tools Appl.*, vol. 78, no. 13, pp. 17701–17718, Jul. 2019, doi: 10.1007/s11042-018-7084-0.
- [89] S. Khan, M. Wahid, T. Khan, N. Ahmad, and M. H. Zafar, "Column level image authentication technique using hidden digital signatures," in *Proc. 23rd Int. Conf. Automat. Comput. (ICAC)*, Sep. 2018, pp. 1–6, doi: 10.23919/ICAC.2018.8748967.
- [90] H. R. Fazlali, S. Samavi, N. Karimi, and S. Shirani, "Adaptive blind image watermarking using edge pixel concentration," *Multimedia Tools Appl.*, vol. 76, no. 2, pp. 3105–3120, Jan. 2017, doi: 10.1007/s11042-015-3200-6.
- [91] T. T. Takore, P. R. Kumar, and G. L. Devi, "A robust and oblivious grayscale image watermarking scheme based on edge detection, SVD, and GA," in *Proc. 2nd Int. Conf. Micro-Electron., Electromagn. Telecommun.*, Singapore, 2018, pp. 51–61, doi: 10.1007/978-981-10-4280-5_6.
- [92] Y. Wang, X. Bai, and S. Yan, "Digital image watermarking based on texture block and edge detection in the discrete wavelet domain," in *Proc. Int. Conf. Sensor Netw. Secur. Technol. Privacy Commun. Syst.*, May 2013, pp. 170–174, doi: 10.1109/SNS-PCS.2013.6553859.
- [93] J. Guo, Y. Zhang, S. Zhi, and P. Cosman, "Adaptive edge masking based on TV decomposition and adjacent similarity for digital watermarking," in *Proc. IEEE Int. Conf. Prog. Informat. Comput. (PIC)*, Dec. 2015, pp. 142–147, doi: 10.1109/PIC.2015.7489826.
- [94] A. B. M. M. Morshed and T. Amornraksa, "Pixel-wise based image watermarking by ignoring edges and its neighbor pixels," in *Proc. 10th Int. Symp. Commun. Inf. Technol.*, Oct. 2010, pp. 475–480, doi: 10.1109/ISCIT.2010.5664886.
- [95] H. Shojanazeri, W. A. W. Adnan, S. M. S. Ahmad, and S. Rahimpour, "Authentication of images using zernike moment watermarking," *Multimedia Tools Appl.*, vol. 76, no. 1, pp. 577–606, Jan. 2017, doi: 10.1007/s11042-015-3018-2.
- [96] S. Dhargupta, A. Chakraborty, S. K. Ghosal, S. Saha, and R. Sarkar, "Fuzzy edge detection based steganography using modified Gaussian distribution," *Multimedia Tools Appl.*, vol. 78, no. 13, pp. 17589–17606, Jul. 2019, doi: 10.1007/s11042-018-7123-x.
- [97] S. Kumar, A. Singh, and M. Kumar, "Information hiding with adaptive steganography based on novel fuzzy edge identification," *Defence Technol.*, vol. 15, no. 2, pp. 162–169, Apr. 2019, doi: 10.1016/j.dt.2018.08.003.
- [98] C. Vanmathi and S. Prabu, "Image steganography using fuzzy logic and chaotic for large payload and high imperceptibility," *Int. J. Fuzzy Syst.*, vol. 20, no. 2, pp. 460–473, Feb. 2018, doi: 10.1007/s40815-017-0420-0.
- [99] A. Miri and K. Faez, "Adaptive image steganography based on transform domain via genetic algorithm," *Optik*, vol. 145, pp. 158–168, Sep. 2017, doi: 10.1016/j.ijleo.2017.07.043.
- [100] K. Gaurav and U. Ghanekar, "Image steganography based on canny edge detection, dilation operator and hybrid coding," *J. Inf. Secur. Appl.*, vol. 41, pp. 41–51, Aug. 2018, doi: 10.1016/j.jisa.2018.05.001.
- [101] S. Mukherjee and G. Sanyal, "Edge based image steganography with variable threshold," *Multimedia Tools Appl.*, vol. 78, no. 12, pp. 16363–16388, Jun. 2019, doi: 10.1007/s11042-018-6975-4.
- [102] S. Chakraborty, A. S. Jalal, and C. Bhatnagar, "LSB based non blind predictive edge adaptive image steganography," *Multimedia Tools Appl.*, vol. 76, no. 6, pp. 7973–7987, Mar. 2017, doi: 10.1007/s11042-016-3449-4.
- [103] S. K. Ghosal, J. K. Mandal, and R. Sarkar, "High payload image steganography based on Laplacian of Gaussian (LoG) edge detector," *Multimedia Tools Appl.*, vol. 77, no. 23, pp. 30403–30418, Dec. 2018, doi: 10.1007/s11042-018-6126-y.
- [104] I. J. Kadhim, P. Premaratne, and P. J. Vial, "High capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform," *Cognit. Syst. Res.*, vol. 60, pp. 20–32, May 2020, doi: 10.1016/j.cogsys.2019.11.002.
- [105] A. M. Ahmadian and M. Amirmazlaghani, "A novel secret image sharing with steganography scheme utilizing optimal asymmetric encryption padding and information dispersal algorithms," *Signal Process., Image Commun.*, vol. 74, pp. 78–88, May 2019, doi: 10.1016/j.image.2019.01.006.



OLEG EVSUTIN was born in Tomsk, Russia, in 1987. He graduated in complex information security of computer systems from the Tomsk State University of Control Systems and Radioelectronics (TUSUR), in 2009, and the Candidate in Engineering degree from Tomsk State University, in 2012.

From 2012 to 2019, he was an Associate Professor with TUSUR. Since 2019, he has been the Head of the Department of Cyber-Physical Systems Information Security, National Research University Higher School of Economics, Moscow, Russia. His current research interests include information security, digital image processing, steganography, steganalysis, and digital watermarking.

Mr. Evsutin became the Laureate of Russian Federation Government Prize in Science and Technology for Young Scientists, in 2018.



ANNA MELMAN was born in Kemerovo, Russia, in 1994. She graduated in information and analytical security systems from the Tomsk State University of Control Systems and Radioelectronics (TUSUR), Tomsk, Russia, in 2018, where she is currently pursuing in theoretical foundations of computer science with the Graduate School.

She is also a Junior Researcher with the Security of Information Systems Sub-Department, TUSUR. Her current research interests include information security, steganography, steganalysis, and digital watermarking.

Ms. Melman received the medal of the Russian Academy of Science for Young Scientists and for Students of Higher Educational Institutions of Russia, in 2017.



ROMAN MESHCHERYAKOV (Senior Member, IEEE) was born in Biysk, Russia, in 1974. He graduated in information processing and measurement equipment and technology from Altai State Technical University, in 1997, the Candidate in Engineering degree, in 2000, and the Doctor in Engineering degree, in 2012.

From 2012 to 2019, he worked as an Associate Professor, a Professor, a Vice Rector for Research and Innovation, and the Head of the Department of Information Systems Security. Since 2018, he has been a Chief Researcher of the Laboratory of Cyber-Physical Systems, the V. A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, Russia. He developed the theory of information processing in heterogeneous hierarchical systems. His current research interests include processing, analysis, synthesis of speech signals and texts, cyber-physical systems, cybersecurity, and robotic systems.

Mr. Meshcheryakov is a member of the Russian Acoustic Society. He received several awards and honors, including the Award of the Government of the Russian Federation in the field of education and the Award of RoboCup.

...