Digital Image Steganography and Reversible Data Hiding: Algorithms, Applications and Recommendations

Heba Ragab[1], Hassan Shaban[2], Kareem Ahmed[3,*], and Abd-Elmgied Ali[2]

[1] Faculty of computer science, Nahda university, Beni Suef, Egypt
[2] Faculty of computers and information systems, Menia university, Egypt
[3] Faculty of computers and artificial intelligence, Beni-Suef university, Minia, Egypt
Email: heba.ragab@nub.edu.eg (H. R.); hassanshaban@minia.edu.eg (H.S.); kareem_ahmed@eng.bsu.edu.eg (K.A.); abdelmgeid@yahoo.com (A.-E.A.)
*Corresponding author

***Abstract*—Image steganography is a science that is interested in how to hide a secret message inside digital images in an imperceptible manner. An attacker listening to communication channel between the two communicating parties will never have any information about the existence of an embedded secret message. After the transmission is completed, the receiver will be able to recover the secret message perfectly. In the other hand, Reversible Data Hiding (RDH) is also a science interested in hiding a secret message in a host image, but the difference between steganography and RDH is that in RDH, the receiver will be able to recover both the secret message and the original host image perfectly without any distortion. In recent years, it is noticed that steganography and RDH have gained a lot of interest because these techniques are widely used in medical images and thermal images that are used in military purposes. This paper presents a comprehensive review of recent techniques for steganography and RDH. The paper also discusses different attacks and attempts to recover the payload, which is known as Steganalysis. In addition to basic approaches, an inclusive study on RDH on encrypted and compressed domains was presented. Finally, an evaluation of different techniques on each approach is presented for both steganography, watermarking and RDH.**

***Keywords*—steganography, Reversible Data Hiding (RDH), watermarking, information hiding**

I. INTRODUCTION

Today, having an internet access is necessary for both daily life and the smooth operation of businesses. When using the Internet, many activities are done more efficiently, such as online transactions, online shopping, the sharing of media on social media, file sharing and uploading, and many other operations related to communication with clients. We use cryptography for protecting data and steganography uses for preserving copyrights. Copyright protection for audiovisual content is achieved by using popular techniques like cryptography and information hiding. With the increasing use of Internet, digital content, and multimedia objects, great attention has been paid to the science of information hiding or embedding. Information embedding has techniques for embedding a sent message or some sensitive information inside any multimedia object.

It is divided into adding a watermark and steganography based on the overall objective of data hiding. It is used to embed data inside different types of media objects such as texts, images, audio, video, or graphs. It is worth noting that cryptography is different from steganography. Cryptography is concerned with scrambling plain text or media to make it unreadable. It preserves data privacy and achieves confidentiality between communicating parties. Only the intended person with the correct key decrypts the encrypted message and reads the original content. Any attacker listening to the communication channel cannot obtain the encrypted message and thus cannot read the original content [1].

In this sense, security systems may use encryption to preserve the confidentiality of the object or use information hiding to communicate securely and imperceptibly. In general, there are also a lot of useful applications for information hiding such as watermarking which is useful to maintain copyright and ensure authenticity of digital content. Fig. 1 shows the type of information security services, which are divided into cryptography and information embedding [2].

Information hiding is classified into steganography, watermarking, and Reversible Data Hiding (RDH) [3]. In all hiding techniques, a function is used along with a key to embed the secret data into the cover object which may be a sound, image, or video. The data is embedded imperceptibly. You cannot differentiate between the original media and the one that contains the embedded message. After the embedded media is sent across the communication medium, the intended person uses another function with the same key to extract the sent message from the received stego object.

Manuscript received February 21, 2024; revised July 4, 2024, accepted July 15, 2024; published February 27, 2025.

doi: 10.18178/joig.13.1.90-114

Steganography is opposite to cryptography. It involves embedding a sent message inside a cover object without changing the message's structure and stego-objects containing embedded information. The cover object looks as same as it was before embedding data. A sent message is a computer file, test, image, or video hidden within another file, text, image, or video. Images are commonly used in steganography applications for their digital content nature. This makes it easy to utilize them in communication. Also, they have much redundancy. Similar techniques are applied to obtain audio digital forms similar to those of the images. Various steganography algorithms exist for the various image file formats [4].

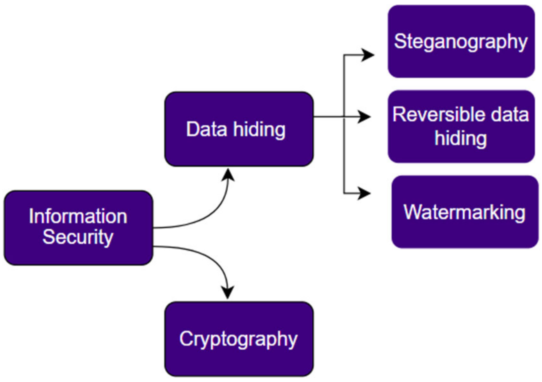

Fig. 1. Classification of information system.

Exchange digital content while keeping its high quality at a low cost. Putting a watermark on a digital image is an alternate method for detecting manipulation and establishing ownership. Watermarking involves adding a piece of information to an image without changing its value. Watermarking gets around the drawbacks of steganography by including a watermark on the used image and hiding it from view. The three stages of a digital watermarking system are watermark generation, embedding, and extraction. When a digital image's copyright is in question, the owner can prove his copyright by extracting the watermark. Watermarking techniques can be applied for confidential communication, copyright protection, embedding fingerprints for data integrity checks, and placing authentication. Tracing illegal users so that the owner can contact regulatory authorities is another significant application of watermarking technology [1]. It can be helpful to make sure that information about the individuals who purchase and sell digital material is recorded for each transaction. To prevent breaches of copyright, this data can be tracked further.

Three key factors are used to determine the efficiency of the method used for information hiding: capacity, security, and robustness. Capacity is the maximum quantity of data bits that can be hidden in the cover object. Security is the ease with which an eavesdropper may discover the concealed data, and robustness is the maximum amount of modification the stego medium can withstand before an opponent can alter or destroy it.

Reversible data hiding is a technique for adding extra information to a digital image, videos, sound files, and other computer files that can be used as a cover to hide a secret message in a way that can be retrieved, allowing the original cover content to be restored without any changes after the secret message that extracted [2]. The technique has significance in advanced communication applications like military and medical applications. As opposed to steganography, reversibility is more frequently utilized in watermarking. The main contributions of this paper are:

i) A review for Image Steganography techniques has been presented. This paper includes many techniques for steganography and many methods used in much previous work.

ii) Literature review of watermarking technique and it is applications.

iii) Reversible data hiding in the encrypted domain and the performance of embedding capacity and visual image quality for different techniques on each approach is presented for both steganography and RDH.

iv) Comparative study in terms of Image quality (PSNR), Embedding Rate (ER) (bpp), Payload capacity and result has been introduced.

v) This paper will aid researchers working in a relevant subject in data hiding and reversible data hiding.

This paper is composed of 8 sections. Section I gives and introduction and Section II presents the image steganography and its techniques. Section III explains the watermarking technique and Section IV introduces the Reverse Data Hiding (RDH). Section V explains the mixing of RDH with encryption of an Image and section VI highlights the evaluation of different techniques of steganography. Section VII Comparison of results of the previous studies and Section VII highlights some conclusions and future work points. Finally, references are listed at the end of the paper.

II. Image Steganography

Steganography is a method for hiding messages, images or video into another object such as file, Text, image or also video. It divided into two types: reverse data hiding and irreverse data embedding techniques based on whether the cover medium can be obtained at the receiving end. The cover medium is where the secret data will be embedded. The secret data is extracted from stego object at the receiving end. The data after extraction must be the same as the original data. Fig. 2 shows the reverse data embedding method in the embedding model.

Images files are most commonly used in Steganography. Each greyscale image pixel is typically 8 bits, and such bits can display up to 8 bits. The format of Graphics Interchange (GIF), Photograph Experts Group (JPEG) format, and Portable Network Graphics (PNG) formats are 256 different colors or shades of gray Image formats [2]. Different formats of image files have different structures of header files. Also the intended information can be embedded either in a header or a footer of the file, in addition to pixels, palette, and Discrete Cosine Transform (DCT) coefficients data values. Image storage types such as Tagged Image File Format (TIFF), PNG, Windows Metafile (WMF), and GIF have a file header that is used to hide secret information. Data is embedded in several formats in the content of image. The user will decode the image size from the header of the file after the image processing for display and any tracking information that exists at the end of the host image is ignored [4].

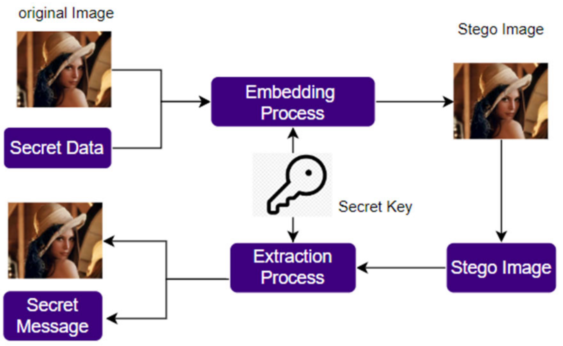

Fig. 2 General steganography process.

Wu *et al.* [3] Proposed a new and powerful computer-based stenographic approach to merge hidden messages into images without making visible changes. When extracting the embedded data from a stego-gif file, there is no need to reference the original image. The technique utilizes the human vision trait of sensitivity to gray value variations. Hidden data is inserted into a cover image by replacing the differential values of the cover image's two-pixel blocks with identical values that contain bits of embedded data.

Seyyedi and Ivanov [4] presented a zero-level unsupervised image classification technique based on image statistical characteristics (edge and texture of image) that help sender's fair cover image selections to improve stenographic method output based on their particular intent. Assigning an image to a certain class ensures that the consumer can predict the extent of the investigation of the requirement. If the sender wants to choose an image with a high payload, to have the necessary amount, he may choose the appropriate class. In the best way, the last elements of each class give stenographic requirements. Increasing the count of classes improves the algorithm's accuracy by reduction of the overlap between classes. Images are the most used objects for steganography. Here, data is embedded like noise, which is almost difficult to detect by human vision. Many approaches of steganography are used. They vary depending on the embedded data, the type of host content as a carrier or compression system, etc.

Kaur *et al.* [5] classified the benefits and problems of techniques of steganography and their security challenges with original images. EL-Latif *et al.* [6] proposed an integrated technique of quantum walks between methods of data embedding to achieve a good protection for the embedded information. The processes of embedding data and extraction data are regulated by S-box QWs. Using the S-box QWs ensures the protection of both phases of embedding and regaining. Only the cover object and the secret keys are required at the receiver to regain the sent message.

Yuan [7] proposed a two-secret sharing method (SS) for original images by multi-cover objects and adaptive steps of steganography. A simple procedure is used to share-construction in each method, and it has lossless hidden reconstruction and high-quality shares. The methods are hidden bits with different objects of covers between textured regions therefore hard to detect. It is easy to extend the process to Red, Green, and Blue (RGB) images and can use to exchange hidden non-image messages.

Khupse and Patil [8] focused on inserting the data into a video frame's skin area. Thus, to remove the skin area, the focus is on the skin detection algorithm. This serves as the area of concern for the hidden message to insert. To perform data embedding, the video frames are then translated into YCbCr color space. Li *et al.* [9] presented a steganography method for color images. The alteration of the pixels of image sides (edges) is less sensitive to the human eye according to the Human Visual System (HVS), while the shift in the place of image sides (edges) is sensitive. Since the edge, information about R, G, and B is associated and identical. Use one plane to select Sobel Operator hiding positions, and then adjust the Least Significant Bit (LSB) of the pixel values for the selected position of one or two other planes to hide data. Tian *et al.* [10] presented a Voice-over IP adaptive steganography scheme (VoIP). Unlike current VoIP steganography techniques, this scheme increases the clarity of embedding by considering similarities between the LSBs and embedded data.

Steganography techniques can be classified as spatial, transform and Distortion domains as Fig. 3. As shown in the next sections, this classification will be described with some research.

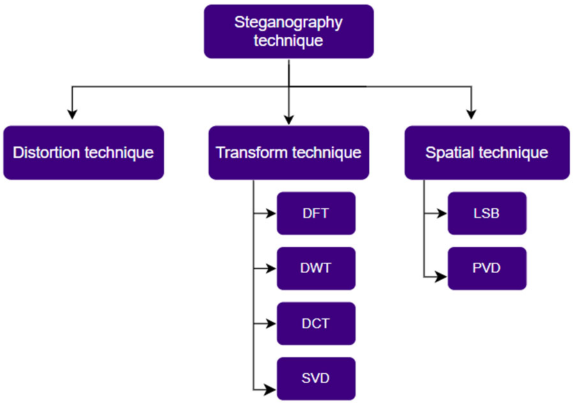

Fig. 3 Steganography techniques classification.

A. *Spatial Domain Technique*

Spatial domain Stenographic techniques are known as replacement techniques. These techniques is embedding hidden data using the cover image. A sensitive categorization based on the giving of the cover domain is utilized because it is possible to insert secret data over the space domain and transform the domain of the cover image. Modifying pixel of the cover object in the space domain is the simplest and easiest technique to embed data in digital images. These methods either directly or indirectly employ the cover image's pixel intensity to encrypt the secret message bits. The LSB and difference of pixels are the main methods in spatial domain technique.

1) Least Significant Bit (LSB) steganography

Least Significant Bit (LSB) method is mostly common for steganography in spatial images. The sent data is directly hidden in a host image by changing the LSBs of chosen pixels and the cover image's original visual quality. The idea here is that the least important bits in an image only provide weak information and that human vision cannot notice even slight changes to those bits.

The least important bit of any or all the bytes within a host image is modified by a bit from the embedded code. A bit of each color of the RGB image is used for the process, where each of them is represented by one byte. For each pixel, one can store 3 bits. Thus, 3 pixels may be used as follows [11]:

$$\begin{bmatrix} 00101101 & 00011100 & 11011100 \\ 10100110 & 11000100 & 00001100 \\ 11010010 & 10101101 & 01100011 \end{bmatrix}$$

When a number (e.g. 300) is inserted at the LSBs of image, (the binary code is 100101100), the result will be:

$$\begin{bmatrix} 0010110\mathbf{1} & 0001110\mathbf{0} & 1101110\mathbf{0} \\ 1010011\mathbf{1} & 1100010\mathbf{0} & 0000110\mathbf{1} \\ 1101001\mathbf{1} & 1010110\mathbf{0} & 0110001\mathbf{0} \end{bmatrix}$$

It was appropriate to adjust only the 3 underlined bits based on the sent message. The LSB steganography is represented by equation 1 for the embedding operation:

$$\mathrm{Yi}=2\left\lfloor \frac{x_j}{2} \right\rfloor + \mathrm{m_i} \tag{1}$$

where, m_i, x_j, and the *Yi* are the message bits and the selected pixel values before and after data embedding Steganos.

Das *et al.* [11] employed image steganography with LSB substitution to hide many secret images within one cover object (image) of 24-bits. Arnold Transform is used to encrypt every image before it is hidden in the host object (image). The suggested approach is successful in securing the high capacity data while maintaining enough image transmission quality.

Bhatt *et al.* [12] used the LSB extraction technique and scale, terminologies of steganography, and watermarking. Invariant Transform Functionality (SIFT). The combination ensures multiple layers of safety and achieves requirements such as capacity, safety, and robustness. Al-Tamimi and Alqobaty [13] utilized Least Significant Bits (LSBs) for a new color image steganography embedding method. The proposed system features three security levels, a variety of possible stego-keys, and a random first-pixel selection to facilitate the hiding process. The transposition applied to each 24-bit block of the message to be embedded begins with the start of the embedding method from the first-pixel position, which is calculated using the stego key.

Santoso *et al.* [14] used the division and modulus method to burst hidden messages to increase the ability of embedding them. The divide and modulus method improves security of the message. Because the messages are divided into two parts and sent separately. As a key extraction, one component is embedded and the other is stored. This methodology is carried out in the spatial domain.

Zhi and Fen [15] introduced a statistical technique to detect stego images based on analyzing the image gradient energy. This does not necessitate the availability of the original cover object (image) for analysis and detection. Instead, it focuses on assessing the gradient energy within the stego image itself to detect potential embedded information. The statistical analysis methods enable the detection of steganography content without comparison with the original cover image. To prevent losing precision, the LSB is quantized in the binary coding system or below the sensor noise energy level. In a similar way in Odat *and* Otair [16] the authors proposed a modified LSB method by segmenting the sent message bits and distributing them through the odd bytes of the cover image.

Hussain *et al.* [17] proposed a method for adaptive LSB embedding in digital images where pixels are divided into non-overlapping blocks. The length of secret bits that can be embedded in each block is determined by calculating the difference between the pixels and their associated ranges. This allows for greater adaptability and secure embedding of the sent data in digital images while preserving the visual quality of the cover image

Reddy [18] discussed the technique of LSB embedding and evaluated it with different file formats. There are different methods for embedding data or information in audio files, similar to the LSB technique, Parity coding method, phase coding method, technique of Spread Spectrum (SS), and Echo hiding techniques. Proposed system added many audio files like speech and music. These files were used to test the effectiveness of the embedding process and both provided impressive results in steganography.

To embed audio sent data in audio cover data, Tayel *et al.* [19]used the LSB method, where the audio sent data is embedded in the LSBs of the audio cover data. This does not affect the audio quality significantly. The technique uses a key-based technique to enhance security of the sent data. The technique was evaluated using many audio files, and the results showed that the technique can effectively embed the sent data in the cover audio data while maintaining a high degree of imperceptibility and security.

2) Pixel Value Differencing (PVD) steganography

Pixel Value Differencing (PVD) can be used to hide the hidden information, by comparing the difference between two consecutive pixel values. During the embedding stage of the PVD process, both the carrier image and the hidden information are divided into blocks. For extensive embedding, pixel value differencing works better than the LSB techniques because the embedding is smoother in the

PVD techniques. Different methods were put out in the area of PVD steganography by testing the correlation of pixels.

To increase the data-hiding capacity in digital images, Singh [20] proposed a new data-hiding method that combines both adaptive technique of PVD and the technique of LSB. The method utilizes diagonal, vertical sides, and horizontal sides to embed a large portion of sent data without introducing any visible changes to the cover object (image). The pixel intensities are utilized to give high rates of embedding. The method achieves high recovery of secret data during the extraction phase and provides a more secure and robust way to hide data in digital images.

Paul *et al.* [21] introduced a high-capacity method using Pixel Value Differencing (PVD) for data embedding. Unlike conventional approaches that solely focus on high-contrast pixel pairs, this method incorporates low-contrast pairs as well to maximize the capacity of embedding. The embedding process is adaptive and varies according to the contrast of the local pixel pairs. To ensure confidentiality, the sent message is encrypted before embedding. Additionally, to increase the method's security, pixel pairs are selected non-sequentially during the embedding process. This non-sequential selection helps to further safeguard the embedded data from detection or unauthorized access.

Swain [22] introduced two techniques of steganography. These are Quotient Value Differencing (QVD) and Modulus Formula Pixel Value Differencing (MFPVD). These techniques offer unique approaches to embed data in digital images. The QVD method works on non-overlapping 3×3 pixel blocks. Each pixel within the block undergoes substitution on its two least value bits, while the remaining six bits form a quotient block. The QVD embedding method is then used by utilizing the sides in eight different directions within the block of quotient. On the other hand, the MFPVD methods works with non-overlapping 2×3 pixel blocks. One of these pixels is assigned to be a center pixel. The technique calculates five differences between the center pixel and the pixels around. These differences are averaged, and according to the average, the hiding capacity is computed for each direction, using the side present.

B. Transform Domain Techniques

Transform domain embedding refers to a group of methods used for embedding data in signals, such as images and audio, in the domain of frequency. It involves breaking down the signal into frequency coefficients before integrating the basic information. Compared to embedding techniques applying in the domain of time, embedding in the transform domain is generally considered to be more robust against attacks that alter the secret data. However, it has some limitations, including a lower payload capacity and higher computational complexity. Most strong steganography systems today operate within the domain of transform, which has several advantages over LSB methods. For example, transform domain methods embed information in regions of the image that are less exposed to compression or cropping and/or processing. They can overcome both lossy and lossless format transformations. Transform domain techniques are classified into several types, including DFT (Discrete Fourier Transformation), DCT (Discrete Cosine Transformation), DWT (Discrete Wavelet Transformation), and SVD (Singular Value Decomposition). The format of JPEG, widely utilized because of its small size, is good example that employs transform domain techniques.

1) Discrete Fourier Transformation (DFT) technique

The DFT is another transform domain method utilized in steganography for data embedding. While the Fourier transformation is commonly associated with processing the signals and frequency analysis, it has also been employed in steganographic algorithms for embedding sent information within a cover media. It's worth noting that Fourier Transform-based steganography is less commonly used compared to techniques like DCT or Wavelet Transform. This is primarily because the Fourier transform does not provide as much localization of frequency information, making it more challenging to embed data in a specific manner without causing noticeable artifacts.

Jamel [23] proposed a steganographic method for hiding three audio signals of different sizes with in a single color digital image. To avoid any suspicion of the existence of hidden data within the cover image, the method utilizes the Fast Fourier Transform (FFT) to embed each audio signal in a specific region with high frequencies in the frequency spectrum of the cover image. By doing so, the method ensures that the embedded message does not change the perception quality of the cover medium (image).

Murthy *et al.* [24] investigated steganography methods using Discrete Cosine Transform (DCT). They divided the cover object (image) into wavelet-based basis functions, with the majority of image information residing in the lowest frequency component. Li *et al.* [25] proposed watermarking method in a color image that utilizes Tensor Decomposition (TD) and Quaternion Discrete Fourier Transform (QDFT). The cover object (image) is divided into blocks which are non-overlapping. On these blocks, the QDFT is applied. To obtain a third-order tensor, which is decomposed using Tucker method to produce a core tensor used the 3 imaginary components frequency of QDFT. An enhanced odd-even quantization approach is used to put a watermark into the used tensor, and the geometric distortion is corrected at the extraction stage using Support methods of Vector Regression based on the Least Squares of Multiple output (MLS-SVR) network model and pseudo-Zernike moments. The method leverages the relationships between a color image's three RGB channels to spread the watermark across the image.

Cao *et al.* [26] introduced a universal image watermarking scheme designed to withstand screen-shooting while embedding extractable information into on-screen images for purposes such as copyright protection or additional information acquisition. To enhance robustness and maintain high image quality in watermarked images, this paper incorporate a channel-attention mechanism into the Discrete Cosine Transform (DCT) domain.

Additionally, utilized a noise layer to guide the watermarking model, incorporating both simulated distortions and screen-shooting distortions during the embedding process. Following training, the universal watermark mask can be directly applied to any cover image, resulting in a watermarked image that effectively withstands multiple distortions.

The Discrete Fourier Transform (DFT), a fundamental tool, can undergo significant enhancement through pre-processing and refining raw data, thus making it suitable for traditional processing while minimizing violations of the underlying assumptions. Pal *et al.* [27] illustrated that the results of traditional mathematical transforms can be notably improved when applied to real-world data by ensuring that the data conforms to the fundamental assumptions of those transforms, such as the DFT.

Qu *et al.* [28] presented a novel approach to enhance the performance of DFT-based vector map watermarking through an algorithmic complementary strategy. This approach integrates DFT and Singular Value Decomposition (SVD) within a hybrid transform domain. Initially, the Douglas Peucker algorithm is employed to extract feature points, ensuring their synchronization across different scales by setting a relative distance threshold. These feature points undergo DFT to derive magnitude coefficients, which are subsequently transformed using SVD. By leveraging the geometric invariance of magnitude coefficients alongside the singular vectors of SVD, an invariant representation with rotation, scaling, and translation invariance is generated. This invariant representation serves as an embedding domain for watermarking, minimizing the impact on the host vector maps during embedding.

Khedmati *et al.* [29] utilized the von Neumann neighborhood and divide the cellular automata into two categories: reversible and irreversible. The key generation algorithm employs irreversible cellular automata, while the encryption algorithm utilizes reversible cellular automata. This paper aims to establish a secure approach for image transfer through cryptography and steganography methods, leveraging a novel uniformly distributed 2D hybrid chaos map, Discrete Framelet Transform (DFT), cellular automata, and various types of shifts as spiral and circular shifts. The 2D hybrid chaos map is employed in key generation, encryption, and steganography processes. For enhancing the security of the algorithms, the keys used in these processes are dependent on both the input images and the number of operations performed.

2) Discrete Cosine Transformation (DCT) technique

Transform Domain Techniques, including DCT-based methods, exploit the characteristics of transform coefficients to hide data. The DCT is particularly suitable for stenographic purposes due to its energy compaction property. The DCT is a spatial domain signal into its frequency domain representation, where the most important information is intensified in the lower-frequency coefficients.

Ayub and Selwal [30] proposed a more effective method to embed information in the cover object side pixels. Because side pixels are distinct from their neighbor's, a hacker is less likely to suspect that there are data bits there, improving security. The suggested method uses various side detection filters, such as Prewitt filter, Sobel filter, Laplacian filter, and Canny filter, in the already-existing algorithm for image steganography that exploits edge-based data concealing in the DCT domain.

In the domain of DCT, a reliable and secure video technique is proposed by Siddiqui and Khare [31]. The suggested technique is randomized, and the sent message is pre-treated using a map of Arnold Cat. Using two pseudo-random sequences, the sent message is embedded at the middle band DCT coefficient. To create these sequences a chaotic map was used. The sent information is embedded using the middle-frequency components LSB of the cover object while the low & high-frequency coefficients are left unmodified in the suggested manner in Khan *et al.* [32]. The image smooth region is preserved by the unchanged low-frequency DCT coefficients, and the sides are preserved by the unaffected high-frequency DCT coefficient. Since the middle-frequency components contribute less to energy & image information, changing the coefficients concealing produces stego images of excellent quality. The distortion brought on by changing the coefficients of medium frequency is hard for humans to notice.

Debnath *et al.* [33] proposed a new key-based method for RGB steganography that allows multiple images to be embedded simultaneously. The method uses the DCT and the DWT to enhance the protection and efficiency of the steganography process. The RGB object is divided into the Red level, Green level, and Blue level. Each level is split into two parts using basic cryptography principles to increase embedding capacity. DWT is then applied to these parts to identify the appropriate band for embedding the sent message. Finally the DCT is applied to the selected part. The modified region is transformed back to the space domain, and the components are inserted to generate the stego. This approach can be applied to grayscale case as well.

Guo *et al.* [34] suggested a refined version of embedding for digital image steganography. The method considers the relative modifications of the statistics model of the images, which is a general uniform hiding technique. The system uses coefficients of DCT, as cover components, which is not the same as the original Uniform Embedding Distortion (UED). The corresponding function of distortion is called revisited UED, considering the DCT complex coefficients.

3) Discrete Wavelet Transformation (DWT) technique

Wavelet Transform (WT) is another popular domain technique used in steganography for data embedding. Like the DCT, the WT allows to transform a space domain signal a frequency domain one, enabling the embedding of sent information in a cover object. The WT-based steganography offers some advantages over other domain techniques. The use of sub-bands with multiple frequency allows for more localized frequency information, giving better embedding capabilities. Also, the ability to control the coefficients resolution enables embedding data in different frequency ranges.

Shahrezaei and Kim [35] proposed a detailed analysis of the probability distribution of multiresolution function of Hidden Markov Model (HMM) and its function modeling of power density at each decomposition scale. To address the negative impact of embedded HMM suppression on pixel anomalies, additional quality assessment methods such as K-means clustering and visualized verification techniques were employed. These methods helped to maintain the balance between high-frequency uncorrelated anomalies and low-frequency joint spatial information within the 2-D data. Over-suppression of HMM at different scales of decomposition can lead to a loss of spatial information, highlighting the importance of selecting the appropriate DWT scale for texture categorization.

Raja *et al.* [36] proposed a new technique of steganography known as Integer Wavelet Transform (RIASIWT) Robust Image Adaptive Steganography, which can conceal substantial amounts of data in a cover image without causing any noticeable degradation. This method embeds the payload, in pairs of two pixels, on either side of the main diagonal, in non-overlapping 4×4 blocks of the low-frequency components of the cover image. Additionally, Voice on the Internet Protocol (i.e., VoIP) and the Public Switching Telephone Network (i.e., PSTN) are alternatively used for making telephone calls over the broadband connection of Internet.

Lai and Chang [37] proposed an adaptive data embedding technique. The image is partitioned into 8x8 sub-blocks, each of them is decomposed into LL1 (Low-Low), HL1 (Horizontal-Low), LH1 (Vertical-Low), and HH1 (High-High) bands using the Haar Discrete Wavelet Transform (HDWT). Since the human eye is insensitive to the side area, more details are integrated when the LL1 band is complex. To study the complexity of the LH1, HL1, and HH1 bands, the power feature of data embedding is employed. If these three sub-bands are complex, extra data bits are hidden in the more decomposed HH2 (High-High at Second Level), LH2 Vertical-Low at Second Level), and HL2 (Horizontal-Low at Second Level) bands, which are obtained after decomposing the LL1 band.

4) Singular Value Decomposition (SVD)

SVD is a powerful mathematical technique used in various applications, including steganography for data hiding. SVD allows the decomposition of a matrix into three separate matrices, representing the singular values, left singular vectors, and right singular vectors. In steganography, SVD can be employed as a transform domain technique for embedding secret data within a cover media. SVD-based steganography offers advantages such as its ability to handle high-dimensional data and its flexibility in selecting the components for data hiding. By modifying the singular values or vectors, it is possible to embed information in a way that is imperceptible to human observers.

Subhedar and Mankar [38] proposed a method to enhance the undetectability of steganography by combining the Contourlet transform with the three best matrix factorization methods namely SVD, QR (Orthogonal Upper Triangular Matrix) factorization, and Nonnegative Matrix Factorization (NMF). This approach leverages the strengths of the Contourlet transform and the mathematical properties of these decomposition techniques. The proposed method embeds a high amount of confidential information without causing any noticeable degradation of the cover image.

Singh and Singla [39] discussed the hybrid stenographic method in digital images that is leads to the high Peak Signal to Noise Ratio (PSNR). The least amount of information can be removed with SVD without sacrificing the image's quality. Yasmeen and Uddin [40] used SVD and QR factorization of the Next-Subsampled Contourlet Transform (NSCT). Arnold transforms are used in this approach to first scramble the hidden image, after which the NSCT separates the carrier and hidden image into corresponding sub-bands. Second, the carrier specified and scrambled hidden image coefficients are subjected to the SVD and QR factorization, respectively. Finally, inserted the secret image that has been adjusted for communication is into the carrier image.

Song and Zhang [41] used SVD transformed tensor, which utilizes single transform matrices as alternative of the conventional discrete Fourier matrix, for robust tensor completion. The authors demonstrated that this approach can produce smaller tubal rank tensors, making it more efficient for robust tensor completion.

Alyousuf *et al.* [42] conducted a review of digital steganography techniques and classified them into three categories: image, audio, and video steganography. The LSB method was the most technique used in image steganography cause its simplicity and speed. The consistency between the original and stego images was measured using PSNR, while the cumulative square error between them was calculated using Mean Squared Error (MSE). Quality degradation was evaluated using certain operations computed by Structural Similarity Index Measure (SSIM), while Normalized Cross-Correlation (NCC) tested the consistency between the cover images and stego images. MAE calculated the variations between them, and to test robustness the Bit Error Rate (BER) was used. For audio and video steganography, Signal-to-Noise Ratio (SNR) tested the amount of noise in the device's signal, and Root Mean Square Error (RMSE) was used to calculate the sum of changes between the cover and stego medium.

Hamid [43] employed file image as the carrier and introduced a taxonomy of existing image steganographic files. These techniques have been studied and discussed not only in terms of their ability to hide information in image files, but also based on the amount and type of information that can be concealed, as well as their robustness against various image processing attacks. The Spread Spectrum Algorithm is one such technique that utilizes encoded deployments to spread messages across any possible frequency spectrum.

Bagaskara *et al.* [44] provided an overview of JPEG digital images steganography and images using the Spread Spectrum algorithm. The study involved analyzing images in both RGB and Grayscale formats and comparing image resolution (in pixels) with message size, message size (in bits) with image resolution, and image size (in KB) with steganographic image size (in KB). The authors used pseudo-random sequences that are weakly associated with each other in communication systems, making them suitable for comparing with numerous networks of subscribers, thus increasing the ability of multiple access and reducing the cost of communication services. Any errors can be repaired using the correlation method, which enhances communication interference immunity.

Kuznetsov *et al.* [45] proposed an approach for steganography that takes into account the statistical properties of cover images. The approach involves using specially constructed pseudorandom sequences to reduce errors in the retrieved messages, rather than correcting errors. This technique, called adaptive generation, considers the statistical properties of the cover image when forming the sequences. Experimental tests show that this technique effectively reduces the error rate in the retrieved messages while maintaining the same degree of distortion in the cover images and achieving a smaller correlation, which increases the accuracy and security of hiding data in digital images.

Marvel *et al.* [46] proposed a digital steganography system called Spread Spectrum Steganography Image. System can hide and recover a long message within digital images while maintaining the size of cover image and dynamic range. The authors also suggested that Voice over Internet Protocol (VoIP) can provide an ideal cover for hidden messages as it is assumed that only voice data is transmitted through VoIP.

Subhedar and Mankar [47] introduced a novel hybrid image scheme based on a combination of bidiagonal Singular Value Decomposition (SVD) and framelet transform . Leveraging the advantages of framelet transform, such as improved time-frequency localization and shift invariance, the scheme achieves enhanced performance. Additionally, the use of bidiagonal SVD increases capacity and strengthens security measures. a series of experiments are conducted to assess the effectiveness of the suggestion method. The results demonstrate that the stego-images exhibit superior visual quality and robustness against various image processing operations. furthermore, the security performance of the suggestion method is thoroughly evaluated using different steganalysis schemes, including Gabor filter-based, wavelet-based, and contourlet-based steganalysis. The results indicate poor detection accuracy across all cases, affirming the undetectability of the scheme.

To enhance the capacity, security, and imperceptibility of image steganography, Xiao and He [48] proposed a novel method that combines framelet transform with Compressive Sensing (CS). Here’s how it works: firstly Singular Value Decomposition (SVD) transform is applied to the measurement values acquired through the compressive sensing technique for the secret data. The resulting singular values are then embedded into the low-frequency coarse subbands of the framelet transform within non-overlapping blocks of the cover image. Finally, inverse framelet transforms are used, followed by combination steps to generate the stego-image. This method aims to maximize the steganographic capacity while ensuring robust security and minimal perceptual distortion in the resulting stego- image.

C. Distortion Techniques

During the decoding phase of a steganography system, distortion methods are used to recover the hidden message, requiring information of the original image. The decoder then searches for differences between the original image and the modified cover image produced by the encoder. Signal distortion is used to describe how information is stored and retrieved. In the case of binary images, which only have two states (black and white), even slight distortions are easily detectable by human eyes. Therefore, practical steganography schemes suggest embedding message bits only in less noticeable parts of the image. Some techniques involve breaking the cover image into overlapping blocks or non-overlapping blocks and finding the best pixels to modify in each block.

Feng *et al.* [49] proposed a binary steganography image method to minimize embedding distortion on texture. This approach uses a novel flipping distortion calculation that considers the Human vision and statistics. The calculation determines the liability of a pixel using the weighted total of Color Robust Local Ternary Pattern (crmiLTP) shifts, where the weight values are set based on the sensitivity of each crmiLTP to embedding distortion. To produce stego images a series of generalized embedding simulators are used with different styles and strengths of distortion to estimate sensitivity. This study also focuses on describing motion vector-based steganography distortion, which made the motion vectors as the cover for embedding due to their primary role in expressing video content during encoding and decoding.

Wei *et al.* [50] proposed a new method to measuring distortion by analyzing both the embedded domain and spatial domain. The method utilizes a combination of RBVs (Residual Block Values) and quantization measures to evaluate the distortion caused by embedding modifications. RBVs are used to determine the complexity of the content in an image block, and quantization measures are taken to assess the risk of changes during the embedding process in the same block. By combining these two measures, the proposed method provides a comprehensive evaluation of the distortion in both domains, making it a useful tool for steganography analysis.

Li *et al.* [51] proposed a method that utilizes the interactions between embedding changes to minimize the chances of detection by steganalysis. Their approach involves Clustering Modification Directions (CMD), which assumes that a cover image is divided into several sub-images. The method involves embedding message segments using well-known steganographic schemes with additive distortion functions. However, when embedding modifications are made in highly textured regions, they are locally directed towards the same direction to reduce the possibility of detection.

III. Watermarking Technique

Digital watermarking is a crucial technique used to prevent information leakage in cases where organizations have a direct legal relationship with their customers and are required to secure their information. It protects digital content and authenticates users by embedding signal information into the original media content. This process allows for the identification of the true owner of the digital media, and the implanted information can be discovered and removed. Typically, a digital watermarking technique consists of three phases: watermark generation, watermark embedding, and watermark extraction, as Fig. 4. The essential elements of a watermarking scheme.

Watermark generation: is the first phase of a digital watermarking system. In this phase, a unique watermark is created for the original content, which could be a binary image or specific personal data that is unique to the individual or organization. The watermark is typically designed to be imperceptible and resilient to various signal processing operation

Watermark embedding: involves the process of inserting a watermark into a digital image using various techniques such as LSB replacement, histogram shifting, and expansion-based methods. The chosen technique typically depends on the requirements of the specific application, as each approach has its advantages and limitations. For instance, LSB replacement is a simple and widely used method, but it can be easily detected and removed by attackers. On the other hand, histogram shifting and expansion-based methods offer better robustness and security, but they require more complex algorithms and computations.

Watermark extraction: refers to the process of retrieving the embedded watermark from the watermarked media. It is used to verify the legal ownership, reliability, and authenticity of the work. The extracted watermark can also be used for copyright protection, proof of ownership, and content authentication. Different extraction algorithms are used based on the type of watermarking approach employed during the embedding phase.

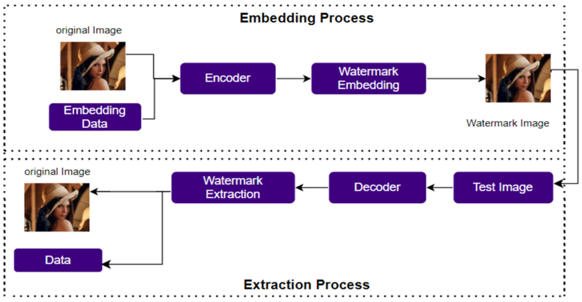

Fig. 4. General watermarking scheme.

A. Digital Watermarking Classification

The classification of digital watermarking based on different factors, including multimedia, robustness, perceptibility, and domain [52, 53].

1) Based on characteristics/robustness

a) Robust

When the need to insert copyright information arises, robust watermarking is chosen. The embedded watermark should be intact even after some sort of attack to prove robustness. It can withstand numerous assaults. We can see that a strong watermark is beneficial for copyright protection.

b) Fragile

If the data has been altered, it is simple to determine from the watermark's condition. This watermark is the best option for integrity protection.

c) Semi-fragile

A watermarked image tolerates to some degree of alteration, such as the addition of quantization noise from lossy compression.

2) Based on perceptibility

a) Visible watermark

It refers to a deliberately placed mark or logo that is made visible in digital content such as images or videos. It serves as a means of branding, copyright protection, or indicating ownership. Visible watermarks are often utilized to discourage unauthorized use or distribution of the content by clearly indicating its origin or ownership.

b) Invisible watermarking

It involves the insertion of hidden information into digital content, such as images, without being visibly noticeable. While it does not prevent theft of the content, it enables the ability to prove ownership or authenticity if unauthorized use occurs. Invisible watermarks typically consist of unique identifiers or digital signatures that are difficult to detect without specialized tools or software. In the event of copyright infringement or unauthorized distribution, the presence of the invisible watermark can be used as evidence to establish ownership or originality [1].

3) Based to detection methodologies

a) **Blind:** It does not need original data and has many applications, but it needs a more advanced watermark technology.

b) **Semi blind:** For detection, an original media is not necessary.

c) **Non-Blind**: This technique of watermarking involves copying the host image, the text data, and the injected data so that the watermark can be retrieved. It is used in copyright protection.

4) Basic characteristics of digital watermarking

a) **Robustness**

The term "robustness" describes a watermark's capacity to endure various processing procedures and malicious attacks. The watermark must then be resistant to criminal attack, geometric change, and general signal processing operations.

b) **Imperceptibility**

Watermarks can only be identified using specialized processing or circuitry; they cannot be seen or heard by the normal eye or ear. Only an authorized organization is capable of detecting it. These watermarks are used to identify unauthorized copying and to authenticate content or authors.

c) **Capacity**

How many bits of data can be embedded is described by capacity. It also discusses the possibility for continuously integrating numerous watermarks into a single document. The capacity requirement always conflicts with imperceptibility and robustness, two additional crucial requirements. Typically, in order to increase capacity, imperceptibility, robustness, or both must be given [1].

5) Applications of watermarking

a) **Copyright Protection**

Digital multimedia has many disadvantages, one of which is that it can easily copied illegally through methods like piracy. Therefore, there is a need for methods to protect digital data's copyright.

b) **Fingerprint**

As technology advances, fingerprinting is now one of the potential applications for digital watermarking. In digital watermarking, fingerprinting is frequently used as a method for adding unique to the image so that it is hard to alter or remove. If the image is shared illegally, the copyright owners can trace the source of forgery.

c) **Copy control**

Digital watermarking can stop the unauthorized copying of digital data. Devices that perform replication can recognize these watermarks, report instances of copying, and so prevent illicit copying.

d) **Medical Application**

The patient's name can be embedded via visible watermarking in the MRI, CT, or X-ray data. These medical reports determine how the patient will be treated. Consequently, the visible watermarking approach can be utilized to prevent the mixing of reports.

Zhang *et al.* [54] proposed a watermarking technique based on difference expansion quadratic for reversible image. Their approach utilizes linear difference expansion to incorporate half-scrambled watermark data into the cover image after removing the pixel locations in the cover grayscale image with the values from 0 to 255. By combining the grayscale values of 0 and 255 with the removed pixel locations and hidden the remaining half of the watermark data into the generated watermarked image previously using a quadratic difference expansion the watermarked image is formed.

Begum and Uddin [55] conducted an analysis of the hybrid digital watermarking image techniques. They proposed a common framework for produced a hybrid approach that meets the fundamental design specifications of watermarking for different purposes. Also provided a comprehensive comparison of the levels of complexity of different hybrid approaches, along with their drawbacks and potential applications.

Su *et al.* [56] proposed a watermarking algorithm for color image that utilizes Singular Value Decomposition (SVD) in conjunction with the spatial domain to safeguard the ownership of color images. Their approach involves the use of a quantization index modulation technique with a variable quantization step to directly embed the watermark information into the Maximum Singular Value (MSV)) in the space domain of the given image. The watermark data can then be extracted from the MSV of the watermarked image block with spatial domain-based geometric correction, without requiring the original image for extraction.

Liu *et al.* [57] proposed a color image watermarking technique based on image rectification and Haar transform-based fusion. Initially, the Haar transform is applied in the spatial domain to obtain the highest energy coefficient. Then, the color watermark, which has been encrypted with an affine transform, is embedded by quantifying the coefficient using variable quantization steps. The watermarking scheme is made robust against geometric attacks by exploiting geometric properties to rectify the attacked image. Finally, using the inverse embedding process to extract the watermark.

Wang *et al.* [58] proposed a watermarking technique for color image that utilizes the DCT domain. The method is setup on the concept of JND (Just Noticeable Difference) and incorporates various properties such as color complexity and orientation diversity. Initially, the Contrast Masking (CM) processing of the JND is employed, which takes into account the variations in texture types and orientation diversity of the Human Vision system. To enhance the robustness of the technique, a new color complexity weight derived from the Cb-channel is introduced. By integrating color complexity, contrast masking, and a new JND model, the proposed approach implements a quantization watermarking method.

Kahlessenane *et al.* [59] proposed a blind and robust technique for protecting medical images by integrating patient data and picture capture information into the image while producing minimal distortion and replicating the original image's clinical reading. The proposed method uses the frequency domain and employs four transforms, including discrete wavelets transform, non-subsampled shearlet transform, non-subsampled contourlet transform, and discrete cosine transform. After combining these transforms using Schur decomposition, to achieve a balance between imperceptibility and robustness the bits of watermark are stored in the upper matrix triangular. The integration is carried out at the image medium frequencies.

Alshanbari [60] enhanced the security of watermarking medical images by using repeated watermarking bits of the original image. The scheme is designed to be resistant to ownership attacks and employs PC (Principle Component) based insertion. Additionally, LZW (Lempel-Ziv-Welch) watermark is used to conceal the area of interest in compressed images, to protect against intentional tampering attempts.

IV. Reversible Data Hiding (RDH)

Reversible Data Hiding (RDH) refers to a technique for embedding additional information, such as messages or data, in digital media files, including images, audio, video, and other computer files. The hidden information embedded in the original cover media can be restored after the extraction of the hidden message, without any loss or alteration of the original data. The process of embedding the data creates a relationship between the cover media and the embedded data, and this relationship can be utilized in various reversible data-hiding application.

Celik *et al.* [61] proposed reversible data concealing technique. It builds upon the LSB modification technique, which is an underlying method for irreversible embedding. However, instead of modifying bit planes, this technique modifies the smallest levels of the host signal to embed the payload data. These small signal attributes are modified in the space domain as raw pixel values. The cover image can be recovered and retrieving these features by compressing, transmitting. This method offers a high capacity for data hiding and low distortion.

Ni *et al.* [62] proposed a technique for RDH. It builds upon the LSB modification technique, which is an underlying method for irreversible embedding. However, instead of modifying bit planes, this technique modifies the smallest levels of the host signal to embed the payload data. These small signal attributes are modified in the spatial domain as raw pixel values. By compressing, transmitting, and retrieving these features, the original image can be fully recovered. This method offers a high capacity for data hiding and low distortion.

Tai *et al.* [63] extended the histogram modification technique by considering the variations between adjacent pixels rather than solely focusing on the simple pixel value. One of the disadvantage of existing histogram modification techniques is the requirement for a side contact channel to handle peak and minimum point pairs. This paper addressed this issue by implementing a binary tree, which predefines multiple peak points for message embedding. This approach reduces the information that needs to be exchanged between the sender and receiver. Additionally, considering the strong correlation and spatial redundancy between adjacent pixels, this technique leverages these characteristics to further enhance the watermarking process. reversible data hiding techniques can be classified into five classes as Fig. 5: quantization-based, histogram modification-based, expansion-based, compressed-based, and dual image-based techniques. Within the expansion-based class, there are three specific methods: prediction error-based, interpolation error-based, and contrast mapping-based techniques.

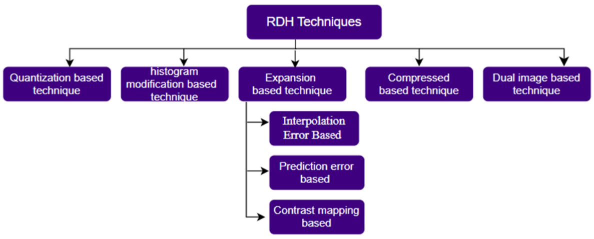
RDH Techniques
Quantization based technique
histogram modification based technique
Expansion based technique
Compressed based technique
Dual image based technique
Interpolation Error Based
Prediction error based
Contrast mapping based

Fig. 5. Reversible data hiding techniques.

A. Quantization Based Techniques

Quantization-based techniques have been widely used for embedding information in digital media like images and videos. These techniques have a long history and are still commonly employed due to their effectiveness. The fundamental principle behind quantization-based methods involves modifying the least significant bits of quantized coefficients while preserving the overall visual quality of the media. This allows for hiding a significant amount of data while introducing minimal distortion. Quantization-based data hiding techniques can be categorized into two main types: lossy and reversible. In lossy techniques, some level of distortion is inevitable during the embedding process, but the embedded data can still be extracted. On the other hand, reversible techniques aim to ensure that the original media can be perfectly recovered after the hidden data is extracted. These techniques find applications in various domains such as copyright protection, content authentication, and covert communication. They offer advantages like high capacity for data hiding, resistance to common attacks, and compatibility with existing compression algorithms. However, there are also limitations to consider, such as potential vulnerabilities to sophisticated attacks and the trade-off between embedding capacity and visual quality preservation.

Braci *et al.* [64] proposed a method that combines Spread Transform (ST) and Quantization Index Modulation (QIM) techniques to improve the invisibility of the hidden message and provide protection in the Cachin context. The Spread Transform Quantization Index Modulation (ST-QIM) approach offers a flexible and effective solution for steganography. The authors also demonstrated how the message propagation through the ST helps to smooth out the probability density function of the stego-signal, making it more similar to the density function of the cover-signal.

Embedding integer data to integer coefficients is possible to oblivious hiding data techniques dedicated to compressed images. method in Seki *et al.* [65] has the advantage of not causing secret data to corrupt during the compression step. Furthermore, the secret data is directly extracted from the transformed domain, without needing for a decoding method. Produced stego images that are comparable in quality to JPEG-coded images. A Discrete Cosine Transformation (DCT) was applied to each block of the JPEG image, and all coefficients in each block using a Q-table were quantized as integers. The Huffman encoder is then used to encode quantized coefficients ordered by the zigzag order scan. To boost coding performance, zeros lasting until the last coefficient ordered using zigzag are replaced rather than encoded with an End of Block (EOB).

Zhang *et al.* [66] presented a quantization index modulation-based image steganography methods that is resistant to scale attacks and statistic detection. It extracts the embedded domain from a spatial image using a watermarking algorithm that is based on quantization index modulation. After that, using Spatial-Uniform Noise Invariant WAvelet-based Redundancy Detection (S-UNIWARD) steganography, they create the embedding distortion feature of the new embedded area and use lowest distortion coding to apply the embedding of the hidden messages. Finally, the amplitude of hidden data in the new embedded area is adjusted according to the embedding update. Using the quantization index modulation to achieve the final embedding of hidden data in the original embedded area.

B. Histogram Modification Based Techniques

Histogram modification-based data-hiding techniques revolve around the modification of an image's histogram to embed hidden data while preserving the visual quality of the image. The key objective of these techniques is to identify an appropriate histogram modification function that enables the embedding of data with minimal distortion to the original image. These methods are widely adopted due to their ability to provide high embedding capacity and maintain good visual quality, making them suitable for various applications including copyright protection, content authentication, and data hiding. By leveraging the characteristics of the histogram, these techniques allow for efficient and effective hiding of information within an image.

Jamel [67] presented a steganography frequency domain of process for data hiding. It employs threshold-based histogram modification methods. The grey level cover image was classified into four sub-bands using the Haar Wavelet Transform. The secret message is concealed in the High-High-frequency (HH) sub-band by applying the histogram modification technique and scrambling procedure. The histogram modification is used To Modify the scale of the secret message the secret message and normalize its values, which transforms the secret image from light to dark. As a result, the secret image fades into obscurity, allowing it to conceal in the high-frequency sub-band. The positions can scramble into rows and then columns, providing good protection for the hiding process.

Marin and Shih [68] used multiple scanning techniques, they introduce an enhancement for histogram modification algorithm. The required payload size is used to evaluate an embedding order according to the level of embedding and scanning methods. The image is then repeatedly modified with varies in value histogram using the overhead and the embedding order data that stored in the image. The main peaks of the difference histograms value created by additional scanning methods are higher than the peaks of raising the Embedding Level (EL) of the single horizontal scanning method, so this method takes advantage of that. This allows more data to embed in an image. In addition, for determining an effective scan order and EL the algorithm was implemented.

Zhao *et al.* [69] proposed a RDH technique using histogram modification, which focuses on modify the histogram of neighboring pixel differences instead of the host image's histogram. The histogram of pixel differences has several peak points around bin zero and several zero points on both sides of bin zero because neighboring pixels tend to have identical values. The algorithm utilizes these points to embed hidden data derived from the differences between labeled adjacent pixels. The variations are divided into two parts ranging from −255 to 255, and each part matching to a histogram, allowing for multi-level hiding. In the decoding process, the pixels host image are retrieve one by one with the help of their already-recovered neighbors. The technique ensures reversibility and achieves high hiding capacity while maintaining good image quality.

Devi and ShivaKumar [70] presented a lossless data hiding scheme tailored for color cover images containing crucial and confidential information. The proposed method leverages the histogram shifting technique to embed secret bits into a confused color cover image, where the confusion is induced by employing Quad tree decomposition. While numerous data hiding techniques exist, such as LSB, Discrete Cosine Transformation, Pixel value differencing, and Discrete Fourier Transform, they often encounter limitations such as low data hiding capacity, image quality degradation, and insufficient security for concealed information. Addressing these constraints, this paper introduces an enhanced histogram shifting method for color images. This method embeds secret information into the three different planes of the RGB image, thereby not only enhancing image quality but also significantly increasing embedding capacity.

C. Expansion Based Techniques (DE)

Expansion-based data-hiding techniques are a category of methods used for embedding secret data into cover media, such as images or videos while ensuring that the original cover media remains intact. These techniques use the advantage of redundancy present in the cover media to insert additional data by manipulating the LSBs of the pixels or blocks in the media. DE techniques can be lossy or lossless, depending on whether the hidden data can be retrieved exactly or with some loss of information. In general, lossless methods are preferred, especially when the cover media contains sensitive information that must be preserved in its original form. The most common expansion-based techniques are those based on prediction errors, where the differences between the predicted and actual pixel values are used for embedding the secret data. These techniques use the prediction errors typically have small magnitudes and can, therefore, be manipulated without affecting the visual quality of the cover media. The histogram modification technique play an important role for this, where the frequency distribution of pixel values is manipulated to create additional room for embedding the secret data and those based on transform coding, where the cover media convert into a frequency domain and then manipulated for data hiding.

Tian [71] proposed the Difference Expansion (DE) method, which embeds hidden data between pairs of pixels in the carrier image by expanding the difference values between them. However, this method causes a significant change in pixel values, leading to a noticeable difference between the original and stego images. To mitigate this, the DE method detects exceeded storage by searching for redundancy in the image and embeds the original image restoration data, an authentication code message, and other additional data in the difference expansion values. Compared to other similar techniques, the DE method has the highest data payload storage capacity, best stego image quality, and the lowest computational complexity.

El-sayed *et al.* [72] proposed a spatial domain-based steganographic technique that can hide 1, 2, or 3 bits using only three global embedding parameters. The approach uses statistical analysis of the surrounding pixels to calculate these parameters, which are utilized for both embedding and extracting data, as well as for restoring the original carrier image. The technique ensures the quality of the image and its payload capacity by monitoring these three global embedding parameters. The method updates only certain pixels (embedding pixels) while retaining the original values of the other pixels, thus preserving the pixel values of the stego image within the pixel's dynamic range and preventing loss of secret data. The technique enhances the payload capacity while maintaining the stego image's quality. Also, its ability to retrieve secret data without having any knowledge of where the data hiding.

Lu and Chang [73] proposed a lossless data embedding technique that uses difference expansion to embed secret information. This technique divides each pixel of the original image into two nibbles, and each pair of nibbles from adjacent pixels is used to hide secret data. The method is effective in concealing large capacity payloads without causing any visual changes in the stego image. Moreover, the technique enables the accurate and fast extraction of secret information and the recovery of the original cover picture from the stego file.

D. *Prediction Error (PE) Based Techniques*

Prediction error based data hiding techniques are commonly used in RDH to embed secret data into the prediction error signals generated during the image compression process. These techniques take advantage of the high correlation between adjacent pixels in an image to predict their values and generate prediction errors, which are then used for data embedding. By embedding data in prediction errors, these techniques ensure that the original image can be fully recovered after data extraction, without any loss of quality. There are different prediction error based techniques used for data hiding, such as Pixel-Value Differencing (PVD), Prediction Error Expansion (PEE), and pairwise prediction error. These techniques aim to optimize the trade-off between data hiding capacity and image quality by selecting the best pixels for embedding and adjusting the magnitude of the prediction errors. They have been widely applied in different areas, including medical imaging, digital forensics, and secure communication.

Ou *et al.* [74] proposed a new technique for RDH using a PEE method based on pairwise prediction errors. Unlike previous PE Expansion techniques, which typically use one-dimensional prediction errors, pairwise PEE takes every two adjacent prediction errors as a unit to generate a sequence of prediction error pairs. This approach involves constructing a Two-dimensional Prediction-error Histogram (2D PEH) and embedding data by extending or shifting the 2D PEH bins. Pairwise PEE can leverage the redundancy in the image better than traditional PEE and produces better results. Additionally, a refined pixel-selection technique is utilized to process pixels in smooth image regions preferentially, which further enhances embedding efficiency.

Li *et al.* [75] presented a novel RDH algorithm for color images. Unlike conventional RDH techniques that embed data into each color channel separately, their approach uses prediction of the error expansion to improve the accuracy of prediction in one color channel using edge information from a different channel. This reduces the prediction error and improves the efficiency of the algorithm. In a similar vein, Wu and Sun [76] proposed two RDH methods for encrypted images based on prediction error. The first method is a joint process that achieves data retrieving and image restoration simultaneously, while the second method separates retrieving data and image recovery. Both approaches increase the reversibility and visual consistency of a lossy image that has been recovered, with the joint approach reducing the number of incorrectly extracted bits significantly at high embedding rates. At high payload embedding rates, the separable technique also offers better retrieving data and good visual quality of the retrieving image.

Prediction-Error Expansion (PEE) methods, employed as spatial domain approaches, have made significant strides in reversible data hiding. However, a notable issue with current state-of-the-art techniques is that as the embedded payload increases, so does the distortion rate of the cover image. To address this challenge, Li *et al.* [77] proposed refining an effective predictor to enable the prediction of all remaining pixels during the embedding process, excluding those situated at the edges of the original image the first row, first column, last row, and last column. During extraction, the process reverses the embedding procedure, ensuring the restoration of both the embedded information and the original carrier image without incurring damage. By optimizing the correlation between image pixels, proposed method mitigated the inherent contradiction between payload size and distortion rate present in contemporary data hiding algorithms.

E. *Contrast Mapping Based Techniques*

Contrast mapping-based data hiding techniques refer to a family of reversible data hiding methods that aim to hide secret information within digital images while improving their contrast simultaneously. In these techniques, the contrast of the host image is selectively enhanced by manipulating the pixel values in certain areas to embed the secret data. Contrast mapping-based techniques are particularly useful for applications where image quality and contrast are critical, such as medical imaging, digital watermarking, and authentication. These techniques are designed to achieve high embedding capacity while maintaining a low distortion in the image. The methods as histogram modification, adaptive histogram equalization, and contrast enhancement proposed to accomplish contrast mapping-based data hiding. These techniques offer a tradeoff between the amount of data that can be hidden and the level of distortion introduced to the image.

Wu *et al.* [78] introduced a novel approach for RDH with contrast improvement, specifically tailored for medical images. The proposed technique involves automated context segmentation to separate the area of Interest from the background, followed by marking the corresponding histogram bins using a threshold to identify the principal pixel values in the segmented context. By continuously extending the largest unlabeled bins, the contrast of the ROI can be selectively improved. The authors also focused on enhancing the pre-processing step to minimize any potential visual changes. The entire process, including data hiding, extraction, and recovery, is part of this reversible data hiding system.

F. Interpolation Error Based Techniques

Interpolation error based techniques are a type of data hiding method that relies on the interpolation errors generated during the image resizing process. These techniques are popular due to their ability to embed a large amount of data in the image without affecting its perceptual quality. The basic idea is to embed the data by modifying the interpolation errors of the image. Interpolation error based techniques can be divided into two types: reversible and irreversible. Reversible techniques allow for the extraction of the original image and the hidden data, while irreversible techniques do not. These techniques have found applications in a wide range of fields, including digital watermarking, steganography, and copyright protection.

Wahed and Nyeem [79] used a parameter in adaptive Image-Related Data Hiding (IRDH) approach to monitor the embedding rate, which used for an interpolated pixel by determine the number of bits to achieve the best possible quality for the embedded image. The approach demonstrated better performance in embedding rate distortion output compared to other well-known IRDH schemes. The embedded image also has a better spatial resolution after being up-sampled, and there is no need for a position map, making the entire image available for data embedding while preserving the original pixels.

Malik *et al.* [80] proposed a new method for image interpolation that improves the interpolated images quality.by consider the account neighboring pixels and assigning varying weights based on proximity of the current neighbor mean interpolation are enhanced. The method also incorporates a two-way data-hiding process to embed a secret data in the interpolated pixels. In the first way, odd-valued pixels are used for data embedding, followed by the use of even-valued pixels in the second way. This approach modifies pixel values exclusively during the data-hiding process, resulting in improved computational efficiency.

G. Dual Image Based Techniques

Dual image-based techniques are a type of data hiding method that utilizes two images for data embedding. One of the images is the cover image, which contains the visible data, while the other is the auxiliary image that carries the hidden data. The auxiliary image can either be an entirely different image or a modified version of the image that carries the hidden data. The primary advantage of dual image-based techniques is that they offer a higher payload capacity than single-image methods, as they have more space available for data embedding. Moreover, since the hidden data is stored in a separate image, it is less susceptible to detection or corruption. This makes dual image-based techniques suitable for applications that require high security and reliability.

Chang *et al.* [81] made advancements in the embedding capacity by utilizing a 5×5 matrix and extending the concept of Exploiting Modification Directions (EMD) to dual images. The authors introduced a modulus function, denoted as M and defined by Eq. (2), to determine the relationship between two pixel values.

$$M = M(P_1, P_2) = (2 \times P_1 + P_2)\, mod\ 5 \qquad (2)$$

To increase the embedding capacity, Chang *et al.* [82] Extended the initial 5×5 matrix to a larger 9×9 matrix. They introduced a function M, defined by Eq. (3).

$$M = M(P_1, P_1) = (P_1 + 3 \times P_1)\, mod\ 9 \qquad (3)$$

Chang *et al.* [81] methods and Chang *et al.* [82] methods are similar except for the direction of coordinates.

Lu *et al.* [83] combined the LSB (Least Significant Bit) matching method with dual stego-images, despite that the LSB matching is typically considered an irreversible data hiding technique. In Lu *et al.*'s method, they introduced a modification rule table to improve the image quality and reversibility of the process. Eq. (4) is utilized to determine the modification bit for a given pair of pixels.

$$M = M(P_i, P_{i+1}) = LSB\left(\frac{P_i}{2} + P_{i+1}\right) \qquad (4)$$

In Lu [83] used the modification rule table to create a dual stego-images by adjusting the pixel pairs. The center folding strategy is employed to enhance the image quality in the dual images. According to Eq. (5), a new pixels are calculated for the secret digits, which is derived using the center folding strategy from the rule table. This process likely involves manipulating the pixel values based on the rule table and the folding strategy to embed the secret digits while preserving the image quality.

$$(\mathrm{p}_1', \mathrm{p}_2') = \ (p_1 + \frac{\mathrm{d}'}{2}, p_2 - \frac{\mathrm{d}'}{2}) \qquad (5)$$

Jung [84] introduced a reversible data hiding technique in dual images aimed at increasing the embedding capacity. They employed neighboring pixel value differencing for non-overlapping sub-blocks to achieve this. The neighboring pixels mean value, denoted as mi, is calculated for pixel pairs within each sub-block of size B×B according to Eq. (6). The calculated mean value mi is then used to determine the length of embedding bits. This approach aimed to enhance the data hiding capacity while maintaining the reversibility of the process.

$$m_{i=|p_i} - \frac{\sum_{j=0}^{i=1} p_j}{(BxB)-1}\ , for\ i \neq j \qquad (6)$$

H. Compressed Domain Techniques

With the increasing demand for high-quality images, the size of image files has become a challenge for storage and transmission. To address this issue, compression techniques have been developed to reduce the size of image files. Image compression can be classified into two types: lossy compression and lossless compression. Lossy compression techniques discard some of the image data to reduce the file size, resulting in an approximation of the cover image but not a replica. JPEG is a common lossy compression format that uses mathematical formulas to introduce data. On the other side, lossless compression techniques retain all the original data of the image, resulting in a replica of the cover image after decompression. The most commonly used lossless compression formats are Graphics Interchange Format (GIF) and 8-bit Bitmap (BMP). These compression techniques allow for efficient storage and transmission of images without compromising their quality.

To compress an image in JPEG format, the RGB color representation is first transformed into a YUV (Luminance (Y) and Chrominance (U and V) representation. The Y component represents luminance, or brightness, while the U and V components represent chrominance. Since the human vision is more sensitive to changes in brightness than hue, the U and V components are halved in both the horizontal and vertical directions, reducing the file size by a factor of 2. The image is then transformed using a mathematical transformation such as the DCT, which spreads the pixel values over the image. The next step is quantization, which takes advantage of the human vision's ability to detect small brightness variations over a wide area but not high-frequency variations.

There are three domains for categorizing data hiding schemes that utilize digital images as cover media: spatial, transformed, and compressed. Compressed domain-based data embedding systems have advantages such as robustness against common attacks and suitability for low-bandwidth transmission lines due to the reduced volume of transmitted data. However, these approaches have a limited capacity for embedding hidden data due to fewer available redundant spaces within the compressed data. Furthermore, the compression and decompression processes add additional time requirements to the system.

The process of natural steganography involves concealing a hidden message in a cover image by adding noise that mimics the heteroscedastic noise introduced during image acquisition. To accomplish this, Denemark *et al.* [85] added independent realizations of pixel noise to the RAW (Raw Image Format) image to make the embedding reconstruct the same cover picture acquired in a larger sensor ISO (International Organization for Standardization) environment. The message is then embedded in quantized DCT coefficients of a JPEG file through a technique called the cover source switch. The system was tested with two digital cameras, one with a monochrome sensor and the other with a color sensor. To explore various variations of the embedding algorithm, the researchers used a model of the added noise in the DCT domain and potential demo seeking to transform the raw image values. The most promising embedding algorithms were found to estimate the distribution of quantized stego DCT coefficients by adding sensor noise to the RAW image capture, developing the images, and then compressing them using Monte-Carlo sampling.

Tseng and Chang [86] described a technique for embedding secret information into a JPEG-compressed image. They used a compressor with a low scaling factor to apply to the high-resolution image to produce a digital image. Then, they applied JPEG with a high scaling factor to the same digital image to produce a low-resolution frame. Between these two stages, the quantization error was computed since most DCT coefficients are quantized to zero.

Johnson and Jajodia [87] proposed a common method for hiding secret data in JPEG compressed images called Jpeg-Jsteg. This method integrates one hidden bit of the quantized DCT coefficients in the LSB where their values are not 0, 1, or −1. While this method enhances the hiding capacity of Jpeg-information steg, the capacity is still reduced. As the compression ratio increases, the capacity for embedding bits decreases.

Kobayashi *et al.* [88] presented a method to hide data in JPEG-compressed images. Their approach involves concealing a single hidden bit within the 64th quantized DCT coefficient of each DCT block, following the zigzag order. To minimize noise resulting from the hidden data, a different quantization table is used during JPEG decoding. Modifying the value in the quantization table corresponding to the embedded data's location to 1 helps mitigate the risk of significant distortion in the decoded image. However, it's worth noting that this technique has limitations. The stego-image may experience slight distortions as a trade-off for data hiding. Additionally, the information-hiding capacity is relatively limited, allowing for only 4,096 bits to be concealed in a 512×512 gray-level image.

Sharma and Kumar [89] presented a new steganographic algorithm designed to conceal text files within an image. To optimize storage space for the data to be embedded, they employed a compression algorithm that works within a 1-bit to 8-bit per pixel ratio range. The authors suggested an enhanced version of the LSB method but found it to be unstable. To improve the hiding power of the algorithm, they also introduced a compression process.

V. Reversible Data Hiding in Encrypted Image

RDH is a technique used in images to extract both the hidden data and the original cover image. To protect privacy, the original content is encrypted before being transferred to the data manager as Fig. 6. However, in certain situations such as authentication or steganography, the data manager may need to add more data to the encrypted image without knowing the original content. The process involves encrypting the original file with an encryption key and then using any data-hiding method to compress the image using a data-hiding key, creating space for additional data.

Zhang [90] proposed a method that involved encrypting the entire data of an uncompressed image using a stream cipher. Then, a small portion of the encrypted data was modified to insert additional information. The original image could be retrieved by decrypting the image using the encryption key. By using a hiding data key and exploiting the spatial correlation in natural images, the embedded data could be extracted, and the original image could be recovered. The image was divided into blocks of the same size, and an extra bit was inserted into each block by utilizing the 3 LSBs plane. The marked encrypted image would decrypt by the receiver, divide it into blocks, and perform data extraction and image recovery based on the fluctuation observed in each block. Zhang's method aimed to achieve data confidentiality while enabling the extraction of the embedded information and the recovery of the cover image by combining encryption, data embedding, and spatial correlation.

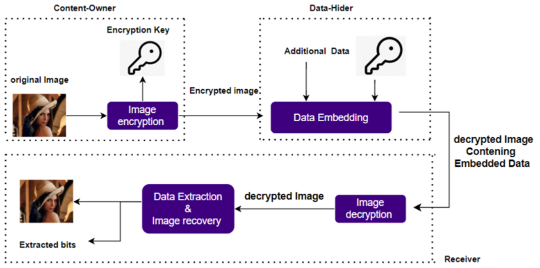

Fig. 6. Reversible data hiding in encrypted image.

Zhang [91] proposed a technique that combines encryption and data hiding for concealing reversible messages within an encrypted image. The process involves encrypting the original image using an encryption key. Subsequently, additional data is inserted into the encrypted image using a data-hiding key. The recipient can retrieve the embedded extra data using the data-hiding key, without having knowledge of the original image content. If the recipient have both the encryption key and the data-hiding key, they can decrypt the obtained data, resulting in an image similar to the original image but without the ability to recover the additional data. It is important to note that if both the encryption key and the data-hiding key are available to the recipient, they can successfully retrieve the additional data and recover it without any errors, as long as the amount of extra data inserted is within reasonable limits. The proposed technique offers a way to combine encryption and data hiding to achieve secure communication while maintaining the ability to embed and retrieve reversible messages within the encrypted image.

Bartwal and Bharti [92] introduced lossless and combined reversible data hiding approaches for cipher text images encrypted using public key cryptosystems with homomorphic and probabilistic properties. In the lossless technique, additional data is hidden into the cipher text by replacing the values of pixels. This is done by modifying LSB of the cipher text pixels, which allows for the embedding of multiple layers of data using different LSB planes. This technique ensures that the embedding data can be exactly retrieved while minimizing any noticeable changes to the image or data. In the reversible method, a histogram shrink preprocessing is performed before encryption, and half of the cipher text values are modified for the hidden data.

Hong *et al.* [93] presented an improved way of Zhang's reversible data-hiding scheme specifically designed for encrypted images. Analyzing the smoothness of image parts to facilitate both data extraction and image recovery processes the primary focus of this scheme. However, they identified certain limitations in Zhang's work, such as the incomplete utilization of pixels within a block and the neglect of pixel correlations at the borders of neighboring blocks. These shortcomings could potentially result in reduced accuracy when extracting embedded data. To overcome these limitations, Hong *et al.* proposed a more advanced approach. They introduced an enhanced method for calculating block smoothness that incorporated a larger number of pixels, enabling more accurate data extraction. Additionally, they implemented a side-match technique to further decrease the error rate. Unlike Zhang's work, which disregarded the pixels at the borders of image parts, Hong *et al.* considered these pixels and analyzed all image blocks that contained additional embedded data.

Liao and Shu [94] computed the image blocks, which takes into account the positions of various adjacent pixels. They referred to this as the data-embedding ratio. The complexity of an image block is approximated by computing the absolute mean difference between pixels and their adjacent pixels. Puteaux and Puech [95] introduced RDH method for encrypted images that utilizes MSB prediction. Since adjacent pixel values in a clear image tend to be similar due to the local correlation between pixels, it is reasonable to predict pixel values based on previously decrypted values. However, there may be errors in some cases. Therefore, the initial step in this method is to extract prediction errors and store them in a binary map for error location. The authors proposed two techniques: High-Capacity RDH with Prediction Error Correction (CPEHCRDH) and High-Capacity RDH with Embedded Prediction Errors (EPE-HCRDH). In CPE-HCRDH, before encryption the prediction errors are corrected, and in the first the cover image is processed according to the map of error location to avoid all prediction errors. In EPE-HCRDH, encrypting the cover image, then the location of prediction errors is inserted after encryption.

Puyang *et al.* [96] proposed RDH method for encrypted images that uses two Most Significant Bits (MSBs), namely MSB and second MSB, to better capture the correlation between neighboring pixels. The original image is first encrypted using the bitwise exclusive-or (XOR) operation, and then prediction errors are highlighted based on an error location map that detects all possible errors. Finally, using two-MSB replacement, new data is embedded into all available pixels. This method achieves reversibility, reparability, and error-free data extraction.

Liu and Pun [97] proposed an approach for RDH in encrypted images based on the concept of Redundant Space Transfer (RST). RST transfers redundant space from the original image to the encrypted image during encryption for embedding more information. This method retains a portion of the redundant area in the encrypted image, in contrast to traditional encryption approaches that deletes most of the redundant space from the original image. RDH techniques are then applied to hide additional information in the remaining redundant space. This approach achieves high embedding capacity while preserving the original image quality and ensuring reversibility and error-free data extraction.

Cao *et al.* [98] proposed a technique for embedding data in encrypted images based on patch-level sparsity representation. The method involves representing each patch in the image using sparse coding with an over-complete dictionary. By approximating the patch with a set of atoms from the dictionary, they obtain residual errors. These residual errors, along with the learned dictionary, are then embedded into the cover image, creating vacant space within the encrypted image. This vacant space allows for the hide additional secret data. The method offers several advantages, including high capacity and security. To recover the embedded data, both the dictionary and the residual errors are required, ensuring that unauthorized individuals cannot retrieve the hidden information without possessing these components.

Zhang *et al.* [99] proposed a novel Reversible Data Hiding with Encrypted Images **(**RDH-EI) framework that utilizes Reversible Image Transformations (RIT). Unlike traditional encryption-based frameworks, which transform the original image as a content of another image have the same size. The resulting "encrypted image" is then sent to the cloud. The advantage of this approach is that by the cloud server any RDH method for plaintext images can hide information into the encrypted image, without any client-side involvement. Two RDH approaches, classic RDH schemes, are used to embed watermarks in the image after encrypted, providing different levels of image quality and high embedding capacity, respectively.

Qian and Zhang [100] proposed an approach for RDH in encrypted images called Distributed Source Coding (DSC). The approach involves the owner of the content encrypting the data, sequence of selected bits extracted from the encrypted image is compressed by data hider used a stream cipher to make area for the hidden data. Low-Density Parity Checks (LDPC) codes used to encode the selected series bits in Slepian-Wolf format. The hidden bits can be recovered on the receiver if the recipient only knows the embedding key, while an image estimate algorithm can be used to approximate the original image with high quality if the recipient only has the encryption key. The approach also allows for the extraction of hidden data and excellent restoration of the original image if the receiver side has the embedding key and encryption key.

Yin *et al.* [101] proposed a high-capacity RDH-EI algorithm that utilizes multi-MSB prediction and Huffman coding. The algorithm begins by adaptively predicting and encoding the multi MSB of each pixel in the original image using Huffman coding. Then, the image is encrypted using the stream cipher technique. Finally, the algorithm utilizes multi-MSB substitution to embed additional data in the space of the encrypted image.

Bao and Zhou [102] introduced a fresh approach to image encryption aimed at mitigating the security vulnerabilities prevalent in many existing encryption algorithms. Rather than yielding encrypted images that resemble texture-like or noise-like patterns, the proposed concept generates visually meaningful encrypted images that appear as normal images. This renders it substantially more challenging for attackers to differentiate and pinpoint the encrypted images amidst a plethora of normal images, thereby bolstering the security level compared to conventional encryption methods. The proposed concept is realized through an image encryption system, which entails a pre-encryption process characterized by excellent diffusion and confusion properties to safeguard the original image contents. Additionally, an effective Discrete Wavelet Transform (DWT)-based content transformation is employed to generate visually meaningful encrypted images with diverse visual appearances. Simulation results and security analyses validate the effectiveness of the proposed encryption concept and system, demonstrating superior encryption performance while maintaining low computational costs.

Kanso and Ghebleh [103] proposed a lossless visually meaningful image encryption scheme based on a single chaotic map, which enhances Bao and Zhou's algorithm by introducing distortions to the cover image that are more challenging to detect. This scheme can be seamlessly integrated with any existing image encryption scheme, thereby inheriting its security properties. Simulations demonstrate that proposed scheme exhibits outstanding security features: it produces high-quality stego-images with minimal or imperceptible disruptions, and ensures complete retrieval of the embedded secret image. Moreover, scheme imposes minimal computational overhead on the encryption process to conceal the encrypted data within a cover image. By embedding scrambled data bytes independently within the host, scheme enables parallel processing of the data, thereby enhancing processing speed.

Singh and Singh [104] presented an approach for generating a visually meaningful multi- encryption image scheme. It involves embedding multiple cipher data image within the unimportant actual data of a scrambled host image, which is subsequently unscrambled to produce a visually meaningful multiple encrypted image. Comparative analysis with existing visually meaningful encryption schemes reveals that our proposed scheme excels in its ability to insert more data with minimal degradation of the host image quality. The PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity Index) values for the embedded host image in Bao and Zhou's scheme is (27.1831, 0.9790) and Kanso and Ghebleh's scheme is (34.1624, 0.9949). In contrast, proposed method achieves significantly higher value for PSNR and SSIMs (86.6209, 0.9999). Furthermore, the proposed scheme demonstrates robustness against various classical attacks as well as specific attacks such as salt and pepper noise and occlusion attacks.

VI. Evaluation of Different Techniques

The essential metrics use in evaluating the performance of different steganography techniques and can assist in selecting the best method for a particular use case are.

A. Peak Signal to Noise Ratio (PSNR)

There are alterations to the cover image's pixel values in order to include the secret info. Analysis of the alterations is necessary because they have an impact on how Stego-image is undetectable the output. The PSNR is used metric for evaluating the quality of a stego-image in steganography. It measures the similar between the original image and the stego-image by analyzing the Mean Squared Error (MSE) between them. Based on the PSNR value, the image quality will be improved as its value is higher. For 8-bit images, the PSNR is calculated as Eq. (7).

$$PSNR(in\ dB) = 10\,log_{10}\left(\frac{255^2}{MSE}\right) \tag{7}$$

$$MSE = \frac{\sum_{i=1}^{N}(c_i - c_i')}{N} \tag{8}$$

where, *N* is the number of cover image pixels, c_i' and c_i are the intensity of ith pixel in the stego-image and the cover image respectively.

B. Structural Similarity Index Measure (SSIM)

SSIM is a metric used to examine the similarity between two images. It is calculated as:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x{}^2 + \mu_y{}^2 + c_1)(\sigma_x{}^2 + \sigma_y{}^2 + c_2)} \tag{9}$$

$$C_1 = (K_1L)^2 \tag{10}$$

$$C_2 = (K_2L)^2 \tag{11}$$

The μ_x, μ_y are the mean intensity values of images *x* and *y*. the $\sigma_x{}^2$ is the variance of *x*, $\sigma_y{}^2$ is the variance of *y* and $\sigma_{xy}{}^2$ is the covariance of *x* and *y*. C_1 and C_2 are the two stabilizing parameters. *L* is the dynamic range of pixel values ($2^{\text{number of bits per pixel}}$–1) and the contents K_1 = 0.01 and K_2 = 0.03.

C. Payload Capacity

It is a measurement of the amount of data conceals in a cover image. Typically, it is represented as BPP (Bits per Pixel), where:

$$BPP = \frac{Number\ o\ f\ secret\ bits\ embedded}{Total\ pixels\ in\ the\ cover\ image} \tag{12}$$

VII. Discussion

This section discusses some Performance of Stenographic, Watermark and Reversible data hiding techniques which were mentioned in Tables I and II. RDH is typically used for authentication, and it is mostly used in situations where distortion is a concern, such the military, satellites, and healthcare. The primary function of this method is to maintain the perceptual quality of the host image. Additionally, a traditional RDH technique must be used to retain the quality of the image with hidden data while maintaining a high PSNR. Fig. 7 shows a count of the different steganography methods, watermark methods and reversible data hiding methods developed to hide secret messages published from 2018 to 2022.

TABLE I. The Performance Evaluation for Different Stenographic Technique

References	Method	PSNR	ER	MSE	SSIM
[2]	adaptive reversible integer transformation	70.6	318	-	-
[7]	multi-cover adaptive steganography	51.25 Db	0.5	-	0.9964
[8]	skin detection algorithm	85.18	2,120	-	-
[10]	adaptive steganography scheme	Acceptable	128	1.96	-
[12]	least significant bits (LSB)	37.8369	High	10.7002	-
[14]		71	915 B	4.5×10^{-3}	-
[15]		57.2226	High	0.1582	-
[18]		50	-	0.999	-
[17]		29.690	-	69.826	-
[19]	Edge Detection based variable LSB	68.38	-	0.0094	-
[24]	least significant bits (LSB)	58.487	8 Bit	0.092125	
[31]	Discrete Fourier Transform (DFT) domain	55.04	3.3	-	0.963
[36]	Integer Wavelet Transform(IWT)	45.01	8,251	4.79	0.9996
[37]	Wavelet Contourlet	59.69	256K b	-	1
[46]	error-control coding, image processing, spread spectrum techniques	43.7179	0.1667	0.191	-
[47]	Human Visual System (HVS)	26. 83	376	-	-
[63]	Histogram Modification Watermarking technique Compression algorithm	48.29	0.0709	-	-
[67]	Wavelet Transform Histogram Modification	34.9533 dB	4,229.12 KB	-	-
[68]	histogram modification	49.13	1.9233	-	-
[69]		40.8925	184,101.5	-	-
[75]	prediction-error expansion and Pixel Value Ordering (PVO)	58.45	10,000 bits	-	-
[80]	least significant bits (LSB)	49.28	524,288 bits	-	0.9973
[82]	pixel value difference Prediction error expansion.	45.58	767,922bits	-	0.99
[96]	prediction errors Most Significant Bit (MSB)	57.4 dB	0.9998	-	1
[97]	Redundant Space Transfer (RST) difference expansion	41.4941	1.6052	8.4583	-
[98]	Redundant Space Transfer (RST) difference expansion	61.1544	0.1	-	-

References	Method	PSNR	ER	MSE	SSIM
	histogram shifting				
[99]	Redundant Space Transfer (RST) difference expansion	48.2584 dB	0.95	2.91h	-
[101]	Most Significant Bits (MSB) Distributed Source Coding (DSC)	63.1dB	1	-	-
[102]	MSB Huffman coding	54.3546	2,000 bits	10.810	0.9999
[105]	Wavelet Transform	49.5106	70 KB	-	0.99389
[106]	Discrete Wavelet Transform (DWT) bit-plane slicing method	87.8919	-	0.0082	1
[107]	Swim Transformer	44.568	-	-	0.9936
[108]	Direct Sequence Spread Spectrum (DSSS) scheme	27.959	-	-	1
[109]	chaos based encryption &chaotic modulation	42.4697	0.5714	-	-
[110]	Rivest-Shamir-Adleman(RSA)Encryption algorithm and Least Significant Bit (LSB)	71.347	1,000	0.0048	-
[111]	(Support vector machine)SVM classifier	44.0719	-	-	-
[112]	hybrid combination of graph-based transform along with Singular Value Decomposition(SVD)	52.5768	-	-	0.99993
[113]	Discrete Fourier Transform (DFT)	38.0535	-	-	0.9414
[114]	Redundant Discrete Wavelet Transform (RDWT) Randomized Singular Value Decomposition (RSVD) Set Partitioning in Hierarchical Trees -Steganographic Techniques (SPIHT-STE)	45.3362	-	-	0.9875
[115]	Pixel-Value-Ordering(PVO)	61	10,000 bits	-	-
[116]	histogram shifting prediction error	63.05	10,000 bits	-	-
[117]	Integer Wavelet Transformed (IWT) and Discrete Cosine Transform (DCT)	57.45	-	0.11	0.99
[118]	Discrete Cosine Transform - Discrete Wavelet Transform - Singular Value Decomposition (DCT-DWT-SVD)	57.6303	-	-	0.9984
[119]	Discrete Wavelet Transform (DWT)	57.21	-	0.12	0.99517
[120]	Pixel Value Differencing (PVD)- Least Significant Bit (LSB)	54.1489	77,244 bits	-	0.9999
[121]	Pixel Value Differencing (PVD)- Least Significant Bit (LSB)	48.40 dB	3.0	-	0.985
[122]	Most Significant Bit (MSB)	69.7156	1,024	0.0070	1.0000

[1] Tables stenographic technique.

TABLE II. THE PERFORMANCE EVALUATION FOR DIFFERENT REVERSIBLE DATA HIDING (RDH) METHODS

References	Method	PSNR	ER	MSE	SSIM
[123]	Difference Expansion (DE) LSB	64.7369	11434 bits	-	-
[124]	Shifting block histogram of pixel differences	49.33	0.1692	0.105862	0.9968
[125]	integer wavelet transform histogram shifting	57.73	0.0400	-	-
[126]	Average Pixel Repetition (APR) and pixel geometry matrix	42.00	2.24	1.65×101	-
[127]	Difference between pixels	53.36	1.50	4.18	-
[128]	Watermark technique	44.8667	-	0.0700	0.9991
[129]	Deep Neural Network (DNN)	43.8073	32	-	0.9852
[130]	Pixel-Value Error Expansion (PEE) Pixel Value Ordering (PVO) prediction	55.88	20,000 bits	-	-
[131]	Histogram Shifting (HS)	57.978	0.05	-	-
[132]	Rhombus Mean Interpolation technique	42.3443	1.5	-	0.9811
[133]	Integer-Integer Wavelet Transformed (I-IWT) pairwise prediction error expansion	49.69	0.3494	-	0.9905
[134]	Pixel to Block (PTB) conversion A fragile watermark Intermediate Significant Bit Substitution (ISBS)	49.6855	0.3494	0.1682	0.9909
[135]	Additive interpolation-error expansion Watermarking technique	48.946495	0.1373	-	0.99958
[71]	Difference Expansion (DE)	41.198659	0.0465	-	0.990796
[136]	integer wavelet transform histogram modification	48.143831	0.0556	-	0.998147
[137]	Interpolation by Neighboring Pixels (INP)	48.420968	0.0412	-	0.998943
[138]	Pixel-Value-Ordering (PVO) multiple histograms generation and modification	59.76	10,000 bits	4.93	-
[139]	Histogram Shifting (HS)	53.10	6,000 bits	-	-
[140]	Discrete Cosine Transform (DCT)	43.12	10,000 bits	-	-
[141]	Multiple Histograms Modification (MHM) Prediction-Error Histogram (PEH)	48.50	0.2	0.10	-
[142]	Discrete Cosine Transform (DCT)	53.3055	8×10^3	7.469	-

References	Method	PSNR	ER	MSE	SSIM
	difference expansion				
	histogram shift				
[143]	Multiple Histograms Modification (MHM)	59.82	2×10^4 bits	0.63	-
[144]	Multiple Histograms Modification (MHM) Error Expansion (PEE) Deep Neural Networks (DNN)	59.97	10,000 bits.	98.99	-
[145]	multiple histograms modification and Pixel-Value Error Expansion (PEE)	59.86	10,000bits	-	-
[146]		60.38	10,000 bits	-	-
[147]	Local Binary Pattern-based (LBP) PVD	52.36	1.98	-	0.9977
[148]	Discrete Cosine Transform (DCT)- Pixel Value Differencing (PVD)- Least Significant Bit (LSB)	44.57	8,096 bytes	2.2	-
[149]	Histogram shift	48.55	48,424 bits	-	-
[150]	Prediction Error (PE) Statistical Distribution (SD)	33.38	2.5 bpmv	-	-
[151]	Histogram shifting	58 dB	0.02 bpp	-	-
[152]	Prediction-Error Expansion (PEE) Pixel-Residual Histogram (PRH)	56.31db	20,000 bits	-	-
[153]	A dual image based reversible data hiding Huffman encoding	49.48	2.69	0.07	0.8873
[154]	prediction-error expansion Pixel Value Ordering (PVO)	63.87	10,000 bits	-	-
[155]	Histogram modification prediction-error expansion Pixel Value Ordering (PVO)	59.29	10,000 bits	-	-
[156]	prediction-error expansion and Pixel Value Ordering (PVO)	59.38	10,000 bits	-	-
[157]		60.71	20,000 bits	1.04	-
[158]		59.18	10,000 bits	1.95	-
[159]	Difference Expansion (DE) technique	35.95	311,966 bits	-	-
[160]	Prediction-Error Expansion histogram shifting	49.14	0.04	-	0.9989
[161]	pixel value ordering–based	52.8	44,000bits	-	-
[162]	Least Significant Bit Technique (LSBT)	69.098	-	.021	0.999
[163]	Direct Sequence Spread Spectrum	87.3147 dB	-	0.9227	-
[164]	Discrete Cosine Transform (DCT)	49.8114	2,950 bits	-	0.99986
[165]		44.4667	-	2.3257	1
[166]	Pairwise prediction-error expansion (pairwise PEE)	52.55	0.1	-	0.9997
[167]	histogram modification	34.73	226497bits	-	-
[168]	Prediction-Error Expansion (PEE) Pixel-Value-Ordering (PVO)	60.82	10,000 bits	-	-
[169]	Block-based adaptive Most Significant Bit (MSB) encoding technique and Huffman coding	89.0940 dB	2.0853	6.2647	-
[170]	Discrete Wavelet Transform (DWT)	59.69	-	-	1

[2] Tables Performance of Reversible data hiding.

To analyze the performance of the Stenographic and RDH Techniques six standard grayscale images of 512×512 pixels were utilized to test the technique. the image is Lena, Airplane, ‘Barbara’, ‘Peppers’, ‘Baboon’ and ‘Boat as Fig. 8 and the Blind Open World Steganalysis (BOWS)-2 database is the most database used.

In the format-based methods shown in Tables I and II. The authors had to take a lot of things into account while using the different strategies to hiding data. The first factor is the Image quality. PSNR is one of the popular metric to estimate the quality difference between the original cover image and stego-image. PSNR with larger value indicates that a good visual quality of the stego-image, means a distortion has occurred. Also a small PSNR value indicate that the stego-image has bad visual quality.

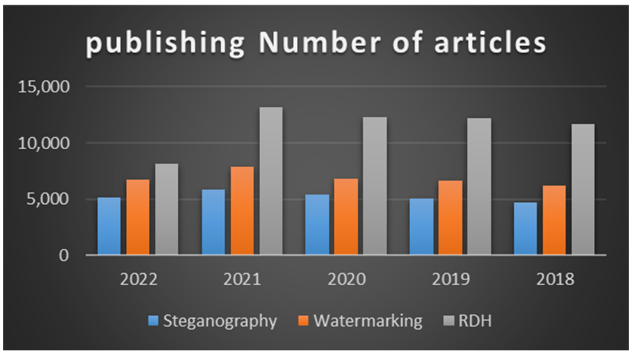

Fig. 7. Published number articles in the last 5 years.

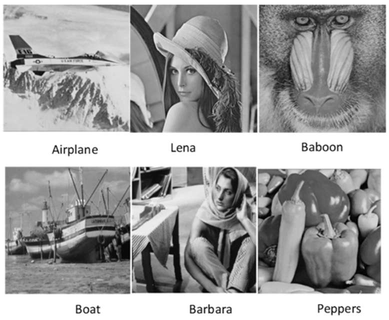

Fig. 8. Cover images with size 512×512.

In Table I for different Stenographic and Watermark Techniques the PSNR is very high in [2, 8, 98, 106, 110, 122, 116] that show high image visual quality and the PSNR of the proposed schema has greatly increased. Several papers [12, 14, 15, 18,17, 24, 80] have employed the same method, specifically utilizing the Least Significant Bits (LSB), yielding varied results. Notably, Santoso *et al.* [14] achieved a high PSNR of 71. Researchers in [117, 118] used Discrete Cosine Transform (DCT) and the Begum *et al.* [118] achieved good PSNR than others with value 57.6303 and have approximate results [117]. Some researches [96, 116] used prediction-error expansion (pairwise PEE) methods with approximate results. Previous papers [75, 115] used Pixel Value Ordering (IPVO) methods with approximate results.

In Table II for different Reversible Data Hiding (RDH) methods [169] show high image visual quality. Xiao *et al.* [139]and Wedaj *et al.* [140] used Histogram Shifting (HS) and Discrete Cosine Transform (DCT) achieved good PSNR but PSNR for [139] higher than [140] with 53.10. Researchers in[143–146, 151, 155, 160] used histogram modification with approximate results. Researchers in [130, 156–158, 168] used the same technique prediction-error expansion and Pixel Value Ordering (PVO) and the results are close where the yielding results with PSNR values around 55.88, 59.38, 60.71, 59.18 and 60.82.

The second factor is the SSIM, a perceptual metric that measures imperceptibility according to the human visual system and quantifies the image quality loss brought on by processing. The results is approximate but papers in [37, 96, 106,108, 165, 170] have the value 1 that is approve there are no difference between original image and image after data hiding.

The third factor is Embedding Rate (ER) is maximum number of bits that a cover-object can hide. The measuring of steganography capacity in the case of embedding steganography is simple because the cover-animation does not change size. The cover-animation might alter the size when encoding steganography. [8, 36, 121, 169] Have high embedding data.

VIII. Conclusions and Future Contributions

Hiding Data is the step of adding secret information to text, image, audio and video files. We present in this paper a review of techniques that using in RDH (Reversible Data Hiding). Steganography is a technique that most use for hiding data, we discuss the most popular stenograph methods as LSB (Least Significant Bit), PVD (Pixel Value Differencing), Discrete Fourier Transformation Technique (DFT), discrete cosine transformation technique (DCT), Discrete Wavelet Transformation (DWT) technique and SVD (Singular Value Decomposition). Digital watermarking is a widely used approach in cases where needs to prevent data from leaking into the public domain. It absolutely essential. When a business has a direct legal relationship with its customers and is required to secure that information. The watermarking techniques and its application are explained. In sensitive data, the encryption plays an important role to prevent intruders to discover data that hiding so we explained RDH in the encrypted domain and algorithms to do this. Finally, the performance of several approaches was explained in terms of the embedding capacity, security of hiding data, and the image visual quality.

Investigating and creating more resilient stenographic algorithms that can resist sophisticated attacks and guarantee safe data hiding. Investigating how steganography can be integrated with emerging technologies such as AI and block chain to enhance privacy protection and data security

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

KA review the research; AA and H Shaban analyzed the data; HR wrote the paper; all authors had approved the final version.

References

[1] P. Singh and R. S. Chadha, "A survey of digital watermarking techniques, applications and attacks," *International Journal of Engineering and Innovative Technology (IJEIT),* vol. 2, no. 9, pp. 165–175, 2013.

[2] Y. Qiu, Z. Qian, H. Zeng, X. Lin, and X. Zhang, "Reversible data hiding in encrypted images using adaptive reversible integer transformation," *Signal Processing,* vol. 167, 107288, 2020.

[3] D.-C. Wu and W.-H. Tsai, "A steganographic method for images by pixel-value differencing," *Pattern Recognition Letters,* vol. 24, no. 9–10, pp. 1613–1626, 2003.

[4] S. A. Seyyedi and N. Ivanov, "Statistical image classification for image steganographic techniques," 2014.

[5] S. Kaur, S. Bansal, and R. K. Bansal, "Steganography and classification of image steganography techniques," in *Proc. 2014 International Conference on Computing for Sustainable Global Development (INDIACom),* 2014, pp. 870–875.

[6] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," *Optics & Laser Technology,* vol. 116, pp. 92–102, 2019.

[7] H.-D. Yuan, "Secret sharing with multi-cover adaptive steganography," *Information Sciences,* vol. 254, pp. 197–212, 2014.

[8] S. Khupse and N. N. Patil, "An adaptive steganography technique for videos using Steganoflage," in *Proc. 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT),* 2014, pp. 811–815.

[9] L. Li, B. Luo, Q. Li, and X. Fang, "A color images steganography method by multiple embedding strategy based on sobel operator," in *Proc. 2009 International Conference on multimedia information networking and security,* 2009, vol. 2, pp. 118–121.

[10] H. Tian, K. Zhou, H. Jiang, Y. Huang, J. Liu, and D. Feng, "An adaptive steganography scheme for voice over IP," in *Proc. 2009 IEEE International Symposium on Circuits and Systems (ISCAS)*, 2009, pp. 2922–2925.

[11] P. Das, S. C. Kushwaha, and M. Chakraborty, "Multiple embedding secret key image steganography using LSB substitution and Arnold Transform," in *Proc. 2015 2nd International Conference on Electronics and Communication Systems (ICECS)*, 2015, pp. 845–849.

[12] S. Bhatt, A. Ray, A. Ghosh, and A. Ray, "Image steganography and visible watermarking using LSB extraction technique," in *Proc. 2015 IEEE 9th International Conference on Intelligent Systems and Control (ISCO)*, 2015, pp. 1–6.

[13] A.-G. T. Al-Tamimi and A. A. Alqobaty, "Image steganography using Least Significant Bits (LSBs): A novel algorithm," *International Journal of Computer Science and Information Security*, vol. 13, no. 1, p. 1, 2015.

[14] H. A. Santoso, E. H. Rachmawanto, and C. A. Sari, "An improved message capacity and security using divide and modulus function in spatial domain steganography," in *Proc. 2018 International Conference on Information and Communications Technology (ICOIACT)*, 2018, pp. 186–190.

[15] L. Zhi and S. A. Fen, "Detection of random LSB image steganography," in *Proc. IEEE 60th Vehicular Technology Conference, 2004. VTC2004-Fall. 2004*, vol. 3, 2024, pp. 2113–2117.

[16] A. M. Odat and M. A. Otair, "Image steganography using modified least significant bit," *Indian Journal of Science and Technology*, vol. 9, no. 39, pp. 1–5, 2016.

[17] M. Hussain, Q. Riaz, S. Saleem, A. Ghafoor, and K.-H. Jung, "Enhanced adaptive data hiding method using LSB and pixel value differencing," *Multimedia Tools and Applications*, vol. 80, no. 13, pp. 20381–20401, 2021.

[18] V. L. Reddy, A. Subramanyam, and P. C. Reddy, "Implementation of LSB steganography and its evaluation for various file formats," *Int. J. Advanced Networking and Applications*, vol. 2, no. 05, pp. 868–872, 2011.

[19] M. Tayel, A. Gamal, and H. Shawky, "A proposed implementation method of an audio steganography technique," in *Proc. 2016 18th International Conference on Advanced Communication Technology (ICACT)*, 2016, pp. 180–184.

[20] S. Singh, "Adaptive PVD and LSB based high capacity data hiding scheme," *Multimedia Tools and Applications*, vol. 79, no. 25, pp. 18815–18837, 2020.

[21] G. Paul, S. K. Saha, and D. Burman, "A PVD based high capacity steganography algorithm with embedding in non-sequential position," *Multimedia Tools and Applications*, vol. 79, no. 19–20, pp. 13449–13479, 2020.

[22] G. Swain, "Two new steganography techniques based on quotient value differencing with addition-subtraction logic and PVD with modulus function," *Optik*, vol. 180, pp. 807–823, 2019.

[23] E. M. Jamel, "Hiding multi short audio signals in color image by using fast Fourier transform," *Al-Nahrain Journal of Science*, vol. 24, no. 1, pp. 57–65, 2021.

[24] N. K. Murthy, S. Sharma, M. J. P. Priyadarsini, R. Ranjan, S. Sarkar, and N. S. Basha, "Image steganography using discrete cosine transform algorithm for medical images," in *Advances in Automation, Signal Processing, Instrumentation, and Control*: Springer, 2021, pp. 2349–2358.

[25] L. Li, R. Bai, J. Lu, S. Zhang, and C.-C. Chang, "A watermarking scheme for color image using quaternion discrete fourier transform and tensor decomposition," *Applied Sciences*, vol. 11, no. 11, p. 5006, 2021.

[26] F. Cao, D. Guo, T. Wang, H. Yao, J. Li, and C. Qin, "Universal screen-shooting robust image watermarking with channel-attention in DCT domain," *Expert Systems with Applications*, vol. 238, 122062, 2024.

[27] P. Pal, S. Banerjee, A. Ghosh, D. R. Vago, and J. Brewer, "DFT21: Discrete Fourier transform in the 21st century," *Authorea Preprints*, 2023.

[28] C. Qu, J. Du, X. Xi, H. Tian, and J. Zhang, "A hybrid domain-based watermarking for vector maps utilizing a complementary advantage of discrete fourier transform and singular value decomposition," *Computers & Geosciences*, vol. 183, 105515, 2024.

[29] Y. Khedmati, R. Parvaz, and Y. Behroo, "2D Hybrid chaos map for image security transform based on framelet and cellular automata," *Information Sciences*, vol. 512, pp. 855–879, 2020.

[30] N. Ayub and A. Selwal, "An improved image steganography technique using edge based data hiding in DCT domain," *Journal of Interdisciplinary Mathematics*, vol. 23, no. 2, pp. 357–366, 2020.

[31] T. J. Siddiqui and A. Khare, "Chaos-based video steganography method in discrete cosine transform domain," *International Journal of Image and Graphics*, vol. 21, no. 02, p. 2150015, 2021.

[32] S. Khan *et al.*, "On hiding secret information in medium frequency DCT components using least significant bits steganography," *Computer Modeling in Engineering & Sciences*, vol. 118, no. 3, pp. 529–546, 2019.

[33] D. Debnath, E. Ghosh, and B. G. Banik, "Multi-image hiding blind robust RGB steganography in transform domain," *International Journal of Web-Based Learning and Teaching Technologies (IJWLTT)*, vol. 15, no. 1, pp. 24–52, 2020.

[34] L. Guo, J. Ni, W. Su, C. Tang, and Y.-Q. Shi, "Using statistical image model for JPEG steganography: Uniform embedding revisited," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2669–2680, 2015.

[35] I. H. Shahrezaei and H.-C. Kim, "Fractal analysis and texture classification of high-frequency multiplicative noise in SAR sea-ice images based on a transform-domain image decomposition method," *IEEE Access*, vol. 8, pp. 40198–40223, 2020.

[36] K. Raja *et al.*, "Robust image adaptive steganography using integer wavelets," in *Proc. 2008 3rd International Conference on Communication Systems Software and Middleware and Workshops (COMSWARE'08)*, 2008, pp. 614–621.

[37] B.-L. Lai and L.-W. Chang, "Adaptive data hiding for images based on harr discrete wavelet transform," in *PSIVT*, 2006.

[38] M. S. Subhedar and V. H. Mankar, "Image steganography using contourlet transform and matrix decomposition techniques," *Multimedia Tools and Applications*, vol. 78, pp. 22155–22181, 2019.

[39] J. Singh and M. Singla, "Image steganography technique based on singular value decomposition and discrete wavelet transform," *International Journal of Electrical and Electronics Research*, vol. 10, no. 2, pp. 122–125, 2022.

[40] F. Yasmeen and M. S. Uddin, "An efficient image steganography approach based on QR factorization and singular value decomposition in non-subsampled contourlet transform domain," *Security and Privacy*, vol. 5, no. 4, p. e229, 2022.

[41] G. Song, M. K. Ng, and X. Zhang, "Robust tensor completion using transformed tensor singular value decomposition," *Numerical Linear Algebra with Applications*, vol. 27, no. 3, p. e2299, 2020.

[42] F. Q. A. Alyousuf, R. Din, and A. J. Qasim, "Analysis review on spatial and transform domain technique in digital steganography," *Bulletin of Electrical Engineering and Informatics*, vol. 9, no. 2, pp. 573–581, 2020.

[43] N. Hamid, A. Yahya, and R. Ahmad, "Image Steganography Techniques : An Overview," *International Journal of Computer Science and Security (IJCSS)*, vol. 6, no. 3, pp. 168–187, 2012.

[44] J. A. Bagaskara, T. W. Purboyo, and R. A. Nugrahaeni, "Analysis of JPEG image steganography using SPread spectrum method," *International Journal of Applied Engineering Research*, vol. 12, no. 23, pp. 13944–13950, 2017.

[45] A. Kuznetsov, O. Smirnov, A. Arischenko, I. Chepurko, A. Onikiychuk, and T. Kuznetsova, "Pseudorandom sequences for spread spectrum image steganography," in *CybHyg*, 2019, pp. 122–131.

[46] L. M. Marvel, C. G. Boncelet, and C. T. Retter, "Spread spectrum image steganography," *IEEE Transactions on image processing*, vol. 8, no. 8, pp. 1075–1083, 1999.

[47] M. S. Subhedar and V. H. Mankar, "Secure image steganography using framelet transform and bidiagonal SVD," *Multimedia Tools and Applications*, vol. 79, no. 3, pp. 1865–1886, 2020.

[48] M. Xiao and Z. He, "High capacity image steganography method based on framelet and compressive sensing," in *MIPPR 2015: Multispectral Image Acquisition, Processing, and Analysis*, vol. 9811, 2015, pp. 226–231.

[49] B. Feng, W. Lu, and W. Sun, "Secure binary image steganography based on minimizing the distortion on the texture," *IEEE transactions on Information Forensics and Security*, vol. 10, no. 2, pp. 243–255, 2014.

[50] Q. Wei, Z. Yin, Z. Wang, and X. Zhang, "Distortion function based on residual blocks for JPEG steganography," *Multimedia Tools and Applications,* vol. 77, pp. 17875–17888, 2018.

[51] B. Li, M. Wang, X. Li, S. Tan, and J. Huang, "A strategy of clustering modification directions in spatial image steganography," *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 9, pp. 1905–1917, 2015.

[52] S. Wadhera, D. Kamra, A. Rajpal, A. Jain, and V. Jain, "A comprehensive review on digital image watermarking," arXiv Print, arXiv:2207.06909, 2022.

[53] S. Kumar, B. K. Singh, and M. Yadav, "A recent survey on multimedia and database watermarking," *Multimedia Tools and Applications,* vol. 79, no. 27, pp. 20149–20197, 2020.

[54] Z. Zhang, M. Zhang, and L. Wang, "Reversible image watermarking algorithm based on quadratic difference expansion," *Mathematical Problems in Engineering,* vol. 2020, 2020.

[55] M. Begum and M. S. Uddin, "Analysis of digital image watermarking techniques through hybrid methods," *Advances in Multimedia,* vol. 2020, 2020.

[56] Q. Su, X. Zhang, and H. Wang, "A blind color image watermarking algorithm combined spatial domain and SVD," *International Journal of Intelligent Systems,* vol. 37, no. 8, pp. 4747–4771, 2022.

[57] D. Liu, Q. Su, Z. Yuan, and X. Zhang, "A fusion-domain color image watermarking based on Haar transform and image correction," *Expert Systems with Applications,* vol. 170, 114540, 2021.

[58] J. Wang, W. B. Wan, X. X. Li, J. De Sun, and H. X. Zhang, "Color image watermarking based on orientation diversity and color complexity," *Expert Systems with Applications,* vol. 140, 112868, 2020.

[59] F. Kahlessenane, A. Khaldi, R. Kafi, and S. Euschi, "A robust blind medical image watermarking approach for telemedicine applications," *Cluster Computing,* vol. 24, no. 3, pp. 2069–2082, 2021.

[60] H. S. Alshanbari, "Medical image watermarking for ownership & tamper detection," *Multimedia Tools and Applications,* vol. 80, no. 11, pp. 16549–16564, 2021.

[61] M. Celik, G. Sharma, E. Saber, and A. J. P. I. C. o. I. P. Tekalp, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 16, no. 3, 2006, pp. 354–362.

[62] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 16, no. 3, pp. 354–362, 2006.

[63] W.-L. Tai, C.-M. Yeh, and C.-C. Chang, "Reversible data hiding based on histogram modification of pixel differences," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 19, no. 6, pp. 906–910, 2009.

[64] S. Braci, C. Delpha, and R. Boyer, "How quantization based schemes can be used in image steganographic context," *Signal Processing: Image Communication,* vol. 26, no. 8–9, pp. 567–576, 2011.

[65] Y. Seki, H. Kobayashi, M. Fujiyoshi, and H. Kiya, "Quantization-based image steganography without data hiding position memorization," in *2005 IEEE International Symposium on Circuits and Systems*, 2005, pp. 4987–4990.

[66] Y. Zhang, D. Ye, J. Gan, Z. Li, and Q. Cheng, "An image steganography algorithm based on quantization index modulation resisting scaling attacks and statistical detection," *Computers, Materials & Continua,* vol. 56, no. 1, 2018.

[67] E. M. Jamel, "Image steganography based on wavelet transform and histogram modification," *Ibn AL-Haitham Journal For Pure and Applied Science,* vol. 33, no. 1, pp. 173–186, 2020.

[68] J. Marin and F. Y. Shih, "Reversible data hiding techniques using multiple scanning difference value histogram modification," *J. Inf. Hiding Multim. Signal Process.*, vol. 5, no. 3, pp. 451–460, 2014.

[69] Z. Zhao, H. Luo, Z.-M. Lu, and J.-S. Pan, "Reversible data hiding based on multilevel histogram modification and sequential recovery," *AEU-International Journal of Electronics and Communications,* vol. 65, no. 10, pp. 814–826, 2011.

[70] A. Devi and K. ShivaKumar, "Protection of confidential color image information based on reversible data hiding technique (PCCIRT)," in *Proc. 2015 International Conference on Computing and Network Communications (CoCoNet)*, 2015, pp. 742–747.

[71] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 13, no. 8, pp. 890–896, 2003.

[72] H. S. El-sayed, S. El-Zoghdy, and O. S. Faragallah, "Adaptive difference expansion-based reversible data hiding scheme for digital images," *Arabian Journal for Science and Engineering,* vol. 41, pp. 1091–1107, 2016.

[73] T.-C. Lu and C.-C. Chang, "Lossless nibbled data embedding scheme based on difference expansion," *Image and Vision Computing,* vol. 26, no. 5, pp. 632–638, 2008.

[74] B. Ou, X. Li, Y. Zhao, R. Ni, and Y.-Q. Shi, "Pairwise prediction-error expansion for efficient reversible data hiding," *IEEE Transactions on Image Processing,* vol. 22, no. 12, pp. 5010–5021, 2013.

[75] X. Li, J. Li, B. Li, and B. Yang, "High-fidelity reversible data hiding scheme based on pixel-value-ordering and prediction-error expansion," *Signal Processing,* vol. 93, no. 1, pp. 198–205, 2013.

[76] X. Wu and W. Sun, "High-capacity reversible data hiding in encrypted images by prediction error," *Signal Processing,* vol. 104, pp. 387–400, 2014.

[77] S. Li, L. Hu, C. Sun, L. Chi, T. Li, and H. Li, "A reversible data hiding algorithm based on prediction error with large amounts of data hiding in spatial domain," *IEEE Access,* vol. 8, pp. 214732–214741, 2020.

[78] H.-T. Wu, J. Huang, and Y.-Q. Shi, "A reversible data hiding method with contrast enhancement for medical images," *Journal of Visual Communication and Image Representation,* vol. 31, pp. 146–153, 2015.

[79] M. A. Wahed and H. Nyeem, "Reversible data hiding with interpolation and adaptive embedding," *Multimedia Tools and Applications,* vol. 78, pp. 10795–10819, 2019.

[80] A. Malik, G. Sikka, and H. K. Verma, "An image interpolation based reversible data hiding scheme using pixel value adjusting feature," *Multimedia Tools and Applications,* vol. 76, pp. 13025–13046, 2017.

[81] C.-C. Chang, T. D. Kieu, and Y.-C. Chou, "Reversible data hiding scheme using two steganographic images," in *Proc. TENCON 2007–2007 IEEE Region 10 Conference*, 2007, pp. 1–4.

[82] C.-C. Chang, Y.-C. Chou, and T. D. Kieu, "Information hiding in dual images with reversibility," in *Proc. 2009 Third International Conference on Multimedia and Ubiquitous Engineering*, 2009, pp. 145–152.

[83] T.-C. Lu, C.-Y. Tseng, and J.-H. Wu, "Dual imaging-based reversible hiding technique using LSB matching," *Signal Processing,* vol. 108, pp. 77–89, 2015.

[84] K.-H. Jung, "Dual image based reversible data hiding method using neighbouring pixel value differencing," *The Imaging Science Journal,* vol. 63, no. 7, pp. 398–407, 2015.

[85] T. Denemark, P. Bas, and J. Fridrich, "Natural steganography in JPEG compressed images," in *Electronic Imaging*, 2018.

[86] H.-W. Tseng and C.-C. Chang, "Steganography using JPEG-compressed images," in *Proc. The Fourth International Conference onComputer and Information Technology, 2004. CIT'04.*, 2004, pp. 12–17.

[87] N. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software," in *Information Hiding*, 1998.

[88] H. Kobayashi, Y. Noguchi, and H. Kiya, "A method of embedding binary data into JPEG bitstreams," *Systems and Computers in Japan,* vol. 33, no. 1, pp. 18–26, 2002.

[89] V. Sharma and S. Kumar, "A new approach to hide text in images using steganography," *International Journal of Advanced Research in Computer Science and Software Engineering,* vol. 3, no. 4, pp. 701–708, 2013.

[90] X. Zhang, "Reversible data hiding in encrypted image," *IEEE Signal Processing Letters,* vol. 18, no. 4, pp. 255–258, 2011.

[91] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE Transactions on Information Forensics and Security,* vol. 7, no. 2, pp. 826–832, 2011.

[92] M. Bartwal and R. Bharti, "Lossless and reversible data hiding in encrypted images with public key cryptography," in *RICE,* 2017.

[93] W. Hong, T.-S. Chen, and H.-Y. Wu, "An improved reversible data hiding in encrypted images using side match," *IEEE Signal Processing Letters,* vol. 19, no. 4, pp. 199–202, 2012.

[94] X. Liao and C. Shu, "Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels," *Journal of Visual Communication and Image Representation,* vol. 28, pp. 21–27, 2015.

[95] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted

images," *IEEE Transactions on Information Forensics and Security,* vol. 13, no. 7, pp. 1670–1681, 2018.

[96] Y. Puyang, Z. Yin, and Z. Qian, "Reversible data hiding in encrypted images with two-MSB prediction," in *2018 IEEE International Workshop on Information Forensics and Security (WIFS),* 2018, pp. 1–7.

[97] Z.-L. Liu and C.-M. Pun, "Reversible data-hiding in encrypted images by redundant space transfer," *Information Sciences,* vol. 433, pp. 188–203, 2018.

[98] X. Cao, L. Du, X. Wei, D. Meng, and X. Guo, "High capacity reversible data hiding in encrypted images by patch-level sparse representation," *IEEE Transactions on Cybernetics,* vol. 46, no. 5, pp. 1132–1143, 2015.

[99] W. Zhang, H. Wang, D. Hou, and N. Yu, "Reversible data hiding in encrypted images by reversible image transformation," *IEEE Transactions on Multimedia*, vol. 18, no. 8, pp. 1469–1479, 2016.

[100]Z. Qian and X. Zhang, "Reversible data hiding in encrypted images with distributed source encoding," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 26, no. 4, pp. 636–646, 2015.

[101]Z. Yin, Y. Xiang, and X. Zhang, "Reversible data hiding in encrypted images based on multi-MSB prediction and Huffman coding," *IEEE Transactions on Multimedia,* vol. 22, no. 4, pp. 874–884, 2019.

[102]L. Bao and Y. Zhou, "Image encryption: Generating visually meaningful encrypted images," *Information Sciences,* vol. 324, pp. 197–207, 2015.

[103]A. Kanso and M. Ghebleh, "An algorithm for encryption of secret images into meaningful images," *Optics and Lasers in Engineering,* vol. 90, pp. 196–208, 2017.

[104]L. D. Singh and K. M. Singh, "Visually meaningful multi-image encryption scheme," *Arabian Journal for Science and Engineering,* vol. 43, no. 12, pp. 7397–7407, 2018.

[105]P. Pan, Z. Wu, C. Yang, and B. Zhao, "Double-matrix decomposition image steganography scheme based on wavelet transform with multi-region coverage," *Entropy,* vol. 24, no. 2, p. 246, 2022.

[106]M. Ganavi, S. Prabhudeva, and H. K. NP, "An efficient image steganography scheme using bit-plane slicing with elliptic curve cryptography and wavelet transform," *International Journal of Computer Network and Information Security*, vol. 14, no. 4, p. 43, 2022.

[107]Z. Wang, M. Zhou, B. Liu, and T. Li, "Deep image steganography using transformer and recursive permutation," *Entropy*, vol. 24, no. 7, p. 878, 2022.

[108]A. A. Krishnan, C. S. Chandran, S. Kamal, and M. Supriya, "Spread spectrum based encrypted audio steganographic system with improved security," in *Proc. 2017 International Conference on Circuits, Controls, and Communications (CCUBE)*, 2017, pp. 109–114.

[109]K. Satish, T. Jayakar, C. Tobin, K. Madhavi, and K. Murali, "Chaos based spread spectrum image steganography," *IEEE Transactions on Consumer Electronics,* vol. 50, no. 2, pp. 587–590, 2004.

[110]P. Yadav and M. Dutta, "3-Level security based spread spectrum image steganography with enhanced peak signal to noise ratio," in *Proc. 2017 Fourth International Conference on Image Information Processing (ICIIP)*, 2017, pp. 1–5: IEEE.

[111]M. Islam, A. Roy, and R. H. Laskar, "SVM-based robust image watermarking technique in LWT domain using different sub-bands," *Neural Computing and Applications*, vol. 32, no. 5, pp. 1379–1403, 2020.

[112]C. Sharma, A. Bagga, B. K. Singh, and M. Shabaz, "A novel optimized graph-based transform watermarking technique to address security issues in real-time application," *Mathematical Problems in Engineering,* vol. 2021, 2021.

[113]Q. Su *et al.*, "New rapid and robust color image watermarking technique in spatial domain," *IEEE Access,* vol. 7, pp. 30398–30409, 2019.

[114]A. Anand, A. K. Singh, Z. Lv, and G. Bhatnagar, "Compression-then-encryption-based secure watermarking technique for smart healthcare system," *IEEE MultiMedia,* vol. 27, no. 4, pp. 133–143, 2020.

[115]S. Weng, Y. Shi, W. Hong, and Y. Yao, "Dynamic improved pixel value ordering reversible data hiding," *Information Sciences*, vol. 489, pp. 136–154, 2019.

[116]S. Kim, X. Qu, V. Sachnev, and H. J. Kim, "Skewed histogram shifting for reversible data hiding using a pair of extreme predictions," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 29, no. 11, pp. 3236–3246, 2018.

[117]R. A. Alotaibi and L. A. Elrefaei, "Text-image watermarking based on Integer Wavelet Transform (IWT) and Discrete Cosine Transform (DCT)," *Applied Computing and Informatics*, vol. 15, no. 2, pp. 191–202, 2019.

[118]M. Begum, J. Ferdush, and M. S. Uddin, "A Hybrid robust watermarking system based on discrete cosine transform, discrete wavelet transform, and singular value decomposition," *Journal of King Saud University-Computer and Information Sciences,* vol. 34, no. 8, pp. 5856–5867, 2022.

[119]V. Seenappa, N. C. Krishnappa, and P. K. Mallesh, "Hybrid compression and DNA sequence of hyper chaos system for medical image steganography," *International Journal of Intelligent Engineering & Systems,* vol. 15, no. 3, 2022.

[120]N. I. Yassin, "Data hiding technique for color images using pixel value differencing and chaotic map," *Jordanian Journal of Computers and Information Technology (JJCIT),* vol. 8, no. 03, 2022.

[121]S. Mukherjee, S. Mukhopadhyay, and S. Sarkar, "A shell-matrix-based image steganography technique for multimedia security and covert communication," *Innovations in Systems and Software Engineering,* pp. 1–16, 2022.

[122]D. R. I. M. Setiadi, "Improved payload capacity in LSB image steganography uses dilated hybrid edge detection," *Journal of King Saud University—Computer and Information Sciences*, pp. 104–114, 2022.

[123]Y. Ke, M.-Q. Zhang, J. Liu, T.-T. Su, and X.-Y. Yang, "Fully homomorphic encryption encapsulated difference expansion for reversible data hiding in encrypted domain," *IEEE Transactions on Circuits and Systems for Video Technology,* vol. 30, no. 8, pp. 2353–2365, 2020.

[124]Y. Fu, P. Kong, H. Yao, Z. Tang, and C. Qin, "Effective reversible data hiding in encrypted image with adaptive encoding strategy," *Information Sciences,* vol. 494, pp. 21–36, 2019.

[125]L. Xiong, Z. Xu, and Y.-Q. Shi, "An integer wavelet transform based scheme for reversible data hiding in encrypted images," *Multidimensional Systems and Signal Processing,* vol. 29, no. 3, pp. 1191–1202, 2018.

[126]R. Bhardwaj and A. Aggarwal, "An enhanced separable reversible and secure patient data hiding algorithm for telemedicine applications," *Expert Systems with Applications,* vol. 186, 115721, 2021.

[127]L.-P. Chi, C.-H. Wu, and H.-P. Chang, "Reversible data hiding in dual stegano-image using an improved center folding strategy," *Multimedia tools and Applications,* vol. 77, pp. 8785–8803, 2018.

[128]S. Agrawal and M. Kumar, "Mean value based reversible data hiding in encrypted images," *Optik*, vol. 130, pp. 922–934, 2017.

[129]L. Liu, L. Meng, W. Zheng, Y. Peng, and X. Wang, "A larger capacity data hiding scheme based on DNN," *Wireless Communications and Mobile Computing,* vol. 2022, 2022.

[130]W. He, G. Xiong, and Y. Wang, "Reversible data hiding based on multiple pairwise PEE and two-layer embedding," *Security and Communication Networks,* vol. 2022, 2022.

[131]J. Wang, N. Mao, X. Chen, J. Ni, C. Wang, and Y. Shi, "Multiple histograms based reversible data hiding by using FCM clustering," *Signal Processing,* vol. 159, pp. 193–203, 2019.

[132]R. Geetha and S. Geetha, "Embedding electronic patient information in clinical images: an improved and efficient reversible data hiding technique," *Multimedia Tools and Applications,* vol. 79, no. 19, pp. 12869–12890, 2020.

[133]R. Geetha and S. Geetha, "Improved reversible data embedding in medical images using I-IWT and pairwise pixel difference expansion," in *International Conference on Next Generation Computing Technologies,* 2017, pp. 601–611.

[134]S. A. Parah, F. Ahad, J. A. Sheikh, and G. M. Bhat, "Hiding clinical information in medical images: A new high capacity and reversible data hiding technique," *Journal of Biomedical Informatics,* vol. 66, pp. 214–230, 2017.

[135]L. Luo, Z. Chen, M. Chen, X. Zeng, and Z. Xiong, "Reversible image watermarking using interpolation technique," *IEEE Transactions on Information Forensics and Security,* vol. 5, no. 1, pp. 187–193, 2009.

[136] G. Xuan, Y. Q. Shi, P. Chai, X. Cui, Z. Ni, and X. Tong, "Optimum histogram pair based image lossless data embedding," in *International Workshop on Digital Watermarking*, 2007, pp. 264–278.

[137] C.-F. Lee and Y.-L. Huang, "An efficient image interpolation increasing payload in reversible data hiding," *Expert Systems with Applications*, vol. 39, no. 8, pp. 6712–6719, 2012.

[138] H. Wu, X. Li, Y. Zhao, and R. Ni, "Improved PPVO-based high-fidelity reversible data hiding," *Signal Processing*, vol. 167, 107264, 2020.

[139] M. Xiao, X. Li, B. Ma, X. Zhang, and Y. Zhao, "Efficient reversible data hiding for JPEG images with multiple histograms modification," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 7, pp. 2535–2546, 2020.

[140] F. T. Wedaj, S. Kim, H. J. Kim, and F. Huang, "Improved reversible data hiding in JPEG images based on new coefficient selection strategy," *EURASIP Journal on Image and Video Processing*, vol. 2017, no. 1, pp. 1–11, 2017.

[141] B. Ou and Y. Zhao, "High capacity reversible data hiding based on multiple histograms modification," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 8, pp. 2329–2342, 2019.

[142] D. Hou, H. Wang, W. Zhang, and N. Yu, "Reversible data hiding in JPEG image based on DCT frequency and block selection," *Signal Processing*, vol. 148, pp. 41–47, 2018.

[143] W. Qi, X. Li, T. Zhang, and Z. Guo, "Optimal reversible data hiding scheme based on multiple histograms modification," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 8, pp. 2300–2312, 2019.

[144] J. Hou, B. Ou, H. Tian, and Z. Qin, "Reversible data hiding based on multiple histograms modification and deep neural networks," *Signal Processing: Image Communication*, vol. 92, 116118, 2021.

[145] Q. Chang, X. Li, Y. Zhao, and R. Ni, "Adaptive pairwise prediction-error expansion and multiple histograms modification for reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 12, pp. 4850–4863, 2021.

[146] W. He, G. Xiong, and Y. Wang, "Reversible data hiding based on adaptive multiple histograms modification," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 3000–3012, 2021.

[147] M. Sahu, N. Padhy, S. S. Gantayat, and A. K. Sahu, "Local binary pattern-based reversible data hiding," *CAAI Transactions on Intelligence Technology*, 2022.

[148] R. Roselinkiruba, T. S. Sharmila, and J. J. Julina, "A novel pattern-based reversible data hiding technique for video steganography," 2022.

[149] S.-M. Jung, "Reversible data hiding technique applying triple encryption method," *The Journal of Korea Institute of Information, Electronics, and Communication Technology*, vol. 15, no. 1, pp. 36–44, 2022.

[150] Y. Yao, W. Zhang, N. Yu, and X. Zhao, "Defining embedding distortion for motion vector-based video steganography," *Multimedia tools and Applications*, vol. 74, pp. 11163–11186, 2015.

[151] Y. Jia, Z. Yin, X. Zhang, and Y. Luo, "Reversible data hiding based on reducing invalid shifting of pixels in histogram shifting," *Signal Processing*, vol. 163, pp. 238–246, 2019.

[152] M. Xiao, X. Li, Y. Zhao, B. Ma, and G. Guo, "A novel reversible data hiding scheme based on pixel-residual histogram," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 19, no. 1s, pp. 1–19, 2023.

[153] S. Gull, S. A. Parah, and K. Muhammad, "Reversible data hiding exploiting Huffman encoding with dual images for IoMT based healthcare," *Computer Communications*, vol. 163, pp. 134–149, 2020.

[154] B. Ou, X. Li, and J. Wang, "Improved PVO-based reversible data hiding: A new implementation based on multiple histograms modification," *Journal of Visual Communication and Image Representation*, vol. 38, pp. 328–339, 2016.

[155] F. Peng, X. Li, and B. Yang, "Improved PVO-based reversible data hiding," *Digital Signal Processing*, vol. 25, pp. 255–265, 2014.

[156] M. Abdul Wahed and H. Nyeem, "Reversible data hiding with dual pixel-value-ordering and minimum prediction error expansion," *Plos one*, vol. 17, no. 8, e0271507, 2022.

[157] R. Kumar and K.-H. Jung, "Enhanced pairwise IPVO-based reversible data hiding scheme using rhombus context," *Information Sciences*, vol. 536, pp. 101–119, 2020.

[158] W. He, K. Zhou, J. Cai, L. Wang, and G. Xiong, "Reversible data hiding using multi-pass pixel value ordering and prediction-error expansion," *Journal of Visual Communication and Image Representation*, vol. 49, pp. 351–360, 2017.

[159] T.-S. Nguyen, V.-T. Huynh, and P.-H. Vo, "A novel reversible data hiding algorithm based on enhanced reduced difference expansion," *Symmetry*, vol. 14, no. 8, p. 1726, 2022.

[160] R. Motomura, S. Imaizumi, and H. Kiya, "A reversible data-hiding method with prediction-error expansion in compressible encrypted images," *Applied Sciences*, vol. 12, no. 19, p. 9418, 2022.

[161] R. Abbasi *et al.*, "Generalized PVO-based dynamic block reversible data hiding for secure transmission using firefly algorithm," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, p. e3680, 2022.

[162] S. Rahman, J. Uddin, H. U. Khan, H. Hussain, A. A. Khan, and M. Zakarya, "A novel steganography technique for digital images using the least significant bit substitution method," *IEEE Access*, 2022.

[163] P. Rupanshi, "Vandana, audio steganography by direct sequence spread spectrum," *International Journal of Computer Trends & Technology*, vol. 13, no. 2, 2014.

[164] M. R. Khosravi and S. Samadi, "Efficient payload communications for IoT-enabled ViSAR vehicles using discrete cosine transform-based quasi-sparse bit injection," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–10, 2019.

[165] E. H. Rachmawanto, C. A. Sari, and N. Rijati, "Imperceptible and secure image watermarking using DCT and random spread technique," *TELKOMNIKA (Telecommunication Computing Electronics and Control)*, vol. 17, no. 4, pp. 1750–1757, 2019.

[166] B. Ou, X. Li, W. Zhang, and Y. Zhao, "Improving pairwise PEE via hybrid-dimensional histogram generation and adaptive mapping selection," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 29, no. 7, pp. 2176–2190, 2018.

[167] W. He and Z. Cai, "An insight into pixel value ordering prediction-based prediction-error expansion," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 3859–3871, 2020.

[168] W. He, Z. Cai, and Y. Wang, "Flexible spatial location-based PVO predictor for high-fidelity reversible data hiding," *Information Sciences*, vol. 520, pp. 431–444, 2020.

[169] X. Wang, C.-C. Chang, and C.-C. Lin, "Reversible data hiding in encrypted images with block-based adaptive MSB encoding," *Information Sciences*, vol. 567, pp. 375–394, 2021.

[170] M. S. Subhedar, "Cover selection technique for secure transform domain image steganography," *Iran Journal of Computer Science*, vol. 4, no. 4, pp. 241–252, 2021.