A Survey of Reversible Data Hiding in Encrypted Images

Ghadeer Asiri, Atef Masmoudi
Department of Computer Science
King Khalid University, Abha, Saudi Arabia

***Abstract*—The creation and application of multimedia has undergone a revolution in the last several years. This is a result of the rise in internet-based communications, which involves the exchange of digital data in the forms of text files, audio files, video files, and image files. For this reason, multimedia has emerged as a vital aspect of people's everyday existence. Information security is crucial since there are several threats that target multimedia integrity, confidentiality, and authentication.Multimedia data needs to be safeguarded, perhaps using encryption, in order to solve these numerous issues. Reversible data hiding in encrypted pictures (RDHEI) is investigate in this survey. (RDHEI) process, which functions by adding extra data to a picture, has surfaced. Employers and academics alike are becoming more interested in and focused on the RDHEI due to its vast range of applications. The purpose of this review is to introduce the various RDHEI schemes, identify the most important RDHEI techniques with varying embedding rates, and then examine the applications and future prospects of RDHEI. The main characteristics of each representative RDHEI Technique taken into consideration in this survey are enumerated in a comparison table.**

***Keywords*—Reversible data hiding; encrypted image**

I. Introduction

Within the maze of contemporary digital communication, the necessity to protect confidential data frequently clashes with the requirement to hide more data for a variety of reasons. This conflict is most evident in the transfer and storage of images, where data concealing techniques allow for the implantation of additional information or clandestine communication, but encryption guarantees confidentiality. Up to the introduction of a novel idea, Reversible Data Hiding in Encrypted Images, reconciling these seemingly incompatible goals has been an enormous difficulty.

"Reversible Data Hiding in Encrypted Images," the title itself, reflects a revolutionary strategy that promises to completely change the way safe data is transmitted and stored. It refers to the merging of two fundamental tenets of contemporary information security: data concealing, the craft of covert communication, and encryption, the cornerstone of confidentiality. However, it offers a paradigm-shifting synthesis that goes beyond conventional trade-offs and constraints, going beyond simple juxtaposition.

Fundamentally, reversible data concealing in encrypted images is significant because it may balance the requirements of information concealment and data security. This synthesis offers promise in an era beset by cyber threats and privacy breaches, where the secrecy and integrity of digital data are continuously under attack.It offers a tantalizing prospect: the capacity to embed extra data into photos and encrypt them to protect their privacy without jeopardizing the security of the encryption scheme or the integrity of the original image.

This title serves a multitude of purposes. It captures an innovative idea with significant ramifications for a wide range of fields, including multimedia applications, cloud computing, digital forensics, and secure communication. It promises to open up new possibilities by smoothly integrating reversible data concealing into the encrypted image domain. These applications include digital watermarking, covert communication, safe transmission of sensitive data, and authentication.

The benefits of reversible data hiding in encrypted images are as multifaceted as they are profound. Foremost among them is the enhancement of data security. By leveraging encryption to safeguard the confidentiality of image content and reversible data hiding to conceal auxiliary information, this technique offers a robust defense against eavesdropping, interception, and unauthorized access. It ensures that sensitive information remains shrouded in a cloak of encryption, impervious to prying eyes, while auxiliary data is clandestinely embedded within the encrypted image, hidden in plain sight.

Furthermore, encrypted photos with reversible data concealing offer unmatched adaptability. This technique works directly on encrypted data, in contrast to typical data concealing methods that frequently need decryption before embedding or extraction. This allows for reversible embedding and extraction operations without jeopardizing the security or integrity of the encryption scheme. This adaptability enables users to maintain the security and integrity of the original image while embedding extra data inside encrypted images, transmitting them safely, and extracting the concealed information at the recipient's end.

Furthermore, resource efficiency is inherent to reversible data hiding in encrypted images. It is ideal for resource-constrained situations like mobile devices, embedded systems, and cloud computing platforms because it minimizes the requirement for repeated decryption and encryption steps, which lowers computational overhead and conserves system resources. This effectiveness guarantees that the advantages of reversible data masking can be experienced in a wide range of applications, ranging from multimedia communication and medical imaging to secure messaging and picture sharing.

To summarize, the concept of reversible data concealed behind encrypted images is a revolutionary idea that breaks through conventional limitations and harmonizes seemingly incompatible demands. It provides a powerful synthesis that

improves data security, permits covert communication, and opens up new avenues for the safe transmission and storage of sensitive data by blending encryption and data hiding within the picture domain.

This survey is organized as follows: Section II provides the necessary theoretical foundations and key concepts of RDHEI. Section III explores various RDHEI schemes, categorizing and discussing existing methods and their respective strengths and weaknesses. Section IV delves into the practical applications of RDHEI in various domains, illustrating its real-world benefits and impact. Finally, Section V summarizes the key findings and discusses future prospects.

II. Background

Reversible Data Hiding in Encrypted Images (RDHEI) [1] is a sophisticated method that perfectly recovers the original image content while enabling the concealment of auxiliary data within encrypted image data streams. It does this by combining the concepts of reversible data hiding and encryption. With this novel method, the inherent conflict between information hiding and data security is resolved by allowing extra data to be embedded into encrypted images without jeopardizing the security or integrity of the encryption process.

RDH-EI works as follows:

- Encryption [2]: Using cryptographic techniques and keys, the original image data is encrypted to start the process. Without the decryption key, encryption jumbles the picture data, making it impossible for anyone to understand. By doing this, the image content is kept private and shielded from unwanted access or interception.
- Reversible Data Hiding [3] [1]: After encryption, supplementary data is embedded into the encrypted image using reversible data hiding techniques. Reversible data hiding guarantees that, following the retrieval of concealed information, the original image may be precisely recreated, in contrast to irreversible approaches. The security and integrity of the encryption system are maintained by this embedding procedure, which works directly on the encrypted picture data.
- Transmission and Concealment [4] [5]: The composite data stream that results from embedding the auxiliary data within the encrypted image can be safely sent to the designated destination. Even for those who intercept the communication, the hidden information is invisible within the encrypted image.
- Decryption and extraction [6]: To get the original image data, the encrypted image is first decoded at the recipient's end using the relevant decryption key. Reversible data concealing techniques allow the embedded auxiliary data to be recovered from the decrypted image simultaneously, without sacrificing quality or integrity. The original image content is maintained while the hidden information is revealed through this extraction method.

Additionally, RDHEI has improved security. By using encryption to safeguard the privacy of the original image content, RDHEI makes sure that private information is safe even when more data is inserted into the encrypted image. additionally Reversibility caused by Because data hiding is reversible, the original image may be precisely recreated once the hidden information has been extracted, maintaining the image's fidelity and quality.

As RDHEI supports reversible embedding and extraction processes, it can be used in a variety of applications where maintaining the authenticity and integrity of visual data is essential. RDHEI minimizes computational overhead and conserves system resources by reducing the need for repeated encryption and decryption operations. This makes it appropriate for resource-constrained applications like embedded systems and mobile devices.

Additionally, as RDHEI combines data concealing with encryption, it improves security, but if not used properly, it might create new vulnerabilities. It is important to take precautions against potential hazards like algorithmic or cryptographic defects. additionally Reversible data concealing may need more processing overhead when used with encryption, especially when embedding and extracting data. This might affect how well high-throughput applications or environments with limited resources perform.

Fig. 1 depicts the RDHEI path [7] [8], as follows:

- The content owner: The person or organization who is in possession of the original image data and wishes to send it safely while hiding additional information is known as the content owner. Before transmission, the content owner encrypts the picture data and embeds the auxiliary data to start the RDH-EI procedure.
- The data hider: Using reversible data hiding techniques, the data hider is in charge of embedding auxiliary data into the encrypted image data stream. By using a data hider, the encrypted image's hidden information is kept undetectable and can be recovered by the recipient without compromising its integrity.
- The receiver: The encrypted picture data with the hidden auxiliary information is meant for the receiver. The recipient encrypts the picture and then uses the right decryption key to get the original image data. In order to disclose the hidden information, the receiver simultaneously extracts the encoded auxiliary data utilizing reversible data hiding techniques.

III. Different Schemes of RDHEI

The figure labeled as Fig. 2 illustrates the existence of distinct categories of RDHEI, first one is reserving a room before encryption and the second one is vacating the room after encryption third Secret Sharing (RRB) (VRAE) (SS). Vacating the Room After Encryption (VRAE) is a concept that, in reversible data hiding strategies, is complementary to Reserving a Room Before Encryption (RRBE). After the encryption procedure is finished, VRAE entails removing or clearing the space inside the encrypted image that was previously set aside for inserting auxiliary information. By keeping the encrypted image safe and clear of any evidence of the embedded data, VRAE helps to reduce the possibility of unwanted access or detection. The following steps are commonly included in

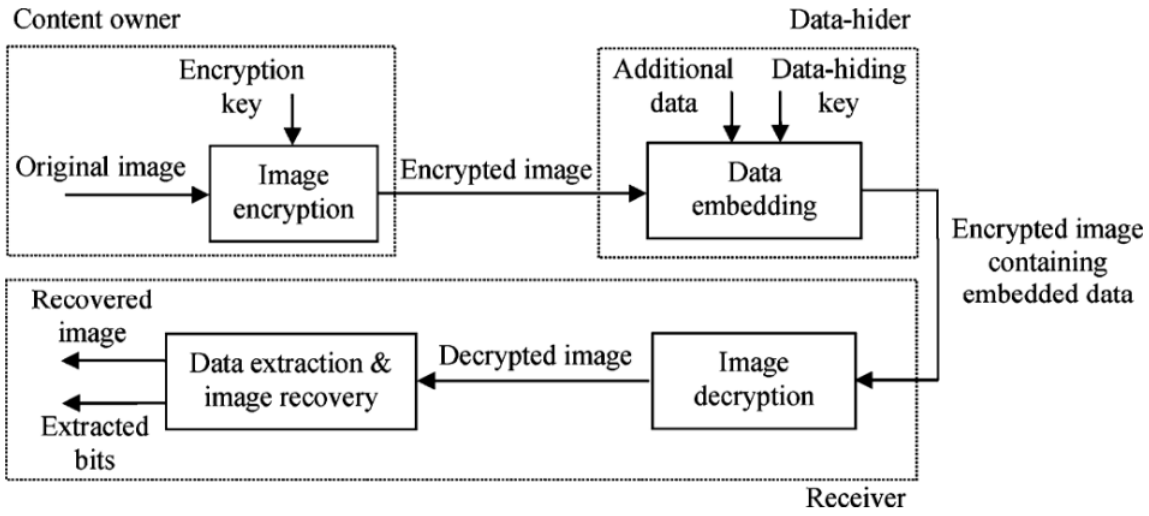

Fig. 1. The general framework for (RDHEI).

the VRAE process: Encryption: To preserve its confidentiality and integrity, the image is first encrypted using cryptographic methods. A piece of the image's data space might be set aside during this phase so that supplementary information can be included utilizing RRBE techniques. Data Hiding and Clearing: Following encryption, the encrypted image has any remaining evidence of the encoded auxiliary data erased or cleared. In doing so, the area that was set aside for embedding auxiliary information is essentially cleared out by overwriting it with random or null data. In order to prevent unwanted parties from accessing or recovering the embedded information, the cleaning process makes sure that no traces of the hidden data are left inside the encrypted image.

Safe Storage or Transmission: The encrypted image can be safely kept or transmitted without running the danger of revealing the secret data once it has been released from encryption. The lack of residual traces guarantees the security of the encrypted image against steganalysis and other detection methods, protecting the integrity and secrecy of the contained auxiliary data. Reversible data hiding techniques, such as Vacating the Room After Encryption (VRAE), improve the secrecy and integrity of sensitive data by guaranteeing that encrypted images stay safe and devoid of any evidence of hidden data. This method is appropriate for applications needing strong data concealment and private communication since it adds another degree of security and privacy protection [9] [10] [11] [12] [13].

One idea utilized in reversible data hiding techniques, especially in the context of image encryption, is Reserving a Room Before Encryption (RRBE). Prior to the encryption procedure, a portion of the image's data capacity is allocated for the embedding of auxiliary information. Ensuring that enough space is set aside inside the image to embed more data while maintaining the security and integrity of the original image content is the aim of RRBE. The following steps are commonly included in the RRBE process:

Estimation of Capacity: Prior to encryption, the image's potential to include supplementary data is calculated. This entails examining the image's properties, like its size, color depth, and pixel distribution, to ascertain the most auxiliary data that can be incorporated without appreciably lowering image quality or jeopardizing encryption security. Room Reservation: After estimating the capacity, a specific amount of the image's data space is set aside for the embedding of supplemental data. This reserved space is usually found in portions of the image, like smooth areas or areas with little texture details, that are less perceptually relevant or have lower entropy. The space that has been set aside guarantees that there is enough room to insert more data without creating observable artifacts or compromising the encryption procedure. Data Embedding: The auxiliary data is inserted into the image's designated space after the room has been booked. A variety of data concealing strategies can be employed to hide the auxiliary information with the least amount of negative effects on image quality, including frequency domain embedding, histogram shifting, and least significant bit (LSB) substitution. To guarantee that, following encryption, the original image can be precisely recreated, the embedding procedure needs to be reversible. Encryption: To safeguard the image's secrecy and integrity after the auxiliary data is included, cryptographic algorithms are used to encrypt it. Encryption protects the embedded auxiliary information from exposure or tampering by preventing unauthorized parties from accessing or manipulating the image's content. Reversible data hiding and encryption techniques can be seamlessly integrated with RRBE by booking a room in advance of encryption. This guarantees that concealed data can be inserted inside the image while maintaining its security and integrity. With the use of this technique, private information can be discreetly hidden inside encrypted photos, enabling safe communication, digital watermarking, and content authentication across a range of applications [8] [14] [11].

A category for secret sharing is also included. Secret sharing (SS)-based techniques for reverse data hiding in encrypted photos make use of these concepts to embed extra

data into encrypted images while maintaining their integrity and security. A cryptography technique called "secret sharing" splits a secret into several shares that are then given to a group of participants. While each of these shares by itself doesn't provide any information about the original secret, they can be combined to piece it together. When it comes to reversible data hiding in encrypted photos, SS-based techniques guarantee that only authorized persons having access to the necessary shares may retrieve the concealed data.

Secret sharing entails the following crucial elements and procedures: Creating the secret that needs to be shared with the parties is the first stage in the secret sharing process. A cryptographic key, private information, or any other confidential material that needs to be kept safe could be this secret. After the secret is created, an algorithm for secret sharing divides it into several shares. Each share is generated in a way that prevents any information about the original secret from being revealed by an individual share. Shamir's Secret Sharing Scheme (SSSS), threshold secret sharing, and visual cryptography are examples of common secret sharing techniques.

The authorized parties receive the shares once they are generated. A distinct portion is given to each party, and the distribution procedure makes sure that no one party has access to the full secret. Securing this distribution can be accomplished through a variety of protocols or communication methods.

A set number of shares must be obtained from the approved parties in order to recreate the original secret. The original secret data can be recovered by combining the shares using the secret reconstruction technique after the threshold is reached. By combining a sufficient number of shares, the secret will remain confidential and only be accessible through this rebuilding process.

Various security measures are put in place during the secret sharing procedure to guard the shares and secret against illegal access or interception. To avoid tampering or eavesdropping, this may involve secure communication lines, authentication procedures, and encryption of information.

For reverse data concealing in encrypted photos, there are a number of Secret Sharing-based techniques available, each with a unique methodology and set of fundamental ideas.

Typical techniques include the following:

1. Shamir's Secret Sharing Scheme (SSSS): Shamir's Secret Sharing Scheme is a well-known technique that uses polynomial interpolation to split a secret into several shares. To rebuild the original secret using polynomial interpolation, a minimum threshold of shares is needed. Each share is a point on a polynomial curve. SSSS can be modified to separate the concealed data into shares in the context of reversible data hiding in encrypted images. The shares are then integrated into the encrypted image through the use of methods like LSB replacement or pixel alteration.

2. Visual Cryptography (VC): This is a cryptographic method in which an image is split up into several shares, each of which keeps the original image's contents hidden. The original image is seen when the shares are stacked or layered. When reversible data hiding is involved, VC can be used to split the concealed data into shares that are subsequently included into the encrypted image by the use of dithering or halftoning, among other approaches. By merging the shares that were received from the decrypted image, the original data can be retrieved.

3. A variation of Shamir's Secret Sharing Scheme, Threshold Secret Sharing necessitates a minimum threshold of shares in order to reconstruct the original secret. This threshold adds a layer of security against unwanted access by guaranteeing that a specific quantity of shares must be present in order to recover the hidden data. Threshold secret sharing can be used to split up concealed data into shares in the context of reversible data hiding in encrypted images. The shares are then embedded into the encrypted image using techniques specific to the current encryption scheme.

4. Block-Based Secret Sharing: In this method, the secret data is separated into blocks or segments, each of which is embedded into the encrypted image and encrypted separately. By distributing the hidden data throughout the entire image, this method makes the data more resistant to detection and attacks. Block-based secret sharing can be used to separate the concealed data into blocks for reversible data hiding in encrypted images. The blocks are then encrypted and inserted into the encrypted image using methods like block modulation or LSB substitution.

All things considered, secret sharing is an effective cryptographic mechanism that permits the safe reconstruction and distribution of secrets across several parties while guaranteeing access control, confidentiality, and integrity. [15] [16] [17] [18]

A. VRAE

1) Adaptive MSB (most significant bit) Prediction: Using adaptive prediction to efficiently free up embedding space within pixel blocks, the Adaptive MSB Prediction (AMP) approach enhances the embedding capacity in reversible data concealing in encrypted images. The approach adjusts its prediction strategy based on the variations between the pixels by utilizing the upper-left pixel inside a block to forecast the other pixels. The block's available embedding room can be well utilized thanks to this adaptive prediction. When the discrepancies between the pixels are minor, the approach maintains the Least Significant Bits (LSBs) of the anticipated pixels. By preserving the LSBs, space is made available for the embedding of extra data while preserving the quality of the image. More data can be embedded without significantly distorting the cover image when the approach vacates the embedding room within the block when the pixel differences are modest. additionally The technique maximizes the capacity for data hiding within the encrypted image by vacating the embedding room based on adaptive prediction and LSB preservation, therefore maintaining a high capacity. There are three primary phases to the technique: To guarantee privacy and preserve the integrity of the image, the owner first encrypts the cover image using an encryption key.

There are two ways to do this with encryption:

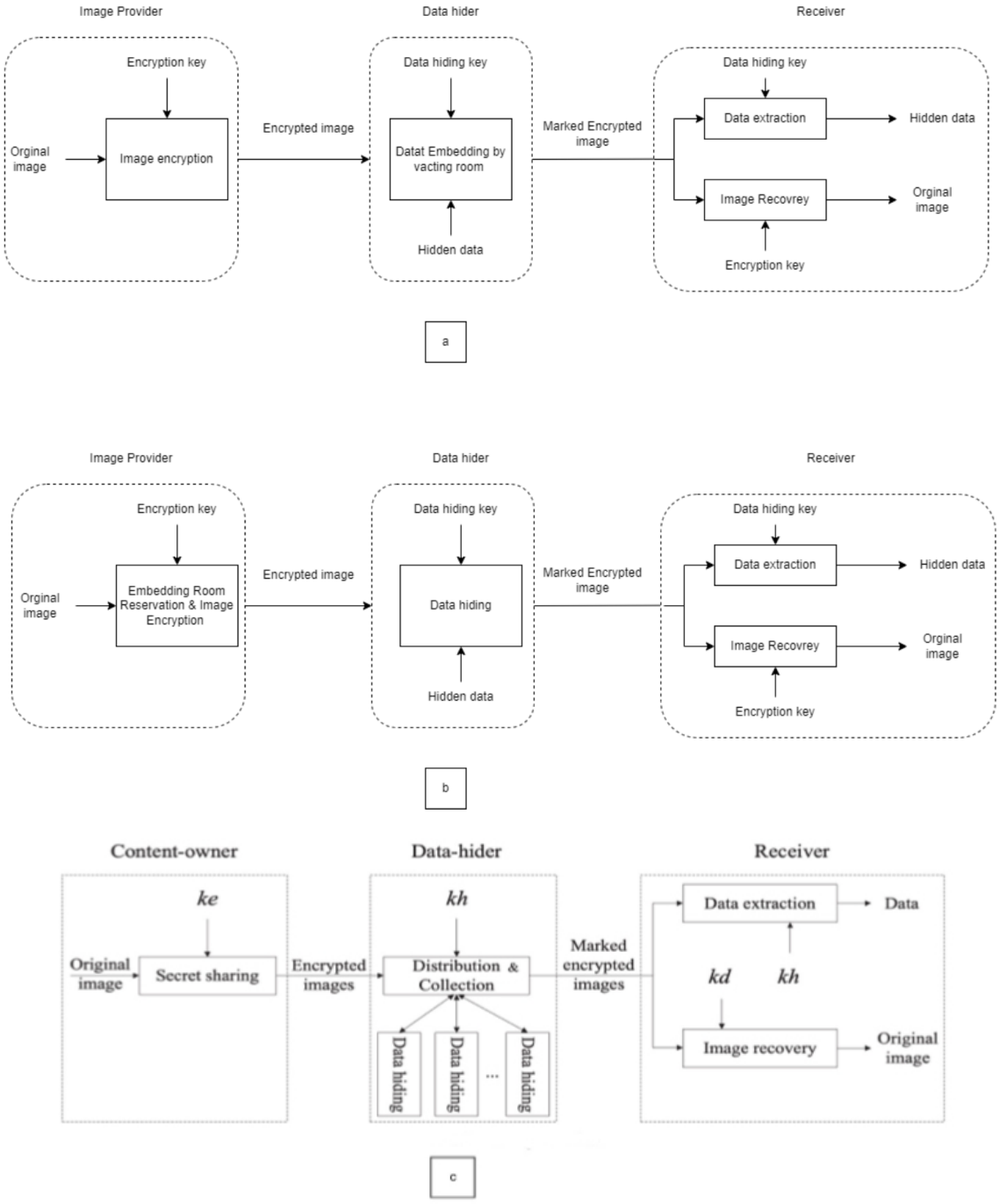

Fig. 2. Types of RDHEI: (a) vacating room after encryption (VRAE), (b) reserving room before encryption (RRBE), and (c) Secret Sharing (SS).

1-block-level encryption The procedure of stream encryption on block level :

Involves dividing the original image into non-overlapping blocks.
Calculates the average pixel value for each block and computes the difference between each pixel and the average.
Based on a predefined threshold, pixels are modified to enhance privacy protection.

2-block permutation:

After the first phase of encryption, the cover image is divided into 2x2 blocks again.
To create the final encrypted image, each block is permuted using the encryption key.
This process ensures that no image content can be revealed through complexity analysis, enhancing privacy protection.

and also Additional data is embedded into the encrypted image

by a **data hider** using a data-hiding key. Through these steps:

- Step 1: Image partition.
- Step 2: Block selection using AMP.
- Step 3: Block rearrangement.
- Step 4:Data encryption.
- Step 5: Data hiding.

for **Data Recovery and Image Extraction** Depending on whether the decryption key and the data-hiding key are available, the recipient can either get the image content or extract concealed data. In order to extract data and retrieve the tagged image, the decoding method splits the image into non-overlapping, 2x2 blocks.

Finally technique combines encryption, data hiding, and reversible data extraction to enable high-capacity data hiding in encrypted images while maintaining image quality and privacy [19].

2) Pixel prediction and entropy encoding: Using the adjacency prediction and median edge detector (MED), this approach first generates the prediction-error histogram (PEH) of the chosen cover. This is done by use of the ERGA (Efficient Embedding Room Generation Algorithm). The pixels are separated into joint and independent encoding pixels in this step. Following self-embedding and arithmetic coding compression of the prediction errors, a sizable embedding room for reversible data hiding in encrypted pictures (RDHEI) is produced. The approach creates a huge embedding room for data hiding by first using pixel prediction to generate prediction mistakes, which are then compressed using entropy encoding. In both the vacating room before encryption (VRBE) and vacating room after encryption (VRAE) scenarios, this method enables high-capacity reversible data concealing.

Encryption process: *In VRBE-based RDHEI scheme,* Using self-embedding, the picture owner removes the embedding room from the original image and creates the encrypted image with the removed room. With a given encryption key, the owner uses a stream cipher to create a pseudo-random sequence. The picture is encrypted with the room cleared out by employing a stream cipher and a pseudo-random sequence.

In the VRAE-based RDHEI scheme, To maintain spatial redundancy, the cover picture is encrypted using an enhanced block modulation and permutation encryption algorithm. All things considered, the encryption procedure in both schemes makes sure that, both before and after data concealing by unauthorized users, the original image can scarcely be found from the encrypted version. then,The *data hider* finds the room that has been vacated for embedding in the encrypted image, then embeds the encrypted extra data into the encrypted image together with the room that has been vacated. The data hider embeds the encrypted additional data into the encrypted image by using the efficient embedding room generation algorithm (ERGA) on the encrypted blocks to free up space.

Data Extraction: Inside the designated encrypted image, the authorized receiver finds the embedding chamber first. Then, using the relevant keys (such as the data hiding key), the recipient extracts the embedded data from the indicated encrypted image. To acquire the original supplementary data without errors, the extracted data is decrypted.

image Recovery: The original cover picture can be recovered without loss from the designated encrypted image if the recipient possesses the required keys, such as encryption keys. To recover the original image error-free, the designated encrypted image must be decrypted as part of the image recovery procedure [20].

B. RRBE

1) Huffman coding and differences of high nibbles of pixels: **Huffman coding method** is employed to encode the variations in high pixel nibbles in order to accomplish excellent data hiding, efficient compression, and error-free data retrieval. It also enhances the dependability and efficiency of reversible data hiding in encrypted images.

Here's an overview of how the method works:

High bite values and spatial correlation: In images, adjacent pixels frequently have comparable high values because of spatial correlation. Utilizing this association, the technique effectively compresses the four most significant bit (MSB) levels. Where each pixel's high value is a 4-bit value, the difference is computed. The approach looks at the values close to zero and computes the differences between the high points of adjacent pixels. To encode, these discrepancies are added together. Next, Huffman coding is applied, which is achieved by first figuring out how the disparities between the high points are distributed. Then, Huffman coding is used to encode these differences. Effective data compression is made possible by the variable-length prefix coding method known as Huffman coding, which translates shorter codes to more frequent codes. The compression approach compresses the image's four high MSB levels using encrypted versions that are produced by Huffman coding. There is more room in the MSB levels to conceal data without sacrificing information when the original high segments are swapped out for compressed alternatives.

The encryption process includes the following steps:

Make room for data hiding by first removing any unnecessary space from the plain text picture that the data owner wants to use for data concealing. Using Huffman coding, the four most significant bit (MSB) levels are compressed in this stage to provide more space for the data to be embedded while preserving image quality. Next, an encryption key is used to encrypt the photos using stream encryption. Stream encryption is a homomorphic encryption method that is commonly used to encrypt real-time data streams. It encrypts data either bit by bit or byte by byte. To safeguard data security and preserve its content, the image in this instance is encrypted. Information about the room available to conceal the data at least significant bit (LSB) levels is contained in the encoded image. In order to incorporate sensitive data within the picture without distorting or losing any information, the data hider needs these information.

The data is embedded as the **data hiding tool** receives the encrypted image and extracts the capacity information to determine the space available for data hiding at LSB levels. Different schemes can be used, e.g

- Bit substitution
- (7,4) Hamming code-based Matrix Encoding
- Bit flipping

to include confidential data in the image based on specific requirements.

Confidential data is extracted as follows:

Bit substitution: The receiving device can accomplish this by using a data masking switch. Straight from the encrypted image's data concealing chamber, extract embedded private data. Matrix encoding: The data is extracted by the recipient using a steganographic key. the data hiding chamber's bits and split them up into 7-bit codes. Bit flipping: To decode the bits, the recipient utilizes the encryption key. After tagging the encrypted image, the original embedded LSBs from the MSB aircraft are retrieved. After then, the recipient hides the data using the key. to take the bits from the data hiding room that are embedded with secret data and compare them to the original LSBs.The receiver will extract secret bit 0 if the extracted bit matches the matching original bit; if not, secret bit 1 will be extracted. Information Instead of doing the extraction from the encrypted domain, it should be done in the decrypted domain. This is not the same as matrix encoding or bit substitution. Image recovery also occurs when the designated encrypted image is immediately created as a decrypted image by the receiving device using the encryption key. Next, the four high MSB levels of the decoded image are directly used to retrieve the original embedded LSBs, high compressed differences, Huffman code, and bitstream significance bit. The four high MSB levels of the original image are recovered after the high-resolution compressed versions are decoded in accordance with the Huffman code [10].

2) Adaptive prediction-error labeling: Based on adaptive prediction-error labeling (APL), the technique for reversible data hiding in encrypted images uses two methods: Pessimistic APL (PAPL) and Optimistic APL (OAPL). The suggested methods include a framework with multiple stages, such as image encryption, data concealment, APL labeling, data extraction, and image recovery.

During the APL labeling phase, the original image's prediction errors (PEs) are computed and the high-frequency and low-frequency PEs are adaptively labeled using an APL method. The labeling process entails dividing the PEs into high- and low-frequency categories and labeling them with normal labels (NL) and special labels (SL). The APL approach is used to produce the labels and ignored bits.

the *image encryption process in PAPL* entails bitstream encryption, standard encryption, self-embedding, and assessment of the threshold value's influence on the reserved room. By following these procedures, the encrypted image is guaranteed to be secure and reversible, enabling the full and independent recovery of the original image as well as additional data that is dependent on the secret key.

the *image encryption process in OAPL* entails reordering the bitstream, concatenating unshuffled labels and auxiliary data, and then encrypting the rearranged image using stream encryption.Not a Process of Self-Embedding. The original image and any additional data based on the secret key can be fully and independently recovered using this method, which guarantees the security and integrity of the encrypted image.

and The process of *data hiding* occurs in a way that allows the data hider to get the first unencrypted location marker that is, the pixel coordinate from the start of the sequential bit stream where the reserved room starts. After the initial position, bits can be replaced to use the reserved room for modulation.

1. In PAPL, Additional data encrypted by the data hiding key may be included in the picture encrypted with the random labels, i.e., by multiple LSB replacement, depending on the original location label and the length of each random label.

2. In OAPL, Further encoded data can be added to the encoded image by multiple LSB (equivalent to bit-level rearrangement) or pixel substitution (pixel rearrangement) with the initial location tag.

Finally, a distinctive encrypted image can be easily generated.

Data Extraction: If the recipient has the data hiding key , the encrypted additional data can be extracted perfectly. *In PAPL,* The location of the reserved room may be determined from the initial location flag and the labels without inverse shuffling, which makes it possible to retrieve the encrypted additional data. *In OAPL,* A location marker alone can be used to locate the reserved room, and the extracted encrypted additional data can be decrypted to reveal the original additional data.

Image Recovery: Error-free recovery of the original image is possible if the receiver possesses the encryption key. Using the encryption key, the concatenated bitstream can be extracted before the first location, allowing for the retrieval of the original auxiliary information and unshuffled labels. Both the original image and any extra data can be fully recovered at the same time if the recipient possesses both the data hiding key and the encryption key [21].

3) Reserving room before encryption: The technique used is reversible data hiding in encrypted images by reserving room before encryption (RRBE). The technique involves a general framework that allows for the adoption of different predictors to achieve high embedding capacity in encrypted images.

This is done through:

Preprocessing: The following steps are involved in the preprocessing stage of the reversible data concealing in encrypted images by reserving room before encryption (RRBE) technique: The difference between the expected and actual pixel values in the original image is represented by prediction-errors (PEs), which are computed using various causal predictors. and thereafter The obtained prediction-errors are separated into chunks that do not overlap. There are a number of prediction errors in every block. and a label is allocated for every block of prediction-errors according to the highest prediction-error that occurs in that block. The amount of data that may be embedded in a block is determined by its embedding capacity, which is indicated by this label. In order to create space for data to be embedded in the encrypted image, preprocessing is essential. In order to obtain high embedding capacity, it enables

the effective use of spatial correlation and the selection of the best predictor available.

Then, *the encryption process,* which includes several steps and based on RRBE technology,does the following:

1. Content Encryption: The original image is encrypted using a stream cipher and an input secret key.

2. Secret Data Encryption: The secret data that has to be embedded is encrypted using a standard encryption method and an input secret key.When employing the reversible data hiding in encrypted images by reserving room before encryption (RRBE) technique, the data hider is crucial to embedding secret data into the encrypted image and ensuring the security and integrity of the process.

The *data hider's* responsibilities include:

1. Preprocessing: The preprocessing stage is carried out by the data hider.

2. Secret Data Encryption: Using an input secret key and a normal encryption method, the data hider encrypts the secret data. By doing this, the secret data is safeguarded before being incorporated into the encrypted picture.

3. Embedding Secret Data: The data hider safely and precisely embeds the encrypted secret data into the designated encrypted image by using the prediction-errors and labels acquired during the preprocessing step.

4. Information Sharing: To help with the extraction and recovery process at the receiver end, the data hider occasionally shares information with the content owner, such as the labels and starting block address. In general, the data hider's job is to include the secret data into the encrypted image while making sure that the hidden data can be recovered without distortion and that the original image can be correctly recreated.

The process of extracting data and recovering the original image involves the following steps:

1. Extracting Labels: The labels included in the tagged encrypted image are extracted at the recipient's end. The embedding capacity of each block in the encrypted image is ascertained using these labels.

2. Extracting Secret Data: The embedded secret data is recovered from the tagged encrypted image using the extracted labels. To guarantee error-free data extraction, the labels direct the extraction procedure.

3. Recovering the Original Image: Using the content-owner key and the retrieved data, the original image is rebuilt. The following steps are involved in the process: a. Decryption: The original encrypted image is obtained by decrypting the indicated encrypted image with the content-owner key. b. Reconstructing Pixels: Using the recovered data and the information kept during the embedding process, the original pixels are recreated. This makes it possible to rebuild the original image without any loss [14].

C. SS

1) Secret sharing and hybrid: In order to increase the security of the original image, this approach first performs iterative encryption. Afterwards, the encrypted image is dispersed across several data hiders via block-based Chinese Remainder Theorem-based Secret Sharing (CRTSS). Reversible data hiding (RDH) with hybrid coding can be carried out individually by each data hider. This makes it possible to incorporate sensitive information into the encrypted sharing. Finally, provided that enough uncorrupted marked shares are found, the original image can be reconstructed without any loss in quality using CRTSS. Data security and the original image's lossless recovery are guaranteed by this procedure.

The *encryption process* is carried out using an iterative encryption technique that combines block permutation with block-based modulation. The objective of this procedure is to reposition image blocks in a way that maintains spatial correlation and increases security, while also modifying the pixel values within each block. More redundancy for data embedding is produced by the iterative encryption, which creates an encrypted image with retained spatial correlations. To prevent cryptanalysis, the encryption key is made up of dynamically created parameters, guaranteeing the security of the encrypted image.

then the *data hider* operates by employing hybrid coding to independently carry out reversible data hiding (RDH) on the encrypted shares that are obtained from the content owner. The data hider embeds secret data into the encrypted shares using the hybrid coding technique. By using this method, the original image's security and integrity are preserved while the data hider can participate in the data concealing process.

and *The process of extracting data and recovering the original image involves several steps:*

1. The designated image is used to extract data. It is then divided into blocks, from which embedded data is extracted. Decoding the auxiliary data and removing the embedded bits from the blocks are steps in the extraction process.

2. The encryption and data concealment procedures are undone by carrying out inverse operations to retrieve the original image. This involves recovering the original image from the marked encrypted shares using iterative block-based modulation and inverse block permutation.

3. To get the original secret data, the encrypted secret data is extracted from the embedded portions and decrypted using the data-hiding key.

These procedures enable the decryption and retrieval of the contained secret data as well as the lossless recovery of the original image [22].

IV. Applications of RDHEI

Reversible data hiding in encrypted images has a wide range of applications across various domains. Some of the key applications include:

- Secure Communication: Secret messages or information can be embedded into encrypted images via reversible data hiding, creating a secure communication channel. This tool is especially helpful in situations where maintaining secrecy is crucial, including military communications, diplomatic contacts, or private commercial talks [23] [24].

- Copyright protection and digital watermarking: Reversible data concealing makes it possible to incorporate copyright information or digital watermarks into encrypted images without jeopardizing the security of the encryption. By doing this, publishers, distributors, and content creators can safeguard their copyright claims and intellectual property rights, discouraging unauthorized use or distribution of digital information [25] [26].
- Medical Imaging and Telemedicine: In the medical industry, patient data, diagnostic data, and medical records can be securely transmitted thanks to reversible data concealment in encrypted medical images. This program protects patient privacy and confidentiality while facilitating telemedicine, remote diagnostics, and medical consultations [27] [28].
- Digital Forensics and Authentication: In digital forensics investigations, forensic watermarks or authentication codes can be embedded into encrypted images using reversible data hiding techniques. This makes it possible for forensic analysts, digital investigators, and law enforcement to identify manipulation or tampering, trace the origin of photos, and validate digital evidence [29].
- Digital Rights Management (DRM) and Multimedia Content Protection: By using data embedding and encryption, reversible data concealing techniques can be used to safeguard multimedia content, including audio files, digital documents, and videos. This makes it possible for distributors, service providers, and content owners to set up reliable DRM systems, enforce access restrictions, and stop illegal or pirated digital content from being redistributed or copied [30] [31].
- Steganography and Covert Communication: By embedding hidden messages or data into encrypted images, reversible data hiding enables covert communication and information concealment. This application is frequently used in covert operations, espionage, and intelligence collection, where upholding confidentiality and secrecy is essential [32].
- IoT Security and Embedded Systems: Reversible data concealing techniques can be used in the Internet of Things (IoT) ecosystem to safeguard sensor networks, IoT devices, and embedded systems. IoT devices can securely connect, exchange data, and authenticate with other devices or cloud services by embedding encryption keys, authentication tokens, or configuration data within encrypted pictures [33].
  All things considered, reversible data hiding in encrypted images provides a flexible and effective tool for safeguarding private data, preserving digital assets, and enabling a range of applications in a variety of fields, such as digital forensics, communication, multimedia content protection, and Internet of Things security.

V. Future of RDHEI

Reversible data hiding in encrypted photos has a bright future ahead of it, with more developments in security, privacy, and applications anticipated. The future prospects for this field are shaped by the following important factors: Strengthened Security Protocols: Future developments in reversible data concealment will put more emphasis on strengthening security protocols to fend off new threats and intrusions. This involves creating stronger encryption methods and data concealing strategies to guarantee the integrity and confidentiality of the embedded data as well as the original image. In order to improve the security of reversible data hidden in encrypted images, advanced cryptographic primitives and techniques including homomorphic encryption, lattice-based cryptography, and post-quantum cryptography will be essential.

additionally Reversible data concealing strategies will need to prioritize privacy protection more and more, especially when data privacy laws tighten. Subsequent investigations will concentrate on creating privacy-maintaining technologies that allow data concealment without jeopardizing user confidentiality or privacy. We'll use strategies like federated learning, safe multiparty computation, and differential privacy to reduce the privacy risks related to data embedding in encrypted images [34] [35].

In order to meet new demands and problems, reversible data concealment techniques will be combined with developing technology. To improve data traceability, integrity verification, and tamper resistance in encrypted photos, this involves integrating blockchain technology. Furthermore, more effective steganalysis methods for finding concealed data within encrypted photos will be made possible by the integration of artificial intelligence and machine learning algorithms, improving security and threat detection capabilities.

Reversible data hiding in encrypted graphics will become more widely used in a wider range of sectors. Reversible data concealing techniques have novel applications in healthcare, banking, digital forensics, and Internet of Things (IoT) security, in addition to classic uses like digital watermarking and secure communication. Reversible data concealment, for instance, can improve telemedicine and medical diagnostics by enabling safe patient data transmission while maintaining diagnostic accuracy. The widespread use of reversible data hiding techniques in encrypted photos will be greatly aided by standardization initiatives and interoperability standards. In order to enable safe and effective data interchange and cooperation across various platforms and applications, common frameworks, protocols, and interoperability standards must be established. This will enable smooth integration and interoperability across various data concealing and encryption technologies [36] [37].

Overall, the future of reversible data hiding in encrypted images is characterized by advancements in security, privacy, integration with emerging technologies, diversification of applications, and standardization efforts. By addressing these challenges and opportunities, reversible data hiding techniques will continue to evolve and innovate, enabling secure and efficient data communication, storage, and exchange in the digital age.

VI. Discussion

In this section, a comparison will be made between the *methods*, *Embedding rate*, with *PSNR* as shown in Tables I

and II.

TABLE I. COMPARISON OF THE USED SCHEME AND THE PSNR (DB) OF DIFFERENT RDHEI METHODS

Method	VRAE/VRBE/RRBE/SS	PSNR value(dB)
[19]	VRBE	∞
[10]	RRBE	0.5
[21]	RRBE	∞
[21]	RRBE	∞
[20]	VRBE	8.33
[14]	RRBE	∞
[22]	SS	∞

TABLE II. COMPARISON OF THE EMBEDDING RATES (BPP) OBTAINED FROM NINE DIFFERENT METHODS ACROSS THREE IMAGE DATASETS

Method	Average for 6 images	BOSS	BOWS-2	UCID
[19]	NA	NA	2.26	NA
[10]	2.29865	NA	NA	NA
[21] PAPL	NA	3.826	3.7	3.126
[21] OAPL	NA	3.947	3.7	3.200
[20] PE-VRAE	NA	3.9	3.7	3.1
[20] PE-VRBE	NA	4.0	3.9	3.3
[14] L	NA	3.6	3.7	NA
[14] AL32	NA	3.7	3.8	NA
[22]	NA	4.0	3.9	3.3

The results in the table shows that the Hybrid and Secret Sharing method performs better than other methods in terms of both embedding rate and noise-free image restoration rate. Out of all the strategies examined, this method achieves the highest embedding rate, demonstrating its efficacy in embedding a greater quantity of additional data into the encrypted image. Furthermore, the Hybrid and Secret Sharing method's positive noise rate of infinity implies that it can restore the original image without adding any noticeable distortion or noise. Overall, the results demonstrate the hybrid method's and secret sharing's improved performance and capabilities in reversible data concealing in encrypted images, making it a promising approach for secure and efficient data embedding applications.

VII. CONCLUSION

This survey provides a comprehensive overview of the topic of RDHEI, discussing various schemes and showing different techniques used to implement them. The discussed schemes are: Room Reservation Before Encryption (RRBE), Room Evacuation After Encryption (VRAE), and Secret Sharing(SS), all of which play crucial roles in ensuring the integrity and security of the data hidden within encrypted images. Furthermore, we emphasized the importance of reverse data hiding as one of the most important techniques to hide additional information within encrypted images while maintaining their confidentiality. By discussing their applications across diverse fields such as secure communications, digital watermarking, medical imaging, and digital forensics, we highlight their wide-ranging utility and importance in modern digital environments. Furthermore, theis survey highlighted future prospects for reversing data hiding in encrypted images, envisioning advances in security measures, privacy-preserving solutions, integration with emerging technologies, and diversification of applications. These developments underscore the continued importance and evolution of reversible data steganography techniques in addressing emerging challenges and enhancing steganography practices. Finally, we emphasized the importance of performing comparative analysis, including embedding rates, methods and peak signal-to-noise ratio (PSNR), to evaluate the performance and effectiveness of reversible data hiding techniques. This comparative approach enables researchers and practitioners to make informed decisions and optimize data hiding methods based on specific application requirements and performance metrics. Overall, this survey provided valuable insights into techniques, applications, future prospects, and comparative evaluation criteria for reversing data steganography in encrypted images, contributing to a deeper understanding of this important area in data security and data hiding.

REFERENCES

[1] S. Neetha, J. Bhuvana, and R. Suchithra, "An efficient image encryption reversible data hiding technique to improve payload and high security in cloud platforms," in *2023 6th International Conference on Information Systems and Computer Networks (ISCON)*, 2023, pp. 1–6.

[2] D. Huang and J. Wang, "High-capacity reversible data hiding in encrypted image based on specific encryption process," *Signal Processing: Image Communication*, vol. 80, p. 115632, 2020.

[3] J. Deepthi and T. Venu Gopal, "Pre encryption data hiding techniques using reserving room approach," in *2023 Third International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 2023, pp. 444–450.

[4] D. Vora, H. Ubhare, Y. Chheda, and P. Bhangale, "Review: Converging encryption, hashing and steganography for data fortification," in *2023 6th International Conference on Advances in Science and Technology (ICAST)*, 2023, pp. 443–447.

[5] S. Boppanaa, W. Kane, and L. Ma, "A secured image communication with dual encryption and reversible watermarking," *Soft Computing, Artificial Intelligence and Applications*, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:266470735

[6] B. Maram, "A framework for encryption and decryption using image steganography," in *2023 International Conference on Recent Advances in Information Technology for Sustainable Development (ICRAIS)*, 2023, pp. 71–76.

[7] P. Jagtap, A. Joshi, and S. Vyas, "Reversible data hiding in encrypted images," *International Advanced Research Journal in Science, Engineering and Technology*, pp. 35–38, 2015. [Online]. Available: https://api.semanticscholar.org/CorpusID:55998167

[8] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 3, pp. 553–562, 2013.

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

[10] C.-C. Chen, C.-C. Chang, and K. Chen, "High-capacity reversible data hiding in encrypted image based on huffman coding and differences of high nibbles of pixels," *Journal of Visual Communication and Image Representation*, vol. 76, p. 103060, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1047320321000304

[11] M. Alqahtani and A. Masmoudi, "High-capacity reversible data hiding in encrypted images based on pixel prediction and quadtree decomposition," *Applied Sciences*, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:265493300

[12] Q. Zhang and K. Chen, "Reversible data hiding in encrypted images based on two-round image interpolation," *Mathematics*, 2023. [Online]. Available: https://api.semanticscholar.org/CorpusID:266519767

[13] I.-C. Dragoi and D. Coltuc, "Reversible data hiding in encrypted color images based on vacating room after encryption and pixel prediction," *2018 25th IEEE International Conference on Image Processing (ICIP)*, pp. 1673–1677, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:52188233

[14] A. Mohammadi, "A general framework for reversible data hiding in encrypted images by reserving room before encryption," *Journal of Visual Communication and Image Representation*, vol. 85, p. 103478, 2022.

[15] B. Chen, W. Lu, J. Huang, J. Weng, and Y. Zhou, "Secret sharing based reversible data hiding in encrypted images with multiple data-hiders," *IEEE Transactions on Dependable and Secure Computing*, vol. 19, no. 2, pp. 978–991, 2022.

[16] C. Qin, S. Gao, C. Jiang, H. Yao, and C.-C. Chang, "Reversible data hiding in encrypted images based on chinese remainder theorem and secret sharing mechanism," *Proceedings of the 2021 3rd International Conference on Big-data Service and Intelligent Computation*, 2021. [Online]. Available: https://api.semanticscholar.org/CorpusID:246298060

[17] S. Yi, J. Zhou, Z. Hua, and Y. Xiang, "Reversible data hiding method in encrypted images using secret sharing and huffman coding," in *2021 11th International Conference on Information Science and Technology (ICIST)*, 2021, pp. 94–105.

[18] C. Qin, S. Gao, C. Jiang, H. Yao, and C.-C. Chang, "Reversible data hiding in encrypted images based on chinese remainder theorem and secret sharing mechanism," in *Proceedings of the 2021 3rd International Conference on Big-Data Service and Intelligent Computation*, ser. BDSIC '21. New York, NY, USA: Association for Computing Machinery, 2022, p. 23–32. [Online]. Available: https://doi.org/10.1145/3502300.3502304

[19] Y. Wang and W. He, "High capacity reversible data hiding in encrypted image based on adaptive msb prediction," *IEEE Transactions on Multimedia*, vol. 24, pp. 1288–1298, 2021.

[20] Y. Qiu, Q. Ying, Y. Yang, H. Zeng, S. Li, and Z. Qian, "High-capacity framework for reversible data hiding in encrypted image using pixel prediction and entropy encoding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 9, pp. 5874–5887, 2022.

[21] X. Wu, T. Qiao, M. Xu, and N. Zheng, "Secure reversible data hiding in encrypted images based on adaptive prediction-error labeling," *Signal Processing*, vol. 188, p. 108200, 2021.

[22] C. Yu, X. Zhang, C. Qin, and Z. Tang, "Reversible data hiding in encrypted images with secret sharing and hybrid coding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 33, no. 11, pp. 6443–6458, 2023.

[23] R. Punia, A. Malik, and S. Singh, "Innovative image interpolation based reversible data hiding for secure communication," *Discover Internet of Things*, vol. 3, no. 1, p. 22, 2023.

[24] S. Jaya Prakash and K. Mahalakshmi, "Improved reversible data hiding scheme employing dual image-based least significant bit matching for secure image communication using style transfer," *The Visual Computer*, vol. 38, no. 12, pp. 4129–4150, 2022.

[25] P. V. Sanivarapu, K. N. Rajesh, K. M. Hosny, and M. M. Fouda, "Digital watermarking system for copyright protection and authentication of images using cryptographic techniques," *Applied Sciences*, vol. 12, no. 17, p. 8724, 2022.

[26] P. Kadian, S. M. Arora, and N. Arora, "Robust digital watermarking techniques for copyright protection of digital data: A survey," *Wireless Personal Communications*, vol. 118, pp. 3225–3249, 2021.

[27] H. Abdel-Nabi and A. Al-Haj, "Medical imaging security using partial encryption and histogram shifting watermarking," in *2017 8th international conference on information technology (ICIT)*. IEEE, 2017, pp. 802–807.

[28] S. Ajili, M. A. Hajjaji, B. Bouallegue, and A. Mtibaa, "Joint watermarking\encryption image for safe transmission: application on medical imaging," in *2014 Global Summit on Computer & Information Technology (GSCIT)*. IEEE, 2014, pp. 1–6.

[29] F. Rodríguez-Santos, G. Delgado-Gutierréz, L. Palacios-Luengas, R. Vazquéz-Medina, and E. Culhuacan, "Practical implementation of a methodology for digital images authentication using forensics techniques," *Advances in Computer Science: an International Journal*, vol. 4, no. 6, pp. 179–186, 2015.

[30] M. Zhaofeng, H. Weihua, and G. Hongmin, "A new blockchain-based trusted drm scheme for built-in content protection," *EURASIP Journal on Image and Video Processing*, vol. 2018, no. 1, p. 91, 2018.

[31] J. P. Papanis, S. I. Papapanagiotou, A. S. Mousas, G. V. Lioudakis, D. I. Kaklamani, and I. S. Venieris, "On the use of attribute-based encryption for multimedia content protection over information-centric networks," *Transactions on Emerging Telecommunications Technologies*, vol. 25, no. 4, pp. 422–435, 2014.

[32] D.-C. Wu and Y.-M. Wu, "Covert communication via the qr code image by a data hiding technique based on module shape adjustments," *IEEE Open Journal of the Computer Society*, vol. 1, pp. 12–34, 2020.

[33] B. M. Kannan, P. Solainayagi, H. Azath, S. Murugan, and C. Srinivasan, "Secure communication in iot-enabled embedded systems for military applications using encryption," in *2023 2nd International Conference on Edge Computing and Applications (ICECAA)*. IEEE, 2023, pp. 1385–1389.

[34] A. N. Khan, M. Y. Fan, A. Malik, and M. A. Husain, "Advancements in reversible data hiding in encrypted images using public key cryptography," in *2019 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT)*, 2019, pp. 224–229.

[35] L. Xiong and D. Dong, "Reversible data hiding in encrypted images with public key cryptography: a review of its benefits and open issues," *International Journal of Arts and Technology*, vol. 11, no. 2, pp. 178–191, 2019.

[36] A. K. Rai, H. Om, S. Chand, and C.-C. Lin, "High-capacity reversible data hiding based on two-layer embedding scheme for encrypted image using blockchain," *Computers*, vol. 12, no. 6, p. 120, 2023.

[37] A. El Azzaoui, H. Chen, S. H. Kim, Y. Pan, and J. H. Park, "Blockchain-based distributed information hiding framework for data privacy preserving in medical supply chain systems," *Sensors*, vol. 22, no. 4, p. 1371, 2022.